DCUCI

Data Center Unified Computing Implementation

Version 5.0

Fast Lane LAB Guide

Version 5.2.0 (UCS Software 2.1)

ATTENTION

The Information contained in this guide is intended for training purposes only. This guide contains information and activities that, while beneficial for purposes of training in a close, non-production environment, can result in downtime or other severe consequences and therefore are not intended as a reference guide. This guide is not a technical reference and should not, under any circumstances be used in a production environment. Customers should refer to the published specifications applicable to specific products for technical information. The information in this guide is distributed AS IS, and the use of this information or implementation of any recommendations or techniques herein is a customer's responsibility.

COPYRIGHT

Overview

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

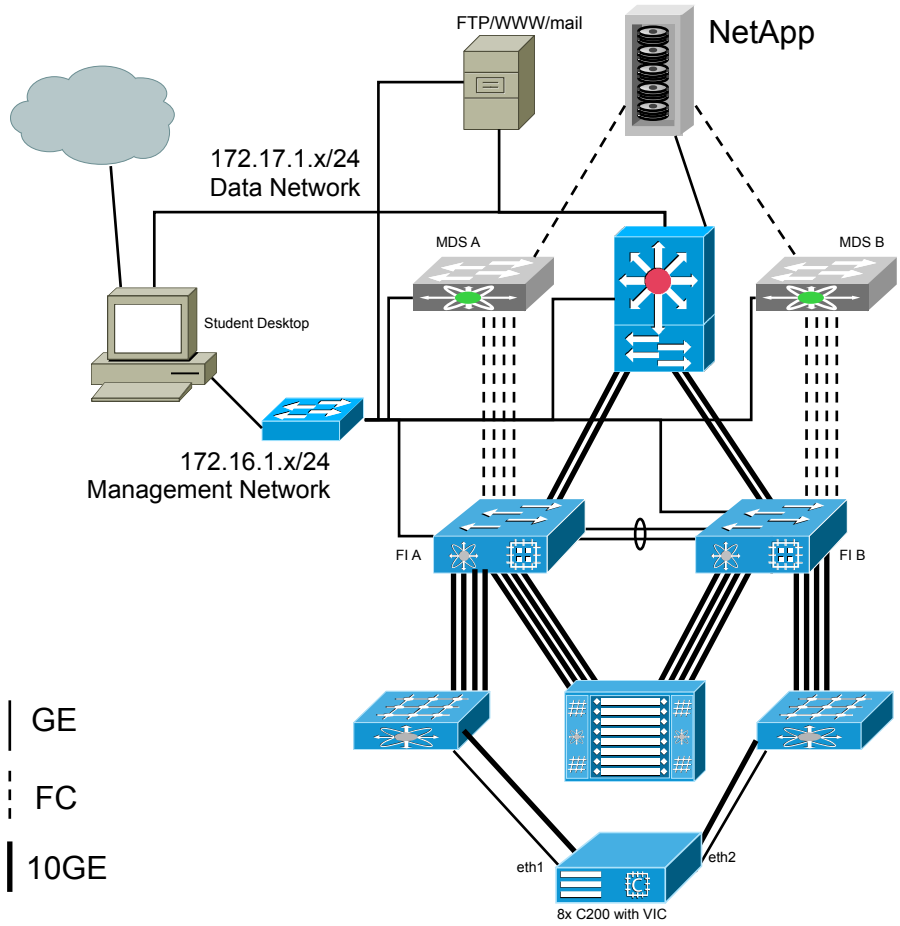
Outline

This guide includes these activities:

- Lab 0-1: FastLane Remote Lab Access
- Demo 2-1: Initial Configuration
- Lab 2-2: Initial configuration continued
- Lab 2-3: Integrating C-Series Servers into UCSM
- Lab 2-4: Configuring Role-Based Access Control
- Lab 2-5: Backing Up and Importing Configuration Data
- Lab 2-6: Reporting
- Lab 4-1: Configuring Resource Pools
- Lab 4-2: Creating Service Profile Templates
- Lab 5-1: Building a VMWare Infrastructure
- Lab 5-2: Configure Cisco VM-FEX

FastLane UCS Lab Layout

FastLane UCS Lab v1.6



Remote Lab login

Note the remote lab access data you received from your instructor in this table:

LAB IDs:

Rack 183 is Lab ID 1, Rack 184 is Lab ID 2, Rack 191 is Lab ID 3, Rack 192 is Lab ID 4, Rack 109 is Lab ID 5, Rack 110 is Lab ID 6, Rack 108 is Lab ID 7.

Ask your instructor for your lab id!

The URL is always: http://remotelabs.flane.de

LAB ID	POD#	Username	Password

FastLane UCS Lab Topology – Lab Aids

Management IP Addresses (P is always your Pod #)

Device	IP Address	Default Gateway
MDS-A	172.16.1.31	172.16.1.254
MDS-B	172.16.1.32	172.16.1.254
UCS Fabric A	172.16.1.101	172.16.1.254
UCS Fabric B	172.16.1.102	172.16.1.254
UCS shared	172.16.1.200	172.16.1.254
Domain Controller/DNS	172.16.1.20	172.16.1.254
Student Desktop	172.16.1.2P 172.17.1.2P	172.16.1.254 n/a
Mail Server	172.16.1.250 172.17.1.250	 172.17.1.254
Nexus 1000v	172.17.P1.10	172.17.P1.254
ESXi server 1	172.17.P1.1	172.17.P1.254
ESXi server 2	172.17.P1.2	172.17.P1.254
W2K3-VM	172.17.P2.1	172.17.P2.254
UCS Central Server	172.16.1.100	172.16.1.254
iSCSI storage (Fabric A)	172.18.L1.250	172.18.L1.254
iSCSI storage (Fabric B)	172.18.L2.250	172.18.L2.254

Device Login Credentials

Device	Username	Password
Student PC	administrator	1234QWer
ESX	root	1234QWer
W2K3-VM	administrator	1234QWer
UCS Manager	admin	1234QWer
MDS	student	1234QWer
Nexus 1000v	admin	1234QWer
UCS Central	admin	1245QWer / key 1245QWer

Demo 2-1: Initial Configuration

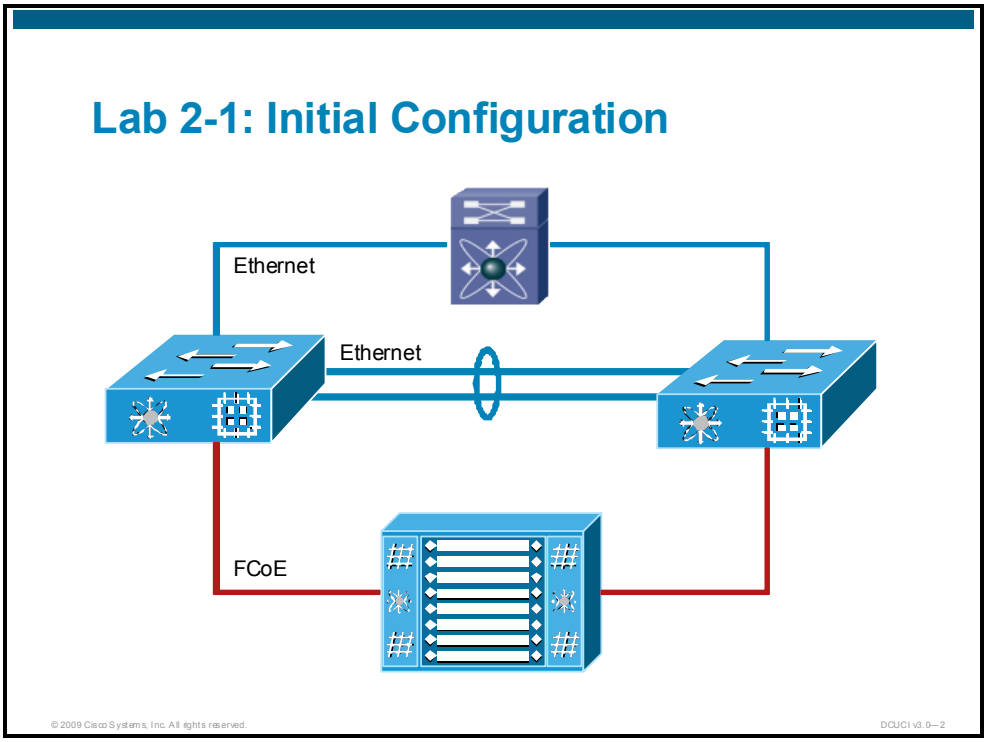
Complete this lab activity to practice what you learned in the related lesson.

Activity Objective

In this activity, you will observe the instructor performing the initial configuration of a Cisco UCS clustered environment. After observing this lab, you should be able to complete the initial configuration of a Cisco UCS 6100 Fabric Interconnect and establish a cluster relationship between two Cisco UCS 6100 Fabric Interconnects.

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
- Serial terminal access to both Fabric Interconnects

Demo: Cisco UCS Fabric Interconnect Initial Configuration

Remember this exercise will be demonstrated by the instructor if time permits.

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

Activity Procedure

The instructor will complete these steps:

Step 1 Log into the serial terminal of the Cisco UCS Fabric Interconnect.

```
Cisco UCS 6100 Series Fabric Interconnect
FastLane-UCS-A login: admin
Password: 1234QWer
Cisco UCS 6100 Series Fabric Interconnect

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

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

Step 2 Connect to the local-mgmt shell.

```
FastLane-UCS-A# connect local-mgmt
Cisco UCS 6100 Series Fabric Interconnect

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

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

…
FastLane-UCS-A#
```

Step 3 Erase the configuration.

```
FastLane-UCS-A# erase configuration
All UCS configurations will be erased and system will reboot.
Are you sure? (yes/no): yes
Removing all the configuration. Please wait....
Configurations are cleaned up. Rebooting....
```

Step 4 Erase the configuration on the second Fabric Interconnect. Note that if the second Fabric Interconnect is not also erased, when the first boots, it will attempt to rejoin the cluster. While this is typically expected behavior in a production environment, this exercise is attempting to demonstrate a true initial configuration.

Step 5 Observe the reboot and POST processes.

Step 6 Choose the console method of initial configuration.

```
System is coming up ... Please wait ...
nohup: appending output to `nohup.out'
           ---- Basic System Configuration Dialog ----

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

```
Type Ctrl-C at any time to abort configuration and reboot
system.
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.


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

Step 7 Specify that you will be setting up the system manually (as opposed to from a backup) and set the **admin** password.

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



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


Enforce strong password? (y/n) [y]: n


  Enter the password for "admin": 1234QWer
  Confirm the password for "admin": 1234QWer
```

Step 8 Set the cluster configuration options. For the first switch, use ‘A’. For the second switch, use ‘B’. Note that the system name will apply to both nodes—the fabric designator (A or B) will be appended to form the hostname.

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


  Enter the switch fabric (A/B) []: A
  Enter the system name: FastLane-UCS
```

Step 9 Set the management IP configuration options. Each Fabric Interconnect has a unique IP address as well as a shared cluster address.

```
  Physical Switch Mgmt0 IPv4 address : 172.16.1.101


  Physical Switch Mgmt0 IPv4 netmask : 255.255.255.0


  IPv4 address of the default gateway : 172.16.1.254


  Cluster IPv4 address : 172.16.1.200


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


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


  Join centralized management environment (UCS Central)?
(yes/no) [n]: n
```

Step 10 Confirm the configuration information and apply it.

```
Following configurations will be applied:

    Switch Fabric=A
    System Name=FastLane-UCS
    Enforced Strong Password=no
    Physical Switch Mgmt0 IP Address=172.16.1.101
    Physical Switch Mgmt0 IP Netmask=255.255.255.0
    Default Gateway=172.16.1.254

    Cluster Enabled=yes
    Cluster IP Address=172.16.1.200

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

Step 11 Log into the switch and view the cluster status.

```
FastLane-UCS-A login: admin
Password: 1234QWer
Cisco UCS 6100 Series Fabric Interconnect

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

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

…
FastLane-UCS-A# show cluster state
Cluster Id: 0x2ebe725040b711de-0x92a7000decb21744

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

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

Step 12 Complete the initial configuration on the second Fabric Interconnect. When starting, it should detect the presence of the cluster.

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

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

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

Type Ctrl-C at any time to abort configuration and reboot
system.
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.

Enter the configuration method. (console/gui) ? console
Installer has detected the presence of a peer Fabric
interconnect. This Fabric interconnect will be added to the
cluster. Continue (y/n) ? y
```

Step 13 Provide the **admin** password to the first switch and the local unique IP address for this Fabric Interconnect. All of the other configuration options will be replicated from the first switch.

```
  Enter the admin password of the peer Fabric interconnect:
    Connecting to peer Fabric interconnect... done
    Retrieving config from peer Fabric interconnect... done
    Peer Fabric interconnect Mgmt0 IP Address: 172.16.1.101
    Peer Fabric interconnect Mgmt0 IP Netmask: 255.255.255.0
    Cluster IP address          : 172.16.1.200
  Physical Switch Mgmt0 IPv4 address : 172.16.1.102
  Apply and save the configuration (select 'no' if you want to
re-enter)? (yes/no): yes
```

Step 14 Log in and display the cluster status.

```
FastLane-UCS-B login: admin
Password: 1234QWer
Cisco UCS 6100 Series Fabric Interconnect

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

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

…
FastLane-UCS-B# show cluster state
Cluster Id: 0x2ebe725040b711de-0x92a7000decb21744

B: UP, SUBORDINATE
A: UP, PRIMARY

HA NOT READY:
No device connected to this Fabric Interconnect
```

Lab 2-2: Initial configuration continued

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

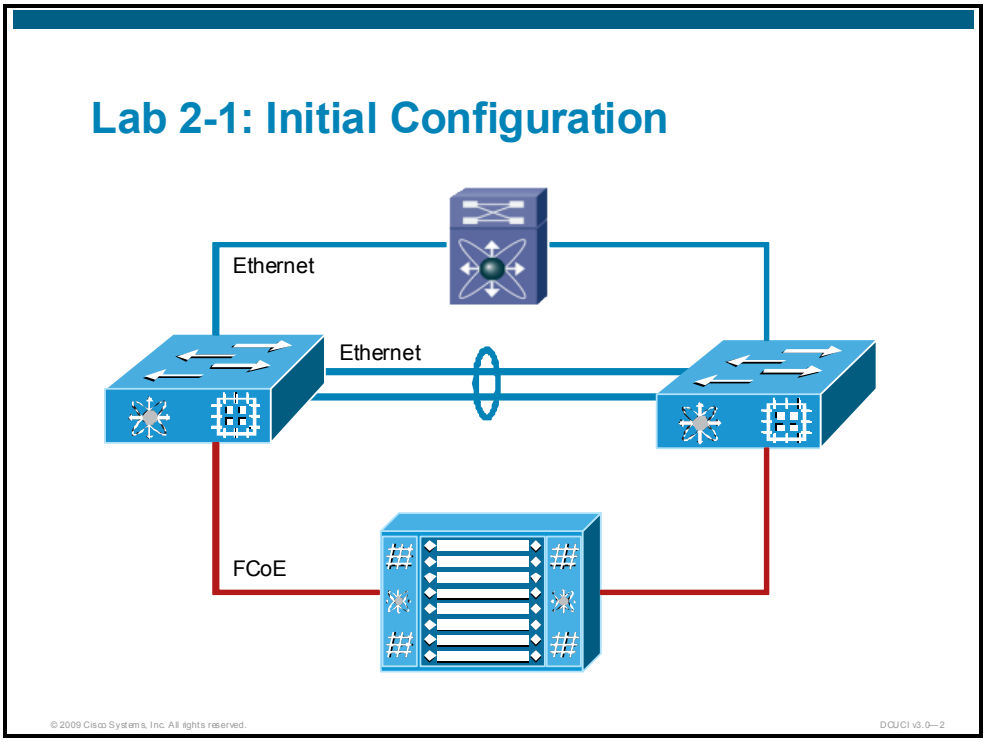
Activity Objective

In this activity, you will continue the initial setup the instructor has started.

Since we are working in a shared infrastructure make sure to ONLY configure Ports, servers etc assigned to your workgroup.
if you are unsure which component/server/port to use ask your instructor.

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:

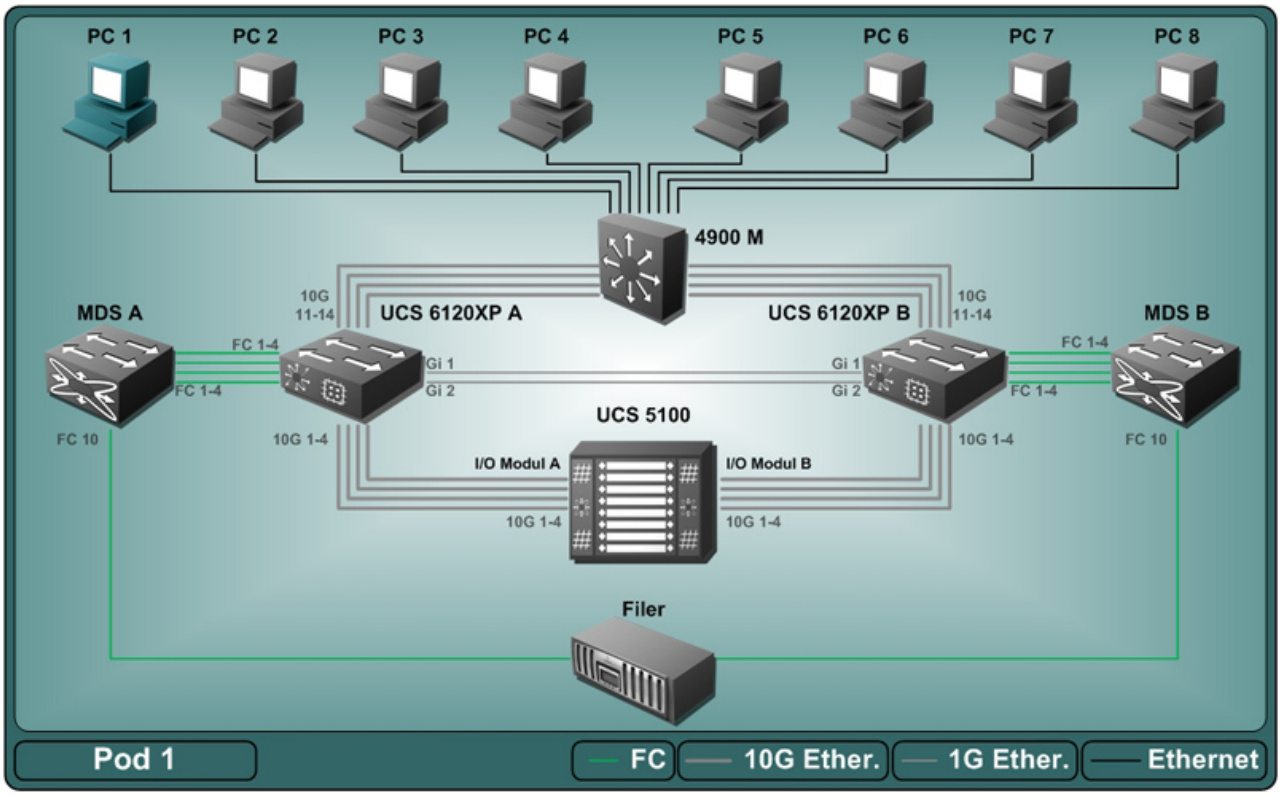
- (2) Cisco UCS 6100 Fabric Interconnects
- Management Station for UCS manager access

Step 1 Log into the FastLane remote lab by starting internet explorer (or any other browser) and navigating to http://remotelabs.flane.de

Step 2 Click the “login” button on the top right (or the “student login” link on the bottom of the page)

Step 3 Login with the credentials of your workgroup (supplied by the instructor)

Step 4 Click on the BLUE PC icon to start your remote access session to the remote lab. ALL lab exercises will be done on this PC, your local PC will only be used for accessing the remote lab GUI. (the GREY components are not manageable by you for now). Use username “Administrator” und passwort “1234QWer”

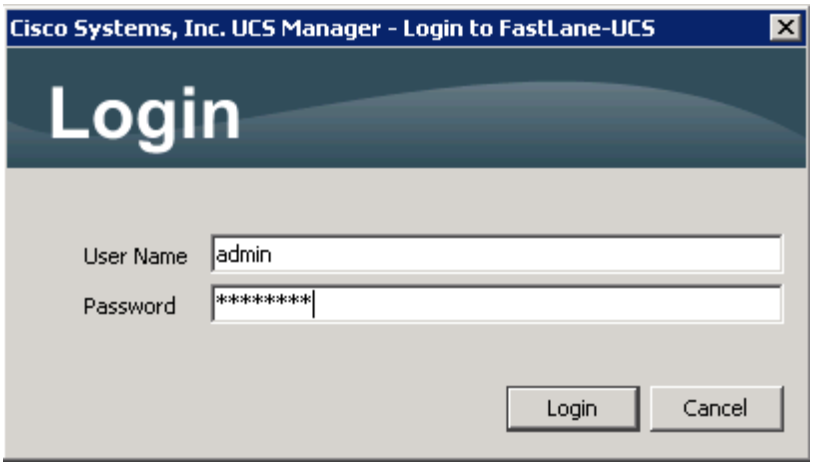


Step 5 Log into the Cisco UCS

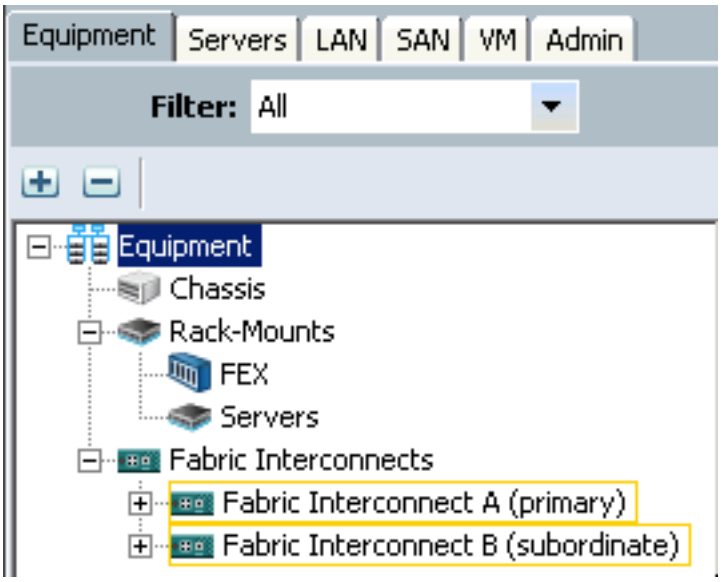
Step 6 Click on the “UCS Manager” icon on the remote desktop to connect to the UCS manager (this icon is just a shortcut to http://172.16.1.200, the cluster IP the instructor specified during the initial setup, you can also start IE manually and type the url.)

Step 7 Wait for the page to load and click the **LAUNCH UCS Manager** link to start the Cisco UCS Manager application.

Step 8 Confirm all security warnings and log in by using the **admin** account and the password that was entered in the configuration wizard (1234QWer)
(NOTE: everybody in the lab is using the admin account, please be cautious not to step on anybody else, configure ONLY your designated ports. If you want to perform some additional tasks or play around, ask your instructor first.)

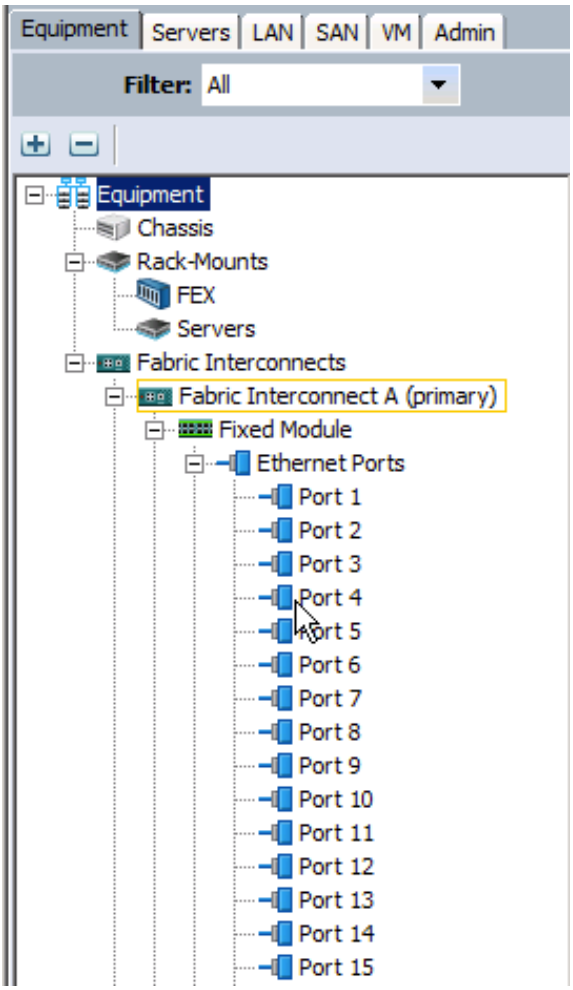


Step 9 Note that in the Equipment tab, both Fabric Interconnects are visible, but no chassis are yet available. This is because the default state of all Ethernet ports is disabled.

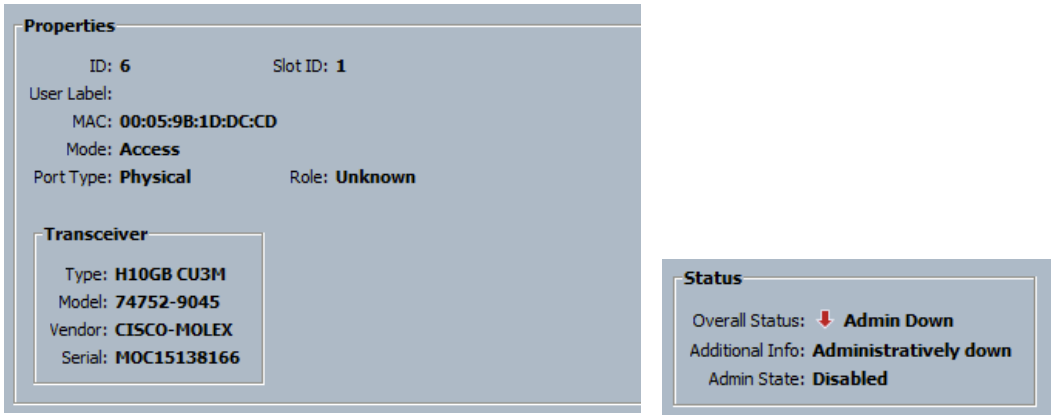


Step 10 Before the chassis is manageable and the cluster becomes fully operational, each Fabric Interconnect must have at least one active link to the chassis. Expand your assigned **Fabric Interconnect** (see table below) in the Equipment tab, and click on **ONLY** the port from the following table under Ethernet Ports of the Fixed Module.

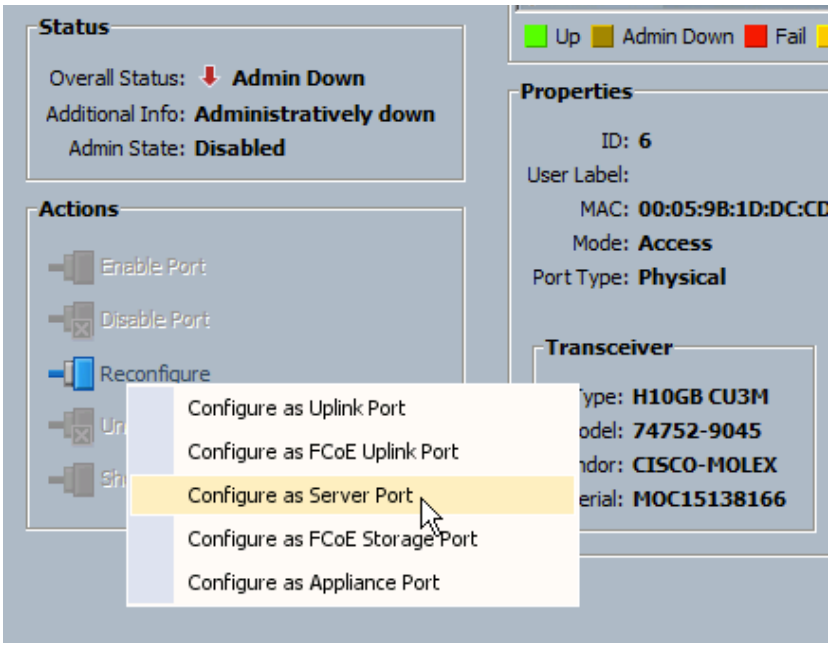
Pod	Fabric Interconnect and Port
1	Fabric Interconnect A, Port 1
2	Fabric Interconnect B, Port 1
3	Fabric Interconnect A, Port 2
4	Fabric Interconnect B, Port 2
5	Fabric Interconnect A, Port 3
6	Fabric Interconnect B, Port 3
7	Fabric Interconnect A, Port 4
8	Fabric Interconnect B, Port 4



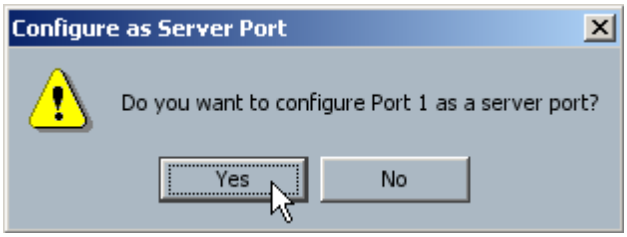
Step 11 Note that the state of the port is administratively disabled (by default)



In the Actions panel, choose **Reconfigure FOR YOUR PORT ONLY** and select "Configure as a Server Port". This tells Cisco UCS that this port will be connecting to an IO module that is located within a chassis.

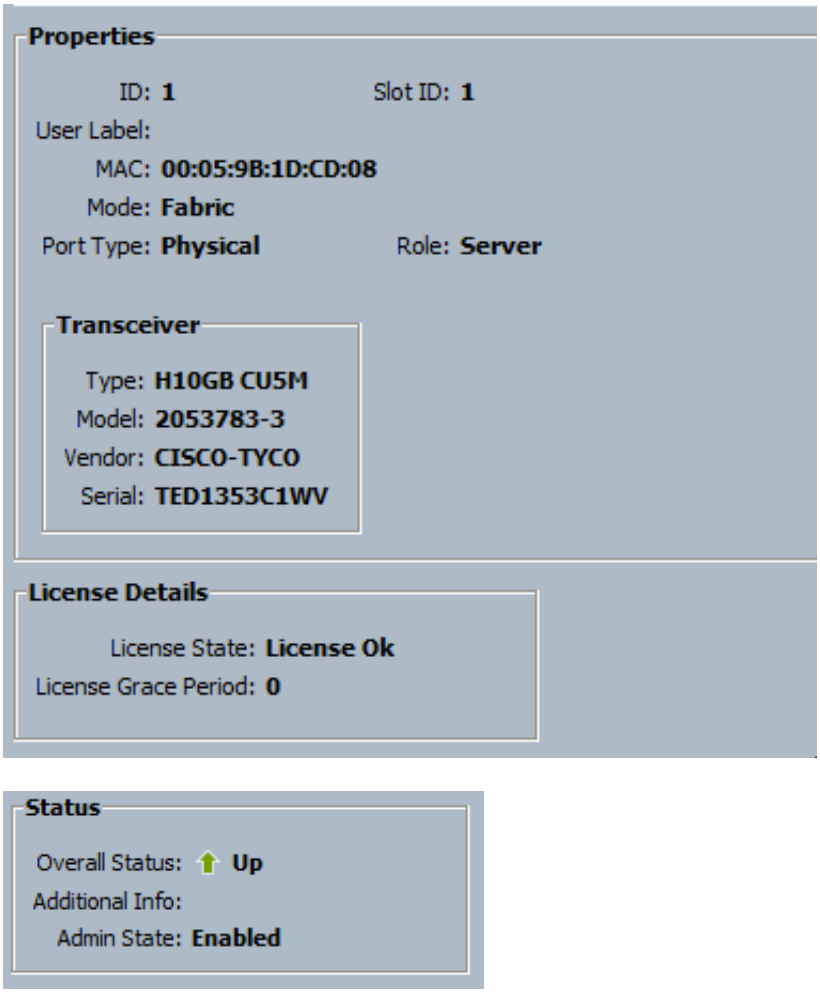


Step 12 Click **Yes** to confirm the port configuration.



Step 13 Click **OK** to dismiss the completion window if it show up (it is optional in newer releases of the UCSM).

Step 14 Note the new state of the port, and that a chassis is now visible in the Equipment tab.



Step 15 Wait for the other workgroups to complete, DO NOT configure any other port. If your port shows up as "FEX unconfigured" do not troubleshoot this issue, we will correct it in a minute.

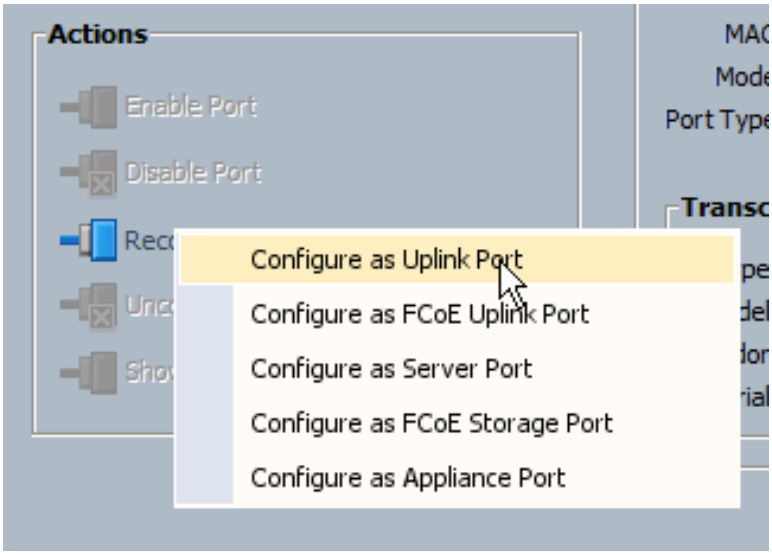
The instructor may show the output of the cluster state show command. This is how it would look like:

```
FastLane-UCS-A# show cluster state
Cluster Id: 0xdc25b7d840bb11de-0xba02000decb21744

A: UP, PRIMARY
B: UP, SUBORDINATE

HA READY
```

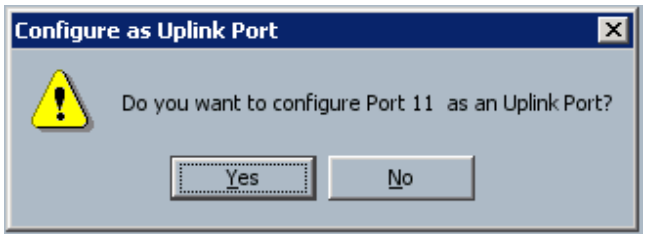
Step 16 Configuring uplink ports is similar to configuring server ports. Choose ONLY **the port from the following table** and then click **Reconfigure** and **Configure as Uplink Port**. This will tell UCS Manager this port is connected to the outside world.

Pod	Fabric Interconnect and Port
1	Fabric Interconnect A, Port 11
2	Fabric Interconnect B, Port 11
3	Fabric Interconnect A, Port 12
4	Fabric Interconnect B, Port 12
5	Fabric Interconnect A, Port 13
6	Fabric Interconnect B, Port 13
7	Fabric Interconnect A, Port 14
8	Fabric Interconnect B, Port 14

Note: some of these ports may not actually be connected in the lab and do not have SFPs plugged in.



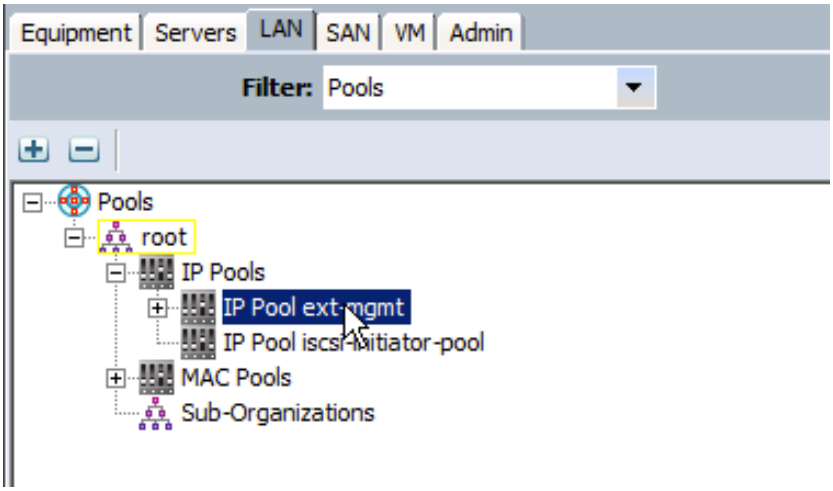
Step 17 Click **Yes** to confirm the port configuration.



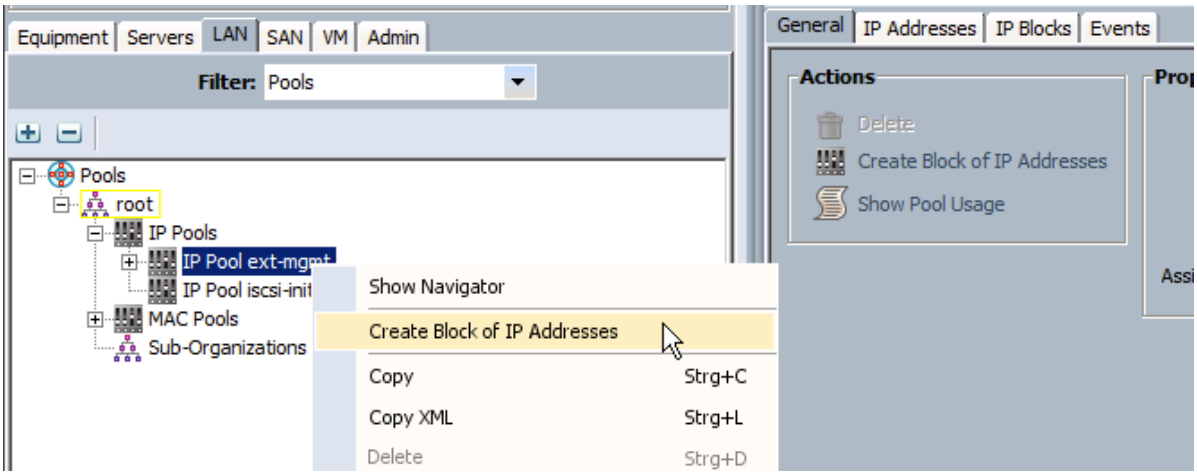
Step 18 Click **OK** to dismiss the completion window.

Note The "Appliance Port" is used to connect an Ethernet device like a Filer for Ethernet network connectivity directly to the UCS fabric.
The "FCoE Storage Port" can used to connect a FCoE-enabled storage system (like a NetApp with a CNA) to connect directly to the UCS fabric.

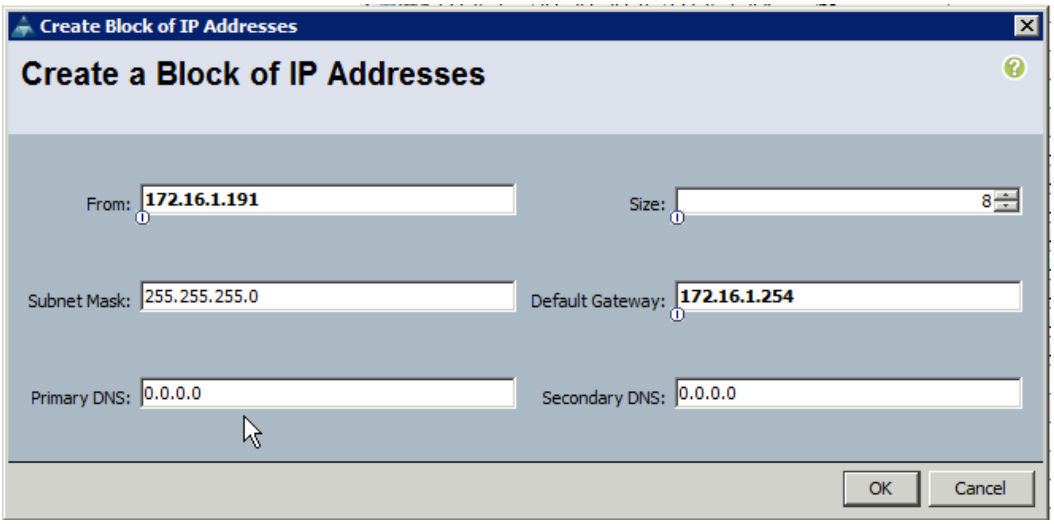
Step 19 Navigate to the **LAN** tab, set the Filter to "**Pools**" and choose the "**IP Pools ext-mgmt"** icon.



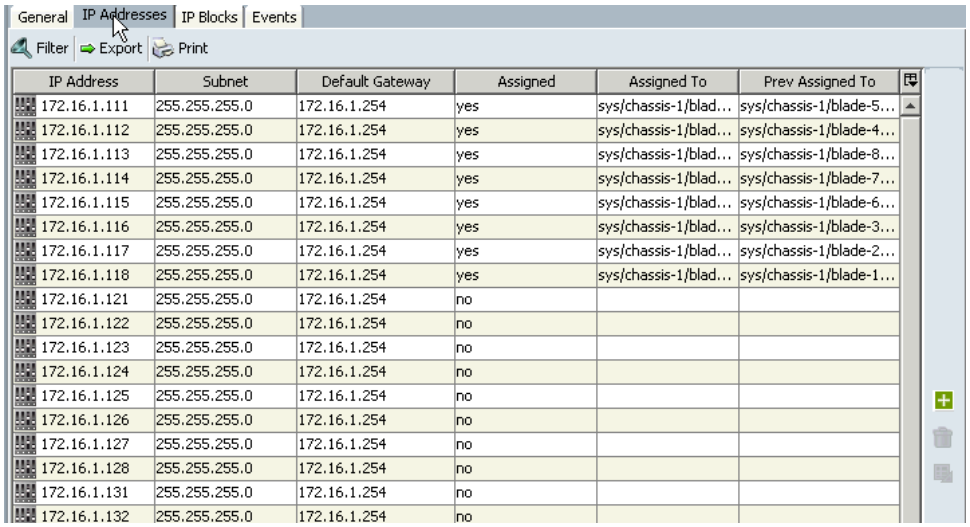
Step 20 Right-click **Management IP Pool** and choose **Create Block of IP Addresses**.



Step 21 Create a block of **eight (8)** addresses starting at 172.16.1.1X1 (X is your Pod #), use a subnet mask of 255.255.255.0, the default gateway 172.16.1.254 and click **OK**. (please note just one of these pools will be used for now for the current chassis, consider the other IP pools as a preparation for more chassis to be deployed later)



Step 22 Click the "IP addresses" tab and notice some addresses have been allocated to the blade servers.



IP Address	Subnet	Default Gateway	Assigned	Assigned To	Prev Assigned To
172.16.1.111	255.255.255.0	172.16.1.254	yes	sys/chassis-1/blad...	sys/chassis-1/blade-5...
172.16.1.112	255.255.255.0	172.16.1.254	yes	sys/chassis-1/blad...	sys/chassis-1/blade-4...
172.16.1.113	255.255.255.0	172.16.1.254	yes	sys/chassis-1/blad...	sys/chassis-1/blade-8...
172.16.1.114	255.255.255.0	172.16.1.254	yes	sys/chassis-1/blad...	sys/chassis-1/blade-7...
172.16.1.115	255.255.255.0	172.16.1.254	yes	sys/chassis-1/blad...	sys/chassis-1/blade-6...
172.16.1.116	255.255.255.0	172.16.1.254	yes	sys/chassis-1/blad...	sys/chassis-1/blade-3...
172.16.1.117	255.255.255.0	172.16.1.254	yes	sys/chassis-1/blad...	sys/chassis-1/blade-2...
172.16.1.118	255.255.255.0	172.16.1.254	yes	sys/chassis-1/blad...	sys/chassis-1/blade-1...
172.16.1.121	255.255.255.0	172.16.1.254	no		
172.16.1.122	255.255.255.0	172.16.1.254	no		
172.16.1.123	255.255.255.0	172.16.1.254	no		
172.16.1.124	255.255.255.0	172.16.1.254	no		
172.16.1.125	255.255.255.0	172.16.1.254	no		
172.16.1.126	255.255.255.0	172.16.1.254	no		
172.16.1.127	255.255.255.0	172.16.1.254	no		
172.16.1.128	255.255.255.0	172.16.1.254	no		
172.16.1.131	255.255.255.0	172.16.1.254	no		
172.16.1.132	255.255.255.0	172.16.1.254	no		

Lab 2-3: Integrating C-Series Servers into UCSM

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 integrate C-Series rackmount servers into a UCS cluster

After performing this lab, you should be able to:

- Configure the FI to manage 2232 FEX
- Configure UCSM to manage C-Series Servers

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
- 2x 2232 FEX connected to the FIs
- C-Series Rackmount servers

Task 1: Configure UCSM to manage C-Series through 2232 FEX

In this task you will enable connectivity between the FI and the FEX.

Activity Procedure

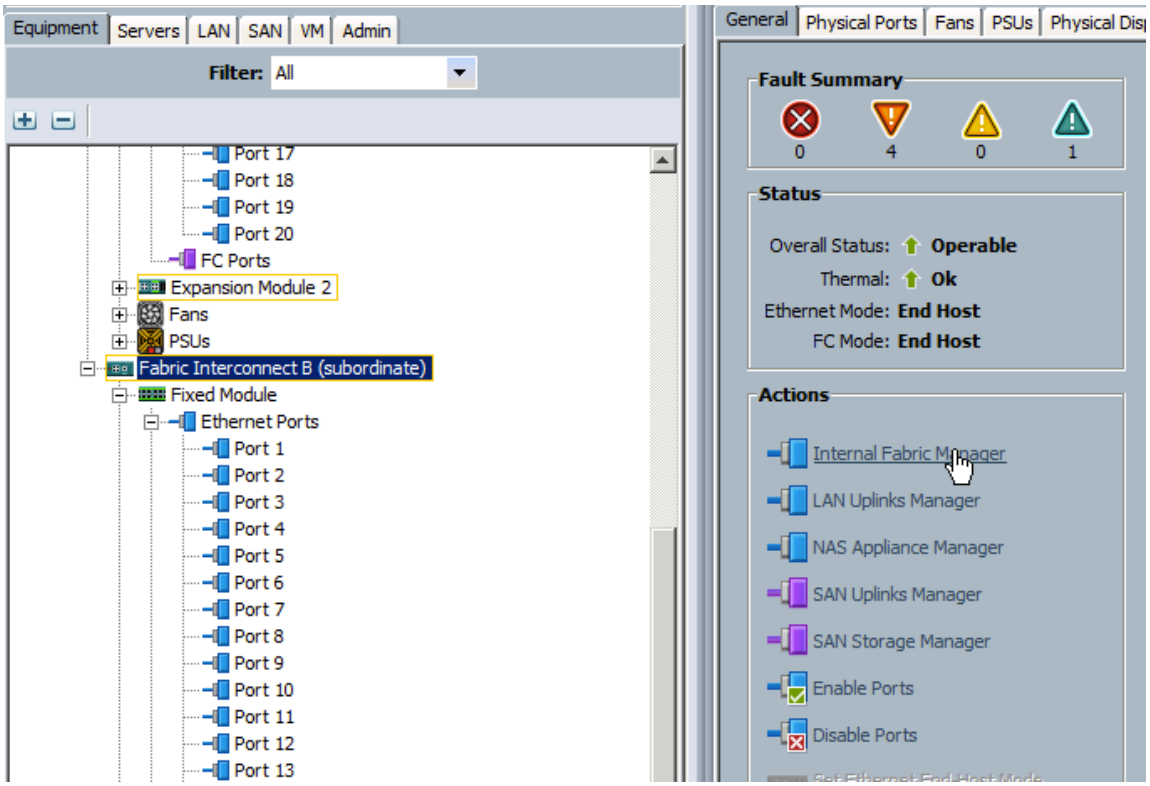
Complete these steps:

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

Step 2 Open Internet Explorer by clicking on the “UCS manager” shortcut on your student desktop.

Step 3 Log into UCS manager with username “admin” and password “1234QWer”

Step 4 Open the “internal fabric manager” from the Fabric Interconnect View

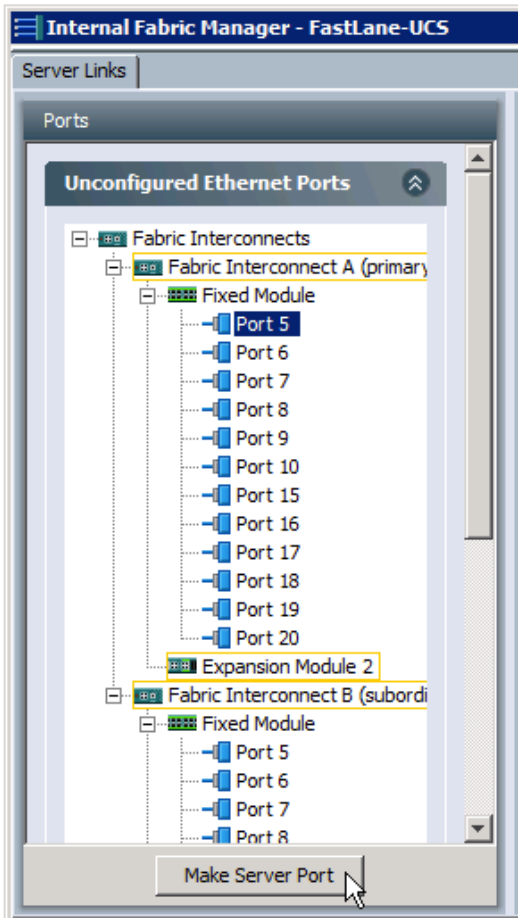


Step 5 Open the “unconfigured ethernet ports” pane, expand your assigned **Fabric Interconnect** (see table below) in the Equipment tab, and click on **ONLY** the port from the following table under unconfigured Ports of the Fixed Module.

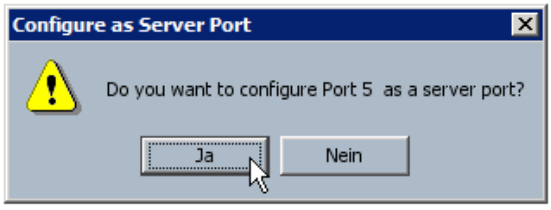
Pod	Fabric Interconnect and Port
1	Fabric Interconnect A, Port 5
2	Fabric Interconnect B, Port 5
3	Fabric Interconnect A, Port 6
4	Fabric Interconnect B, Port 6
5	Fabric Interconnect A, Port 7
6	Fabric Interconnect B, Port 7

7	Fabric Interconnect A, Port 8
8	Fabric Interconnect B, Port 8

Step 6 Click the “make server port” button ON ONLY YOUR ASSIGNED PORT.

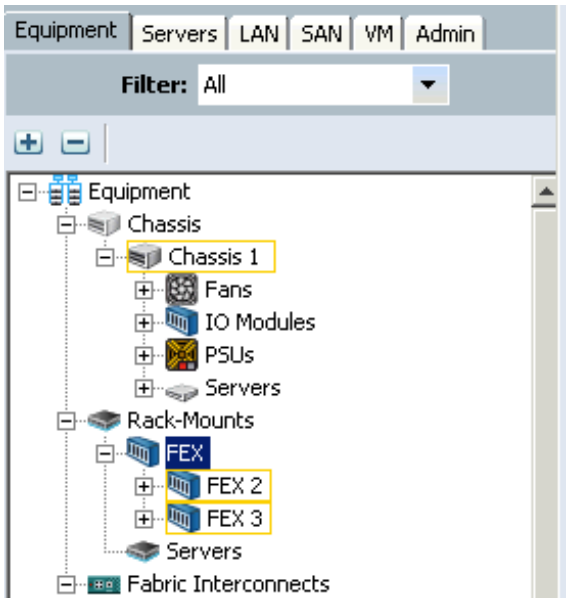


Step 7 Click OK to confirm



Step 8 Close Fabric manager

Step 9 Notice in the Equipment pane the two FEX have shown up



Note	The FEX will now boot. When finished, UCS Manager will discover the C-Series Servers. This will take a couple of minutes.
Caution	**ALL ports (5-8) on BOTH Fabric Interconnects MUST be enabled in server mode and the FEX must be reacknowledged after this lab.**

Lab 2-4: Configure Role-Based Access Control

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

Activity Objective

In this activity, you will implement authentication with local authentication and Microsoft Active Directory. After completing this activity, you will be able to meet these objectives:

- Implement organizations based on a detailed specification for a large data center
- Implement user roles to segregate server, LAN, and SAN, based on job role
- Implement local user accounts
- Test locale restrictions

Required Resources

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

- Student PC
- Identity and resource pools lab implementation information

Lab 2-4 Implementation Information

Use this implementation information to aid in the configuration tasks in Lab 2-4.

Task 1: Implement Organizations Based on a Detailed Specification for a Large Data Center

Pod	Level	Organization	Locale
	Top level	Root	-
1	Level 1	Pod1	Pod1-Loc
2	Level 1	Pod2	Pod2-Loc
3	Level 1	Pod3	Pod3-Loc
4	Level 1	Pod4	Pod4-Loc
5	Level 1	Pod5	Pod5-Loc
6	Level 1	Pod6	Pod6-Loc
7	Level 1	Pod7	Pod7-Loc
8	Level 1	Pod8	Pod8-Loc

Task 2: Implement User Roles to Segregate Server, LAN, and SAN, Based on Job Role

Pod	Custom Role	Privileges
1	Pod1-Admin	All except admin, AAA, fault, and operations
1	Pod1-LAN-SAN	All ext-lan-*, ext-san-*
1	Pod1-SERVER	All service-profile-*
2	Pod2-Admin	All except admin, AAA, fault, and operations
2	Pod2-LAN-SAN	All ext-lan-*, ext-san-*
2	Pod2-SERVER	All service-profile-*
3	Pod3-Admin	All except admin, AAA, fault, and operations
3	Pod3-LAN-SAN	All ext-lan-*, ext-san-*
3	Pod3-SERVER	All service-profile-*
4	Pod4-Admin	All except admin, AAA, fault, and operations
4	Pod4-LAN-SAN	All ext-lan-*, ext-san-*
4	Pod4-SERVER	All service-profile-*
5	Pod5-Admin	All except admin, AAA, fault, and operations
5	Pod5-LAN-SAN	All ext-lan-*, ext-san-*
5	Pod5-SERVER	All service-profile-*
6	Pod6-Admin	All except admin, AAA, fault, and operations
6	Pod6-LAN-SAN	All ext-lan-*, ext-san-*
6	Pod6-SERVER	All service-profile-*
7	Pod7-Admin	All except admin, AAA, fault, and operations
7	Pod7-LAN-SAN	All ext-lan-*, ext-san-*
7	Pod7-SERVER	All service-profile-*
8	Pod8-Admin	All except Admin, AAA, fault, and operations
8	Pod8-LAN-SAN	All ext-lan-*, ext-san-*
8	Pod8-SERVER	All service-profile-*

Task 3: Implement Local User Accounts

Pod	User	Password	Role	Locale
1	pod1-admin	1234QWer	Pod1-Admin	Pod1-Loc
1	pod1-lan-san	1234QWer	Pod1-LAN-SAN	Pod1-Loc
1	pod1-server	1234QWer	Pod1-SERVER	Pod1-Loc
2	pod2-admin	1234QWer	Pod2-Admin	Pod2-Loc
2	pod2-lan-san	1234QWer	Pod2-LAN-SAN	Pod2-Loc
2	pod2-server	1234QWer	Pod2-SERVER	Pod2-Loc
3	pod3-admin	1234QWer	Pod3-Admin	Pod3-Loc
3	pod3-lan-san	1234QWer	Pod3-LAN-SAN	Pod3-Loc
3	pod3-server	1234QWer	Pod3-SERVER	Pod3-Loc
4	pod4-admin	1234QWer	Pod4-Admin	Pod4-Loc
4	pod4-lan-san	1234QWer	Pod4-LAN-SAN	Pod4-Loc
4	pod4-server	1234QWer	Pod4-SERVER	Pod4-Loc
5	pod5-admin	1234QWer	Pod5-Admin	Pod5-Loc
5	pod5-lan-san	1234QWer	Pod5-LAN-SAN	Pod5-Loc
5	pod5-server	1234QWer	Pod5-SERVER	Pod5-Loc
6	pod6-admin	1234QWer	Pod6-Admin	Pod6-Loc
6	pod6-lan-san	1234QWer	Pod6-LAN-SAN	Pod6-Loc
6	pod6-server	1234QWer	Pod6-SERVER	Pod6-Loc
7	pod7-admin	1234QWer	Pod7-Admin	Pod7-Loc
7	pod7-lan-san	1234QWer	Pod7-LAN-SAN	Pod7-Loc
7	pod7-server	1234QWer	Pod7-SERVER	Pod7-Loc
8	pod8-admin	1234QWer	Pod8-Admin	Pod8-Loc
8	pod8-lan-san	1234QWer	Pod8-LAN-SAN	Pod8-Loc
8	pod8-server	1234QWer	Pod8-SERVER	Pod8-Loc

Task 1: Implement Organizations Based on a Detailed Specification for a Large Data Center

In this task, you will implement organizations and locales.

Activity Procedure

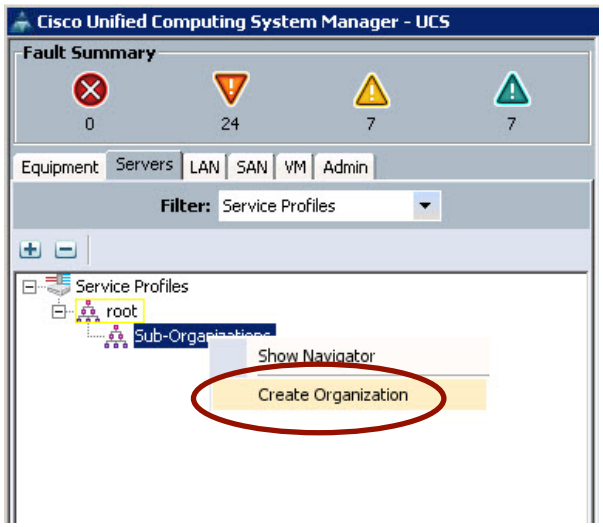
Complete these steps:

Note	The examples shown in all tasks of this lab are based on pod 1. Be sure to use the values that are associated with your assigned pod from the lab implementation information.

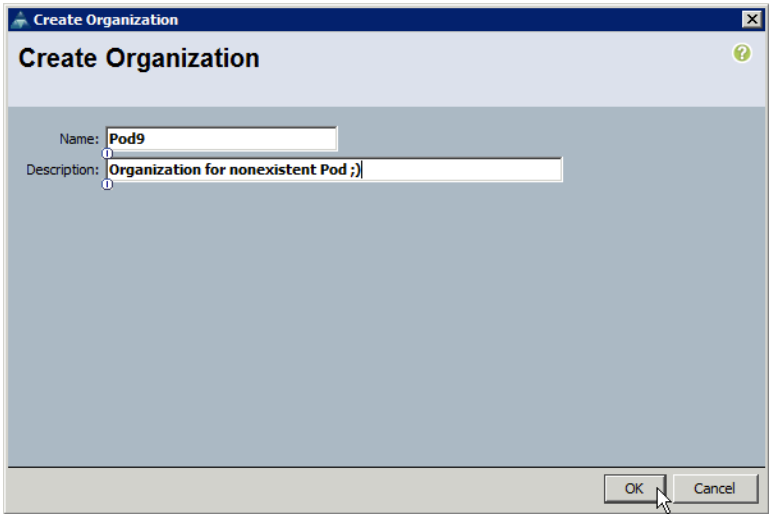
Step 1 In Cisco UCS Manager, select the **Servers** tab.

Step 2 Under **Service Profiles** expand the root organization.

Step 3 Right-click **Sub-Organizations** and choose **Create Organization** from the drop-down list or click the plus sign **(+)** on the right.

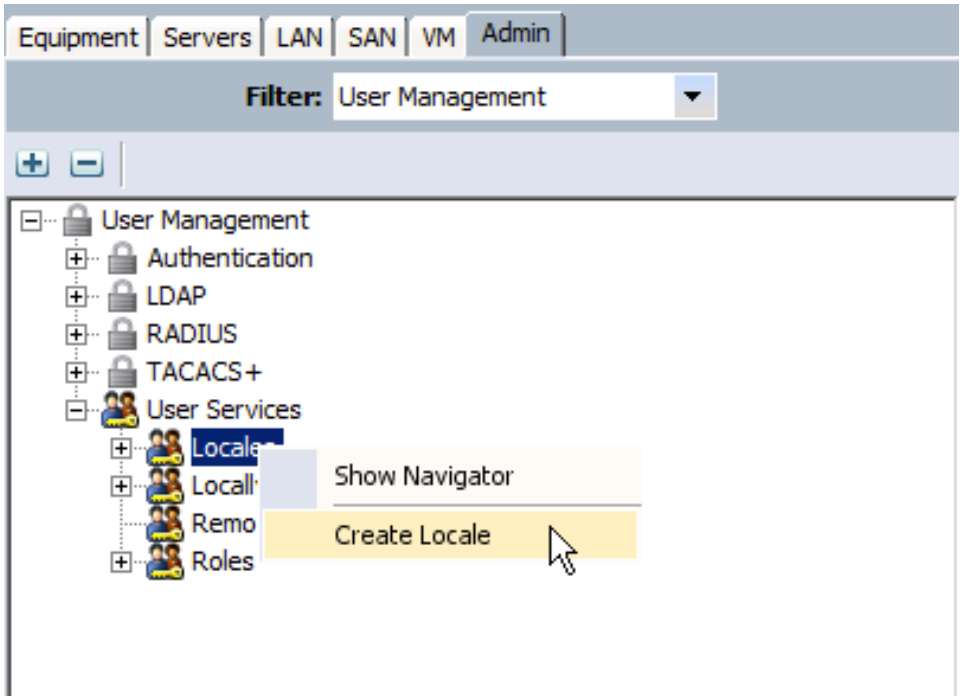


Step 4 Set the organization name for your pod to “Pod#” (where # is your Pod#) you can also check the information found at the beginning of the lab.

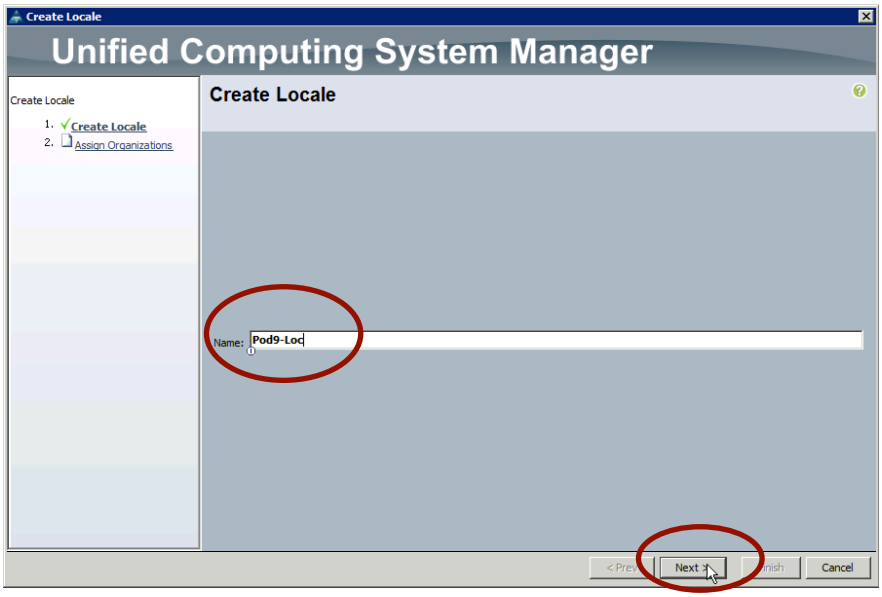


Step 5 From the **Admin** tab, navigate to **User Management > User Services > Locales**.

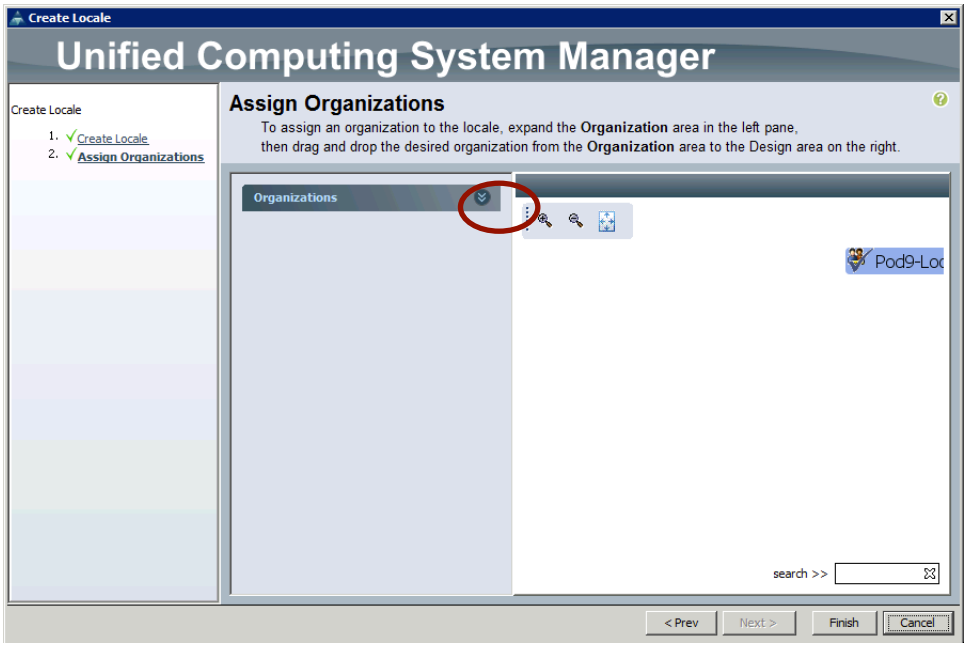
Step 6 Right-click **Locales** and choose **Create Locale** from the drop-down list (or click the plus sign **(+)** on the right)



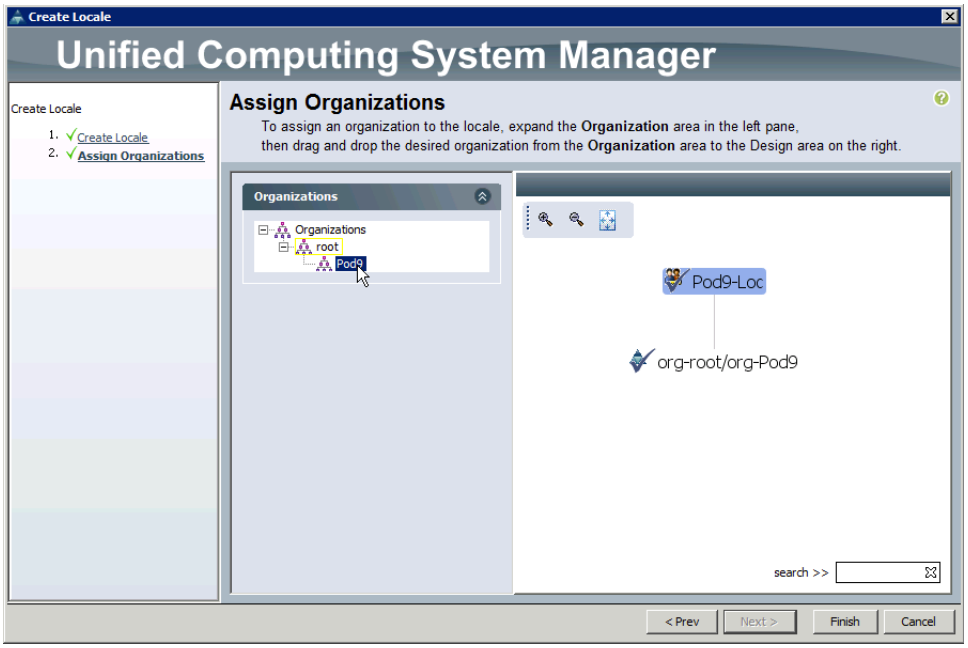
Step 7 Set the locale name for your pod to "Pod#-Loc" (# is your Pod#) according to the lab implementation information for Task 1 found at the beginning of the lab. Click **Next** to continue.



Step 8 Click the double-down arrow icon to the right of **Organizations** to display available organizations.



Step 9 Click and drag your organization to the right and drop it beneath the name of the locale. If the organization does not appear, click the redraw icon to the right of the magnifying glasses.



Step 10 When your organization appears under the new locale, click **Finish** to close the wizard.

Activity Verification

You have completed this activity once you have completed the following:

- You can see your organization.
- You can see your locale.

Task 2: Implement User Roles to Segregate Server, LAN, and SAN, Based on Job Role

In this task, you will create custom user roles.

Activity Procedure

Complete these steps:

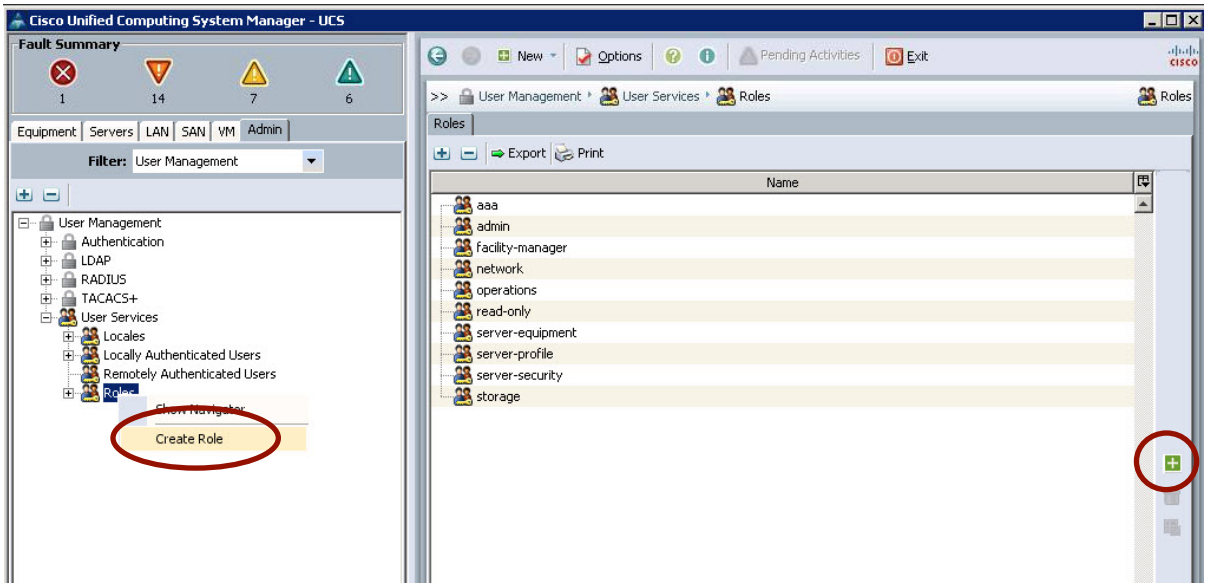
Note	The examples that are used in all tasks of this lab are based on pod9 (which does not exist). Be sure to use the values that are associated with your assigned pod from the implementation information.
Tip	Refer to the lab implementation information for Task 2 at the beginning of the lab.

Step 1 In Cisco UCS Manager, select the **Admin** tab.

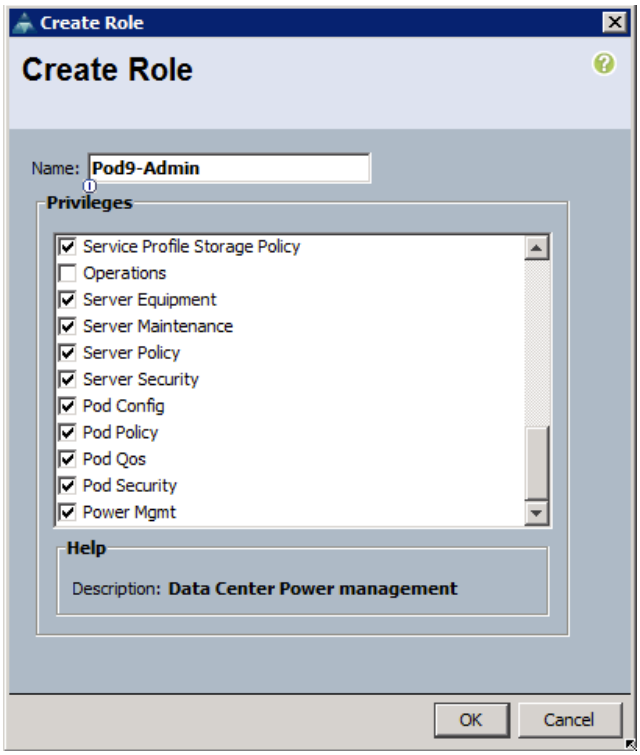
Step 2 From the **Filter** drop-down menu, choose **User Management** to filter other categories.

Step 3 Expand **User Services** and select **Roles**.

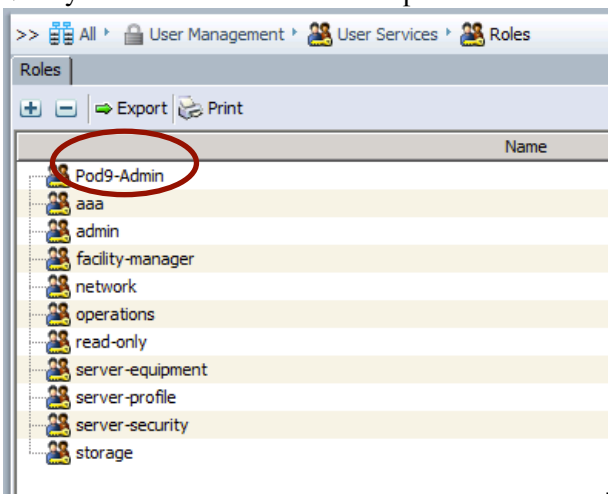
Step 4 Right-click **Roles** and choose **Create Role** from the drop-down list or click the plus sign (+) on the right.



Step 5 Create a custom Admin user for your organization, according to the Task 2 table found at the beginning of this lab. Set the name and select the appropriate features. Click **OK** to finish.

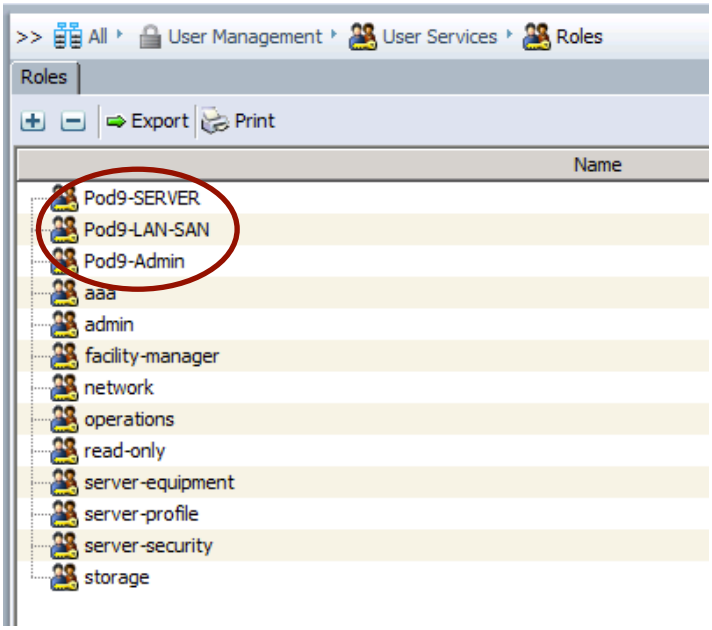


Step 6 Verify that the role is created and present.



Step 7 Repeat Steps 4 to 6 to create the LAN-SAN and Server roles for your organization according to the Task 2 table found at the beginning of this lab.

Step 8 Verify that the three roles for your organization are created.



Activity Verification

You have completed this activity once you have completed the following:

- You have successfully created the three user roles for your organization.

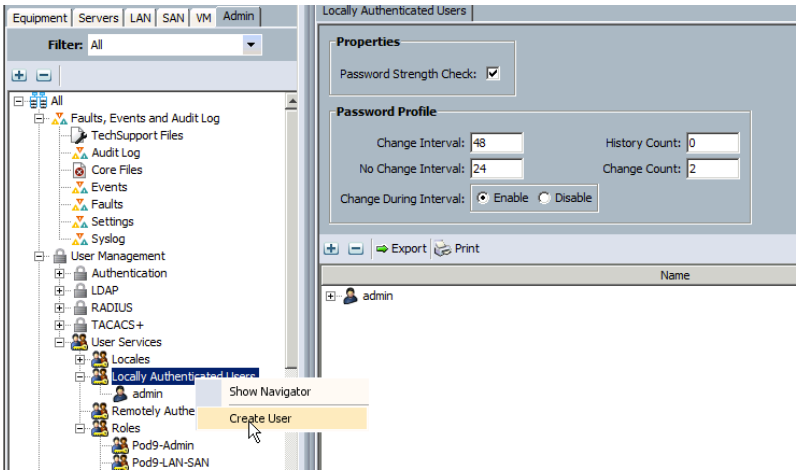
Task 3: Implement Local User Accounts

In this task, you will create local user accounts and map the appropriate roles and locales in Cisco UCS Manager.

Activity Procedure

Complete these steps:

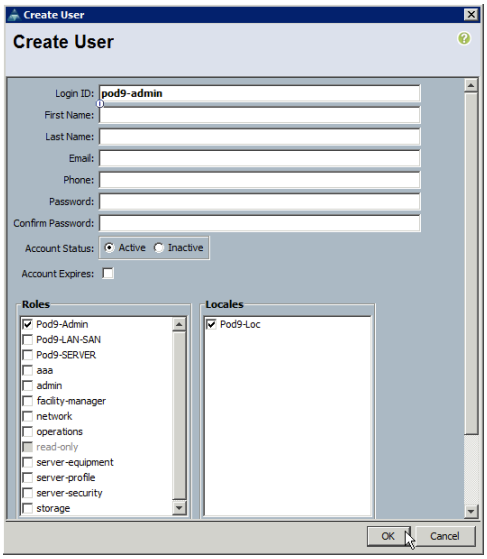
Step 1 In the **Admin** tab, right-click **Locally Authenticated Users**. Choose **Create User**.



Caution Usernames and passwords are case sensitive.

Step 2 When the Create User wizard opens, enter the name of the new user and password. Choose the appropriate role and locale using the table below. (You can also Look for the user names, related roles, and locales in the Task 3 table found at the beginning of the lab.)

User	Password	Role	Locale
pod#-admin	1234QWer	Pod#-Admin	Pod#-Loc
pod#-lan-san	1234QWer	Pod#-LAN-SAN	Pod#-Loc
pod#-server	1234QWer	Pod#-SERVER	Pod#-Loc



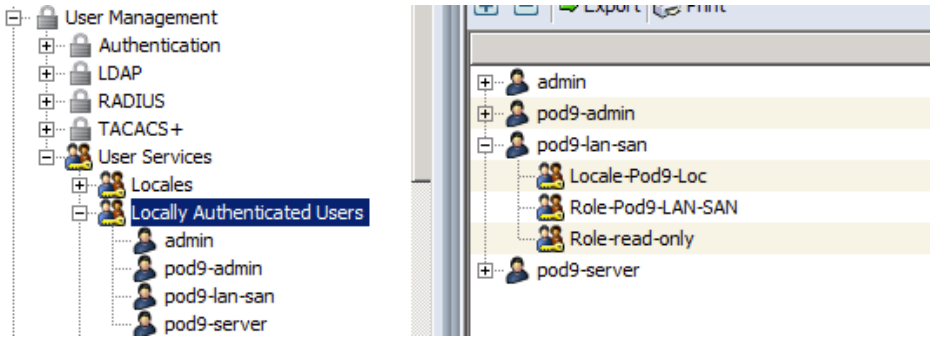
Step 3 Click **OK** to close the user wizard. Repeat until the three users for your pod are created.

Note If an error dialog box appears after clicking OK, go back to the role that is associated with the user. Be certain that you have not assigned the AAA, admin, fault, or operations privileges to the user. Those four privileges are incompatible with locale assignment.

Activity Verification

You have completed this activity once you have completed the following:

- You have successfully created three local users in Cisco UCS Manager.



Task 4: Test Locale Restrictions

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

Activity Procedure

Complete these steps:

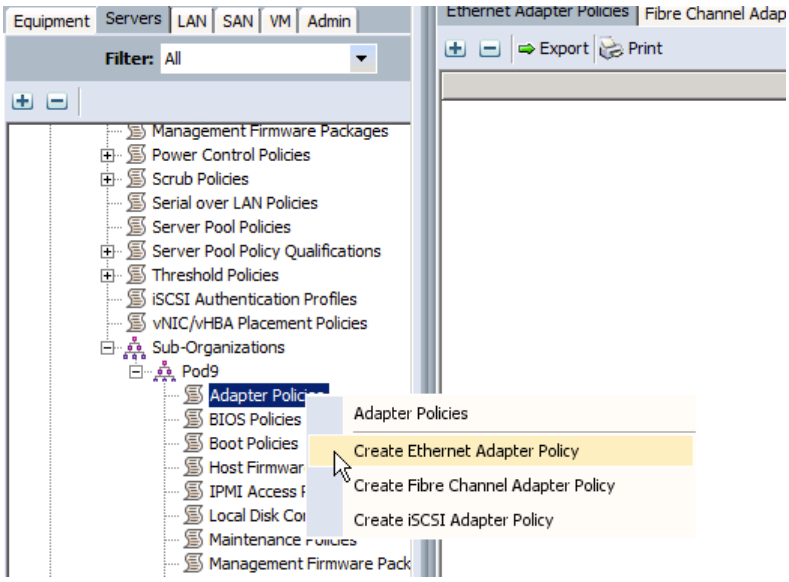
Step 4 **Log out of Cisco UCS Manager and log in with your pod-specific admin account (Pod#-Admin).**

Note	Usernames and passwords are case sensitive.

Step 5 Choose the **Servers** tab from the navigation pane and expand **Policies**.

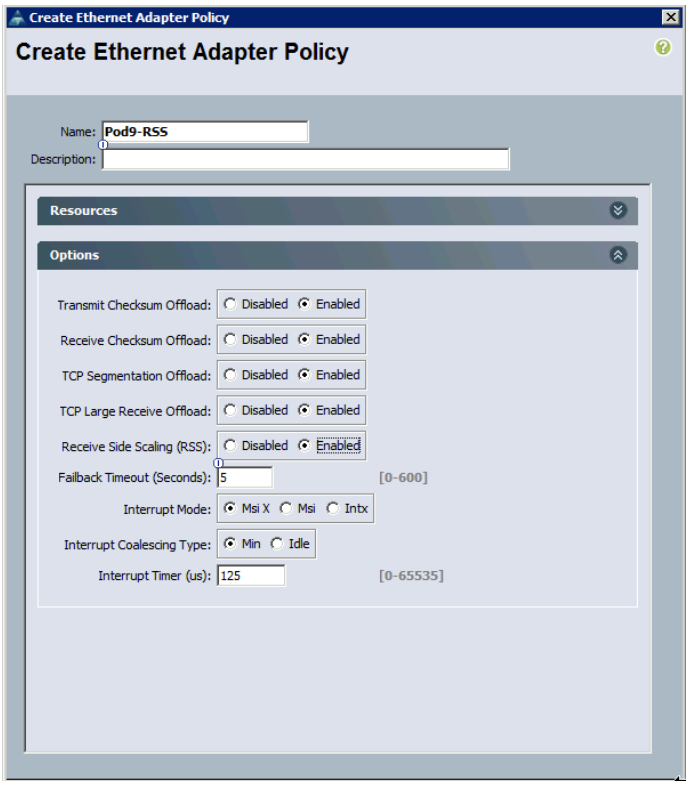
Step 6 Navigate to **Root > Sub-Organizations > Your Organization**.

Step 7 In the organization that is associated with your login, create a new adapter policy. Right-click **Adapter Policies** and choose **Create Ethernet Adapter Policy**.



Step 8 Name the policy with your Pod and RSS (for example, Pod9-RSS).

Step 9 Under Options, enable **Receive Side Scaling (RSS)**.



Step 10 Click **OK** to save the new policy.

Step 11 Scroll down to explore other organizations. Click in the organization of any other pod and attempt to create an adapter policy. You should not be able to create, modify, or delete an object that is created in another organization because your rights are restricted to your locale. The option will be grayed-out.

Activity Verification

You have completed this activity once you have completed the following:

- You have validated locale restrictions.

Lab 2-5: 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

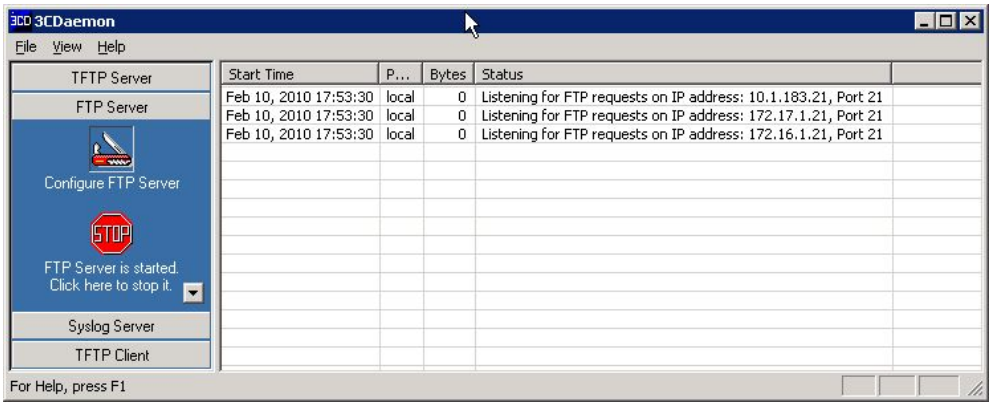
Task 1: Create a Full State Backup

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

Activity Procedure

Complete these steps:

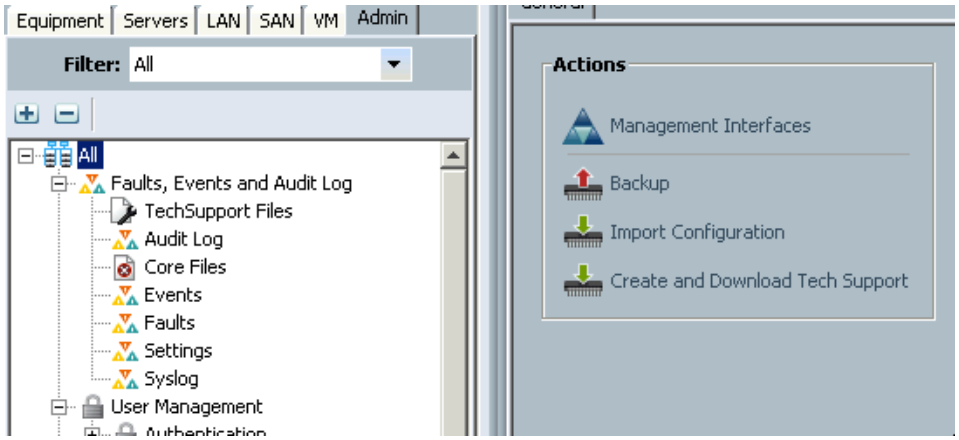
Step 1 Start 3CDaemon (a FTP, TFTP and syslog server) on your local student PC by clicking on the icon on the desktop/in the start menu.



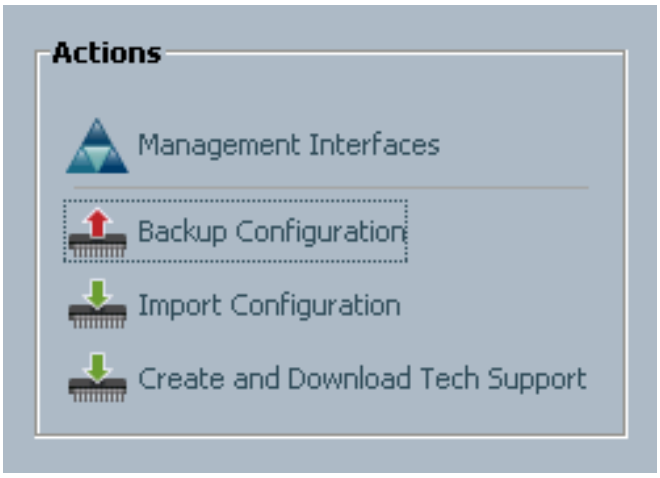
Step 2 Log into the Cisco UCS Manager with the “admin” account and password “1234QWer”

Caution If UCS manager is still open from previous labs make sure NOT to use the pod specific admin user from Lab 2-4.

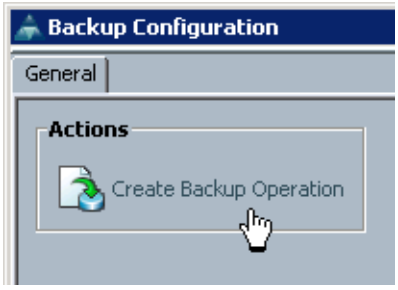
Step 3 Choose the **Admin** tab in the navigation pane. Ensure that the **Filter** value is set to **All**, and choose the **All** icon.



Step 4 Click the **Backup** link.



Step 5 In the resulting Backup Configuration window, click **Create Backup Operation**.

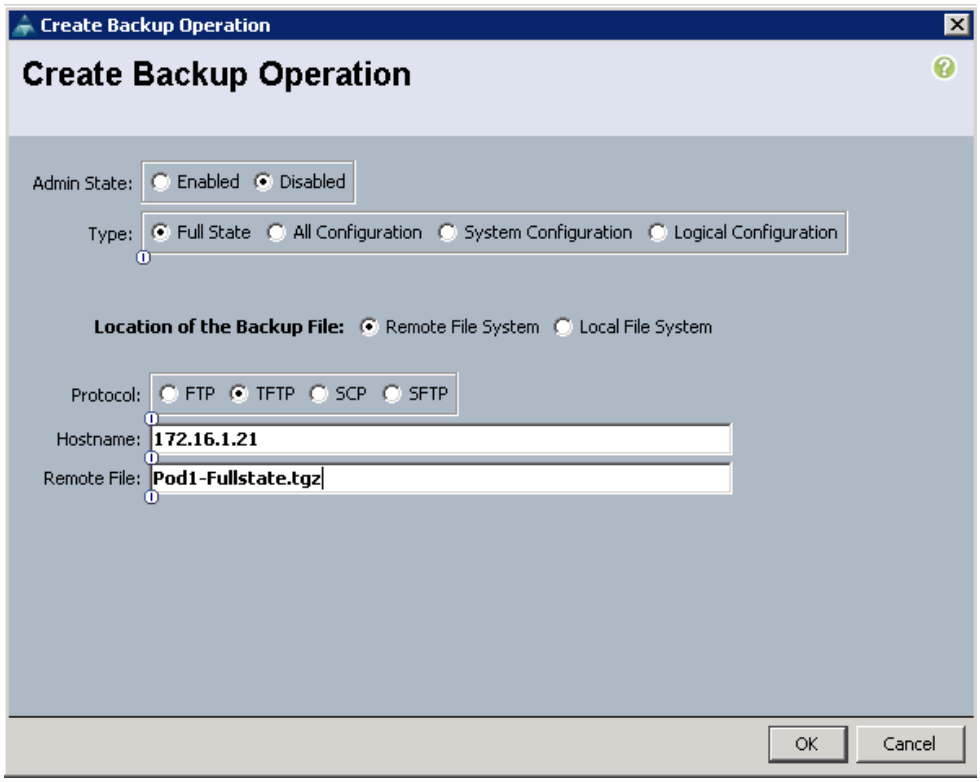


Note	If the “Create Backup Operation” Button is disabled (greyed out) make sure you use the “admin” account and not the “pod#-admin” account!

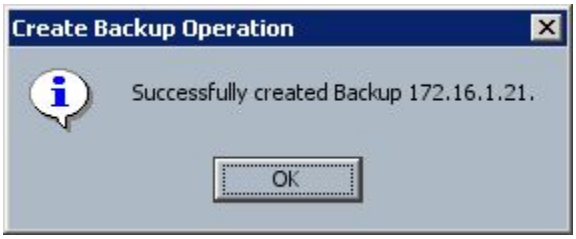
Step 6 Leave the Admin State **disabled**. Choose a **Full state** backup and the **TFTP** protocol. Use 172.16.1.2P (P is your Pod#) as the hostname (which can also be an IP address). Name the remote file **PodX-fullstate.tgz**, replacing X with your Pod number. Click **OK**.

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

Note You could also use FTP, SCP or SFTP.

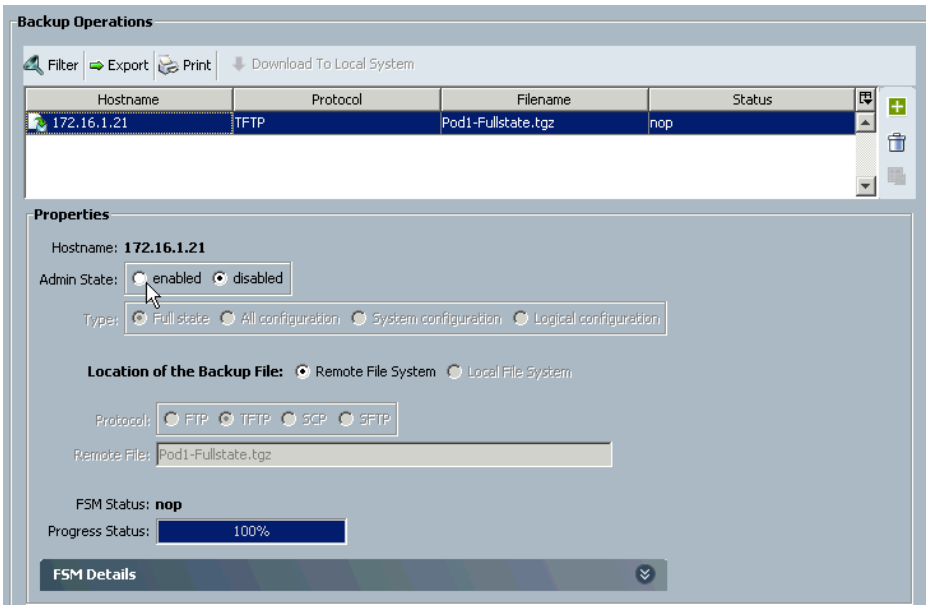


Step 7 Observe the Create Backup Operation status message, and click **OK**.

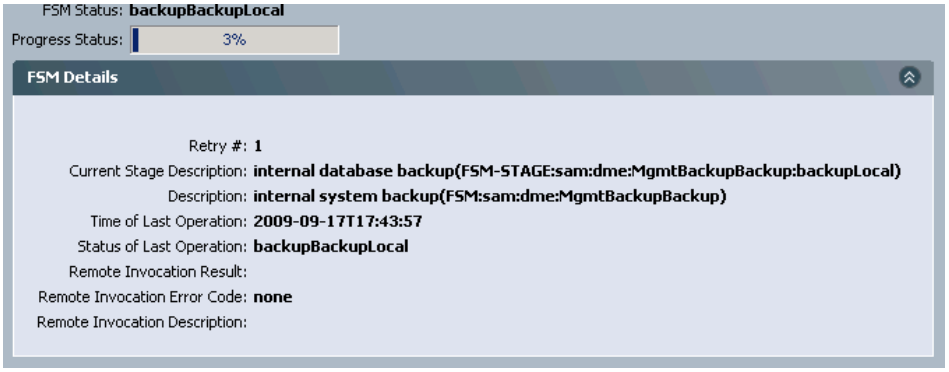


Step 8 Choose your Pod's backup operation in the table and verify the settings. Note the FSM Status of "nop" (No Operation), which indicates that the Finite State Machine for this icon has no further work to do and is not in an error state.

Step 9 Set the Admin State to **enabled** and click **Apply**.

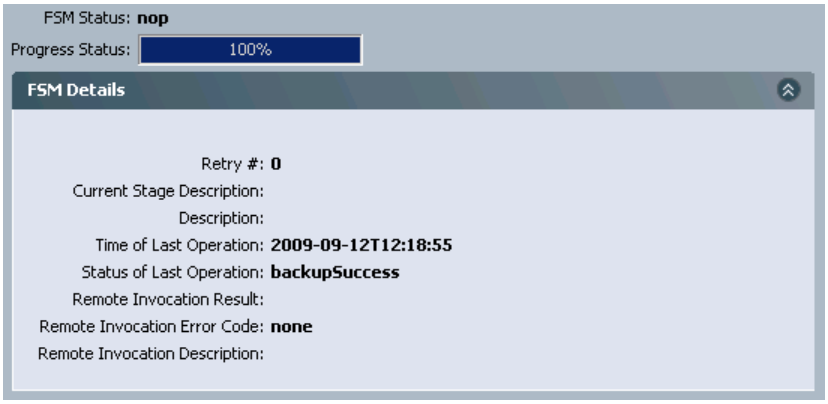


Step 10 Expand the **FSM Status** and watch the backup process complete.



Note It may take a while for your backup to complete, especially if many pods start their jobs at the same time.

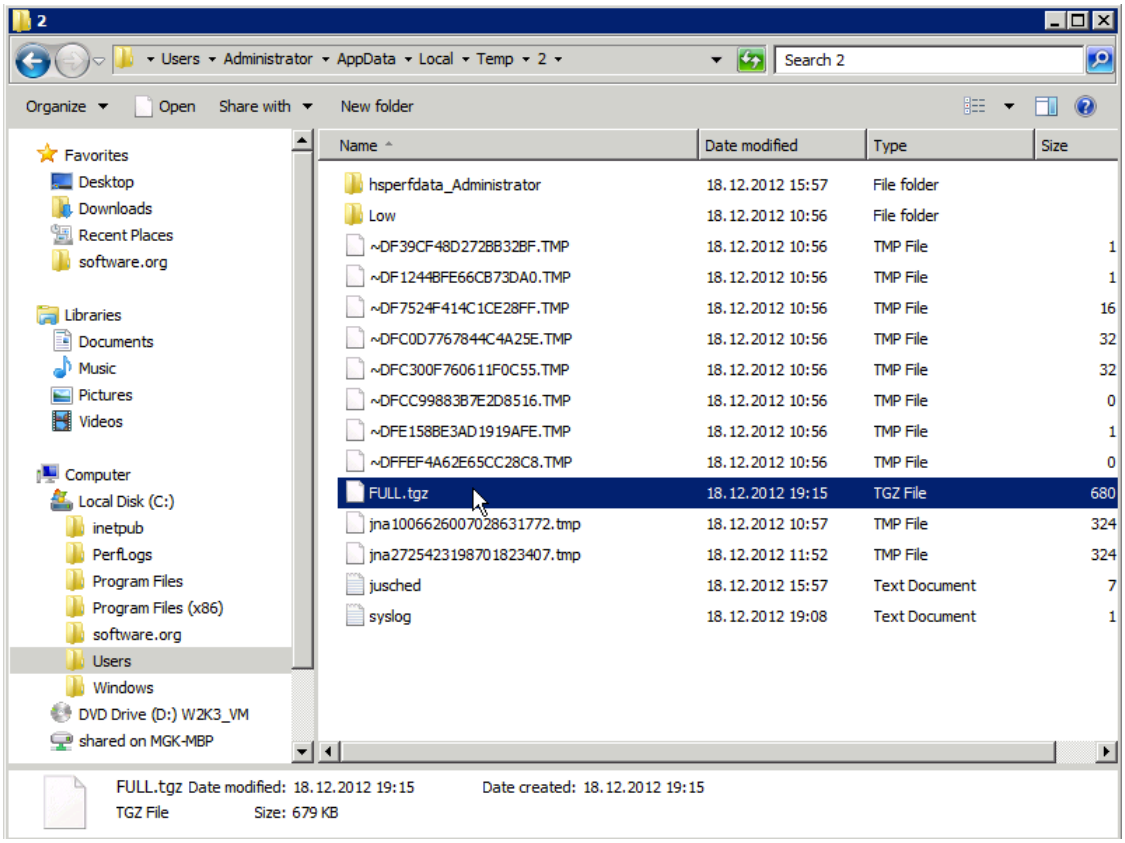
Step 11 When the backup is complete, the progress status should be 100%, the FSM Status should be nop, and the FSM Details should show a status of backupSuccess.



Step 12 Minimize any open Cisco UCS Manager windows and return to your student desktop.

Step 13 The 3CDaemon has shown the progress of the TFTP, if you want to you can backup again and watch 3CDaemon this time.

Step 14 Open windows explorer and navigate to the C:\Users\Administrator\AppData\Local\Temp\2 directory.

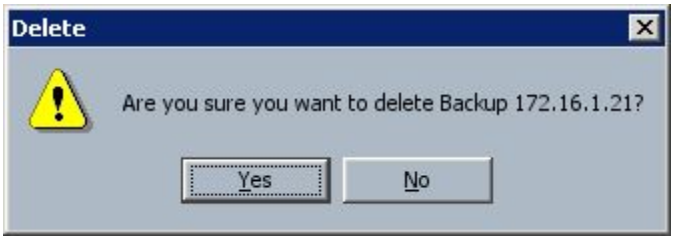


Note If 7Zip is installed you can open the file (you named it .tgz) and look inside, but there is no useable information inside. Note Cisco TAC does NOT support editing the full state backup file.

Step 15 Close the Explorer window and return to the Cisco UCS Manager Backup Configuration window.

Step 16 Choose **your Pod's** full state backup icon and click the trashcan icon to delete the Backup Job.

Step 17 Click **Yes** to confirm the deletion.



Step 18 Click **OK** to apply the changes and **close** the Backup Configuration window.

Task 2: Create a Configuration Backup

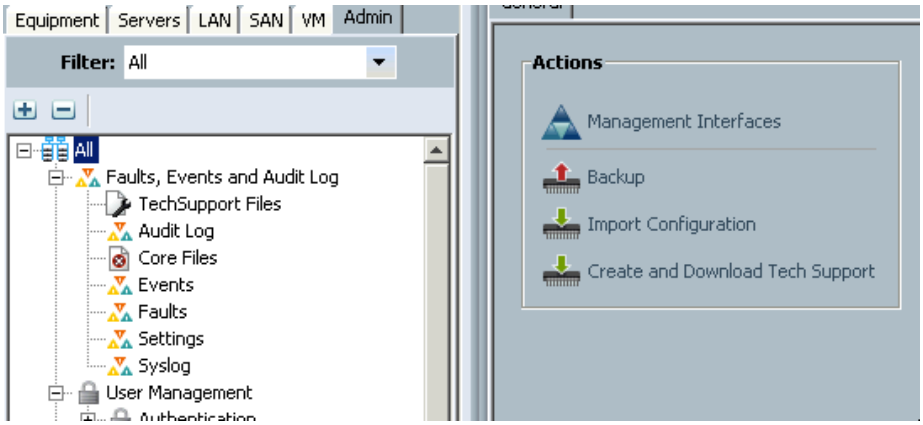
In this task, you will create an XML configuration-level backup of the Cisco UCS configuration.

Activity Procedure

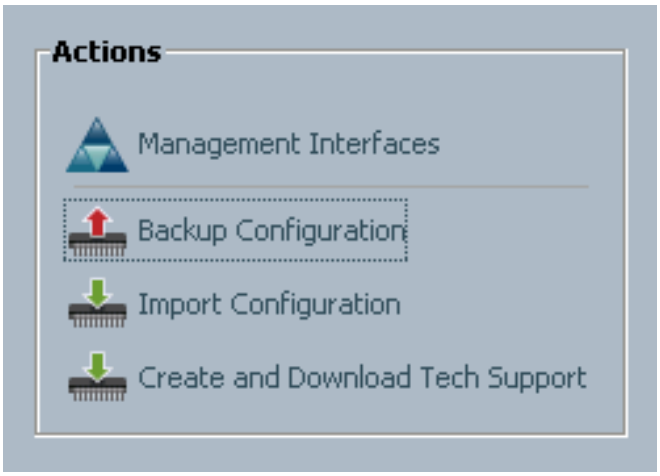
Complete these steps:

Step 1 Log into the Cisco UCS Manager if necessary.

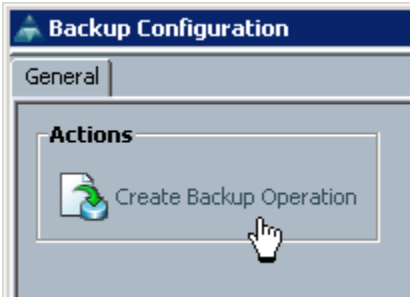
Step 2 Choose the **Admin** tab in the navigation pane. Ensure that the **Filter** value is set to **All**, and choose the **All** icon.



Step 3 Click the **Backup** link.

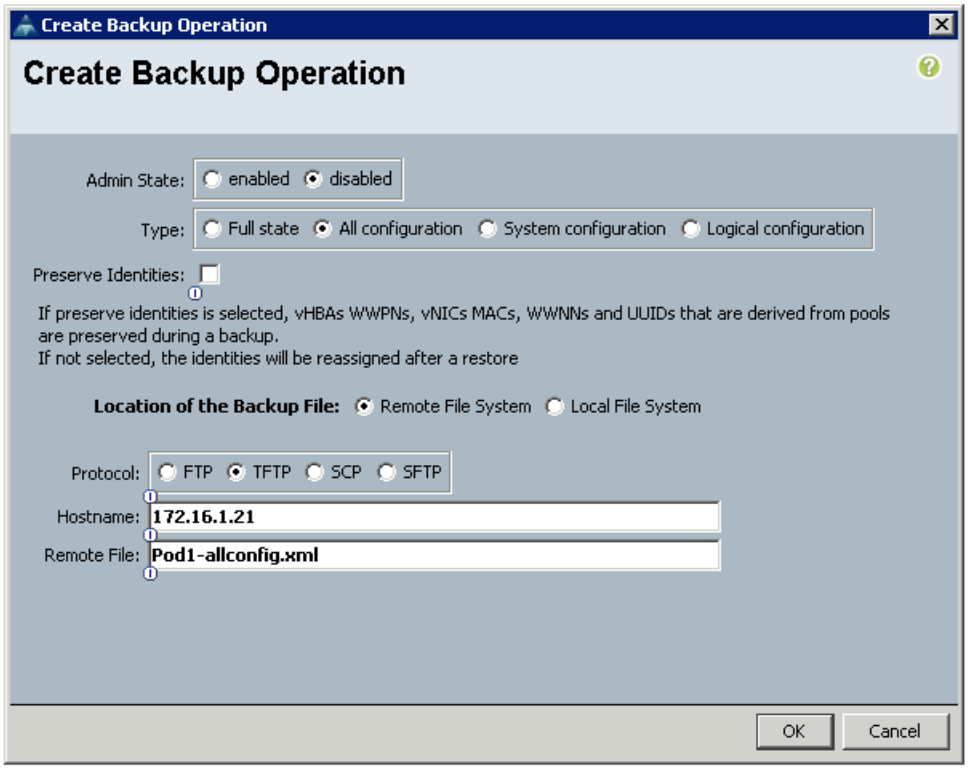


Step 4 In the resulting Backup Configuration window, click **Create Backup Operation**.

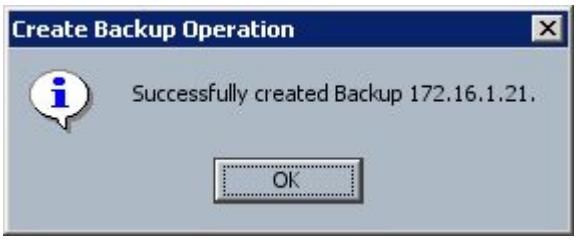


Step 5 Leave the Admin State **disabled**. Choose **All configuration** backup and the **TFTP** protocol. Use 172.16.1.2P (P is your Pod#) as the hostname (which can also be an IP address). Name the remote file **PodX-allconfig.xml**, replacing X with your Pod number. Click **OK**

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

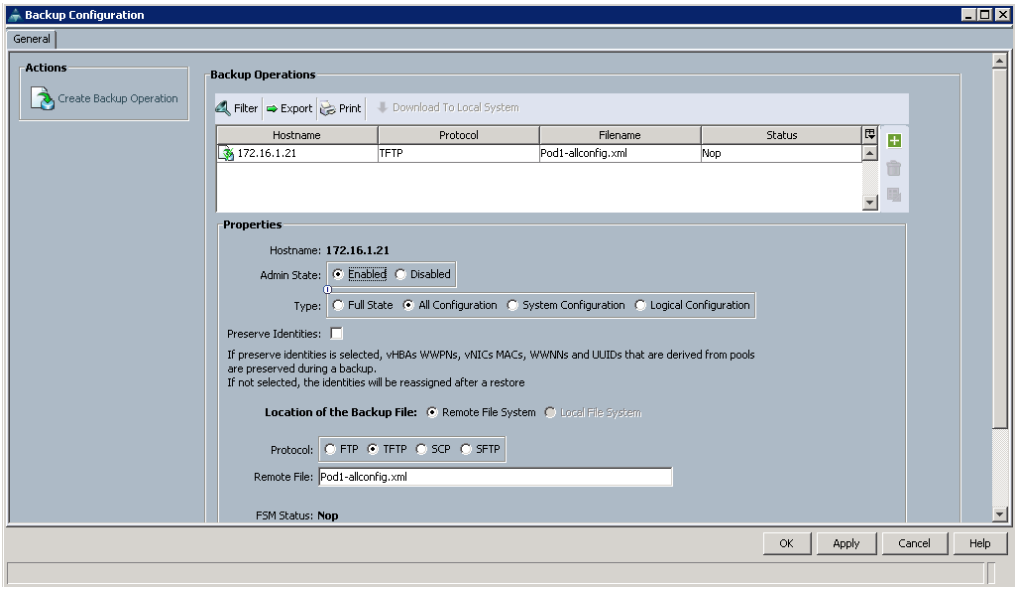


Step 6 Click **OK**.



Step 7 Choose your Pod'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** and click **Apply**.



Step 9 Depending on the speed of the TFTP server, you might not see any activity in the FSM Details before the backup completes.

Note It may take a while for your backup to complete, especially if many pods start their jobs at the same time.

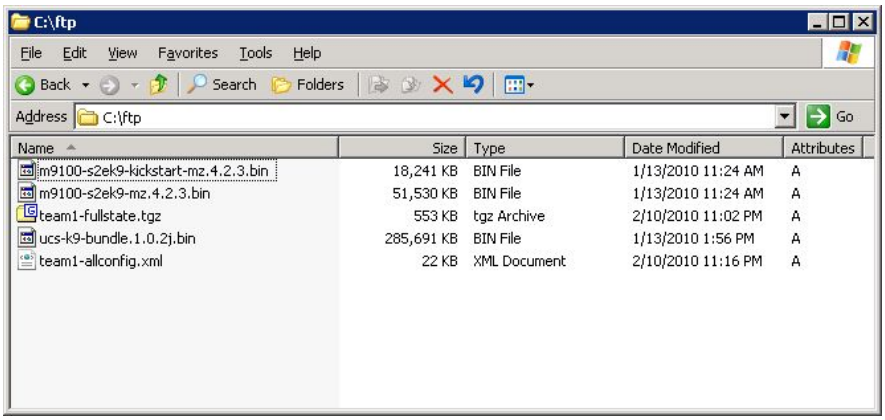
Step 10 When the backup is complete, the progress status should be 100%, the FSM Status should be nop, and the FSM Details should show a status of backupSuccess.

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

Step 12 Open 3CDaemon, you should see the file transfer in the log.

Step 13 Open Windows Explorer and navigate to the C:\Users\Administrator\AppData\Local\Temp\2 directory.

Step 14 Verify that you can see your Pod's configuration backup.



Step 15 Double-click the XML file on the TFTP server. This will launch an Internet Explorer window to display the XML-formatted backup.

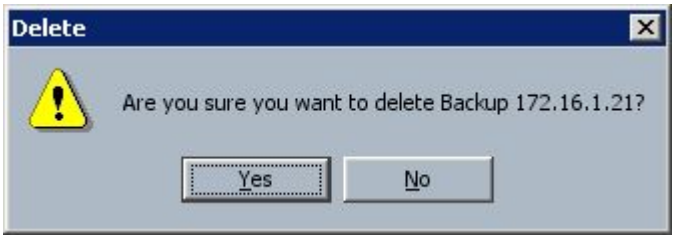
Spend a few minutes reviewing the contents of the backup.

Note You can also use the “XML notepad” application on your desktop to view and edit config files.

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

Step 17 Choose your Pod’s **All** configuration backup icon and click the trashcan icon to delete the Backup Job.

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



Step 19 Click **Apply** to active your changes

Step 20 Click **OK** to close the Backup Configuration window.

Task 3: Create an Import Job

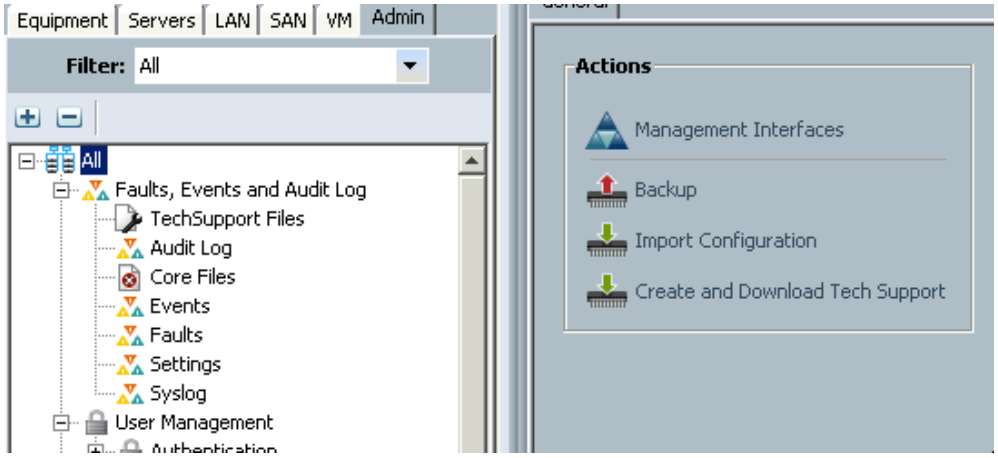
In this task, you will create an import job to restore a configuration backup from an TFTP server.

Activity Procedure

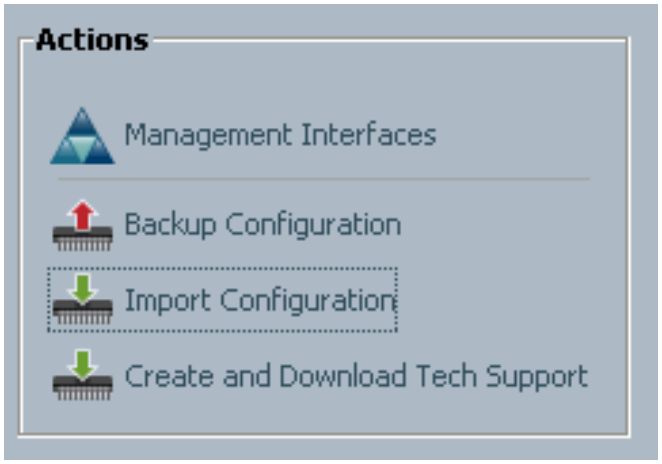
Complete these steps:

Step 1 Log into the Cisco UCS Manager if necessary.

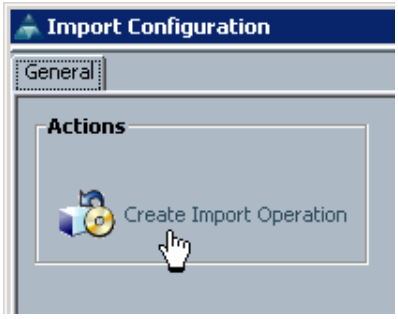
Step 2 Choose the **Admin** tab in the navigation pane. Ensure that the **Filter** value is set to **All**, and choose the **All** icon.



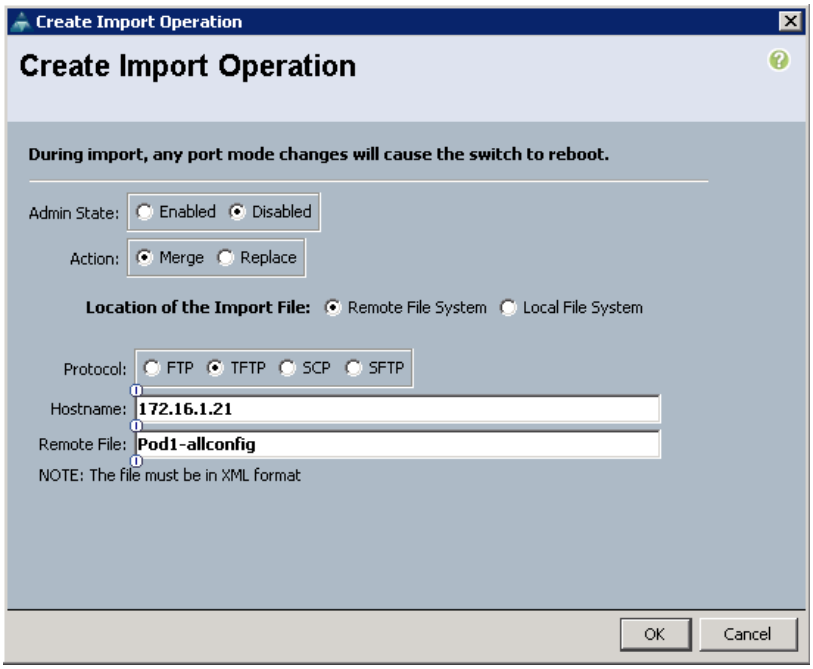
Step 3 Click the **Import Configuration** link.



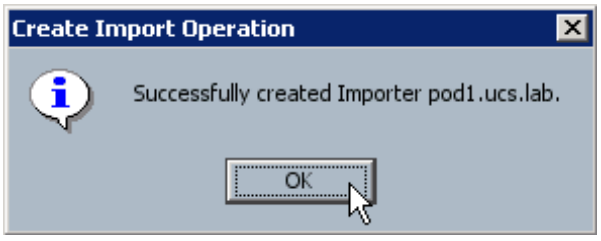
Step 4 In the resulting Import Configuration window, click **Create Import Operation**.



Step 5 **Leave the Admin State disabled** and the Action as merge. Set the hostname as specified in your Lab Reference Guide, "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.



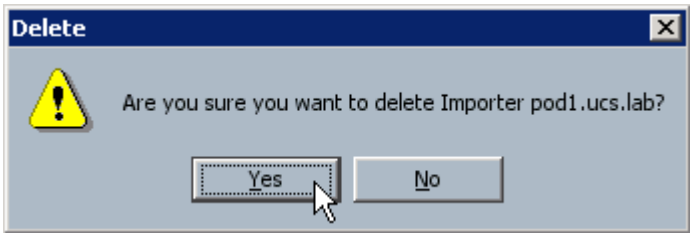
Step 6 Click **OK** to confirm the Create Import Operation status.



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, DO NOT ENABLE but 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.

Task 4: Create a TechSupport file for Cisco TAC (optional)

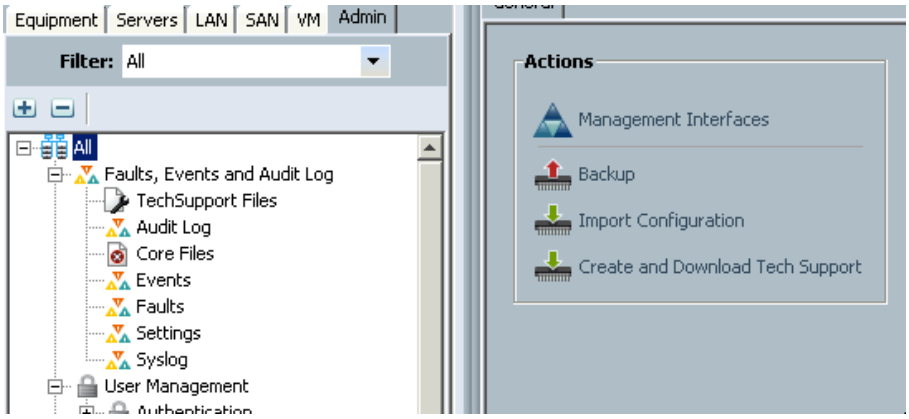
In this task, you will create a Tech support file. This will take a long time because a lot of information is collected and processed.

Activity Procedure

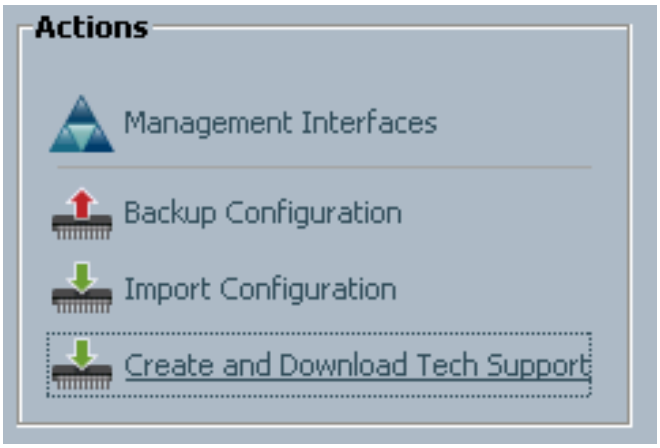
Complete these steps:

Step 1 Log into the Cisco UCS Manager if necessary.

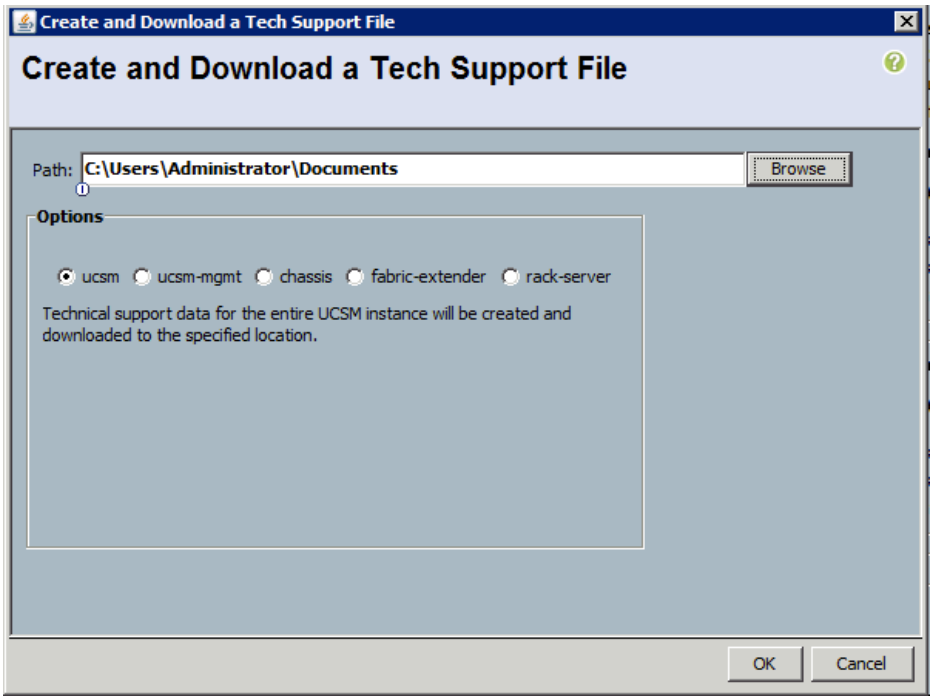
Step 2 Choose the **Admin** tab in the navigation pane. Ensure that the **Filter** value is set to **All**, and choose the **All** icon.



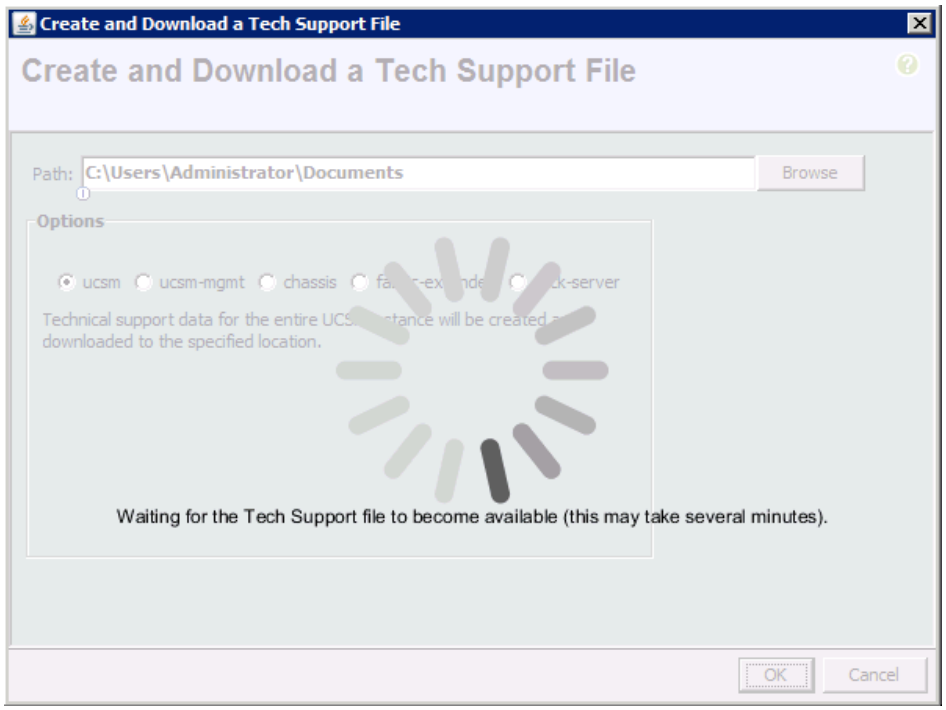
Step 3 Click the **Create and Download Tech Support** link.



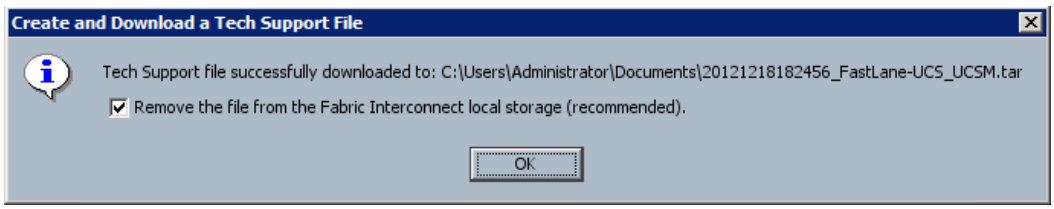
Step 4 Navigate to c:/temp and click OK



Step 5 Wait for the tech.support document to be created and downloaded (note you do NOT need a FTP/TFTP server but the document is downloaded to your student PC.



Step 6 Confirm deletion of the test support document from the FI flash.



Lab 2-6: 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 Call-Home
- Configure external logging servers
- Export event and fault information

Required Resources

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

- (2) Cisco UCS Fabric Interconnects
- email server supporting the SMTP protocol

DEMO: Call Home Global Configuration

In this task, first the instructor will configure the Call Home feature, then you will set detailed parameters and test CallHome.

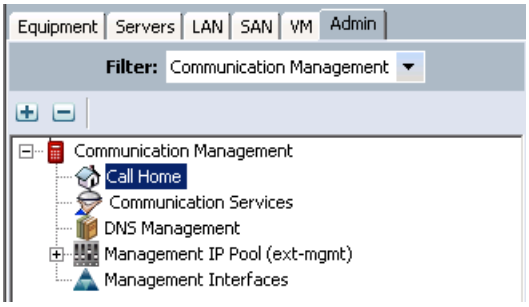
The first part will be the global configuration. Since this can only be done once it will be demonstrated by your instructor.

Activity Procedure

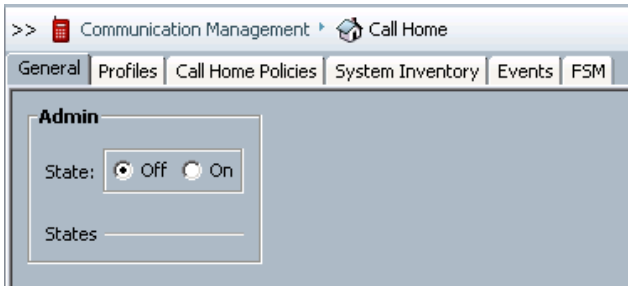
The Instructor is going to complete these steps:

Step 1 Log into Cisco UCS Manager.

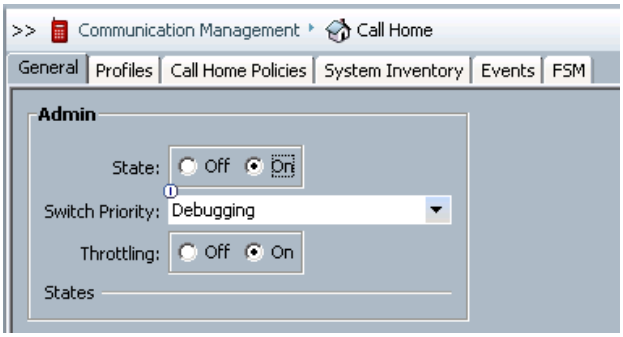
Step 2 Choose the **Admin** tab in the navigation pane. It may be helpful to change the **Filter** field to **Communication Management** for the following steps. Choose the **Call Home** icon.



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



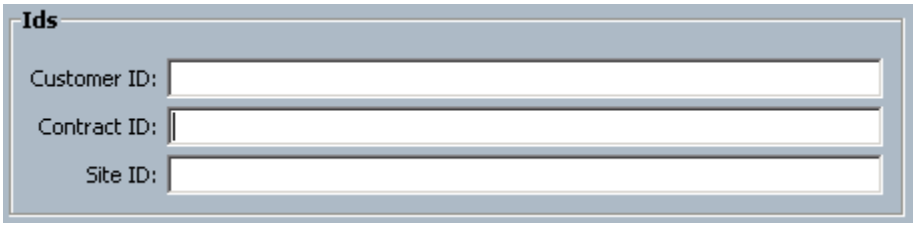
Step 4 Change the Admin state to **On**.



Step 5 Fill in some "contact" information (it is mandatory but doesn't really matter here)

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 The ID section is optional.



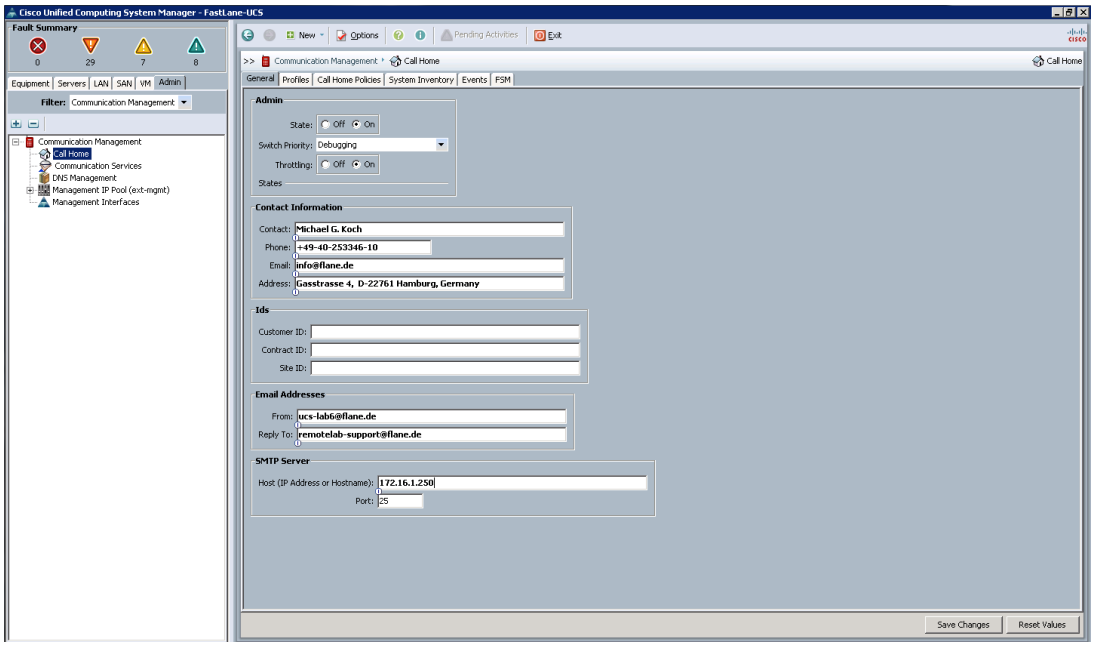
Note All fields in the IDs section are optional. These values will be included in any Call Home messages.

Step 7 Fill in the email addresses. Email today is the only CallHome notification mechanism supported

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 Configure **172.16.1.250** as the SMTP server.

Step 9 Save the Call Home configuration.



Task 1: Call Home Configuration

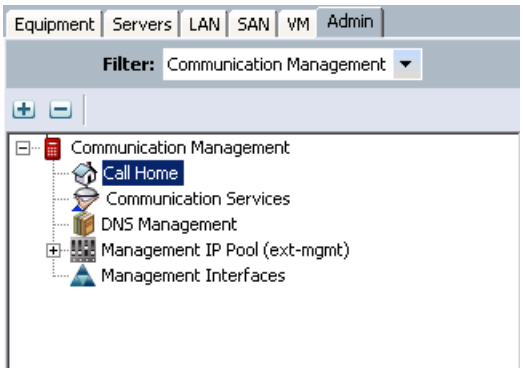
In this task, you will configure the Call Home feature.

The global configuration is done, now each pod will create individual CallHome profiles and send email to a webmail server in the lab.

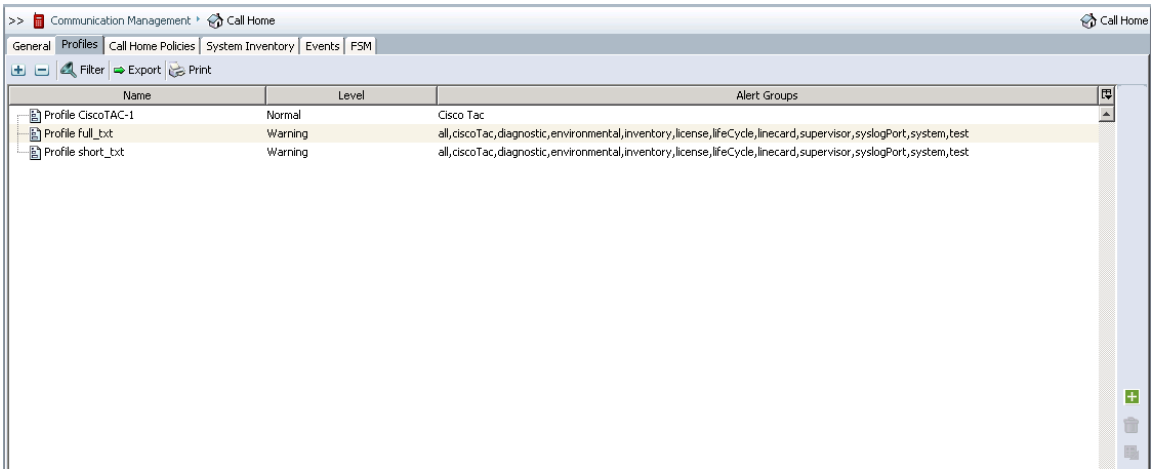
Activity Procedure

Step 1 Log into Cisco UCS Manager.

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.

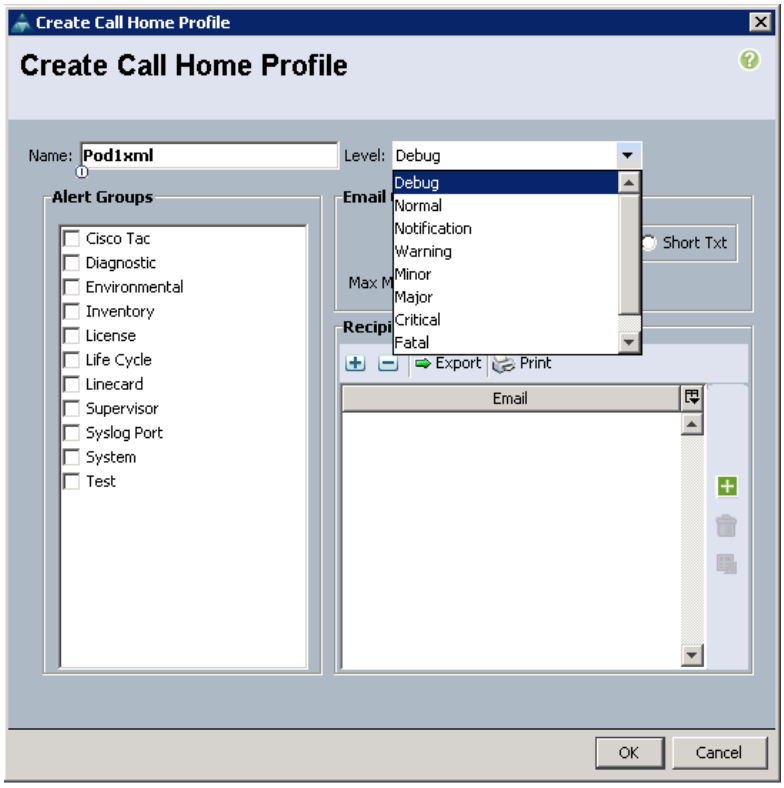


Step 3 In the content pane, choose the **Profiles** tab, and click the **+** sign to add your profile.

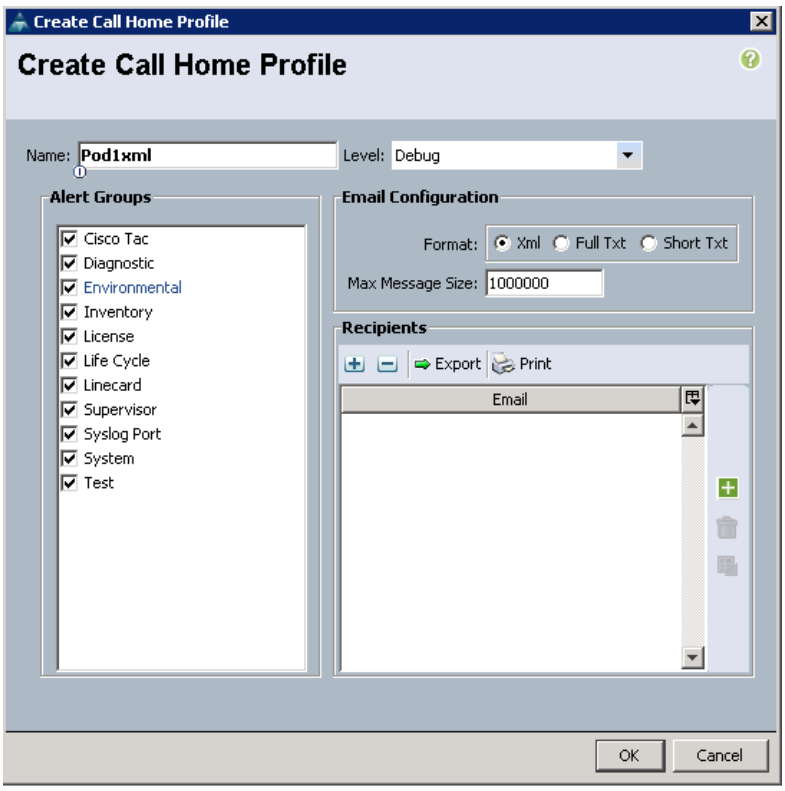


Step 4 Name your profile PodPxml (P is your Pod#)

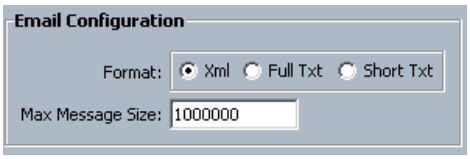
Step 5 Take a moment to review the message levels available. This setting dictates that all messages of the selected level and above (meaning more severe) will be sent to recipients of this profile.



Step 6 Take a moment to review the Alert Groups that are available. This setting dictates which category of messages will trigger this profile. Select ALL Groups.

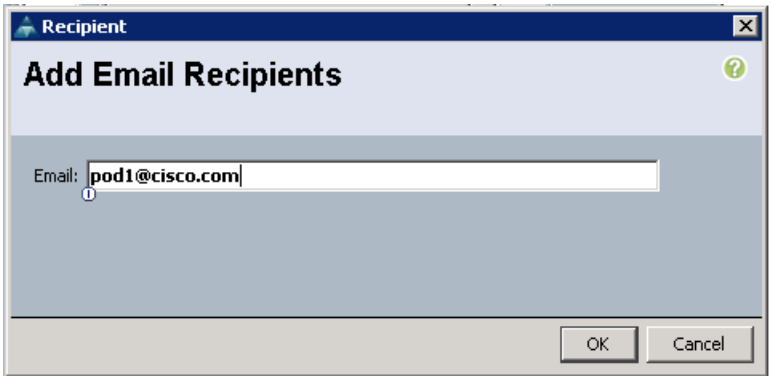


Step 7 Review the Email Configuration section. This section allows you to choose the format of messages that are sent to recipients of this profile, as well as set a maximum message size (in bytes). Any data above this size will be truncated. Make sure "inventory" is selected. Accept the defaults.

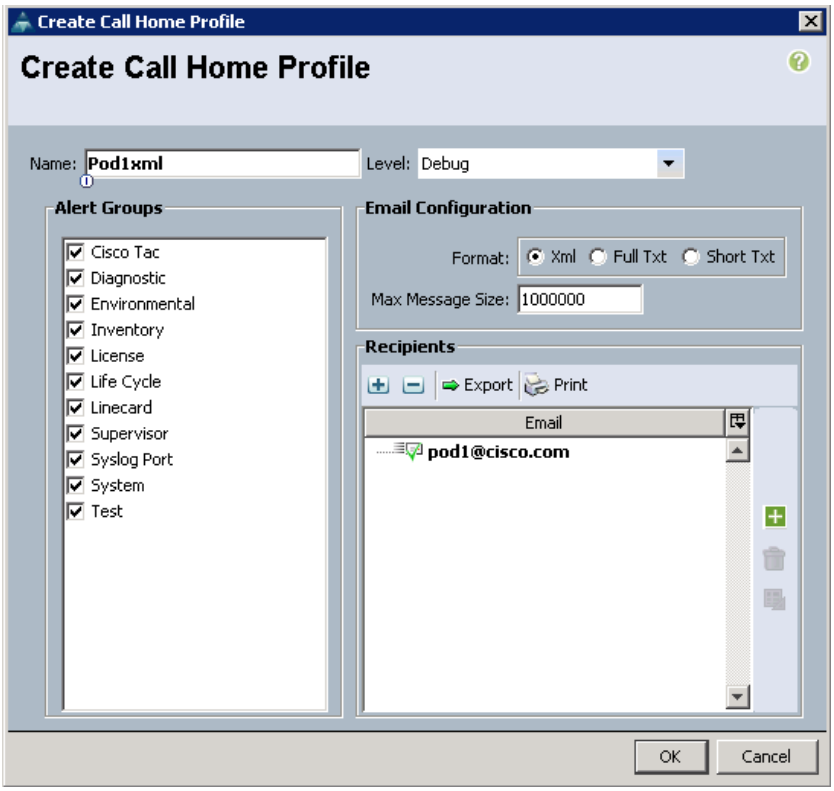


Step 8 Click the "**+**" button to add a recipient to this profile. Add **podP@cisco.com** as a receiver (is your Pod#).

Caution If you use another email recipient address you will not be able to receive the email.

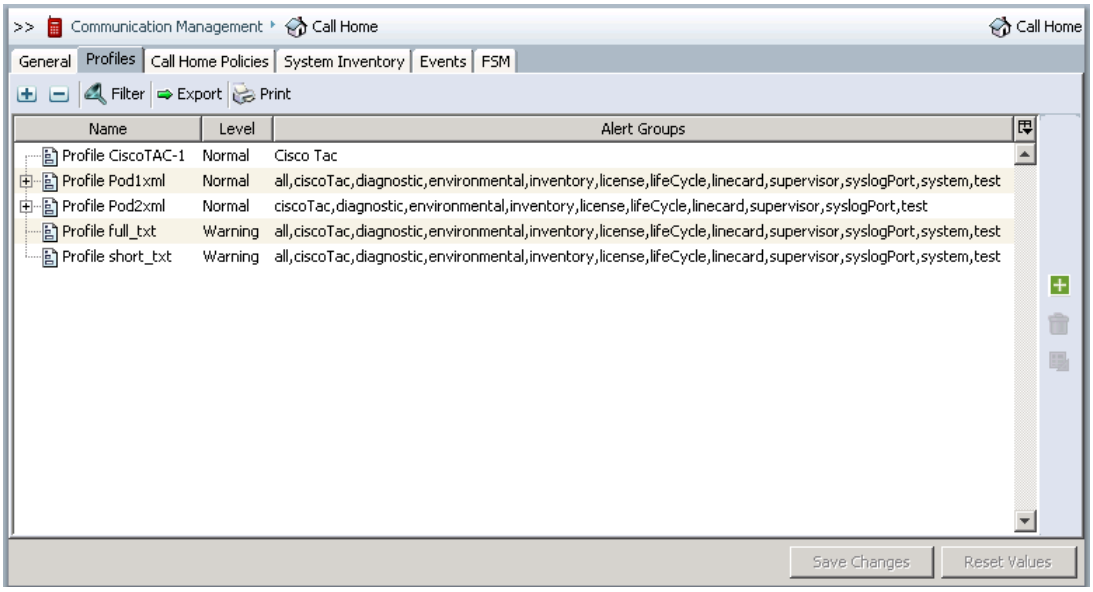


Step 9 Click **OK**.

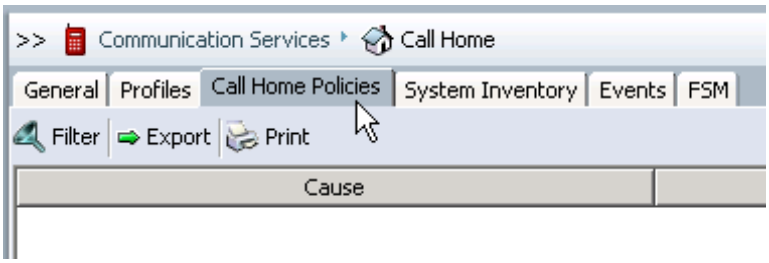


Step 10 Click **OK** to create the CallHome profile

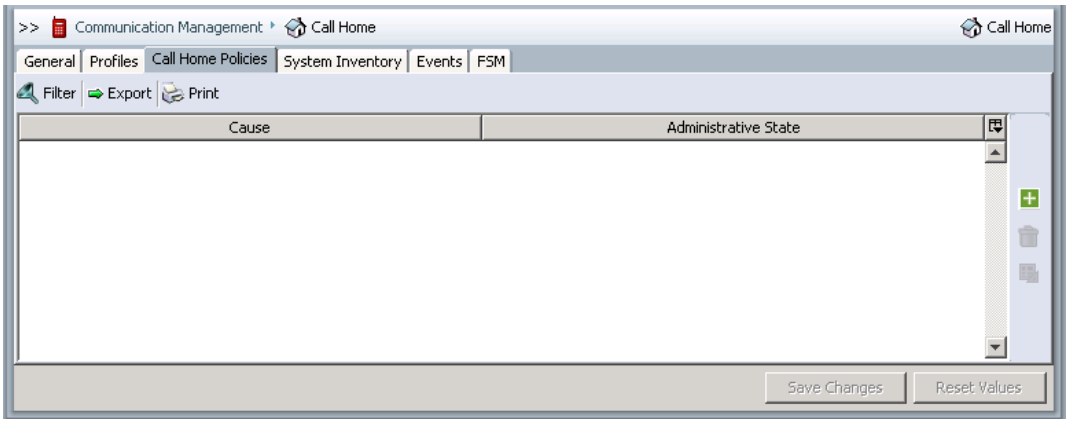
Step 11 Check your profile is now visible. (there may also be profiles from other Pods.)



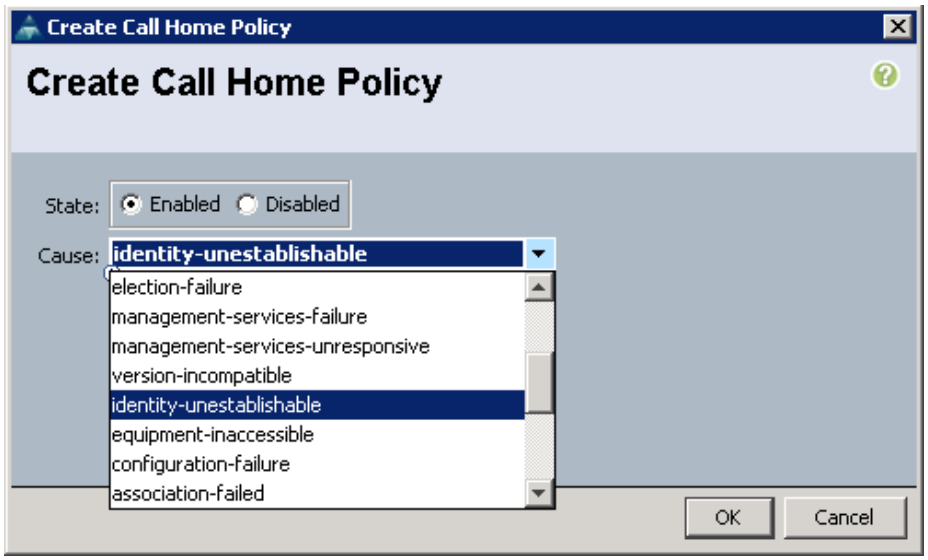
Step 12 In the content pane, click the **Call Home Policies** tab.



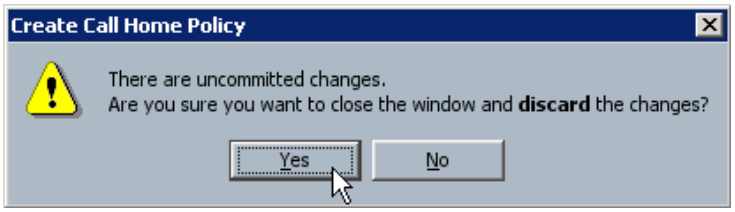
Step 13 Click the "+" button to add a new Call Home Policy.



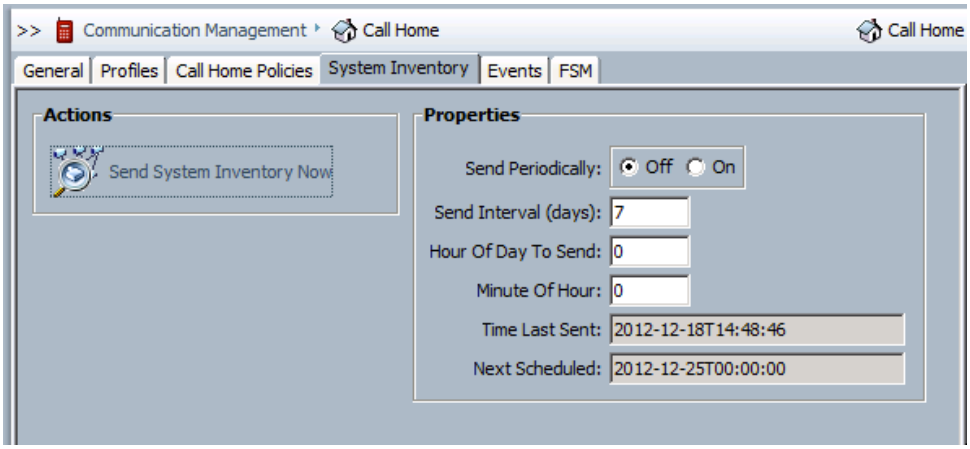
Step 14 Explore the options for creating a new Call Home Policy. When you have reviewed the options available, click **Cancel**. ***Only one of each policy can be created. As the lab is a shared environment, if multiple Pods attempt to create the same policy, errors might occur.***



Step 15 If you receive a warning regarding committed changes, click **Yes** to confirm discarding the changes.



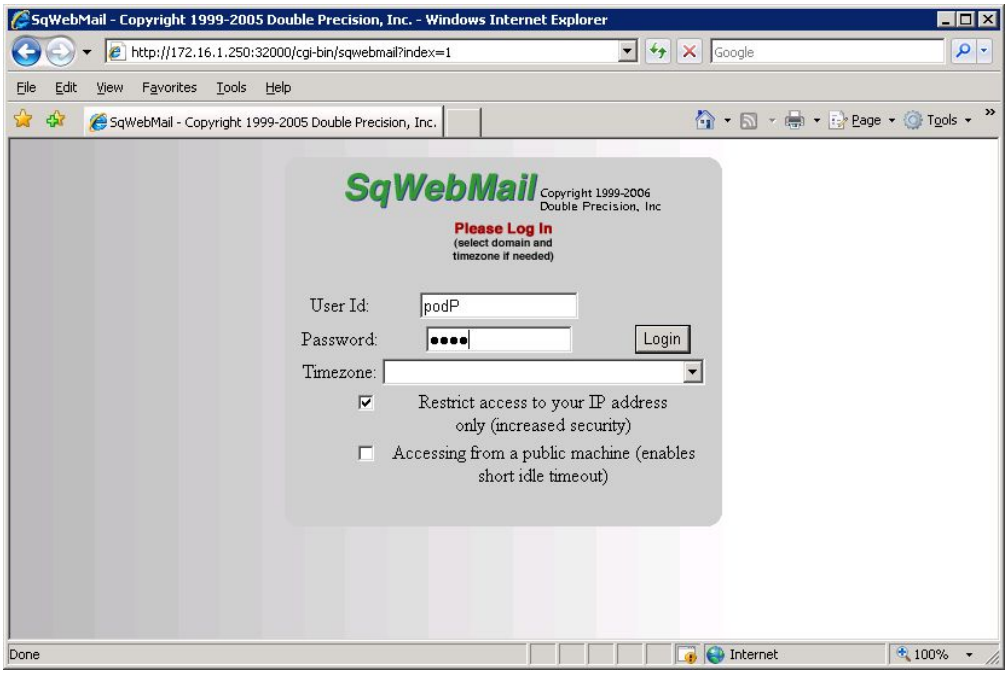
Step 16 In the content pane, choose the **System Inventory** tab. Spend a few moments reviewing the configuration options for System Inventory.



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.

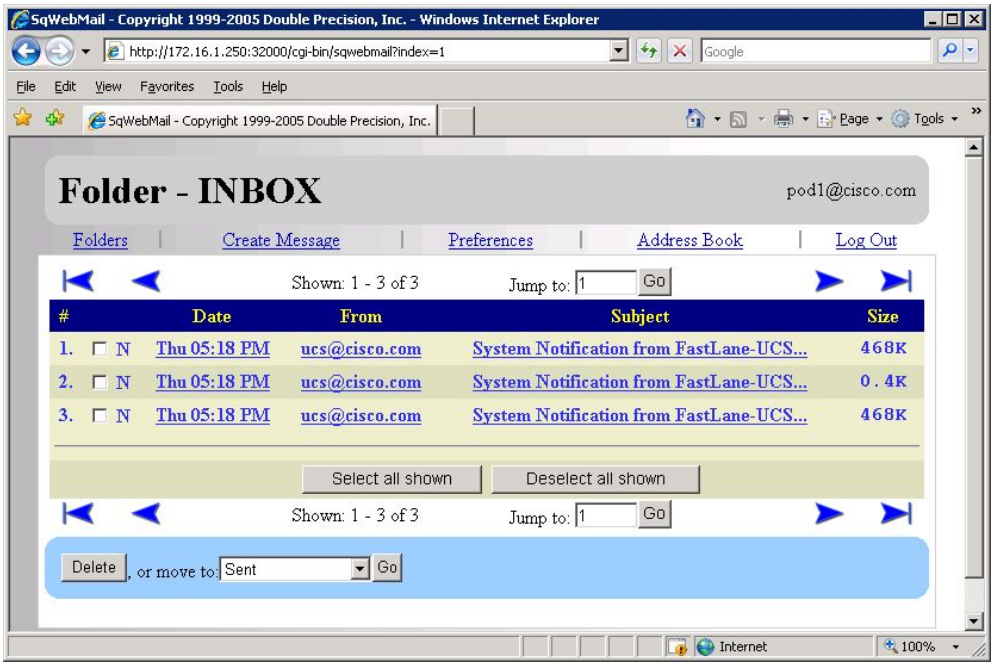
Step 17 Click the “send System Inventory now” action.

Step 18 Open a Internet Explorer window on your student desktop and navigate to http://172.16.1.250/mail (or the SMTP server the instructor configured)

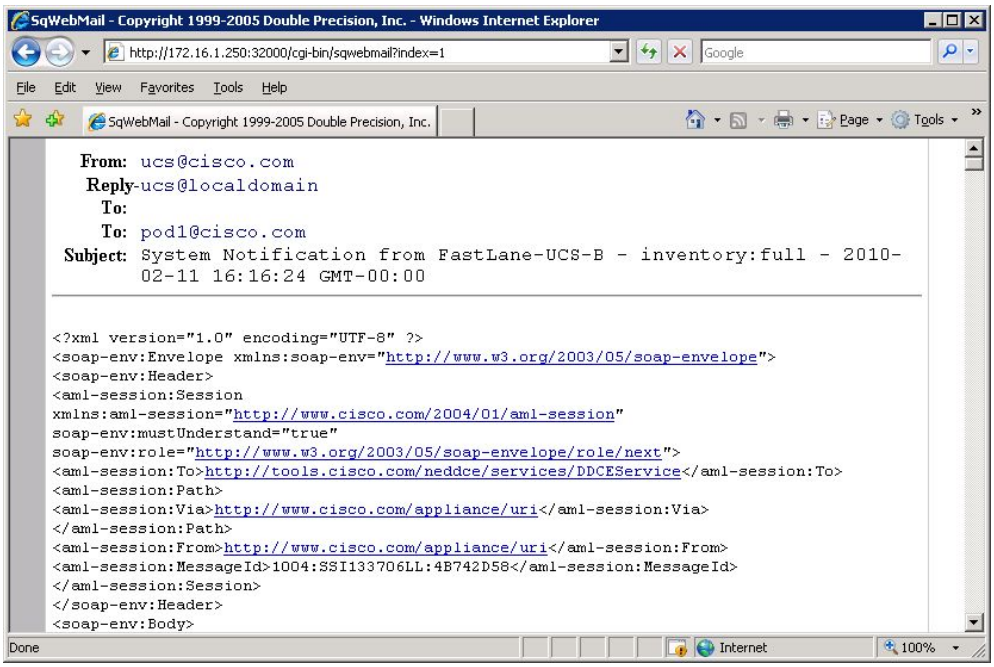


Step 19 Login with **podP** as the username and password (P is your Pod# again)

Step 20 Open the INBOX



Step 21 Open one of the emails.



Note	If no email shows up make sure all parameters were set correctly (the recipient email is the most important parameter) and the “send email now” step 18 has been done.

Step 22 (Optional) Change your message format to shortText or fullText and review those emails.

Task 2: Configure External Logging

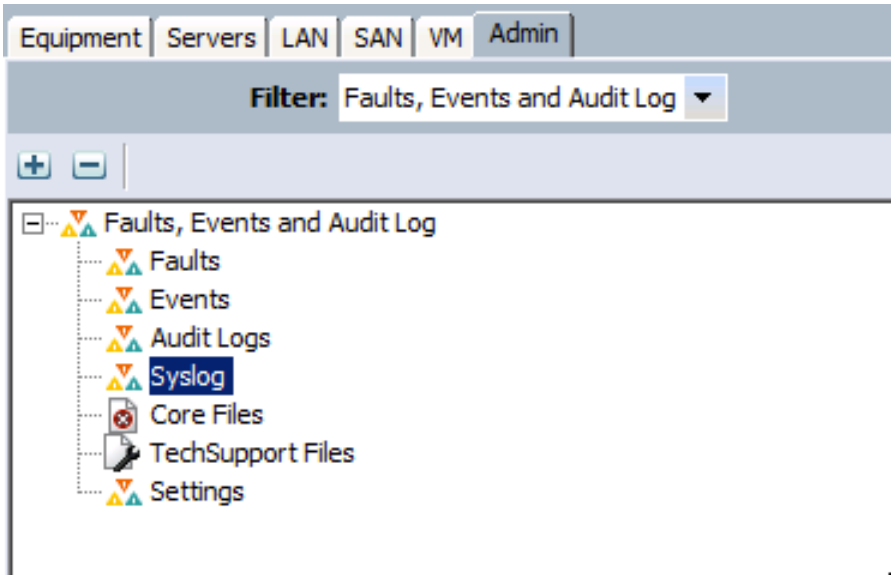
In this task, you will configure options for remote logging.

Activity Procedure

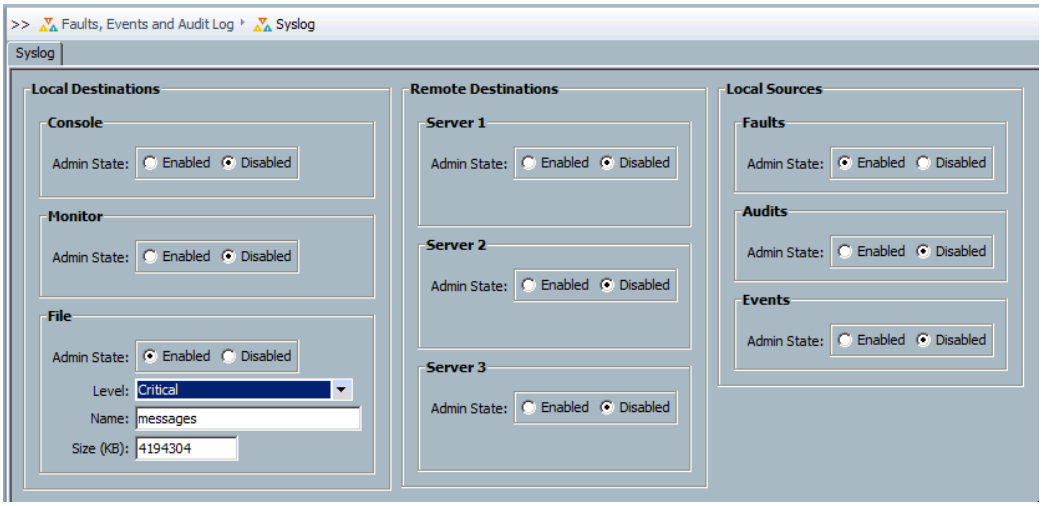
Complete these steps:

Step 1 Log into Cisco UCS Manager if necessary.

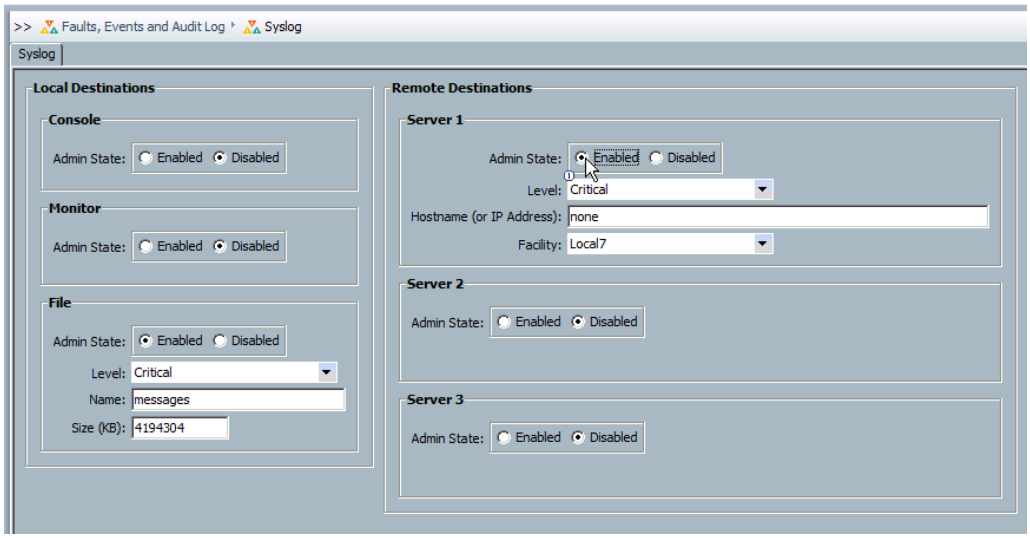
Step 2 Choose the **Admin** tab in the navigation pane. It may be helpful to change the **Filter** field to **Faults, Events and Audit Log** for the following steps. Choose the **Syslog** subicon.



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**.

Only 3 syslog destinations can be configured at the same time.

Task 3: Configuring SNMP and other management access

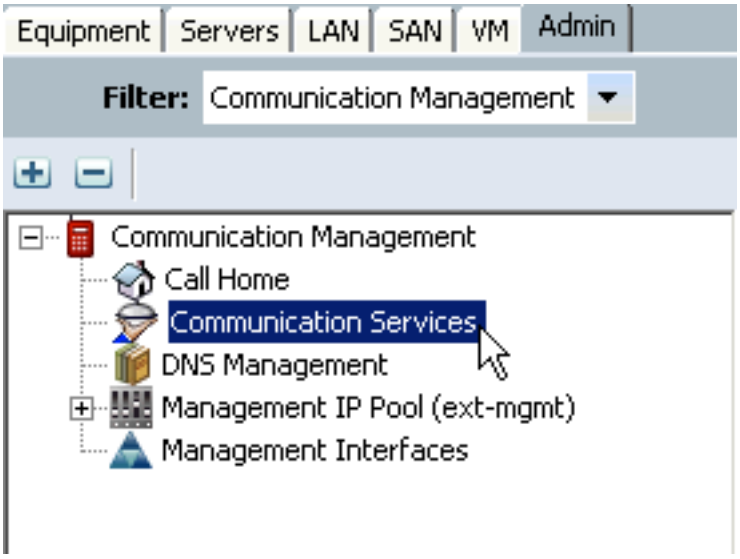
In this task, you will configure options for remote logging.

Activity Procedure

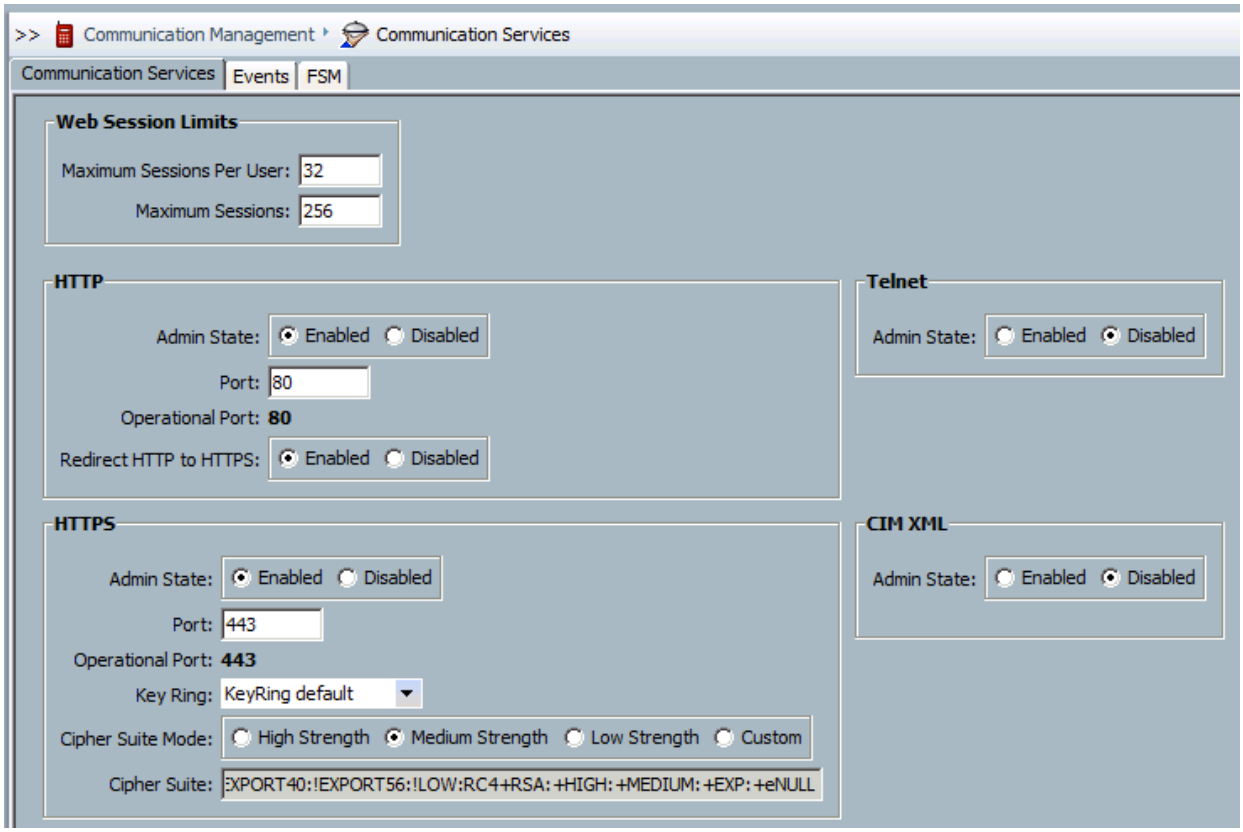
Complete these steps:

Step 1 Log into Cisco UCS Manager if necessary.

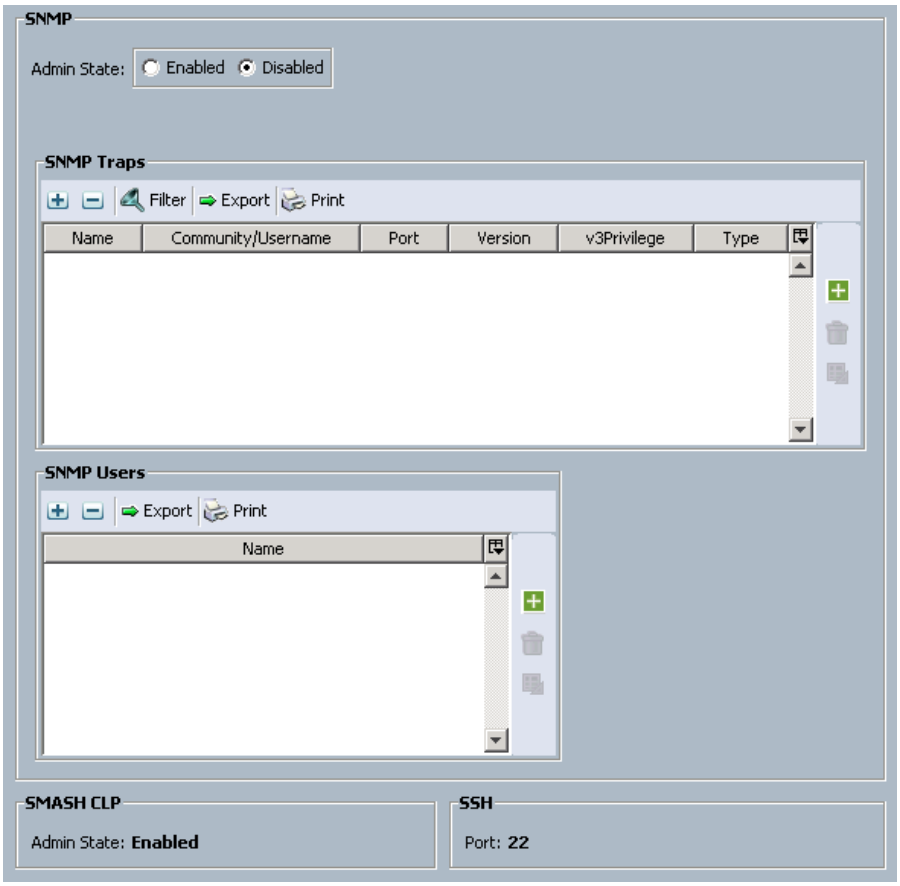
Step 2 Choose the **Admin** tab in the navigation pane. It may be helpful to change the **Filter** field to **Communication Management** for the following steps. Choose the **Communication Services** subicon.



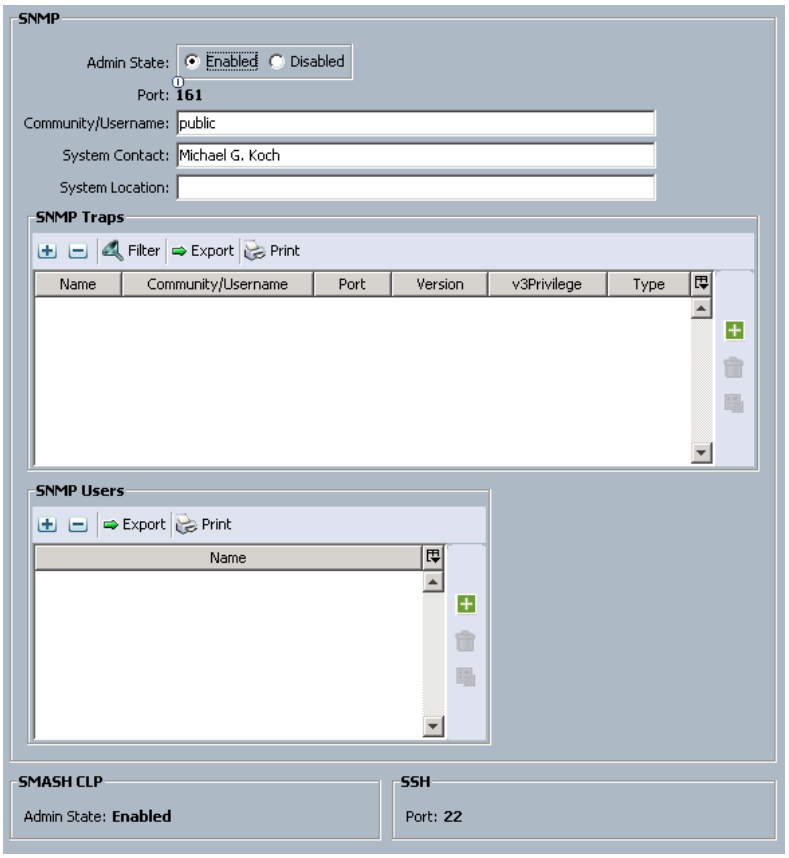
Step 3 Note parameters for Telnet, HTTP(S) and CIM.



Step 4 Scroll down to the SNMP section

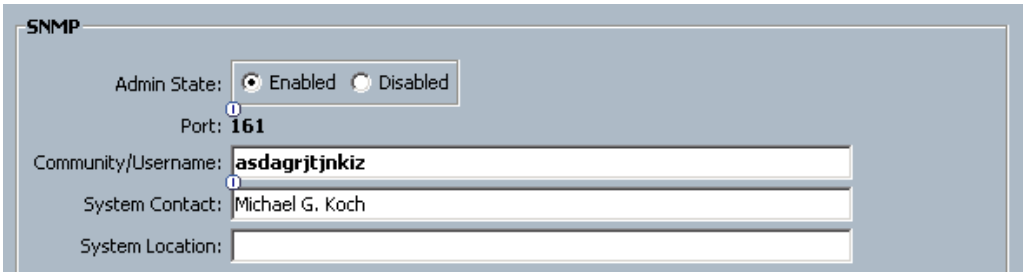


Step 5 Click the “enabled” checkbox, note the default SNMP v1/2c community is “public” ☹

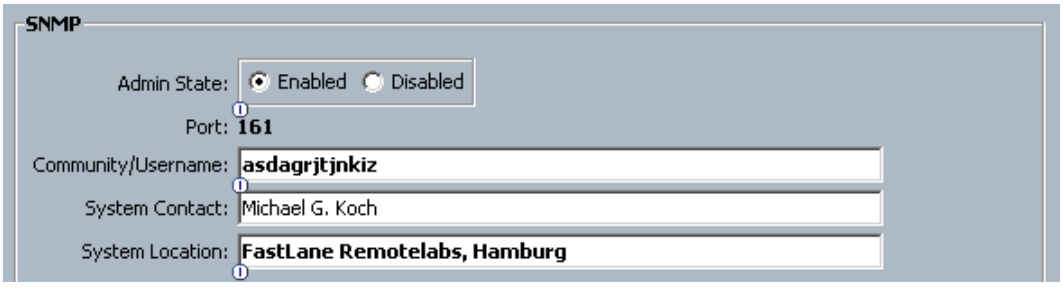


Caution You cannot disable SNMP version 1/2c. It is best practice to use a random community and use SNMP v3 for accessing the UCS system.

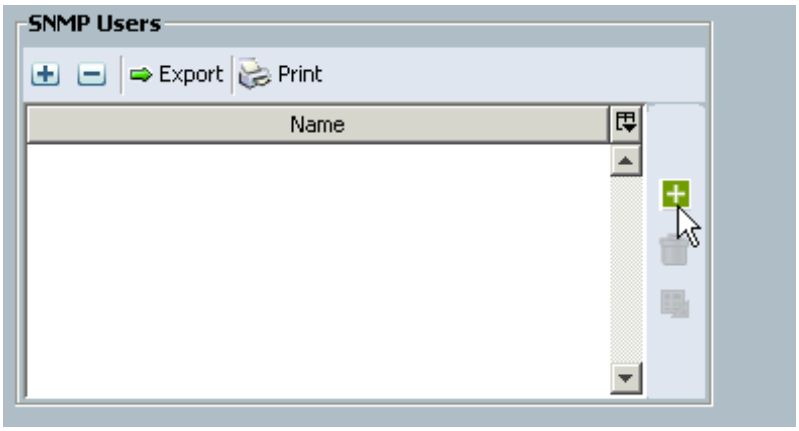
Step 6 Change the SNMP community to random characters



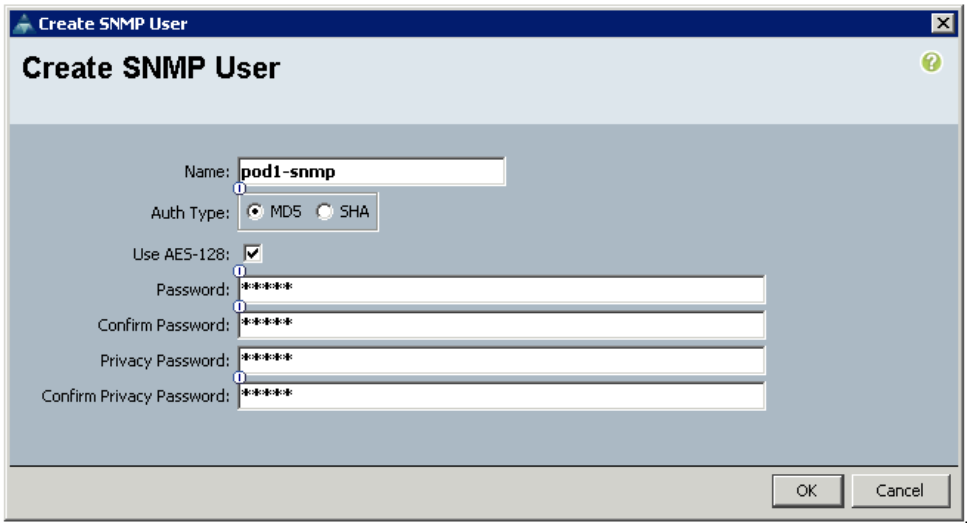
Step 7 Enter contact and location information



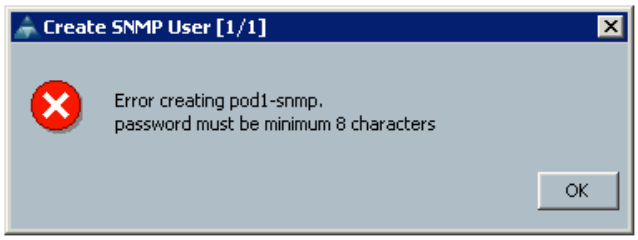
Step 8 Click the + sign in the **SNMP Users** sections to add a SNMPv3 user



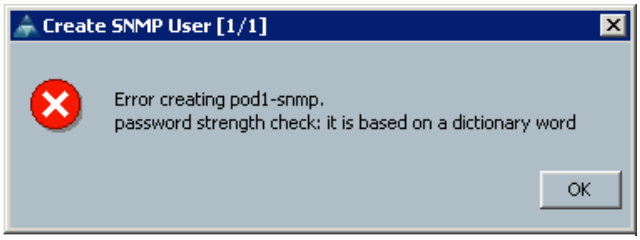
Step 9 Use username podX-snmp, select an authentication algorithm and check the AES checkbox to enable encryption, fill in all 4 password entry fields with the password "public" and click OK.



Step 10 Note the error message.

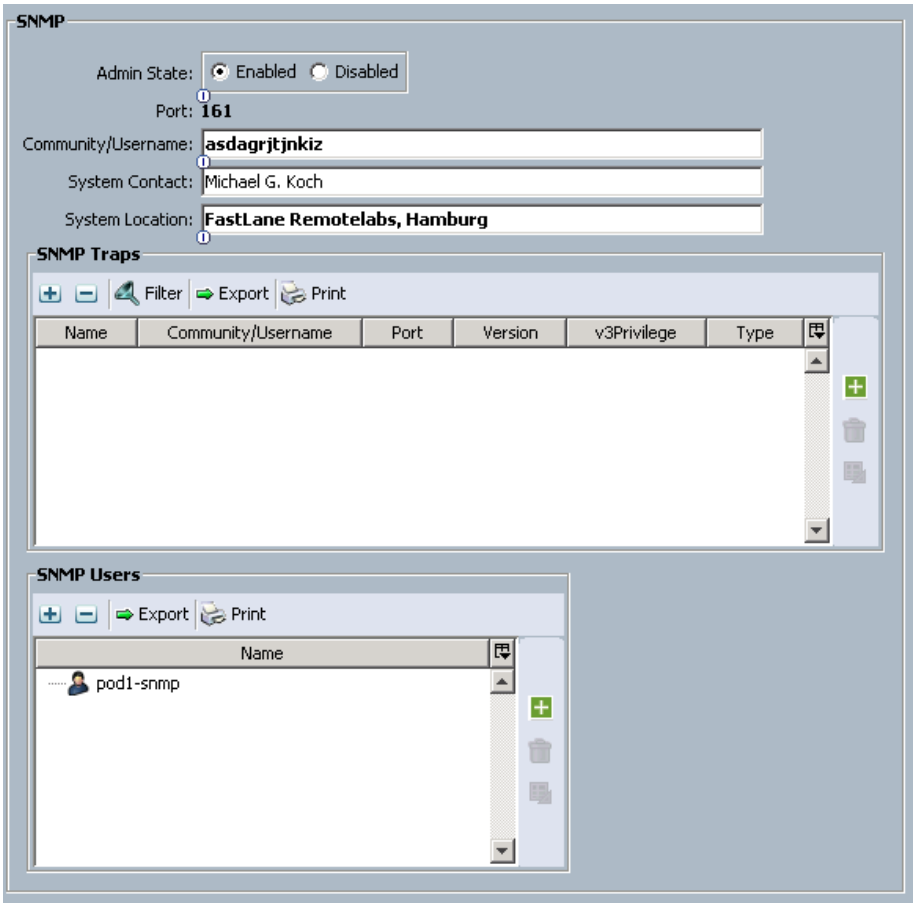


Step 11 Change the password to cisco123 to fulfill the 8-char password restriction



Step 12 Change all password to 1234QWer to pass the password strength-check

Step 13 Check the SNMP configuration.



Task 4: Export Events and Faults

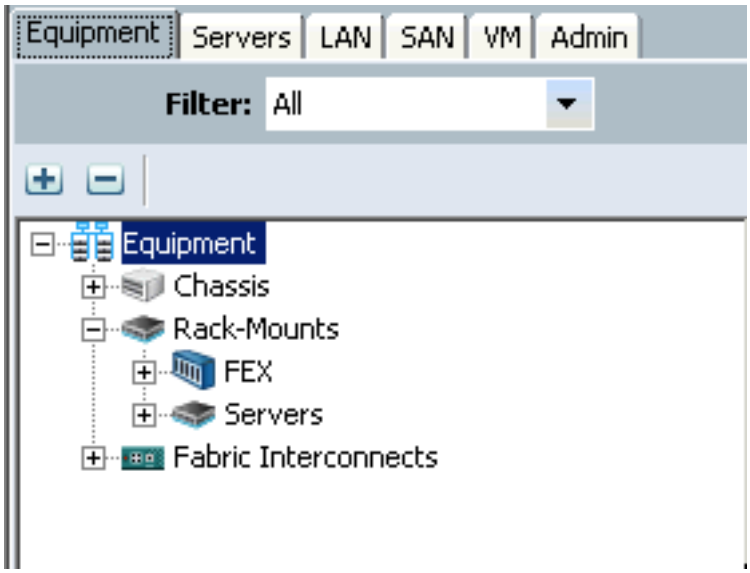
In this task, you will export event and fault data from Cisco UCS Manager.

Activity Procedure

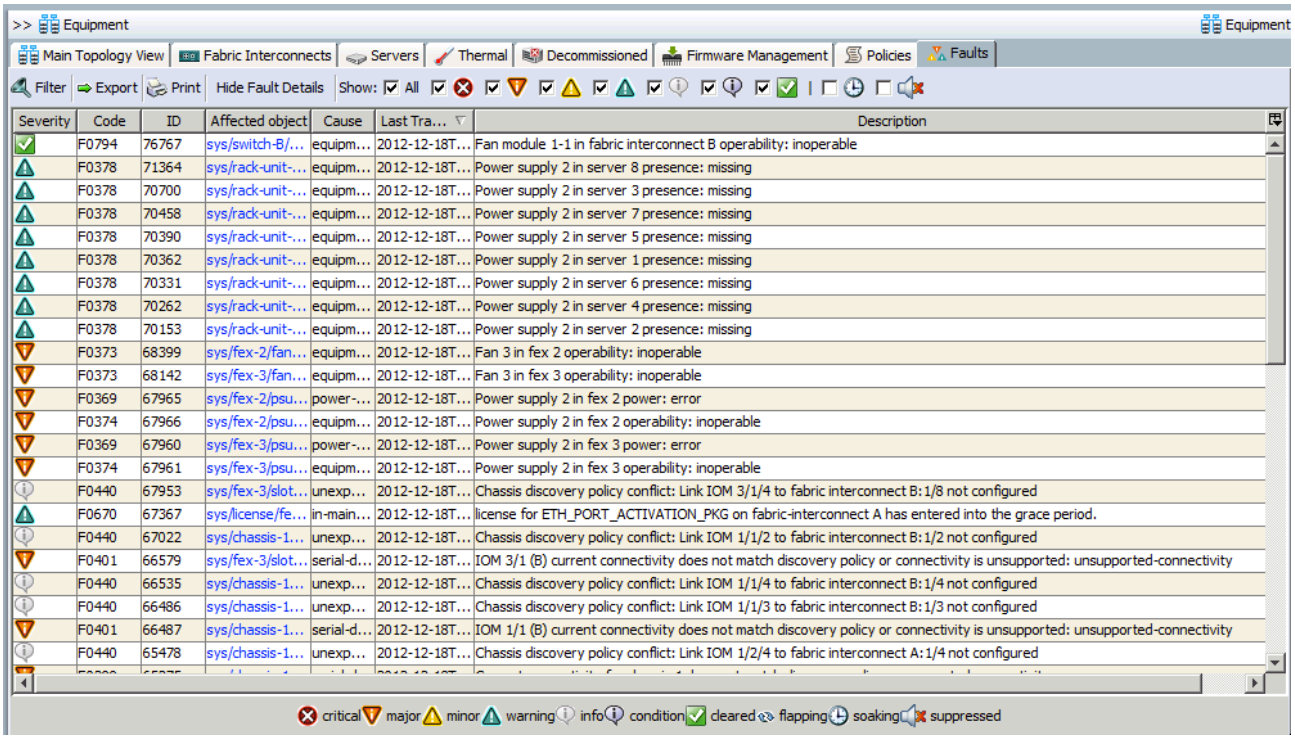
Complete these steps:

Step 1 Log into Cisco UCS Manager if necessary.

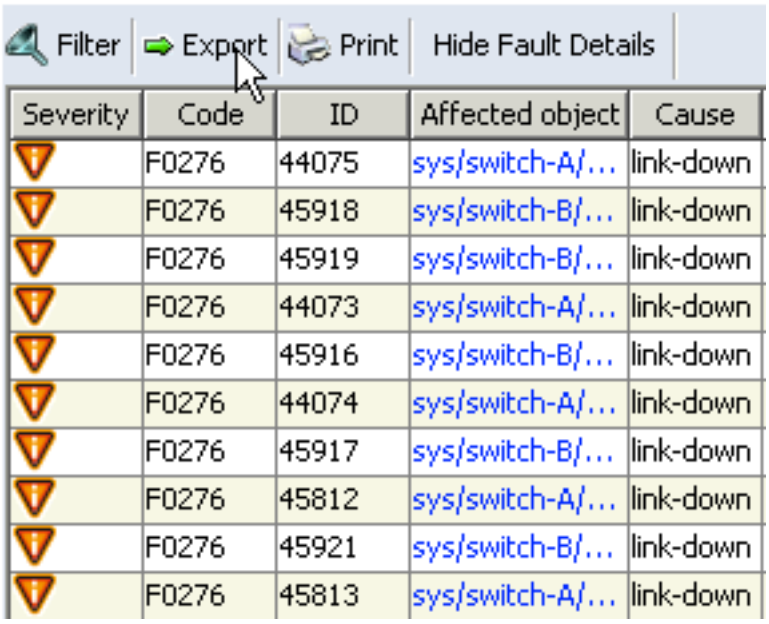
Step 2 Choose the **Equipment** tab in the navigation pane.



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

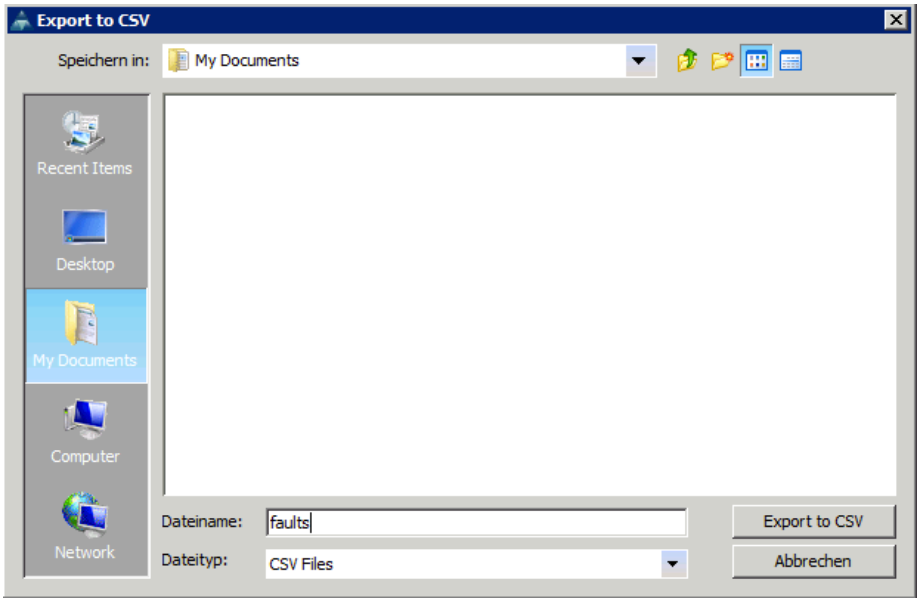


Step 4 Click **Export**.

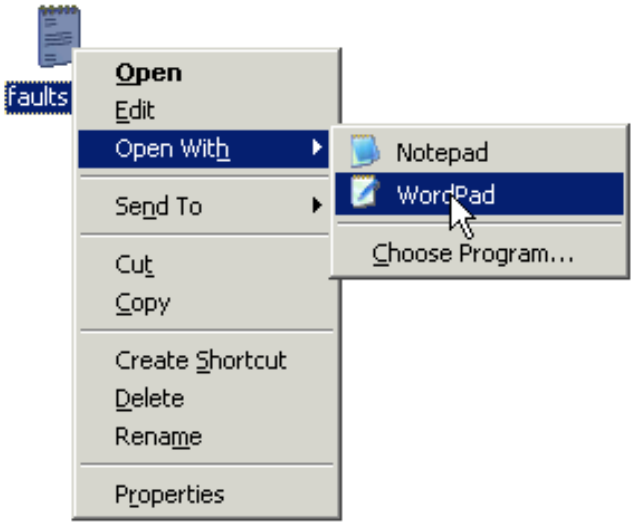


Note Virtually any table of data in Cisco UCS Manager can be exported in this manner. This exercise is exporting Fault data just as an example.

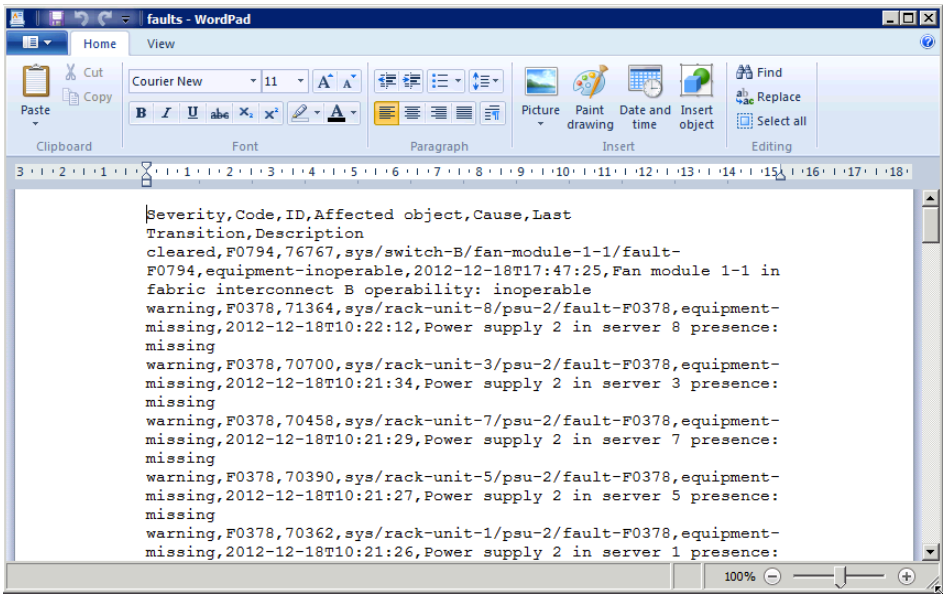
Step 5 Choose the **Desktop** icon in the left navigation pane, name the file **Faults**, and click **Export to CSV**.



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 4-1: 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

Task 1: Create a MAC Pool

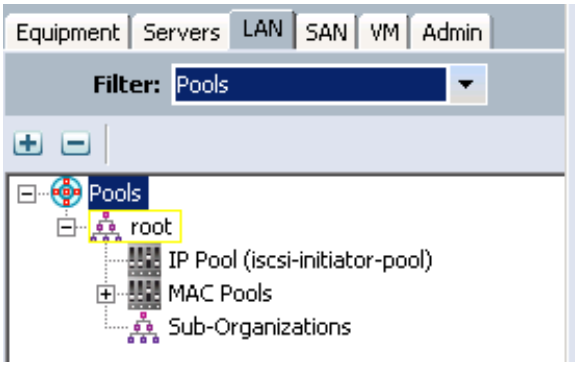
In this task, you will create a MAC pool for your mobile service profiles to use.

Activity Procedure

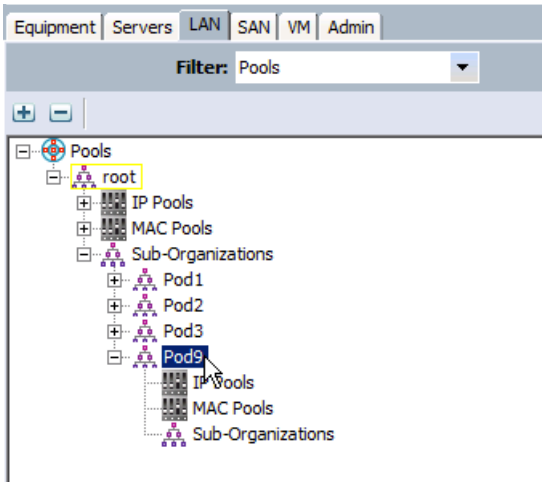
Complete these steps:

Step 1 Log into the Cisco UCS Manager if necessary.

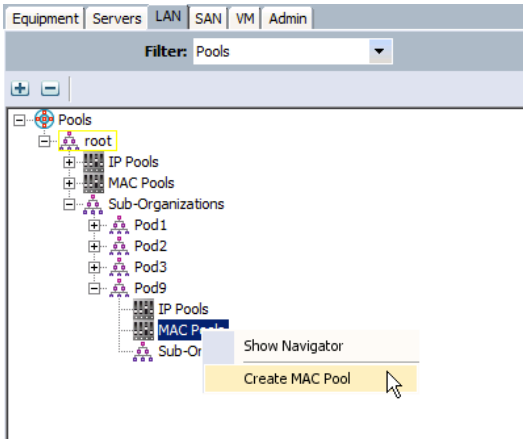
Step 2 Choose the **LAN** tab in the navigation pane. It may be useful to adjust the **Filter** setting to **Pools** for the following tasks.



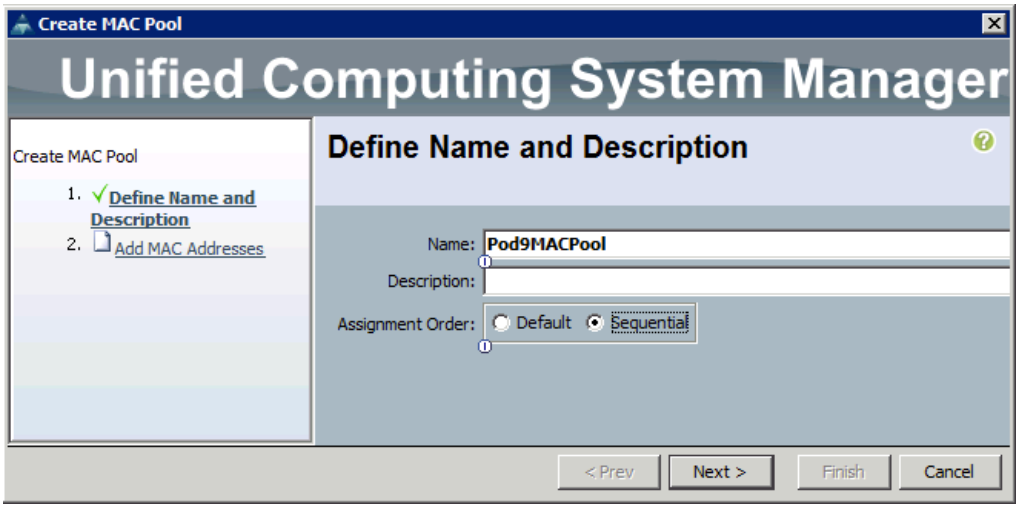
Step 3 Expand “Sub-Organizations” and expand your suborganization



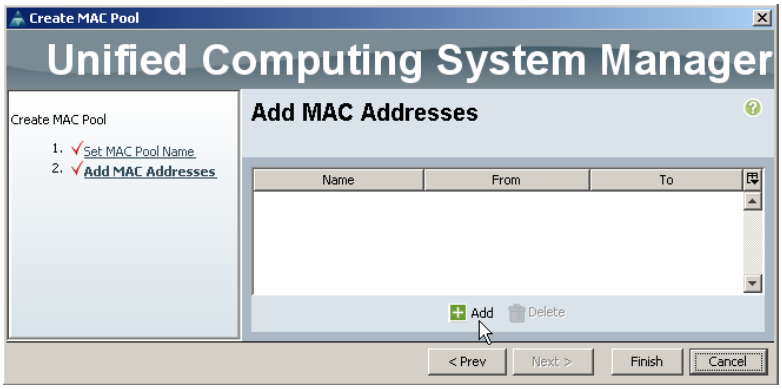
Step 4 Within your suborganization right-click **MAC Pools** and choose **Create MAC Pool**.



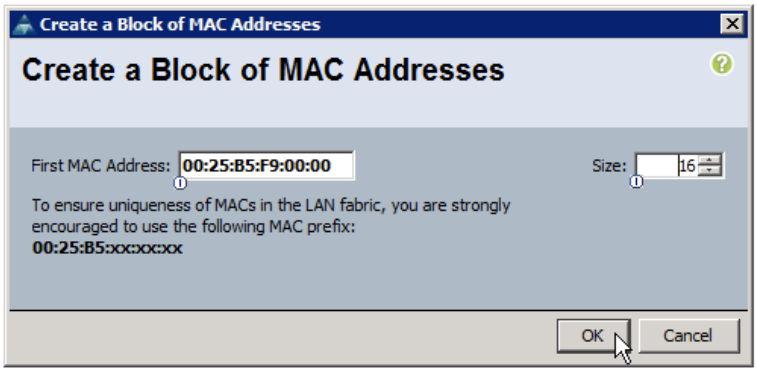
Step 5 Name your MAC Pool **PodXMACPool**. Replace X with your Pod number. Select "Sequential" assignment order.
Optionally, provide a description for your pool and click **Next**.



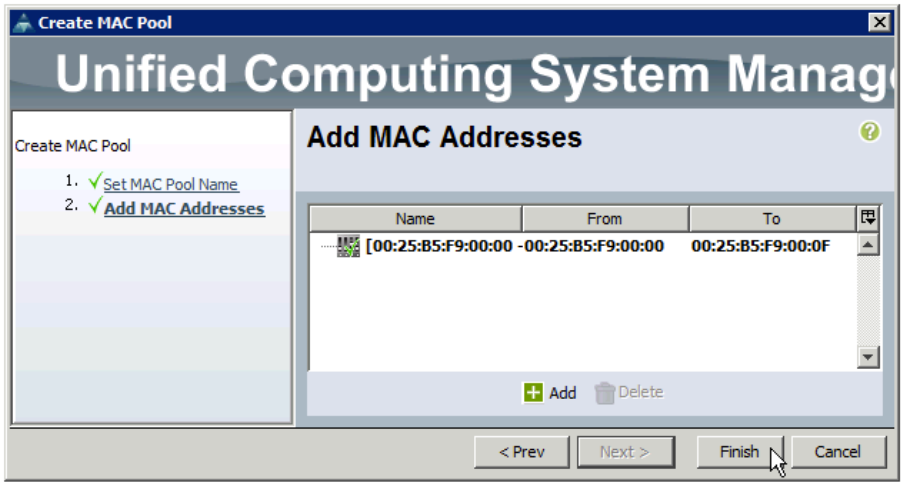
Step 6 Click **Add** to add MAC addresses to your pool.



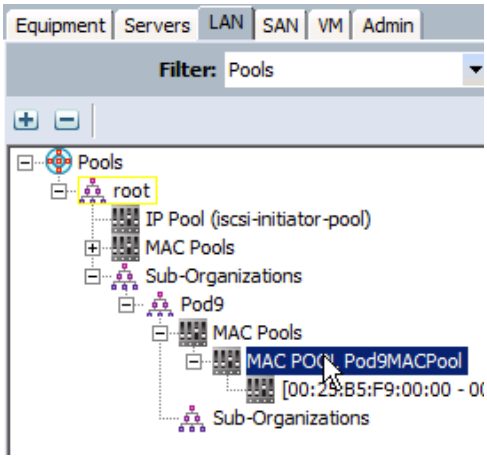
Step 7 Note that the first three octets of the MAC address have been prepopulated with a Cisco OUI and can be modified when you run UCSM 1.4 or later. Change the seventh nibble to the Lab ID number (see page 5) and the eights nibble to the Pod number (00:25:b5:**LP**:00:00) **(L=Lab ID; P=Pod number)**
Specify 16 addresses to be created and click **OK**.



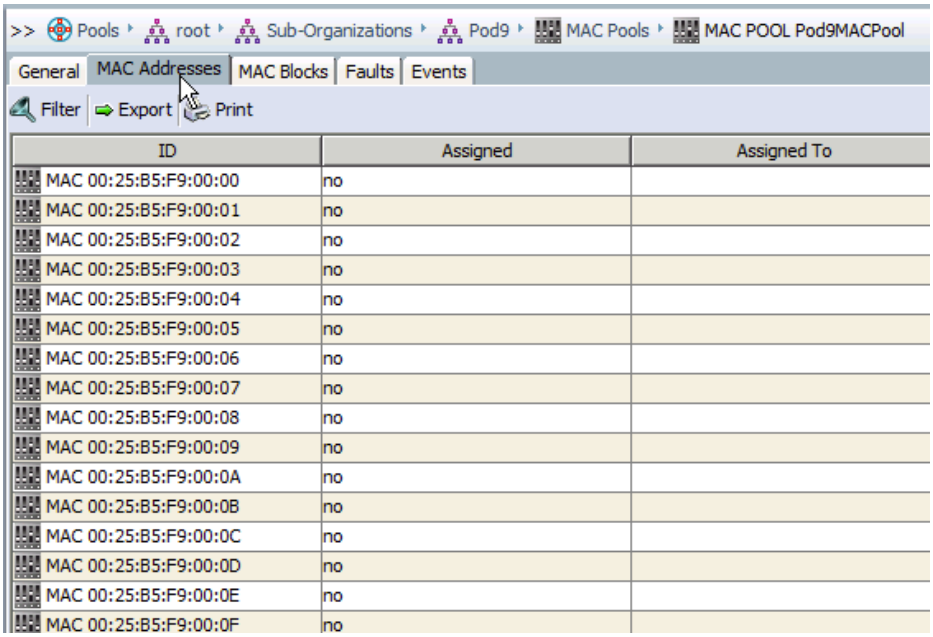
Step 8 Verify that the proper range has been added to the block and click **Finish**. The range should be from 00:25:B5:LP:00:00 to 00:25:B5:LP:00:0F.



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



Step 10 Click the "MAC Addresses" tab on the right pane, note the MAC addresses are available but not assigned (yet).



Task 2: Create a World Wide Node Name Pool

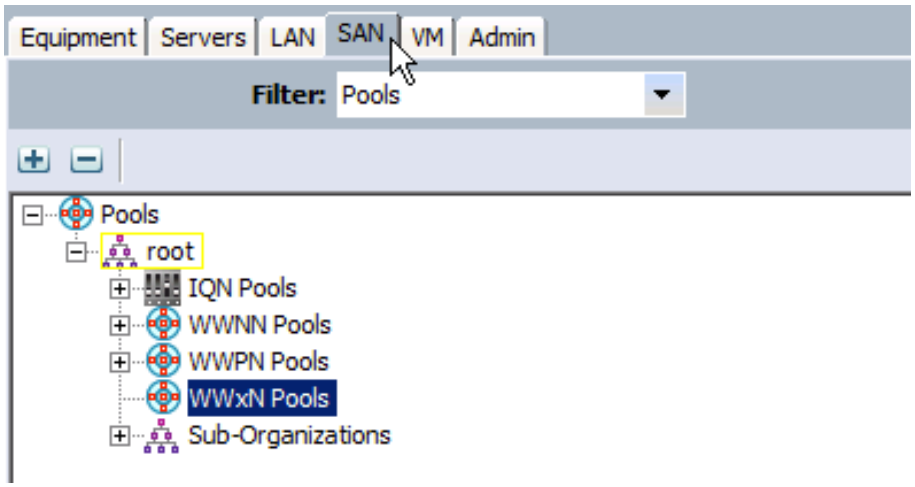
In this task, you will create a WWNN pool for your mobile service profiles to use.

Activity Procedure

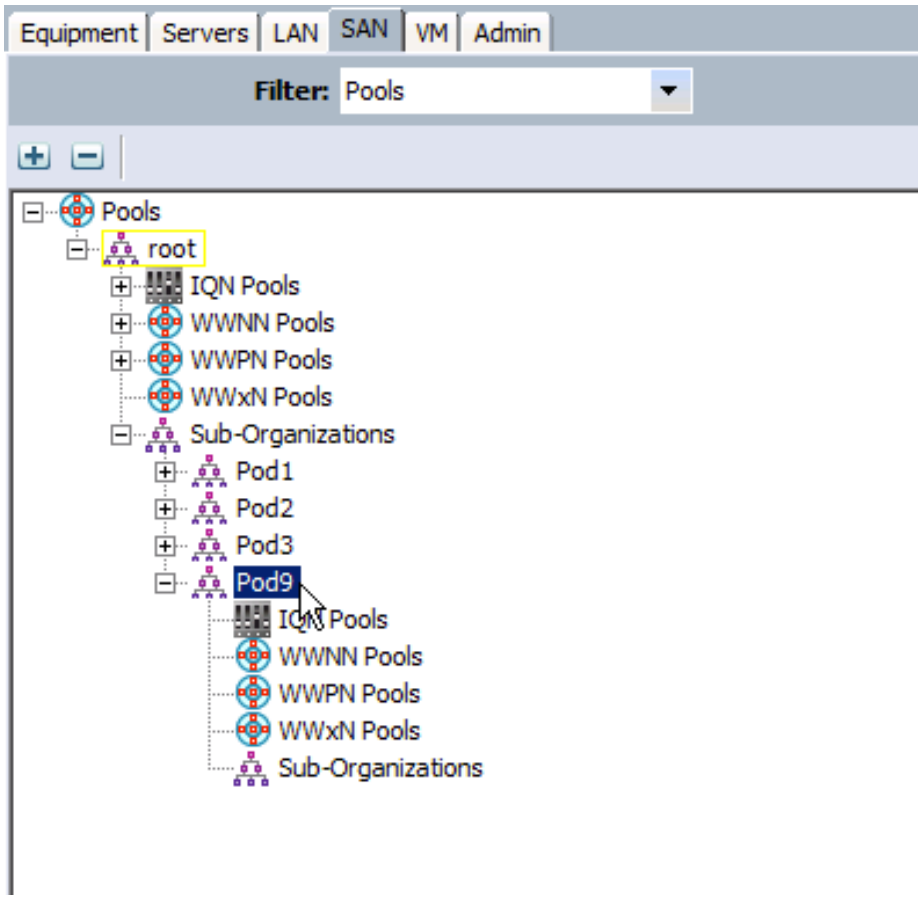
Complete these steps:

Step 1 Log into the Cisco UCS Manager.

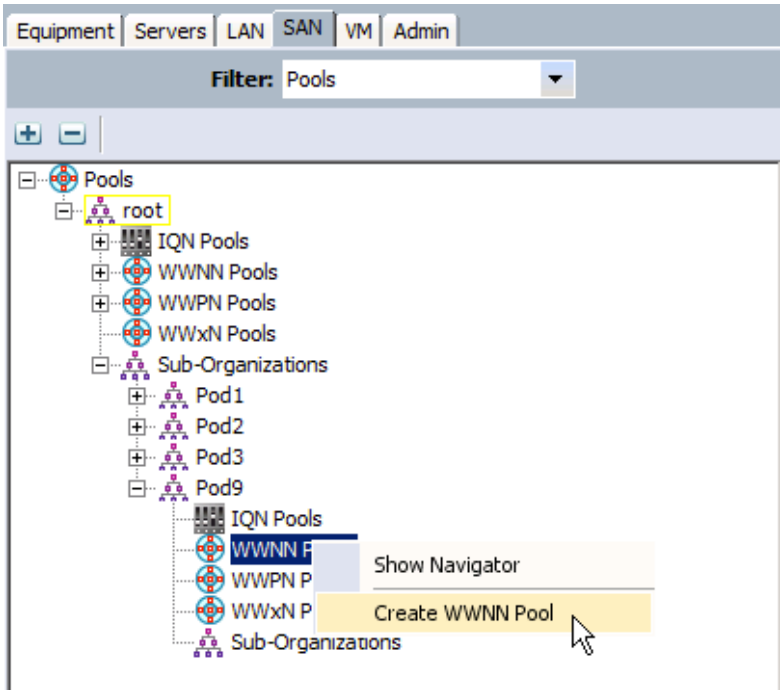
Step 2 Choose the **SAN** tab in the navigation pane. It may be useful to adjust the **Filter** setting to **Pools** for the following tasks.



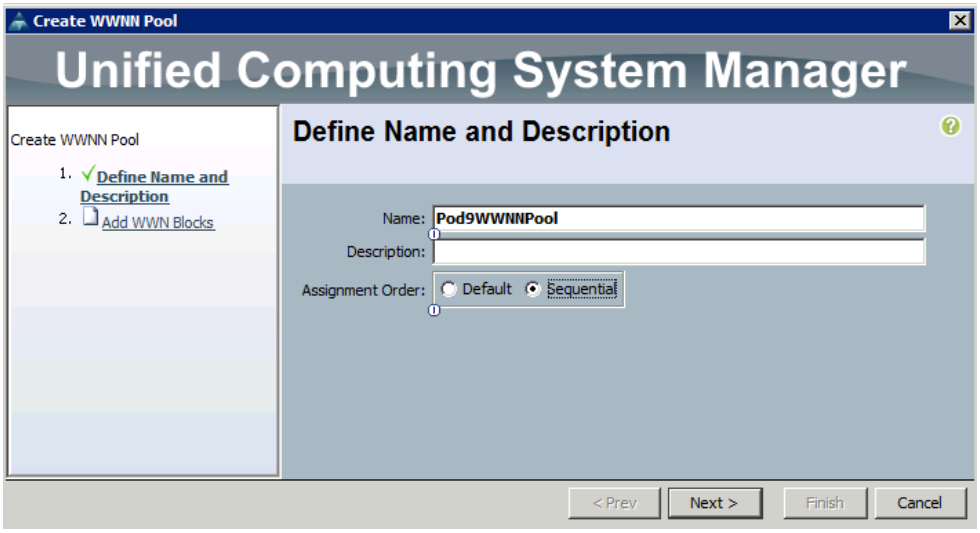
Step 3 Expand “Sub-Organizations” and select your Organization.



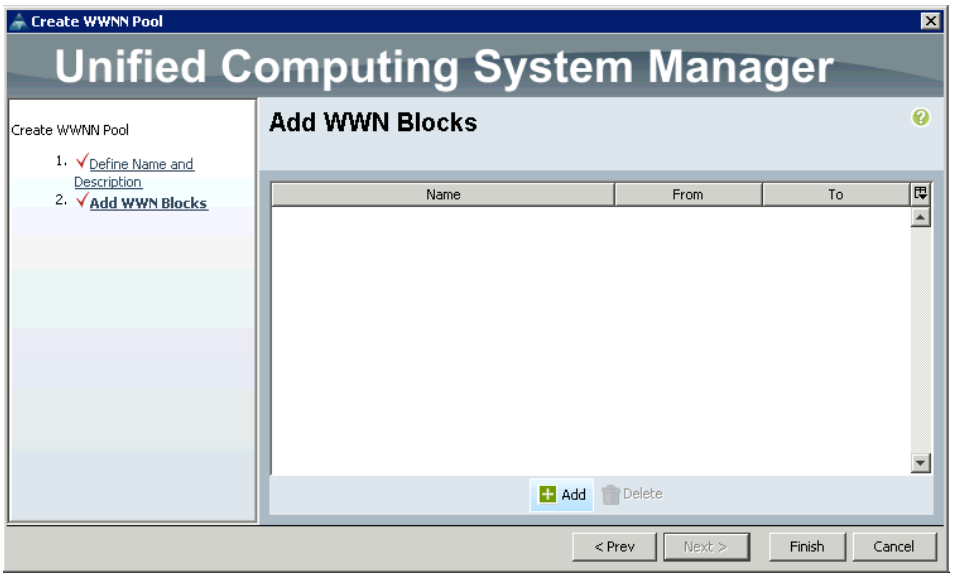
Step 4 Right-click **WWNN Pools** and choose **Create WWNN Pool** inside your Organization!!



Step 5 Name your WWNN Pool **PodXWWNNPool**. Replace X with your Pod number. Select ”sequential” assignment order.
Optionally, provide a description for your pool and click **Next**.

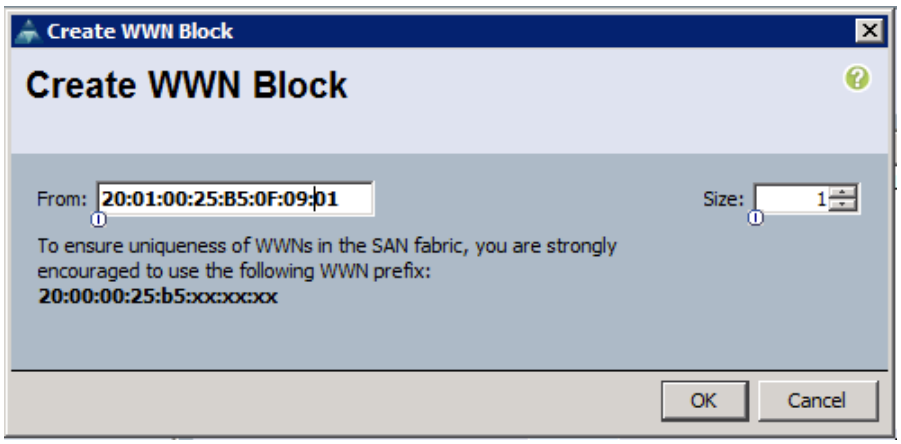


Step 6 Click **Add** to add WWNNs to your pool.

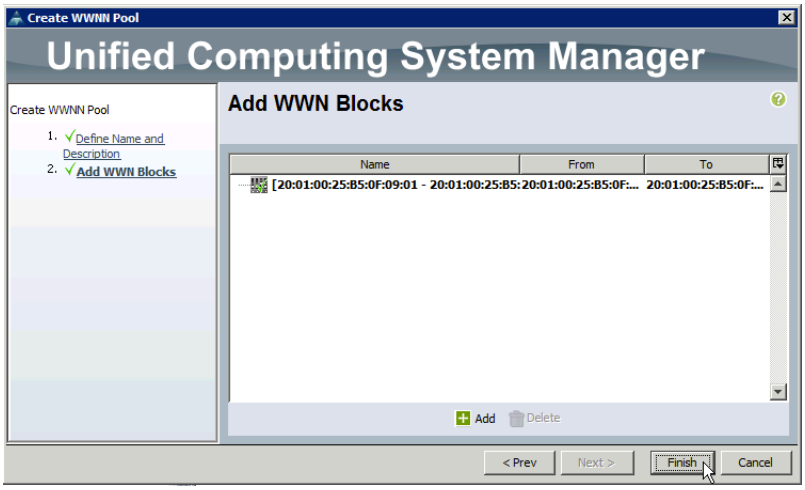


Step 7 Cisco UCS Manager does prepopulate the WWN fields with 20:00:00:25:B5:00:00:00. Additionally, it will only accept values that begin with 20 or 5, in accordance with WWN standards. Create your WWNN pool beginning with **20:01:00:25:B5:0L:0P:01**, replacing L with the lab ID (see page 5) and P with your Pod number. Create a pool of ONE WWNN, and click **OK**.

Caution **Note the WWNN is starting with 20:01:... !!!**

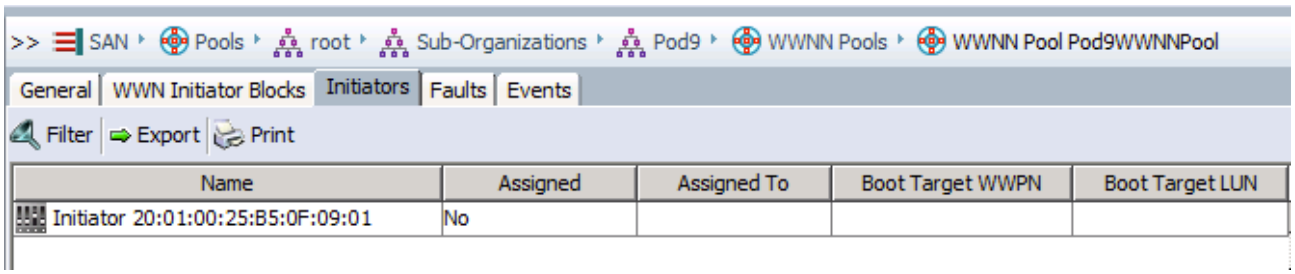


Step 8 Verify that the proper range has been added to the block and click **Next**.



Step 9 Click finish to close the wizard.

Step 10 Click the newly created WWNN pool and select “Initators” on the right pane. Note there is one WWNN available, not assigned (yet)



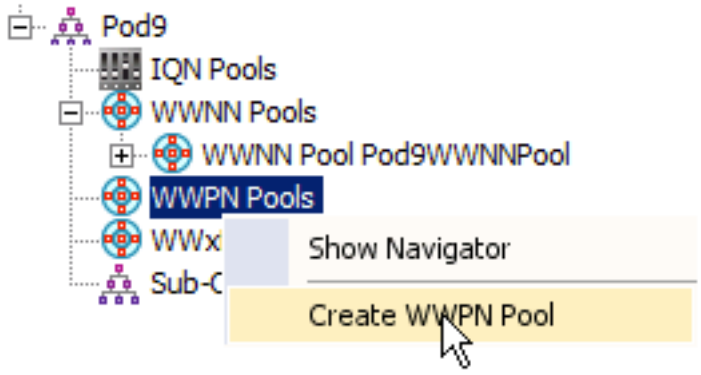
Task 3: Create World Wide Port Name Pools

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

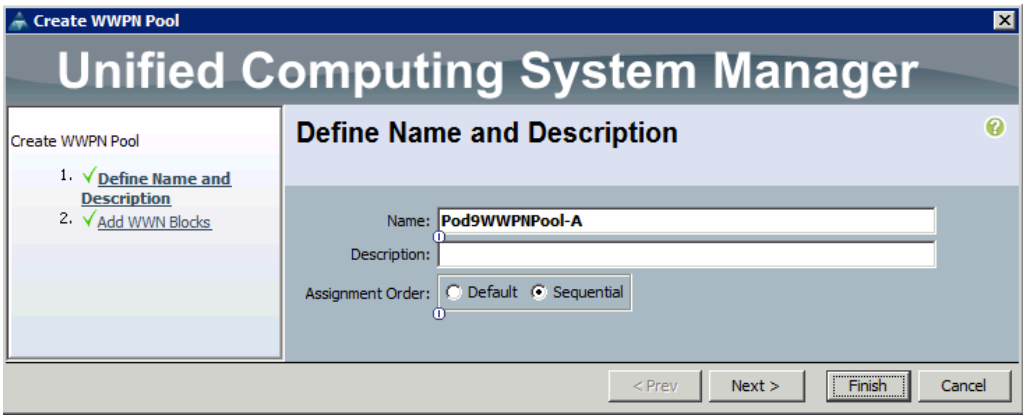
Activity Procedure

Complete these steps:

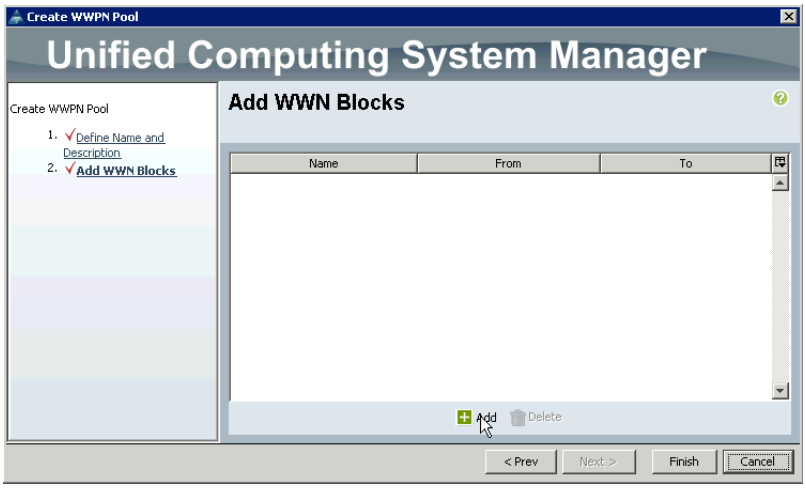
Step 1 Select your Organizations WWPN Pool and right-click display the context menu.



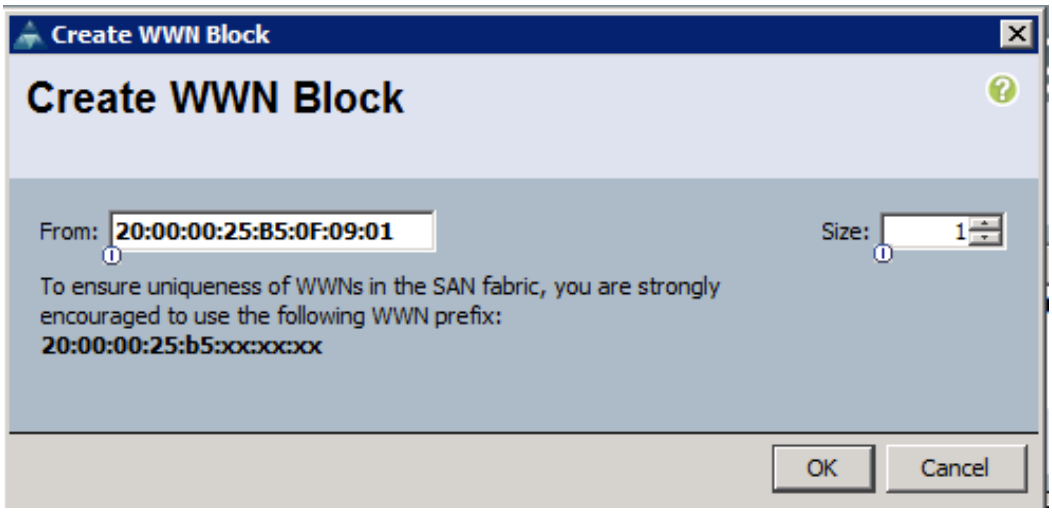
Step 2 Name your WWPN Pool **PodXWWPNPool-A**. Replace X with your Pod number. Optionally, provide a description for your pool and click **Next**.



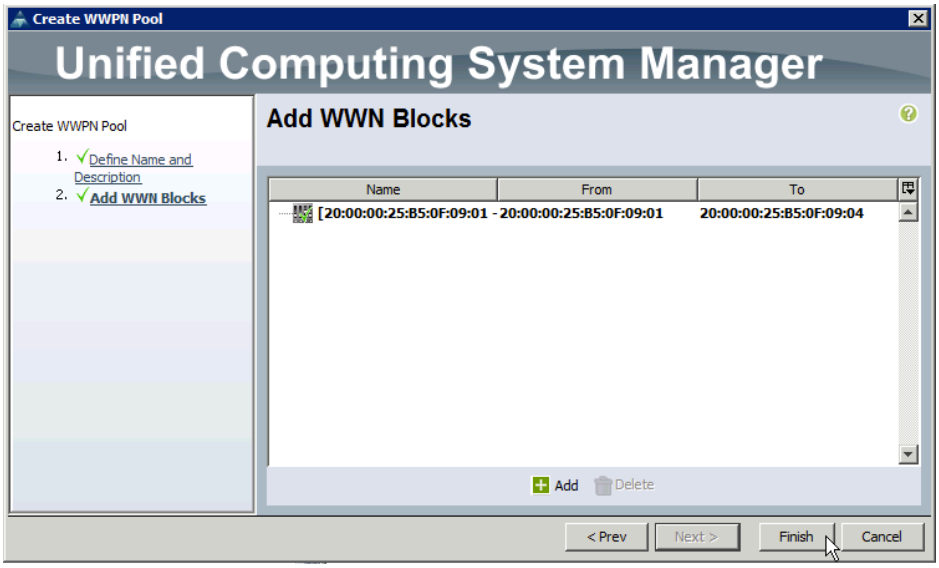
Step 3 Click **Add** to add WWPNs to your pool.



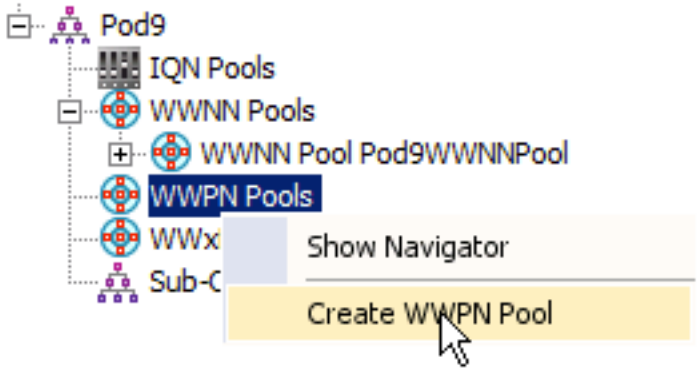
Step 4 Cisco UCS Manager does prepopulate the WWN field with 20:00:00:25:B5:00:00:00. Additionally it will only accept values that begin with 2 or 5, in accordance with WWN standards. Create your pool beginning with **20:00:00:25:B5:0L:0P:01**, replacing L with the lab ID (see page 5) and P with your Pod number. Create a pool of ONE WWPN, and click **OK**.



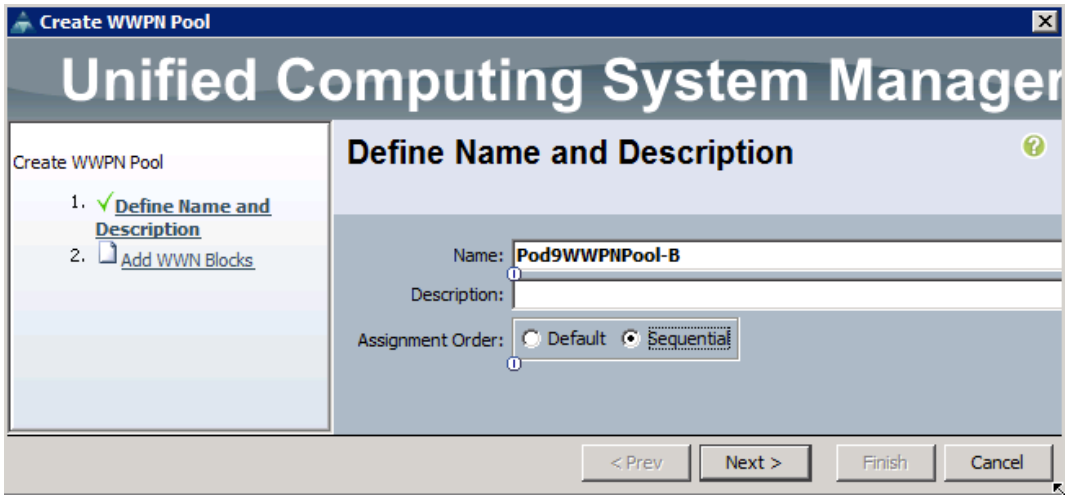
Step 5 Verify that the proper range has been added to the block and click **Finish**.



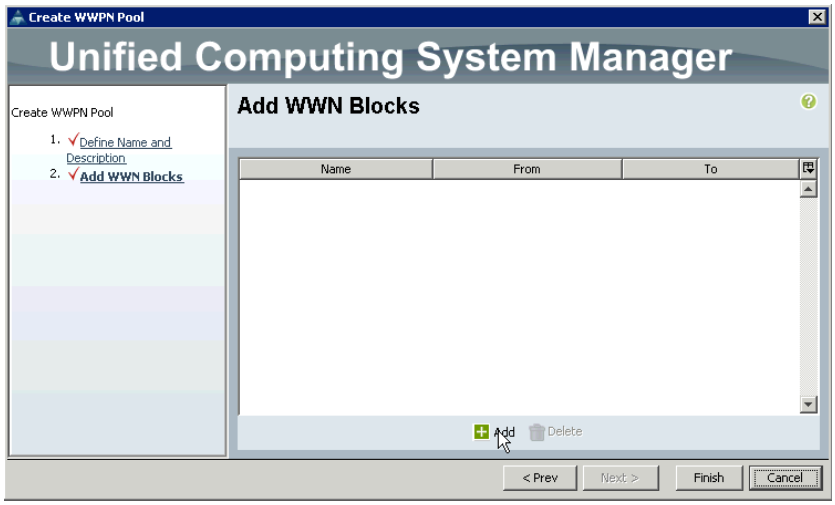
Step 6 Select your Organizations WWPN Pool and right-click display the context menu.



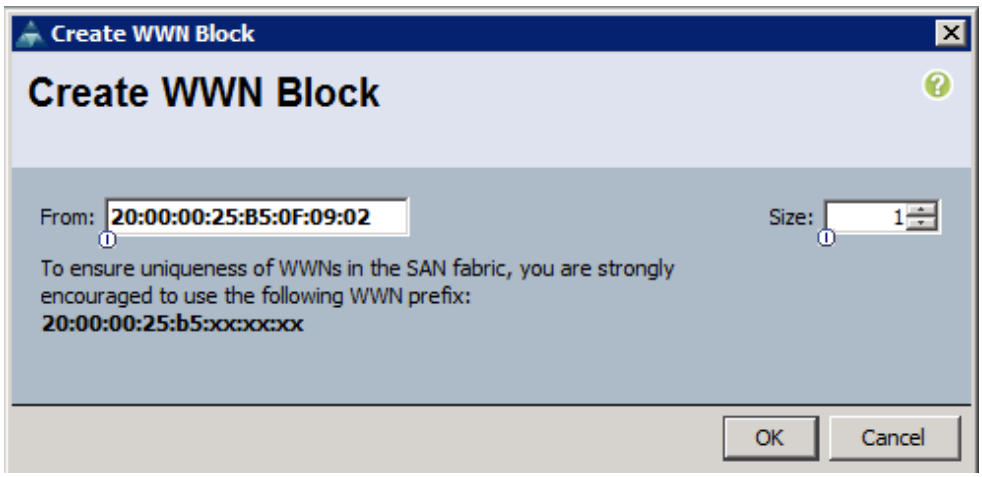
Step 7 Name your WWPN Pool **PodXWWPNPool-B**. Replace X with your Pod number. Optionally, provide a description for your pool and click **Next**.



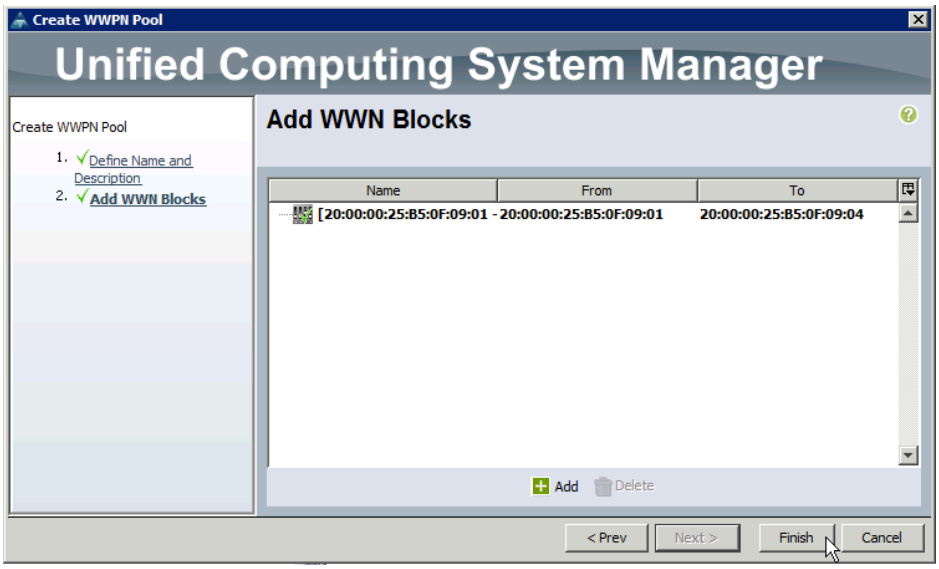
Step 8 Click **Add** to add WWPNs to your pool.



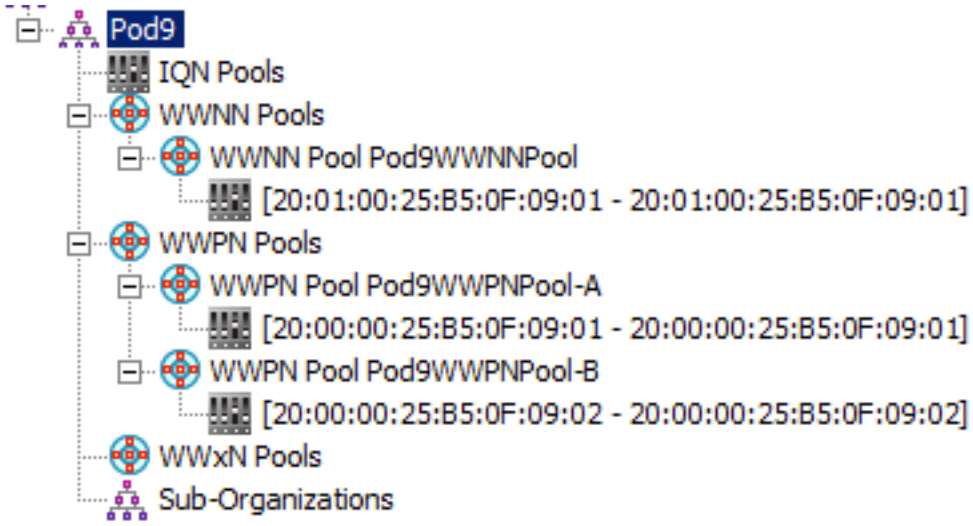
Step 9 Cisco UCS Manager does prepopulate the WWN field with 20:00:00:25:B5:00:00:00. Additionally it will only accept values that begin with 2 or 5, in accordance with WWN standards. Create your pool beginning with **20:00:00:25:B5:0L:0P:02**, replacing L with the lab ID (see page 5) and P with your Pod number. Create a pool of ONE WWPN, and click **OK**.

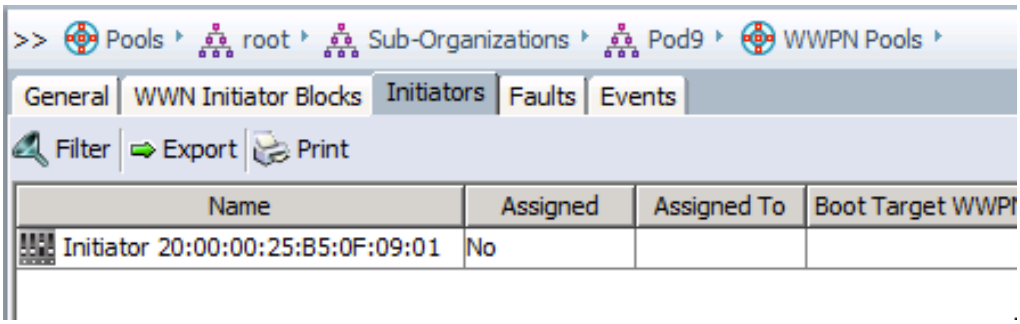


Step 10 Verify that the proper range has been added to the block and click **Finish**.



Step 11 Expand the **WWPN Pools** icon in the navigation pane and verify that your pool has been created and the correct values are used. Click the pool, then "Initiators" on the right pane to verify. (also here, none are assigned)





Task 4: Create a UUID Suffix Pool

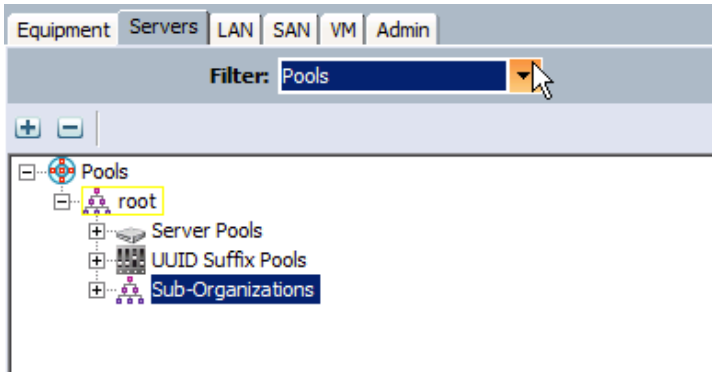
In this task, you will create a UUID Suffix pool for your mobile service profiles to use.

Activity Procedure

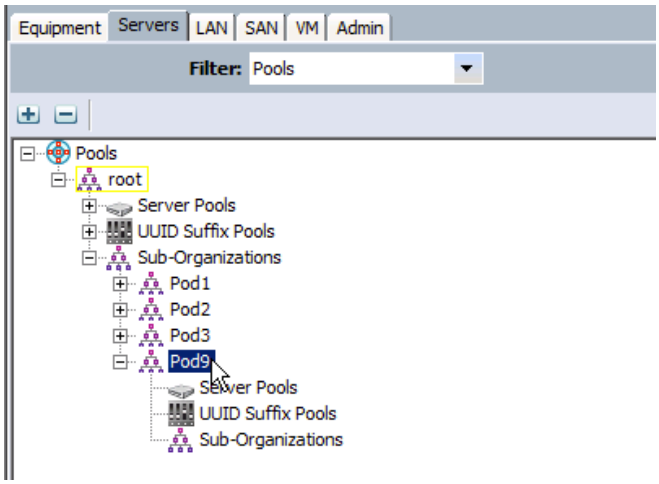
Complete these steps:

Step 1 Log into the Cisco UCS Manager if necessary.

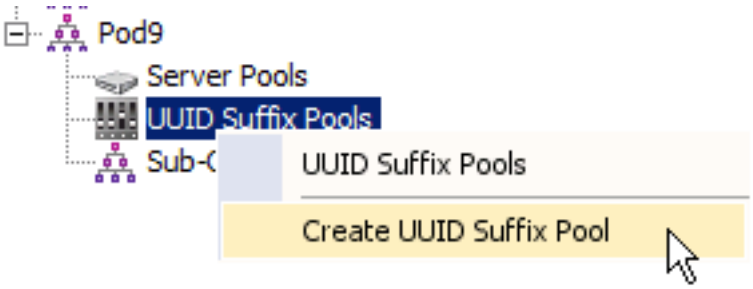
Step 2 Choose the **Servers** tab in navigation pane. It may be useful to adjust the **Filter** setting to **Pools** for the following tasks.



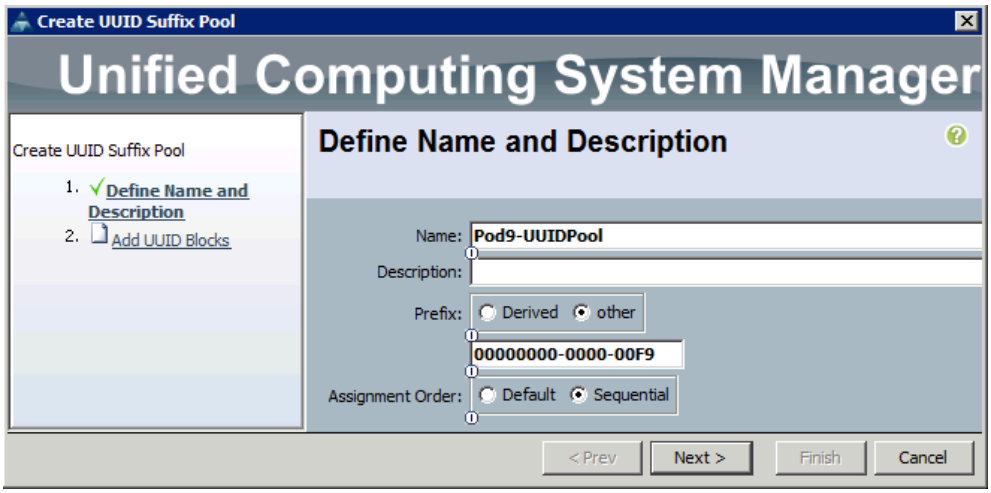
Step 3 Expand the tree to your Organization



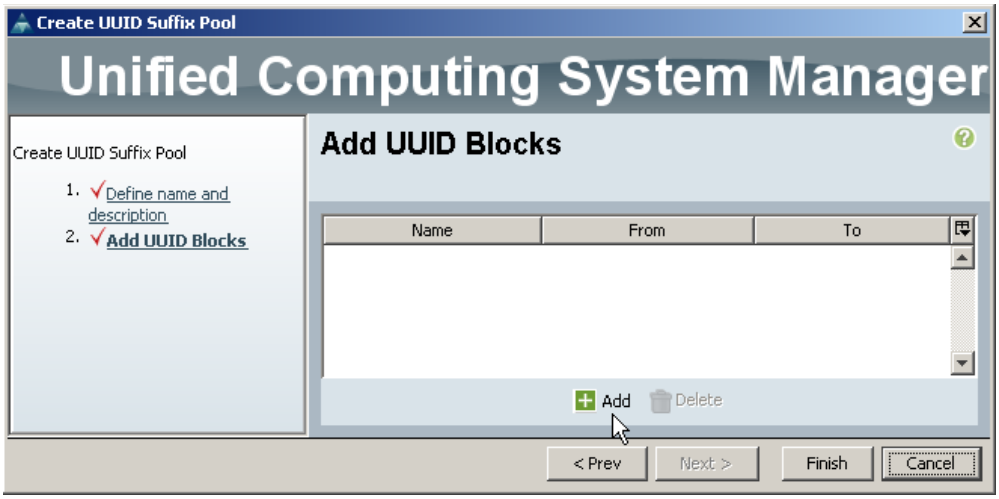
Step 4 Right-click **UUID Suffix Pools** and choose **Create UUID Suffix Pool**.



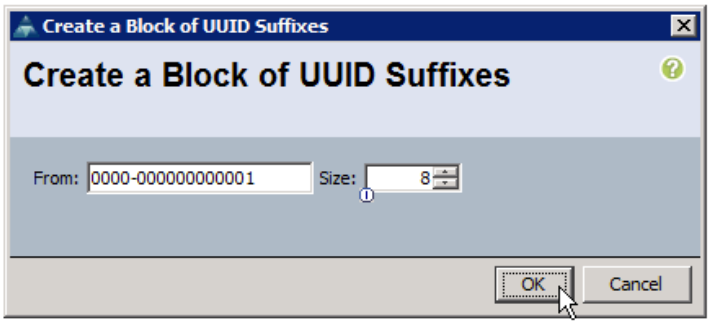
Step 5 Name your UUID Pool **PodX-UUIDPool**. Replace X with your Pod number. Optionally, provide a description for your pool. Set the last two nibbles (digits) of the prefix to your Lab ID (see page 5) and Pod number (00000000-0000-00LP), select "Sequential Assignment" and click **Next**.



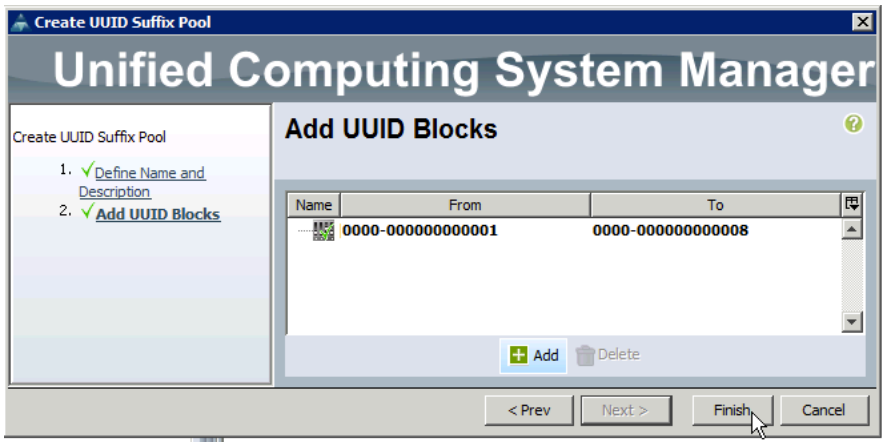
Step 6 Click **Add** to add UUIDs to your pool.



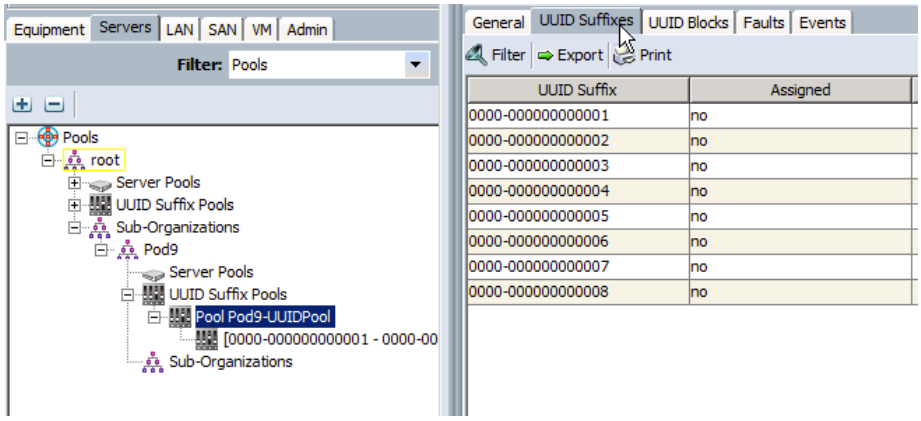
Step 7 Create a pool of 8 UUIDs and click **OK**.



Step 8 Verify that the proper range has been added to the block and click **Finish**.



Step 9 Expand the **UUID Suffix Pools** icon in the navigation pane and verify that your pool has been created. Click "UUID suffixes" on the right pane to verify.



Task 5: Create a Manually Populated Server Pool

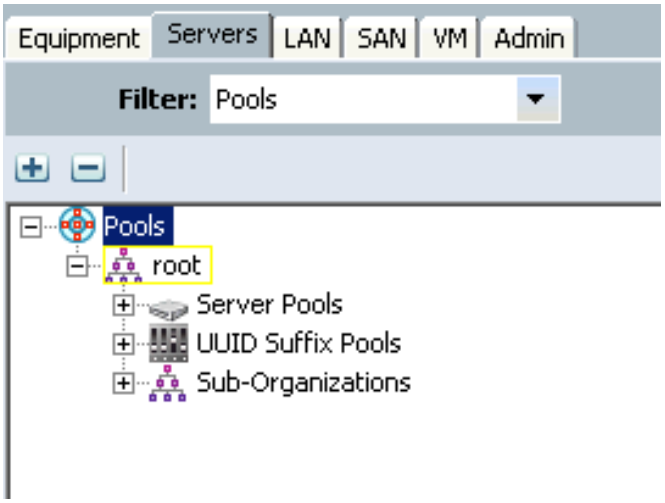
In this task, you will create a manually populated server pool that contains your assigned server.

Activity Procedure

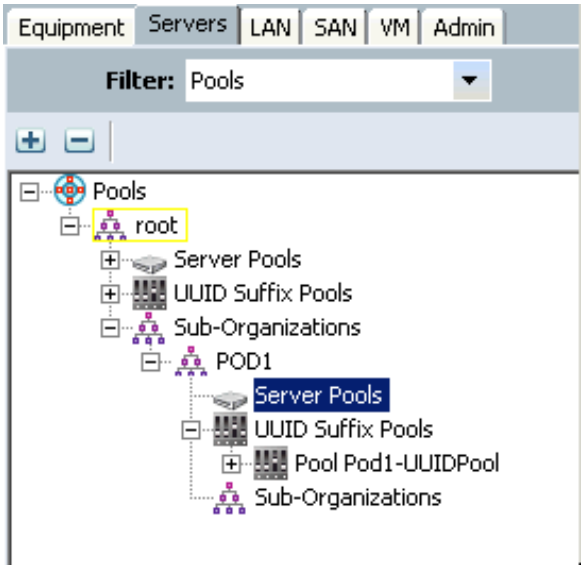
Complete these steps:

Step 1 Log into the Cisco UCS Manager.

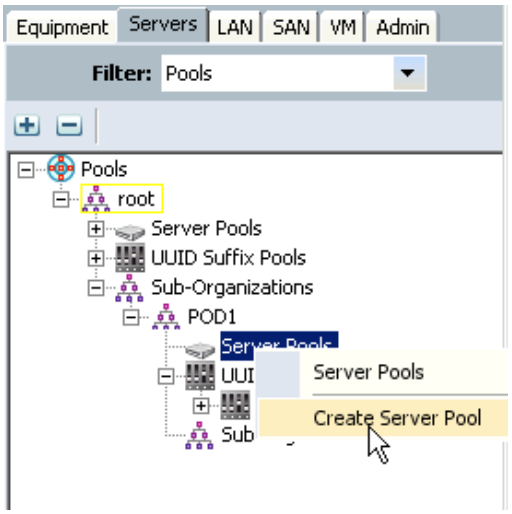
Step 2 Choose the **Servers** tab in the navigation pane. It may be useful to adjust the **Filter** setting to **Pools** for the following tasks.



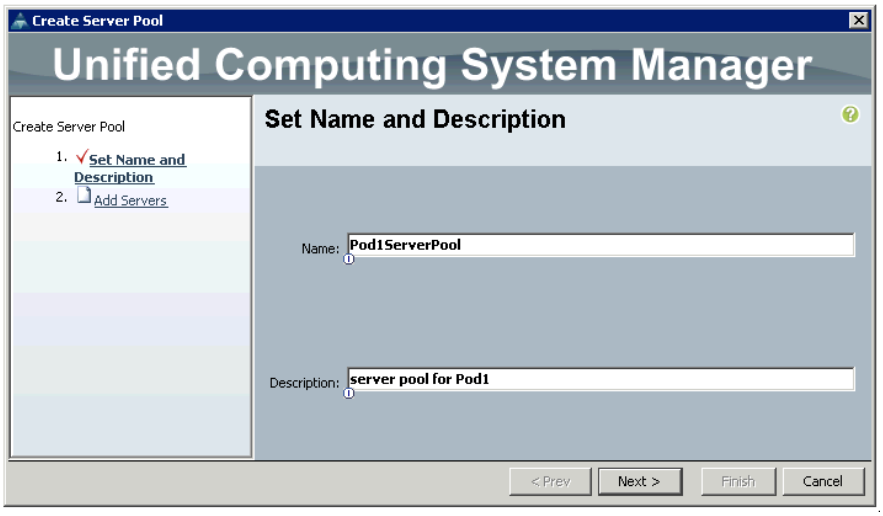
Step 3 Navigate and expand to your Organziation,



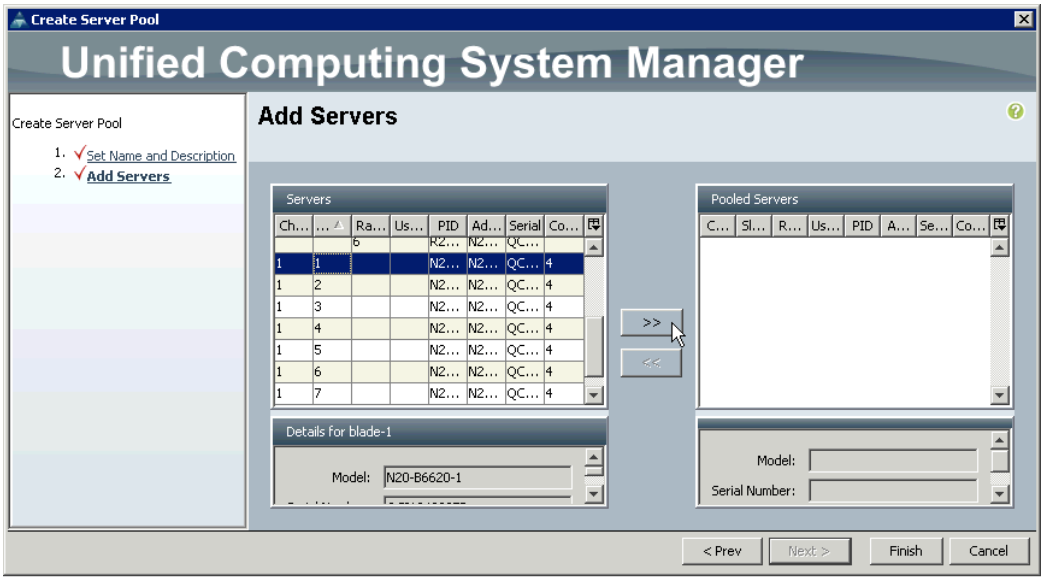
Step 5 right-click **Server Pools** and choose **Create Server Pool**.



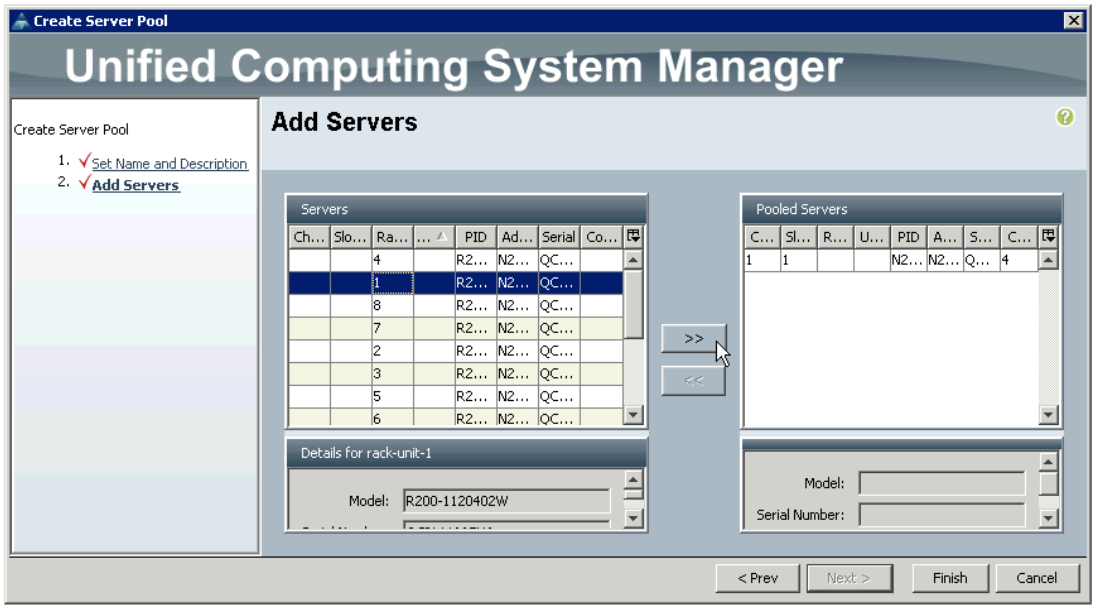
Step 6 Name your server pool **PodXServerPool**. Replace X with your Pod number. Optionally, provide a description for your pool and click **Next**.



Step 7 Choose Chassis 1, Server/Slot P (P is your Pod#) and add it to your pool. Click the column heading to sort (Hint: you can also change the size of this window)

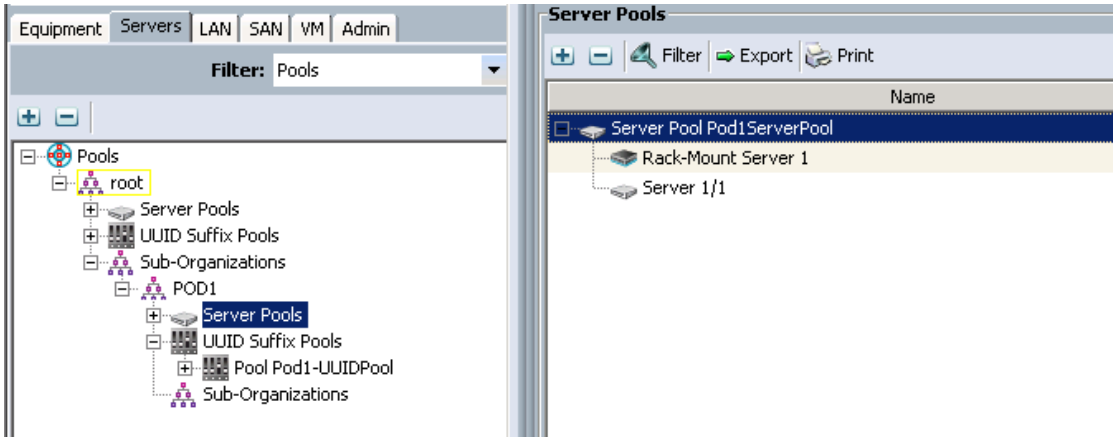


Step 8 Choose Rackmount Server P (P is your Pod#) and move it into your Pool



Step 9 Make sure that ONLY your Pod servers now appears in the right column and click **Finish**.

Step 10 Expand the **Server Pools** icon and verify that your pool has been created. Expand your pool and verify that it contains your Pod server.



Task 6: Create an Automatically Populated Server Pool

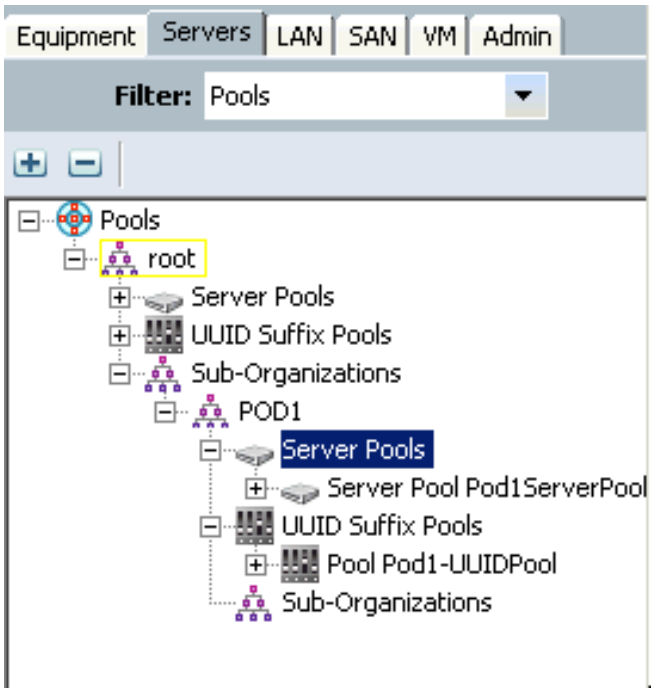
In this task, you will create an automatically populated server pool that contains your assigned server.

Activity Procedure

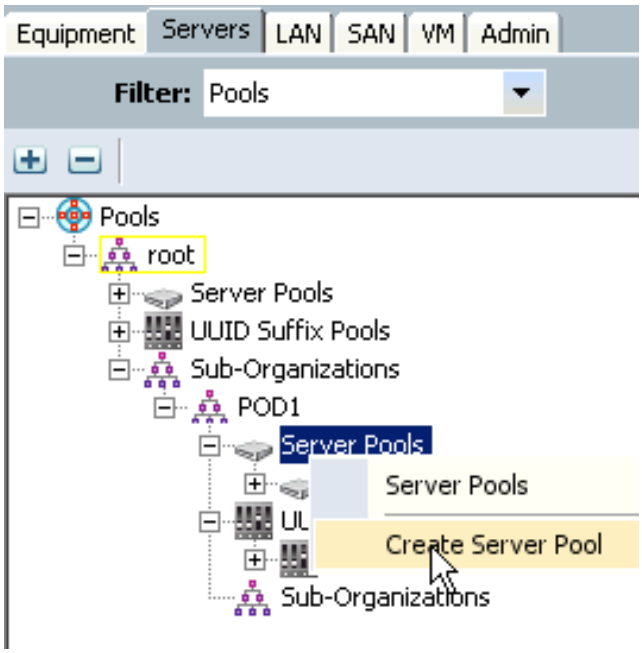
Complete these steps:

Step 1 Log into the Cisco UCS Manager.

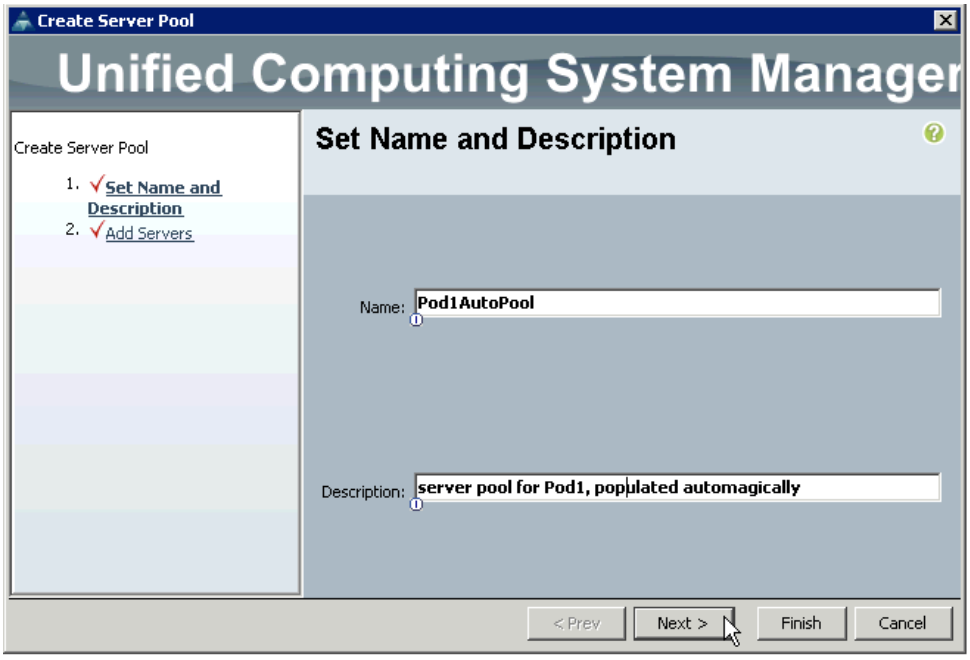
Step 2 Choose the **Servers** tab in navigation pane. It may be useful to adjust the **Filter** setting to **Pools** for the following tasks. Expand the tree and navigate to your organization.



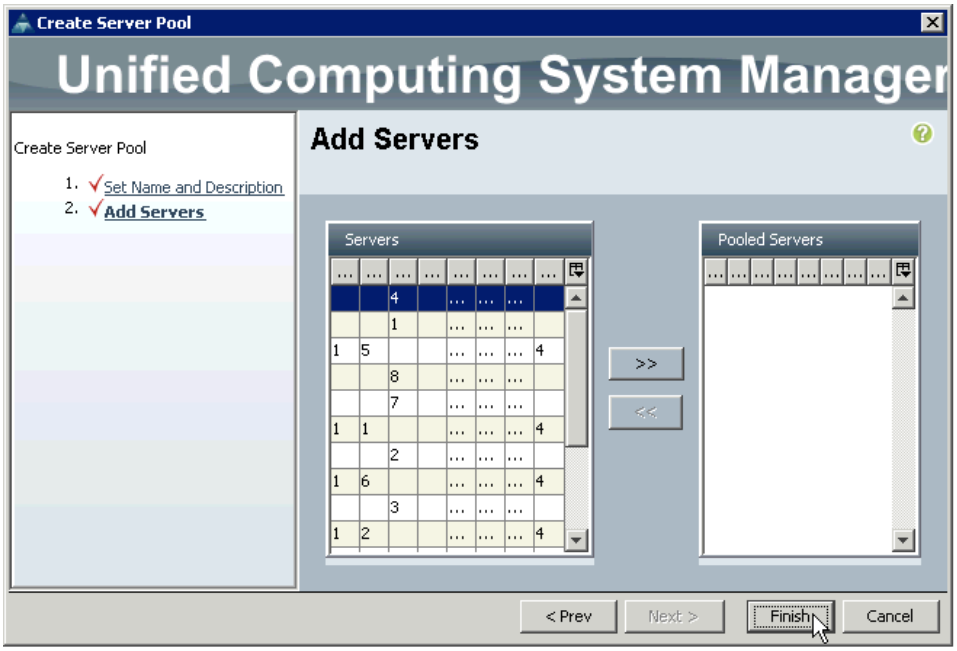
Step 3 Right-click **Server Pools** and choose **Create Server Pool**.



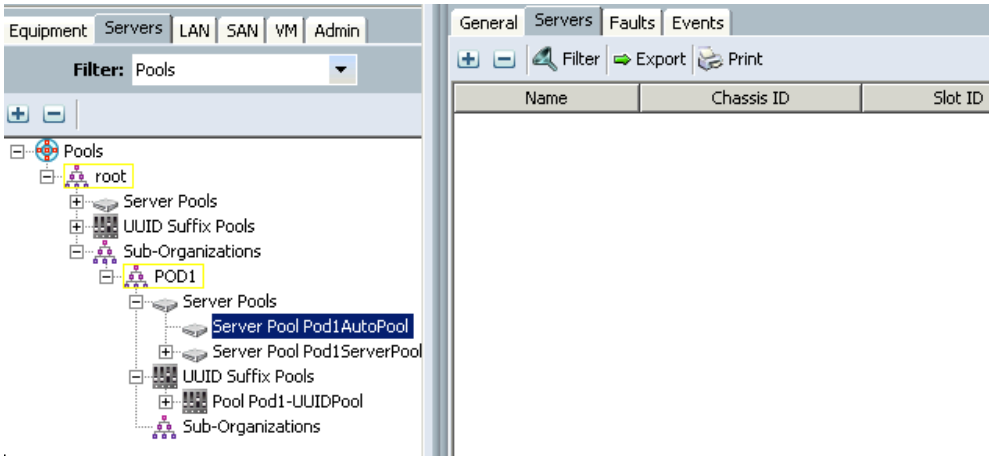
Step 4 Name your server pool **PodXAutoPool**. Replace X with your Pod number. Optionally provide a description for your pool and click **Next**.



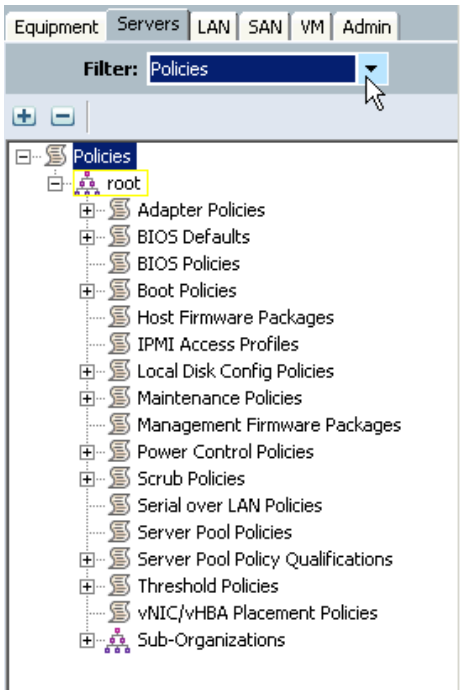
Step 5 Do **not** choose any servers and click **Finish**.



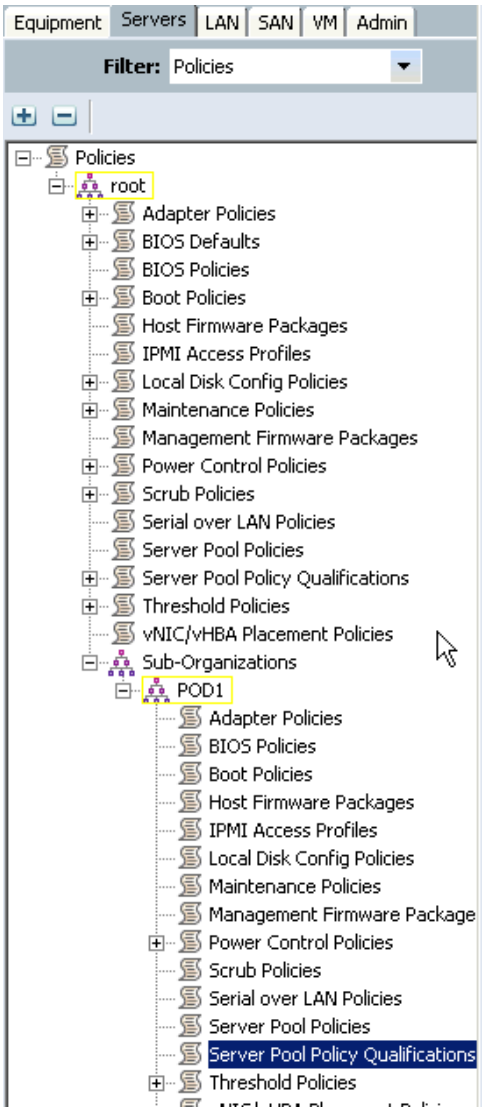
Step 6 Expand the **Server Pools** icon and verify that your pool has been created. Expand your pool and verify that it does not contain any servers.



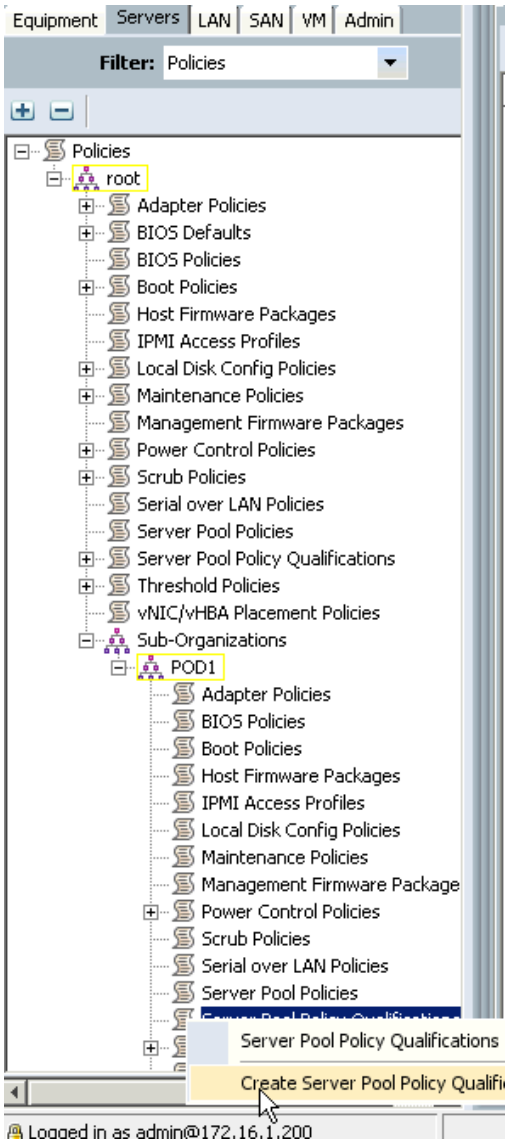
Step 7 Change the **Filter** setting in the navigation pane to **Policies**.



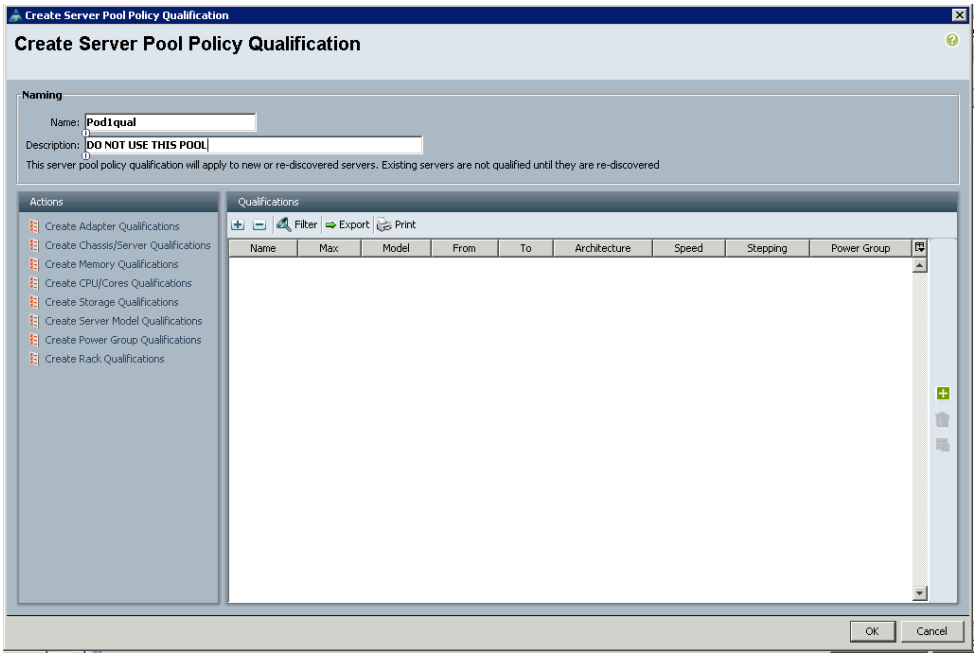
Step 8 Navigate to your Organization



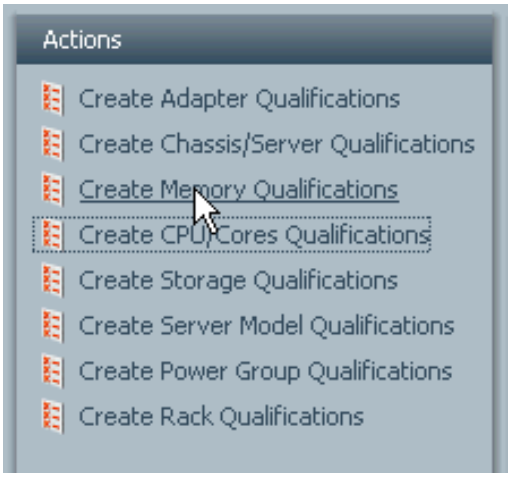
Step 9 Right-click **Server Pool Policy Qualifications** and click **Create Server Pool Policy Qualification**.



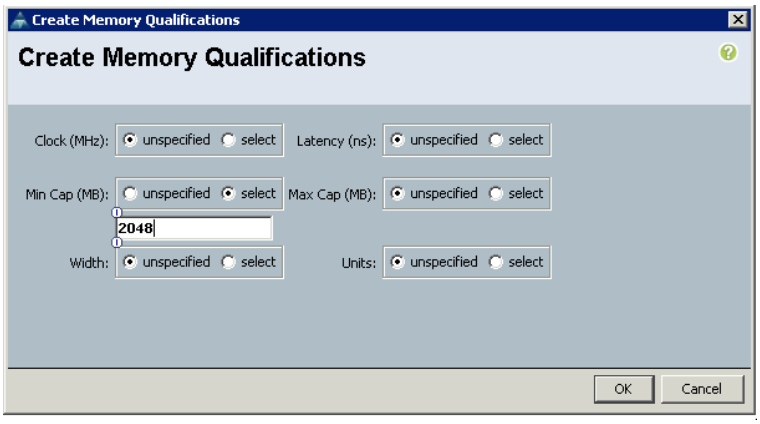
Step 10 Name your qualification **PodXQual**. Replace X with your Pod number. Provide an optional description.



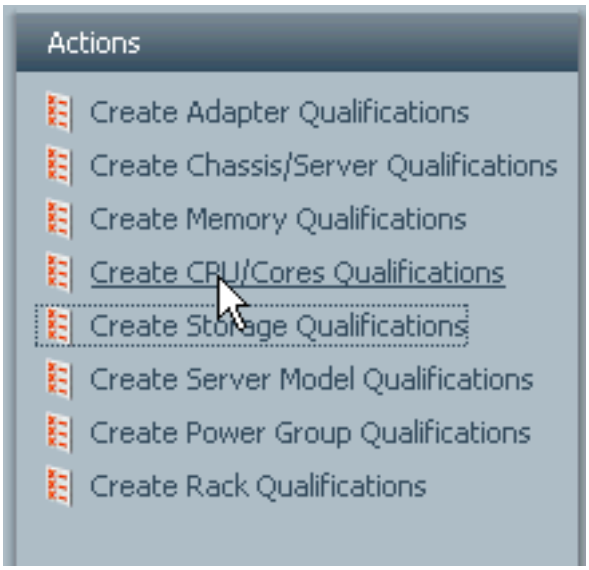
Step 11 Click "Create Memory Qualifications"



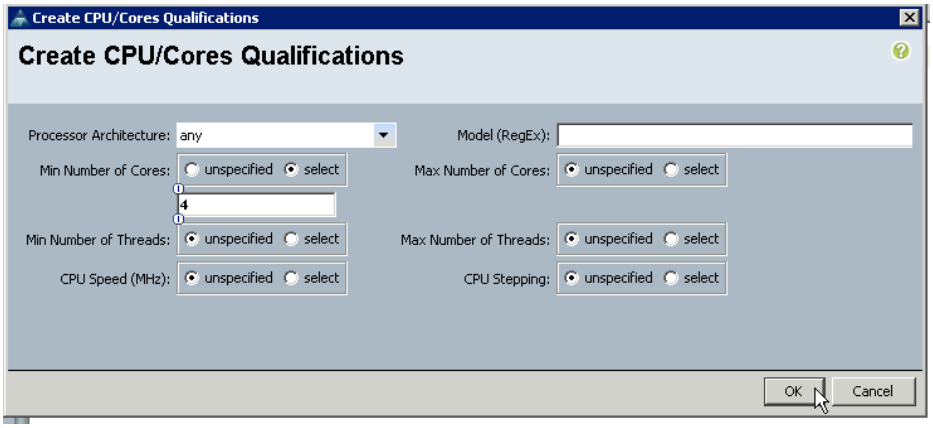
Step 12 Configure a minimum of 2048 MB RAM and click OK.



Step 13 Click “Create CPU/Cores Qualifications”

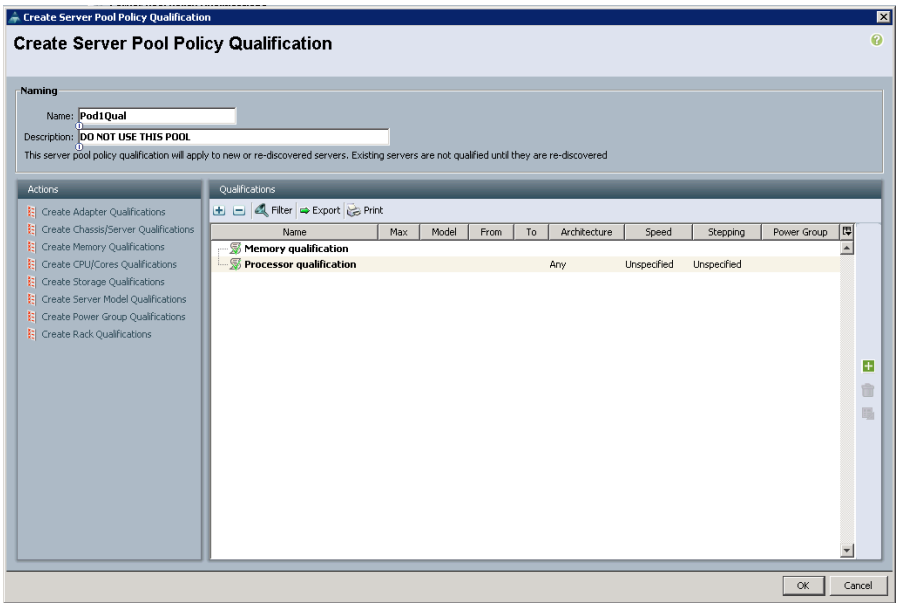


Step 14 Configure a minimum of 4 cores.

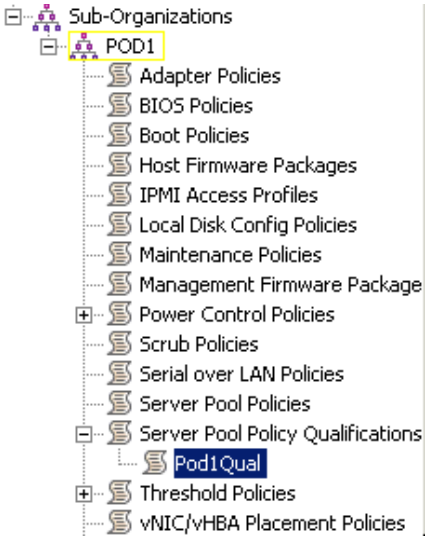


Step 15 Spend a few minutes exploring the other qualifications that could be added to your policy. If you would like to experiment with other qualifications, verify with your instructor which policies will match your assigned server. Keep in mind all qualifications must be fulfilled (logical AND)

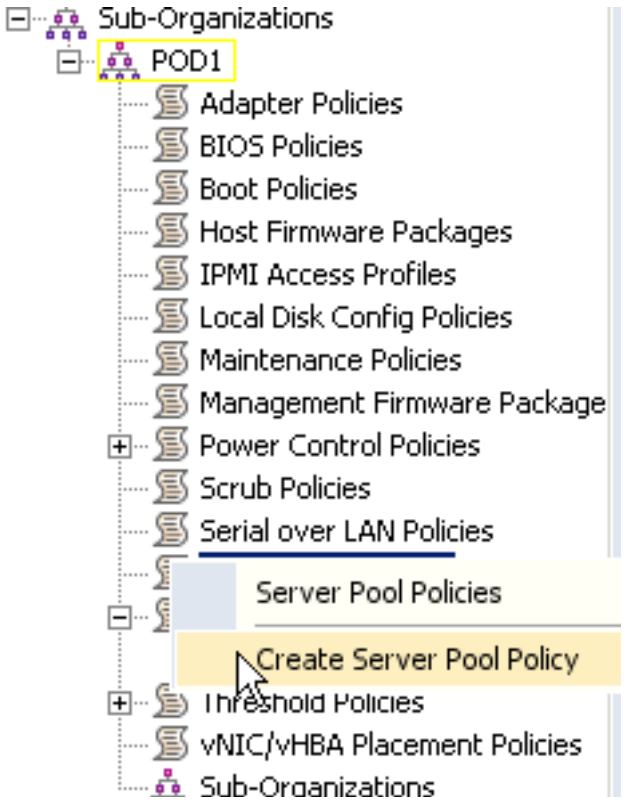
Step 16 When you are satisfied with your qualifications, click **OK**.



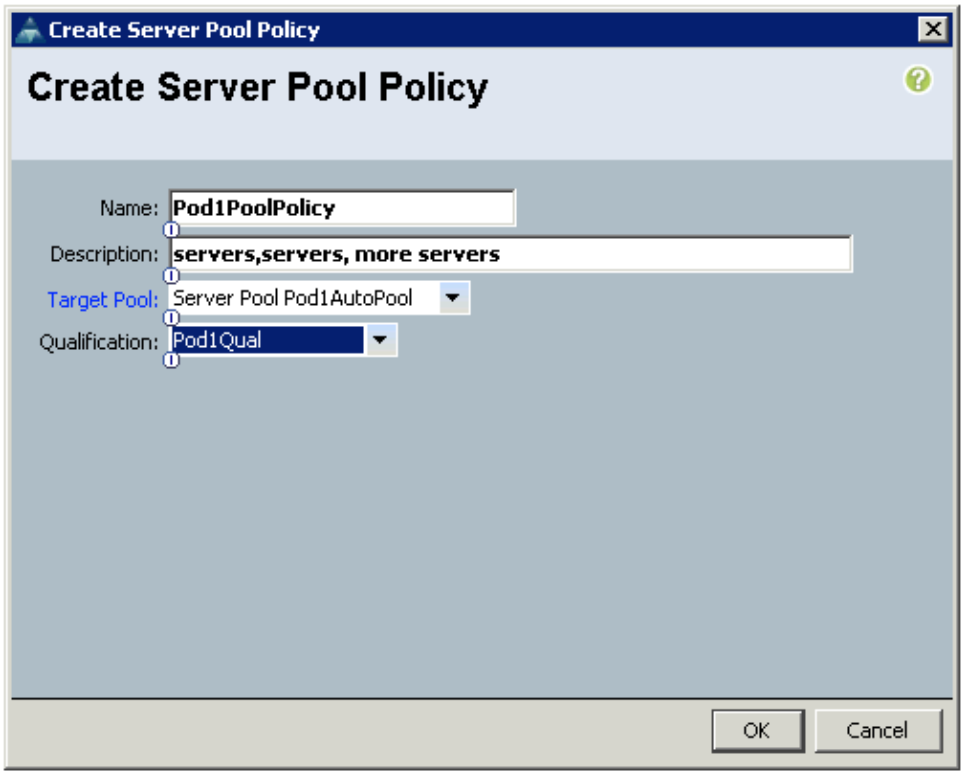
Step 17 Check your Server Qualification Policy.



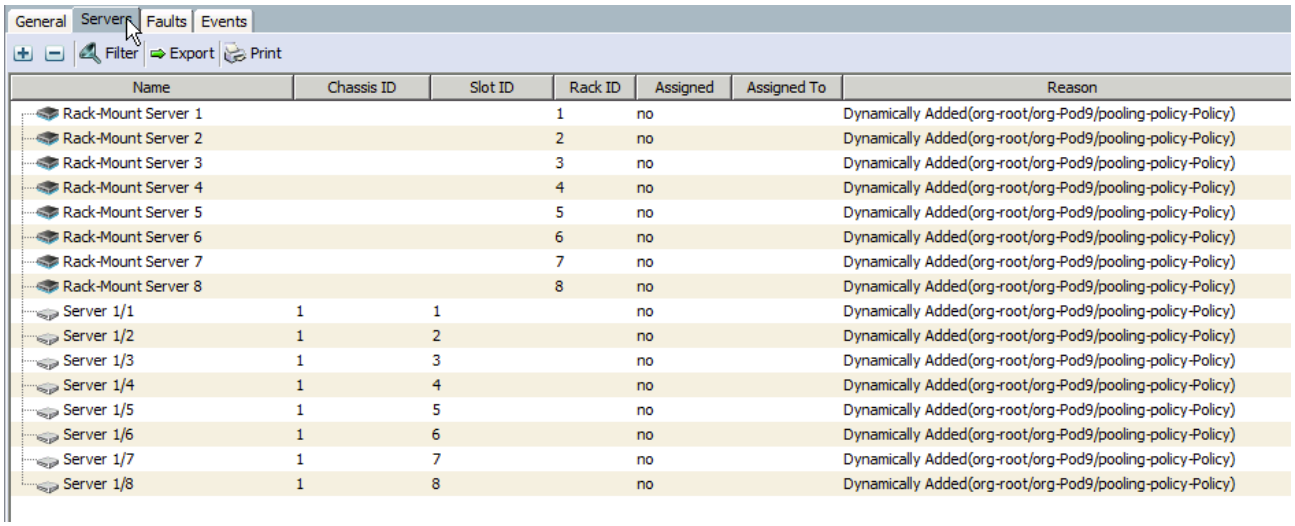
Step 18 Navigate to Server Pool Policies within your Organization, right-click “server pool policies” and “Create Server Pool Policy”



Step 19 Name your Server Pool Policy **PodXPoolPolicy**. Replace X with your Pod number. Add an optional description, choose the PodXQual qualification that you created and your PodPAutoPool. Click **OK**.



Step 20 Verify that your policy has been created and associated with your Pod's qualification policy.



Name	Chassis ID	Slot ID	Rack ID	Assigned	Assigned To	Reason
Rack-Mount Server 1			1	no		Dynamically Added(org-root/org-Pod9/pooling-policy-Policy)
Rack-Mount Server 2			2	no		Dynamically Added(org-root/org-Pod9/pooling-policy-Policy)
Rack-Mount Server 3			3	no		Dynamically Added(org-root/org-Pod9/pooling-policy-Policy)
Rack-Mount Server 4			4	no		Dynamically Added(org-root/org-Pod9/pooling-policy-Policy)
Rack-Mount Server 5			5	no		Dynamically Added(org-root/org-Pod9/pooling-policy-Policy)
Rack-Mount Server 6			6	no		Dynamically Added(org-root/org-Pod9/pooling-policy-Policy)
Rack-Mount Server 7			7	no		Dynamically Added(org-root/org-Pod9/pooling-policy-Policy)
Rack-Mount Server 8			8	no		Dynamically Added(org-root/org-Pod9/pooling-policy-Policy)
Server 1/1	1	1		no		Dynamically Added(org-root/org-Pod9/pooling-policy-Policy)
Server 1/2	1	2		no		Dynamically Added(org-root/org-Pod9/pooling-policy-Policy)
Server 1/3	1	3		no		Dynamically Added(org-root/org-Pod9/pooling-policy-Policy)
Server 1/4	1	4		no		Dynamically Added(org-root/org-Pod9/pooling-policy-Policy)
Server 1/5	1	5		no		Dynamically Added(org-root/org-Pod9/pooling-policy-Policy)
Server 1/6	1	6		no		Dynamically Added(org-root/org-Pod9/pooling-policy-Policy)
Server 1/7	1	7		no		Dynamically Added(org-root/org-Pod9/pooling-policy-Policy)
Server 1/8	1	8		no		Dynamically Added(org-root/org-Pod9/pooling-policy-Policy)

Step 21 In the navigation pane, choose the **Equipment** tab and ensure that the Filter value is set to **All**. Expand the **Fabric Interconnects**, **Expansion Module**, and **FC Ports** objects.

Lab 4-2: Creating Service Profile Templates

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

Activity Objective

In this activity, you will create two SAN-booted service profiles (one FC, one iSCSI) 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 vNIC and vHBA templates
- Create a service profile template
- Create a mobile service profile from a template
- Install ESXi on your server
- Move service profiles between physical blades/servers
- Observe how blade servers communicate with devices outside of the Cisco UCS platform

Required Resources

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

- (2) Cisco UCS Fabric Interconnects
- B-Series Blade Server
- C-Series Rackserver
- SAN-attached storage system
- UUID, WWNN, WWPN, and MAC pools that are created from the previous exercise.

Task 1: Establish SAN Connectivity

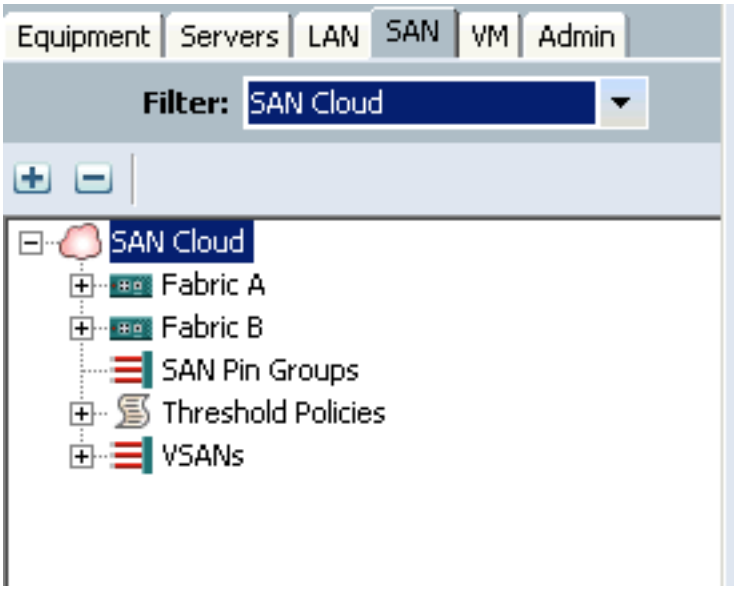
In this task, you will configure Fibre Channel uplinks to provide SAN connectivity to the Fabric Interconnects.

Activity Procedure

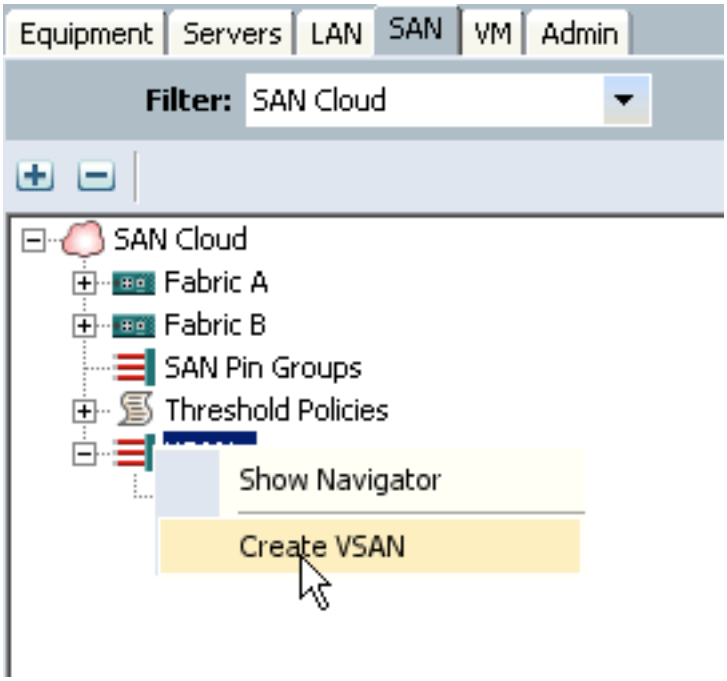
Complete these steps:

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.

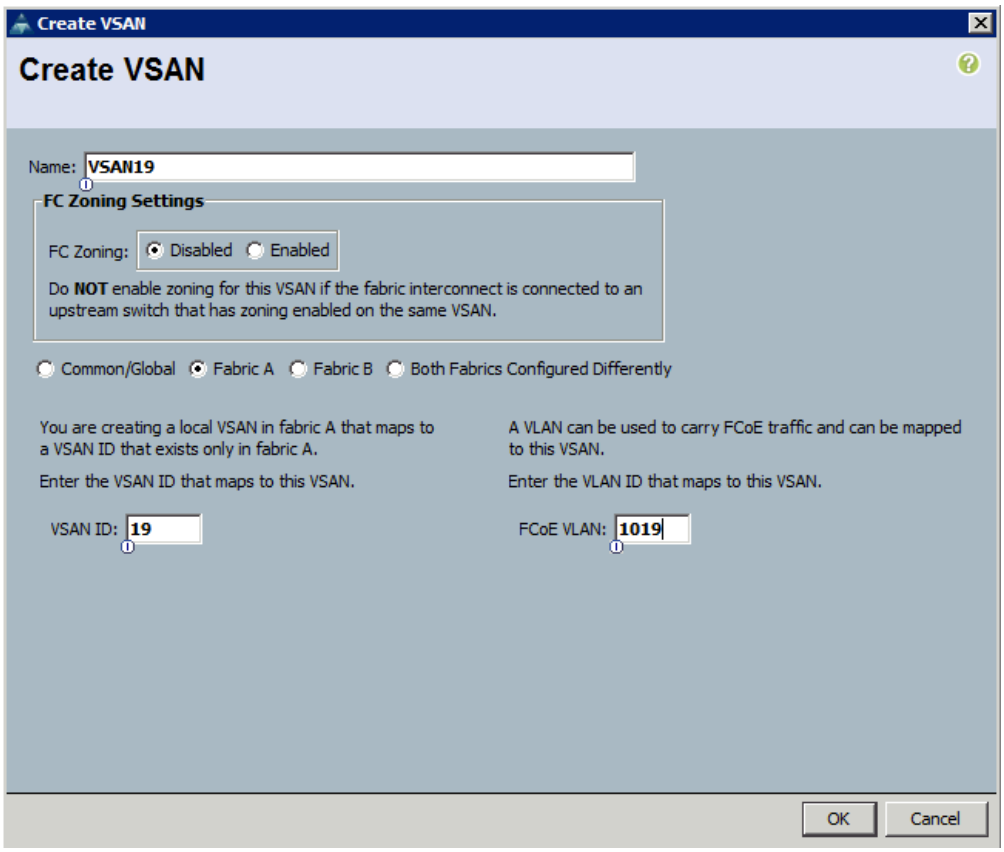


Step 3 Right-click the **VSANs** icon and choose **Create VSAN**.



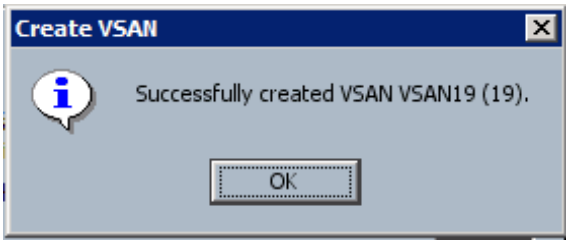
Step 4 Create a VSAN according to the table:

Pod/Team	VSAN #	VSAN name	FCoE VLAN	UCS Fabric
1	11	VSAN11	1011	A
2	12	VSAN12	1012	B
3	13	VSAN13	1013	A
4	14	VSAN14	1014	B
5	15	VSAN15	1015	A
6	16	VSAN16	1016	B
7	17	VSAN17	1017	A
8	18	VSAN18	1018	B

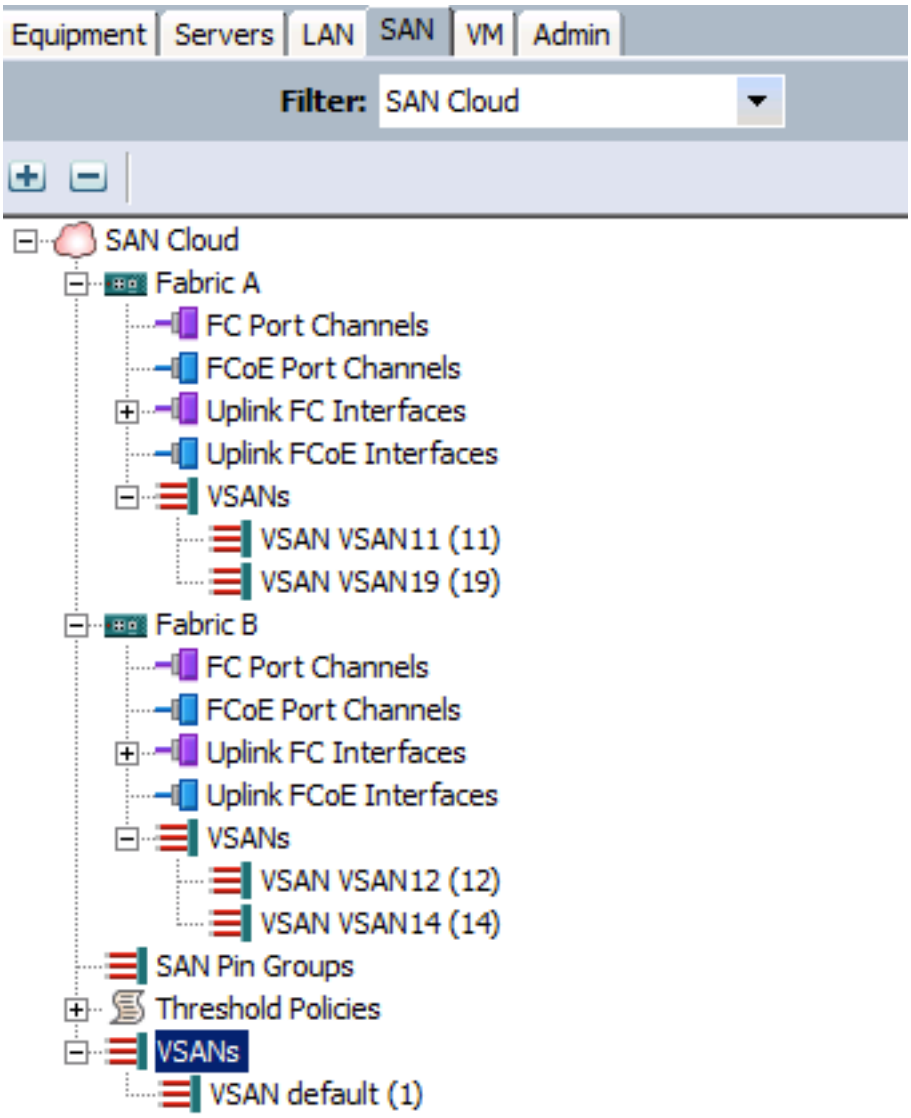


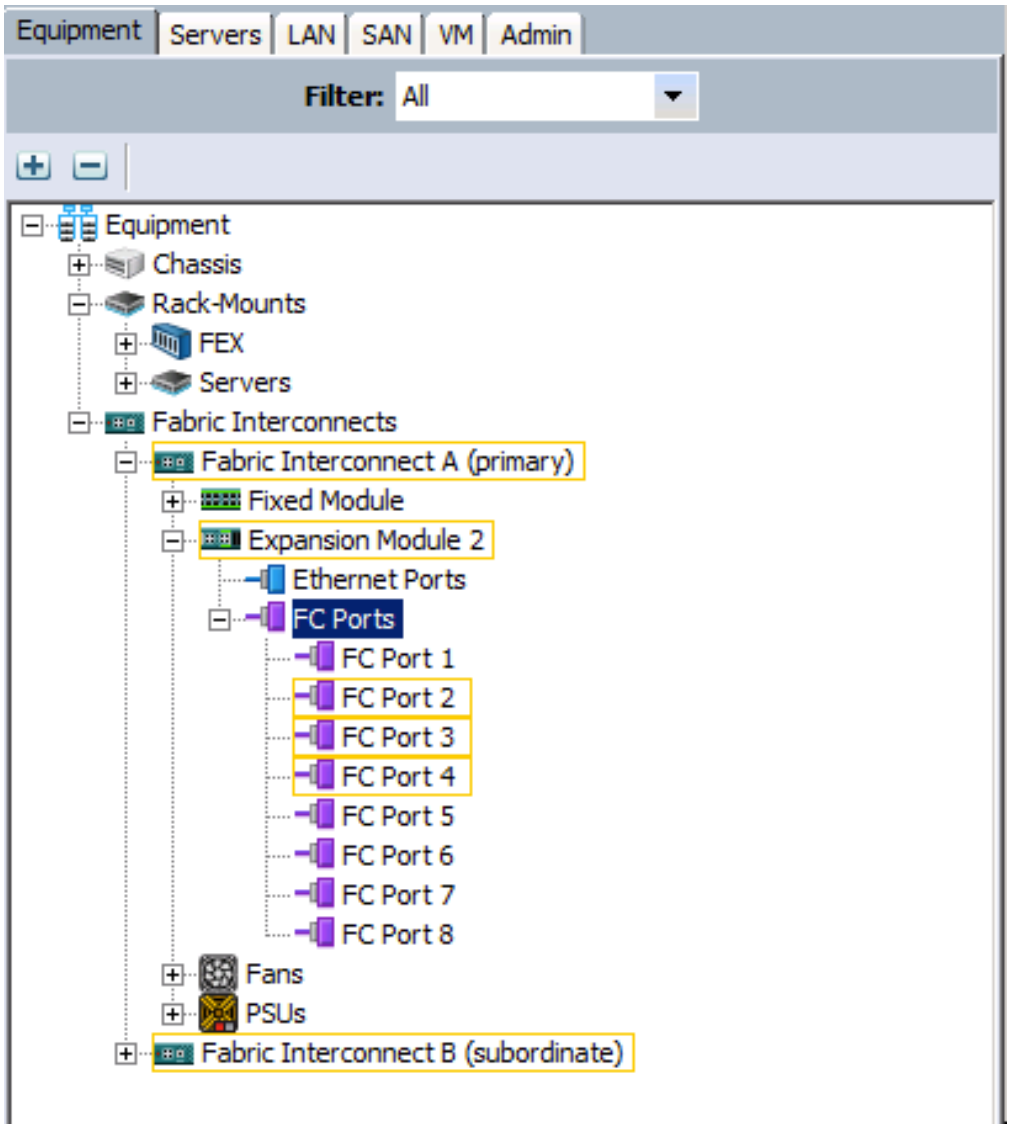
Note In this lab topology, only the two VSANs 11 and 12 will be used and shared by all Pods. **Each Pod is given the opportunity to create a VSAN to practice this task, but be careful to use the designed VSAN in the later steps**.
Some Ports may not be connected or do not have SFPs in them.

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



Step 6 Note odd have been created on Fabric A only and even VSANs have only been created on Fabric B only, The SAN-Cloud->VSAN shows just the default VSAN 1 on both fabrics.



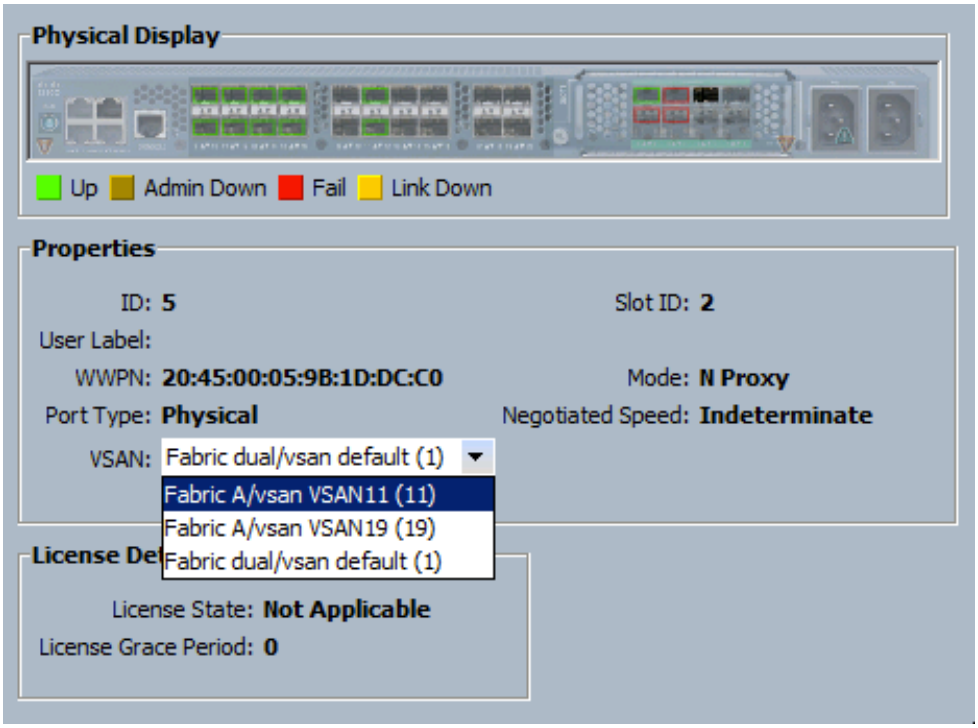


In the content pane, change the VSAN field **of your assigned interface ONLY** according to the table

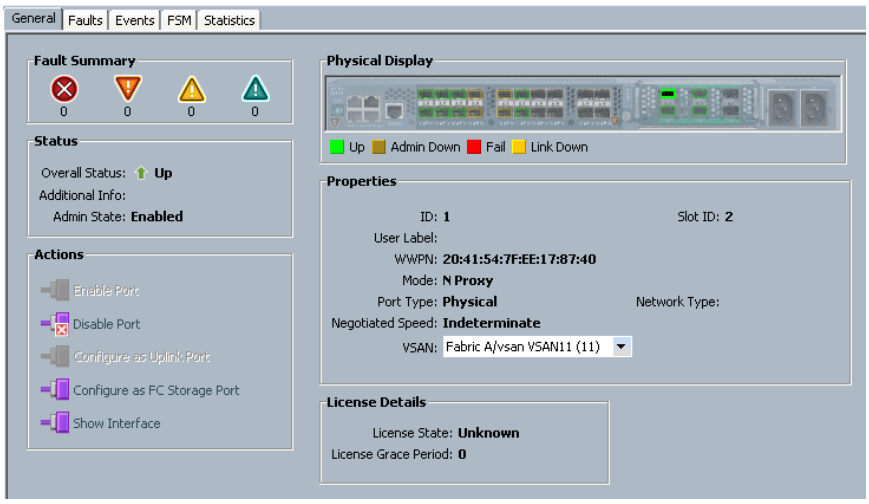
(**make sure to use the VSAN numbers from the table and not the VSAN you**

created earlier!!)

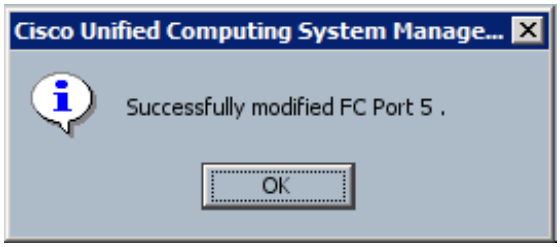
Pod/Team	UCS Fabric Interconnect	Port	VSAN#
1	A	1	**11**
2	B	1	**12**
3	A	2	**11**
4	B	2	**12**
5	A	3	**11**
6	B	3	**12**
7	A	4	**11**
8	B	4	**12**



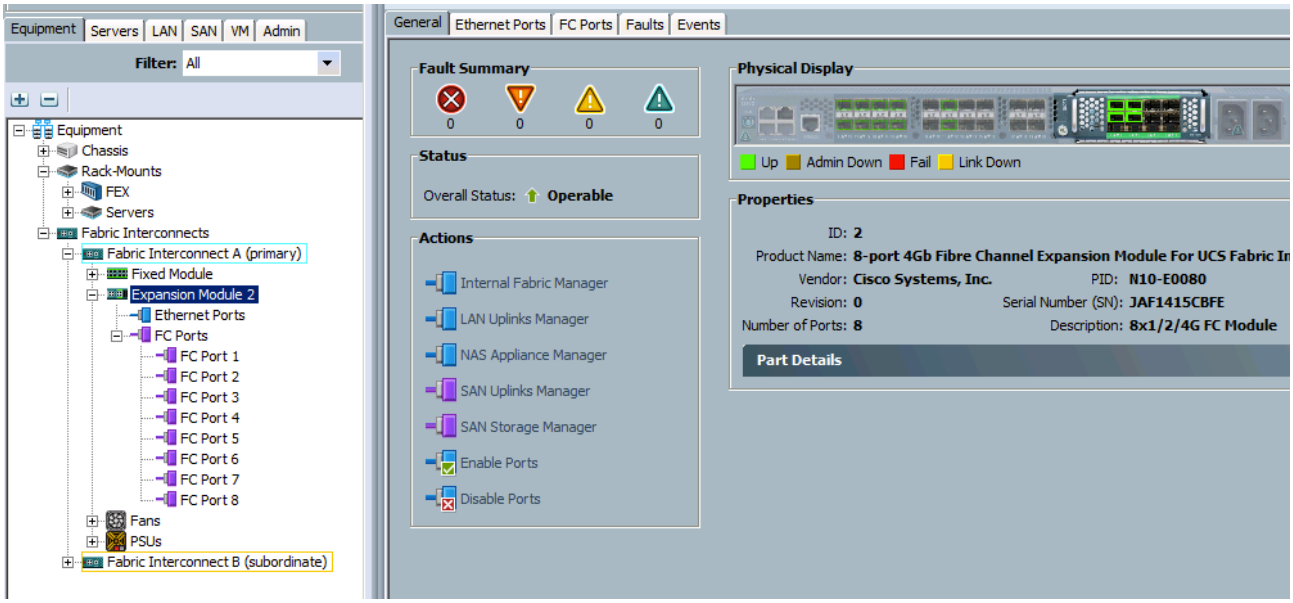
Step 7 Click **Save Changes** to apply the VSAN configuration to this port.



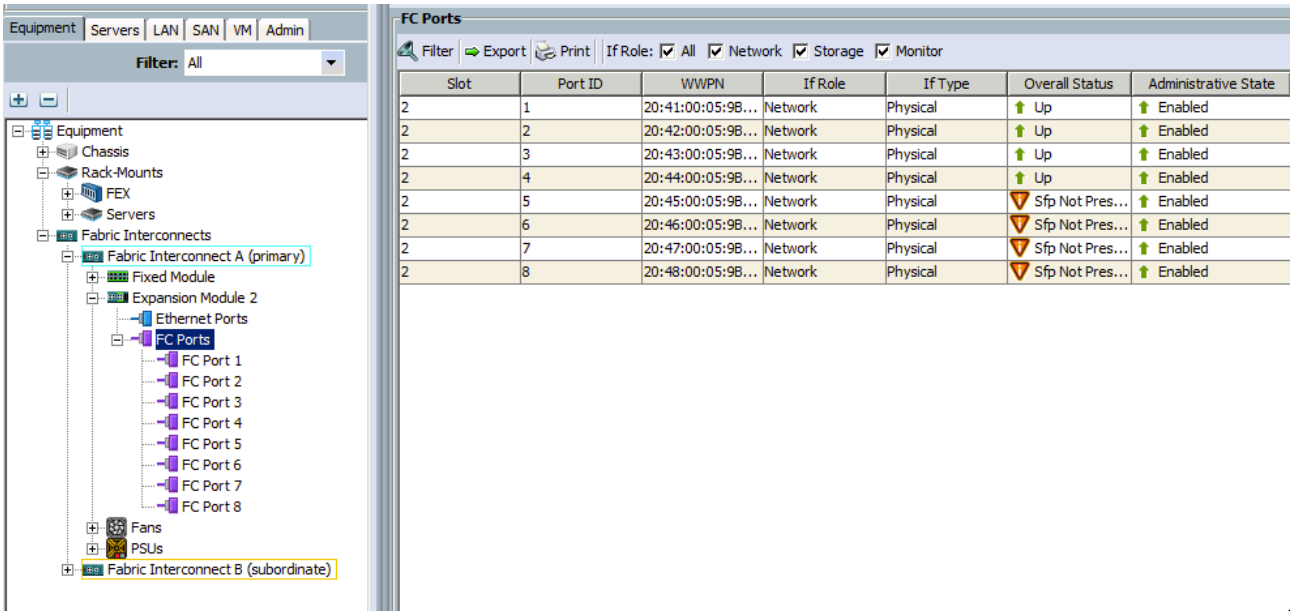
Step 8 Click **OK** to confirm the configuration change.



Step 9 Click the “Expansion Module” in the Equipment navigation pane to check to ensure that the Admin state of the ports is enabled and that the Overall Status is now up.



Step 10 Click the “FC ports” in the equipment tab to check interfaces.



Note If your port does not move to an “Up” state, check to ensure that you have selected VSAN11 on Fabric A and VSAN12 on Fabric B, which may not be the VSAN that you created in the earlier steps. Also check to ensure that you are modifying the port on the correct Fabric Interconnect. If you verify both of these items and the port still does not initialize, contact your instructor for assistance.

Task 2: Establish LAN Connectivity

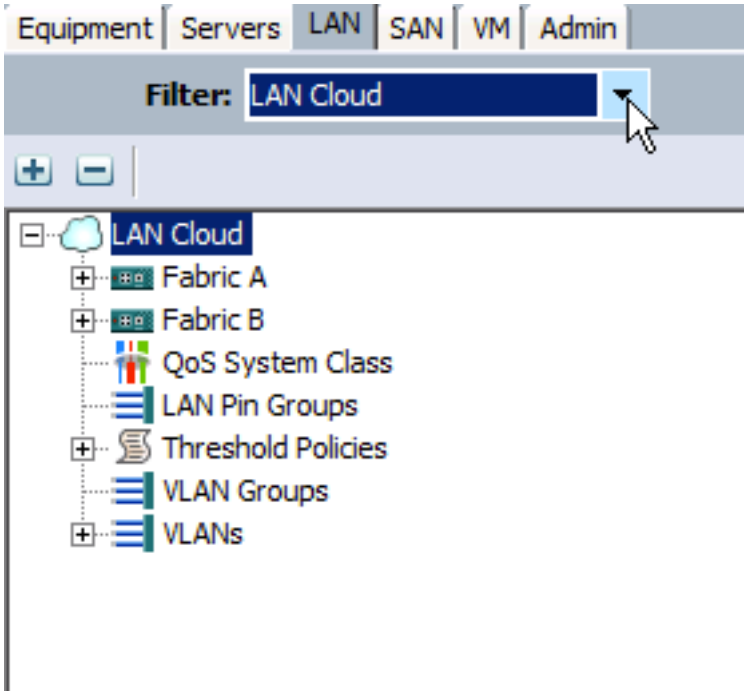
In this task, you will configure a VLAN for your blade server.

Activity Procedure

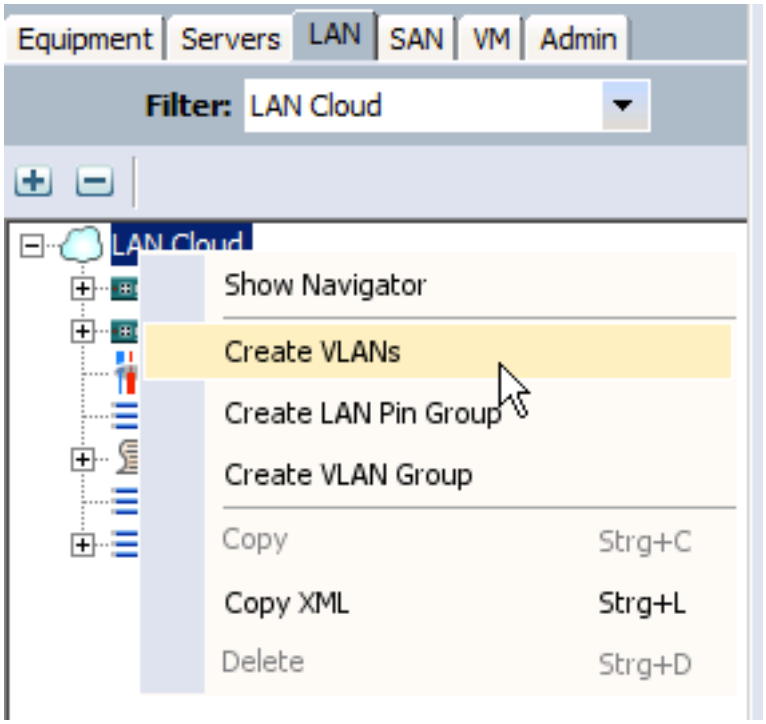
Complete these steps:

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.

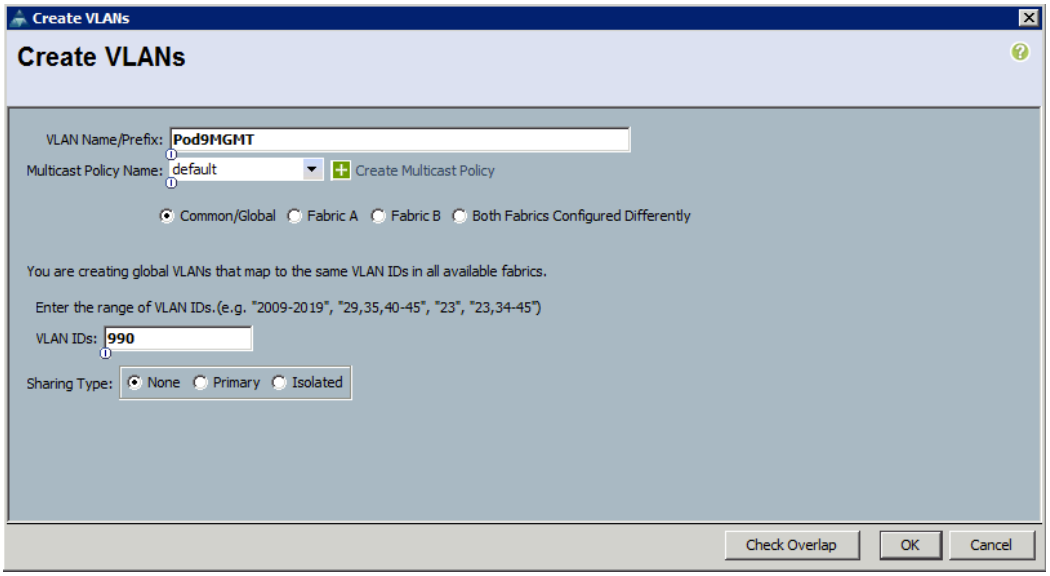


Step 3 Right-click the **LAN Cloud** icon and choose **Create VLANs**.



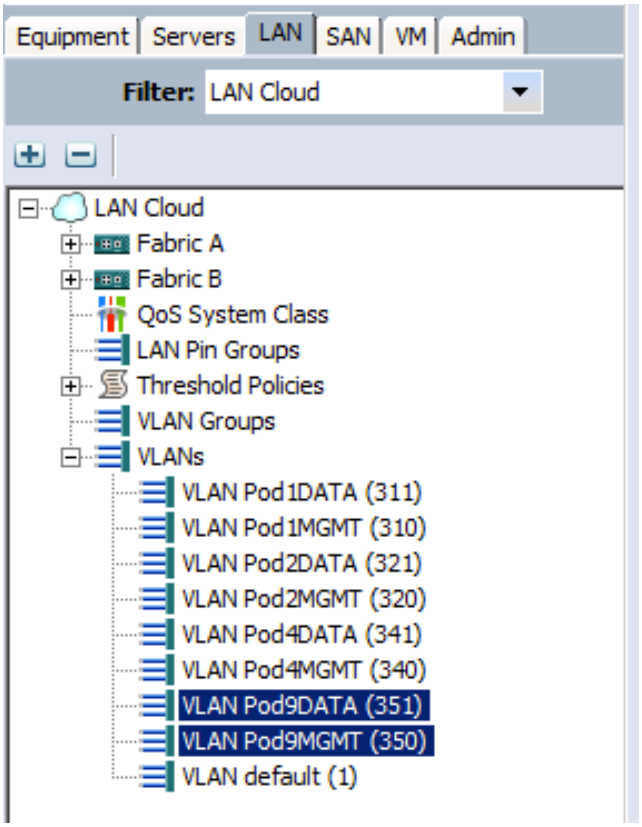
Step 4 Name your VLAN **PodXMGMT** replacing X with your Pod number. Set the Multicast Policy to "default" and set the VLAN ID to **LP0**, replacing L with the Lab ID and P with your Pod number. For example, on Lab ID 1 Pod 1 will use 110, Pod 2 will use 120, and so on.

For your lab ID and pod# refer to page 5 or ask your instructor.



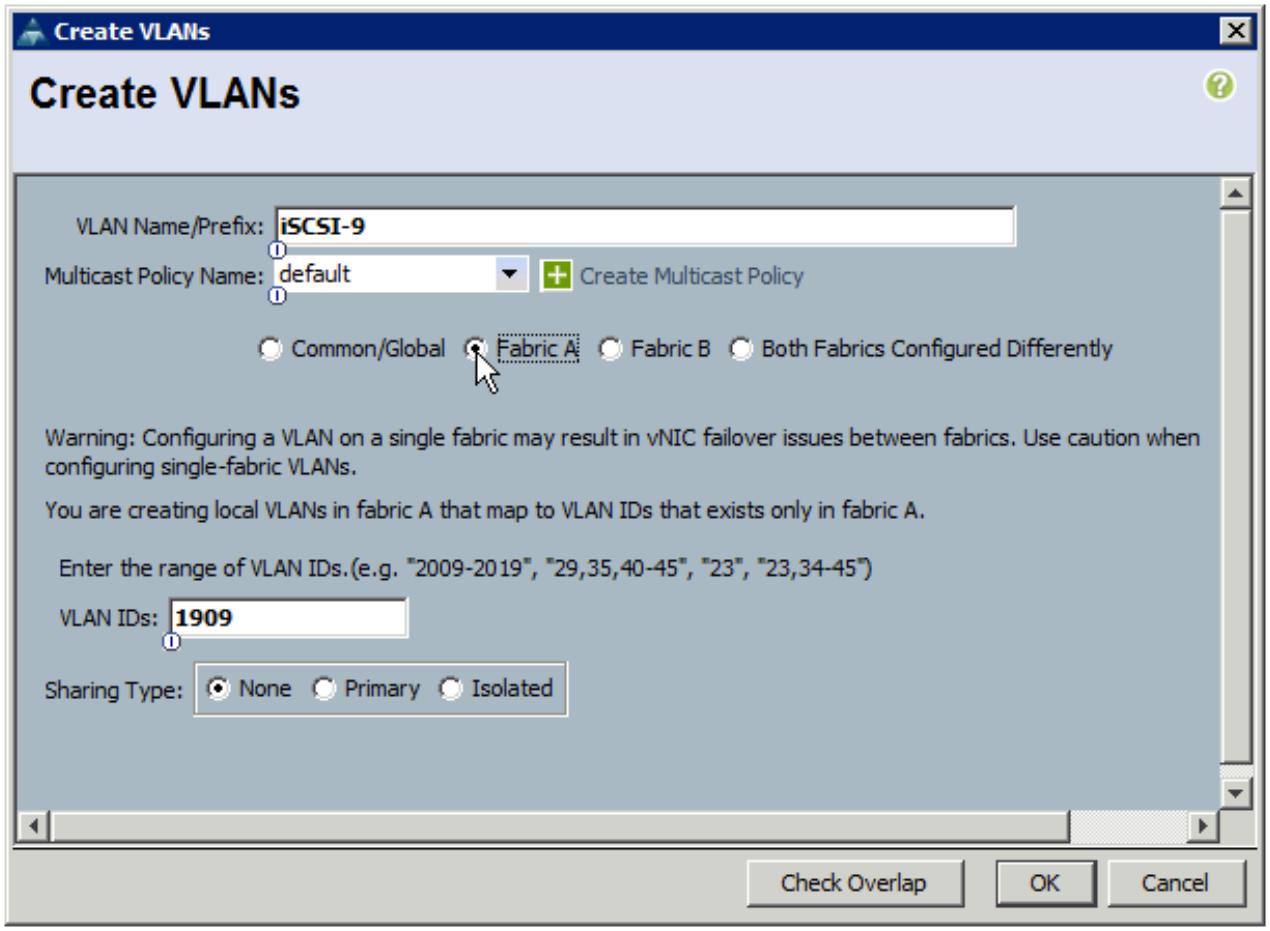
Step 5 **Create a second VLAN LP1 (L=Lab ID, P=Pod Number), named PodXDATA (X is your Pod#)**

Step 6 Expand the VLANs icon and ensure that BOTH your Pod's VLAN now appears.



Step 7 Create an iSCSI VLAN. Refer to the table and make sure to create the VLAN ONLY on the assigned Fabric Interconnect (L is the Lab ID)

Pod Number	Fabric Interconnect	VLAN ID	VLAN name
1	A	1L01	iSCSI-1
2	B	1L02	iSCSI-2
3	A	1L03	iSCSI-3
4	B	1L04	iSCSI-4
5	A	1L05	iSCSI-5
6	B	1L06	iSCSI-6
7	A	1L07	iSCSI-7
8	B	1L08	iSCSI-8



Task 3: Create vNIC templates and Connectivity Policies

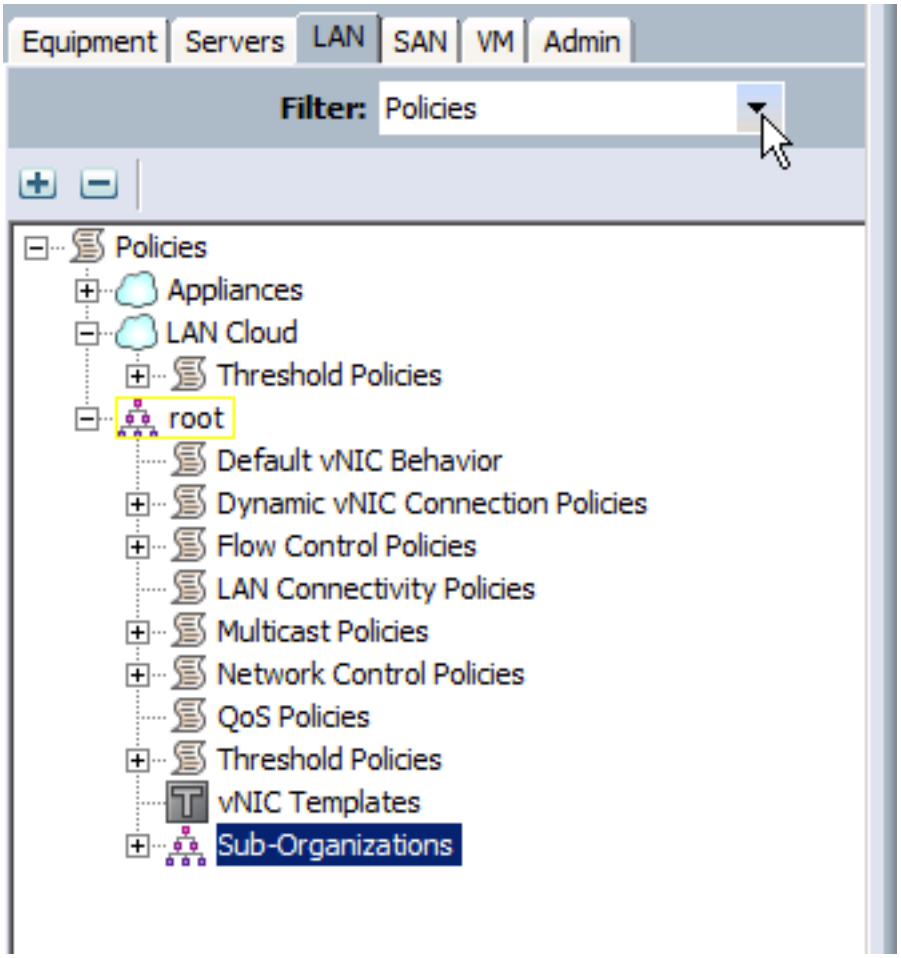
In this task, you will create templates and Connectivity Policies for vNICs. This can save a lot of work because may servers have very similar requirements for NICs.

Activity Procedure

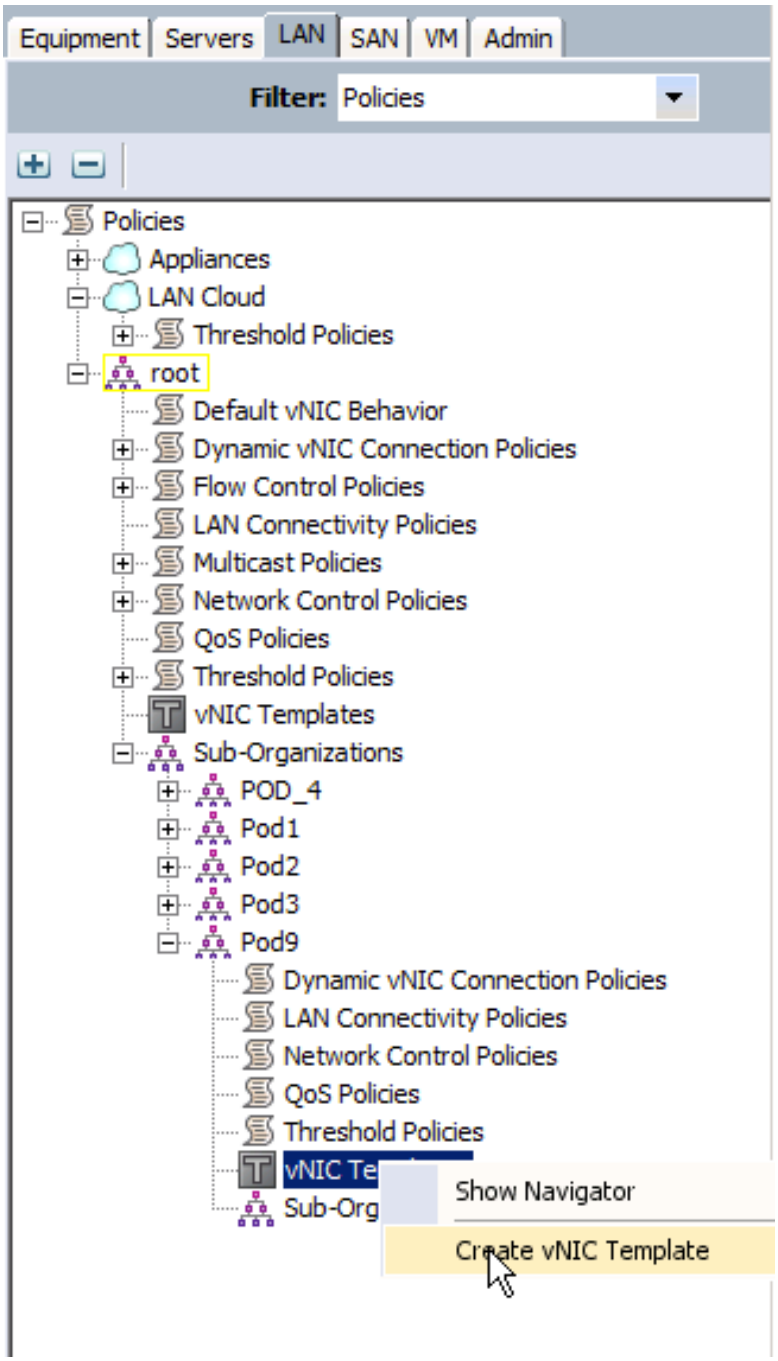
Complete these steps:

Step 1 Log into Cisco UCS Manager if necessary.

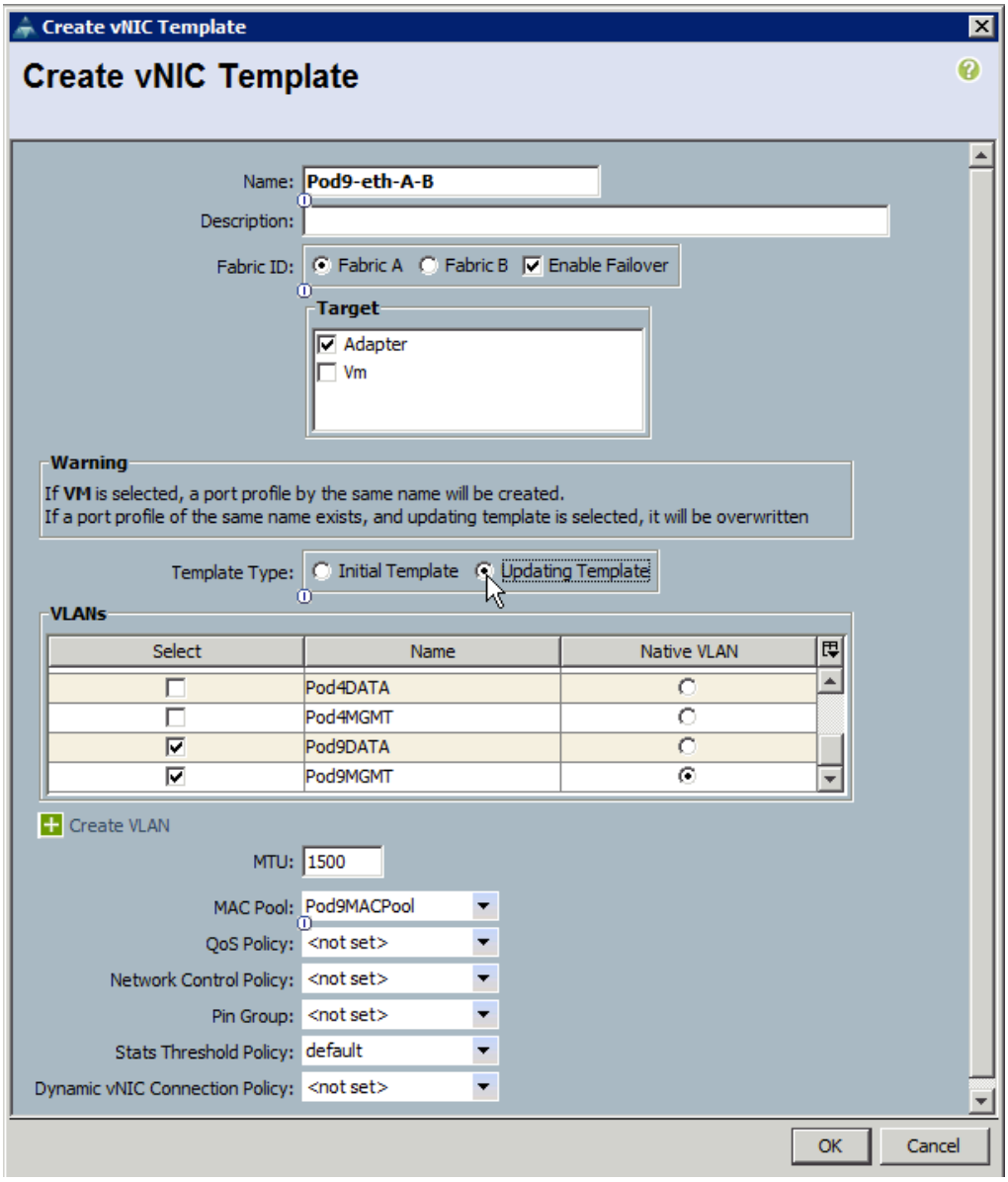
Step 2 In the navigation pane, choose the **LAN** tab. It may be helpful to set the **Filter** field to **Policies** for the following steps.



Step 3 Expand your Organziation and right click “vNIC Templates”

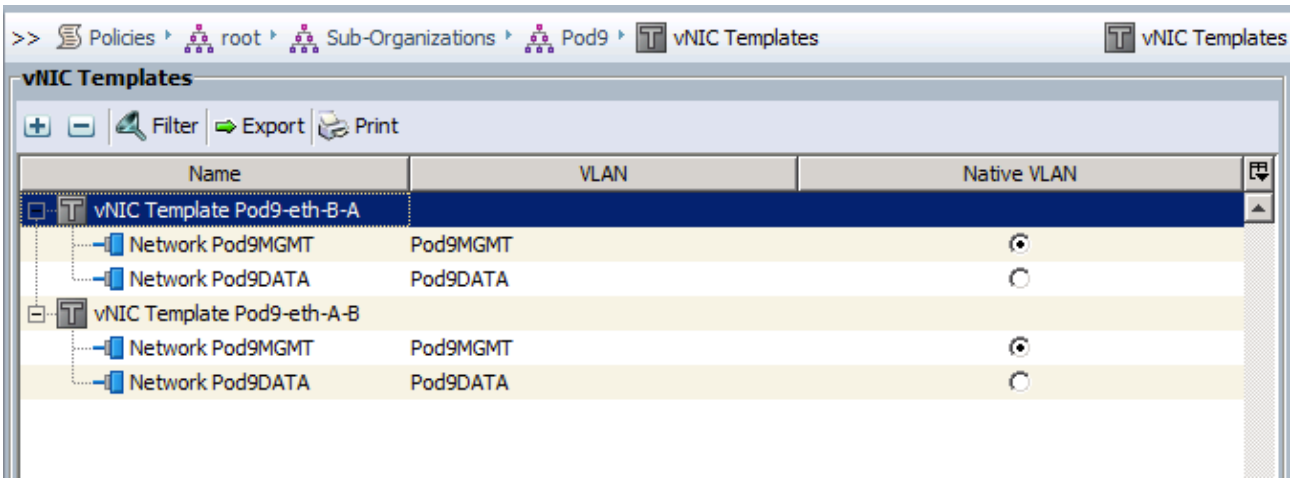


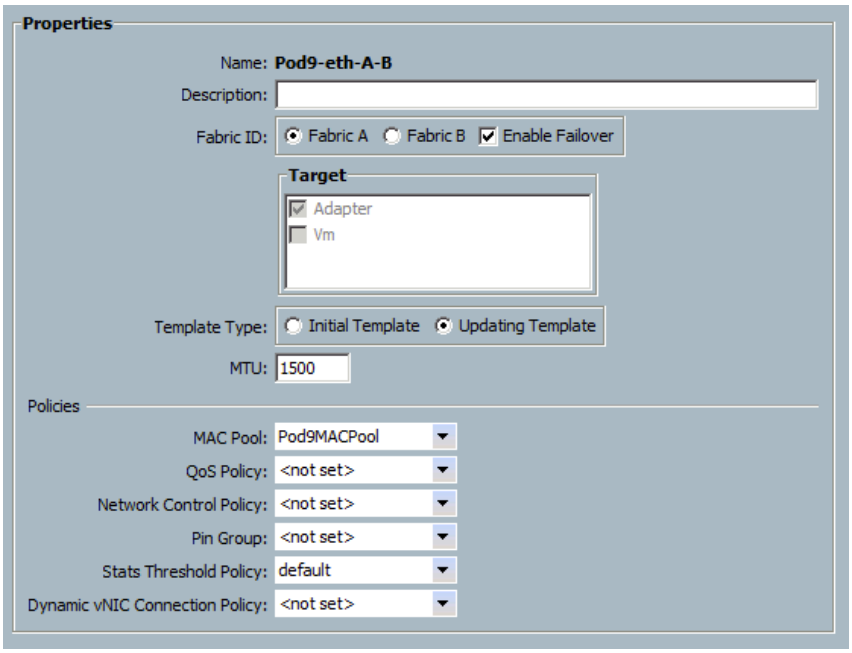
Step 4 Create an **updating** vNIC adapter (do not select the "VM" target) template named "PodX-eth-A-B" (X is your Pod#) using Fabric A with Failover, enable DATA and MGMT Vlans (**mgmt. is native**) using your Pod MAC Pool created earlier.

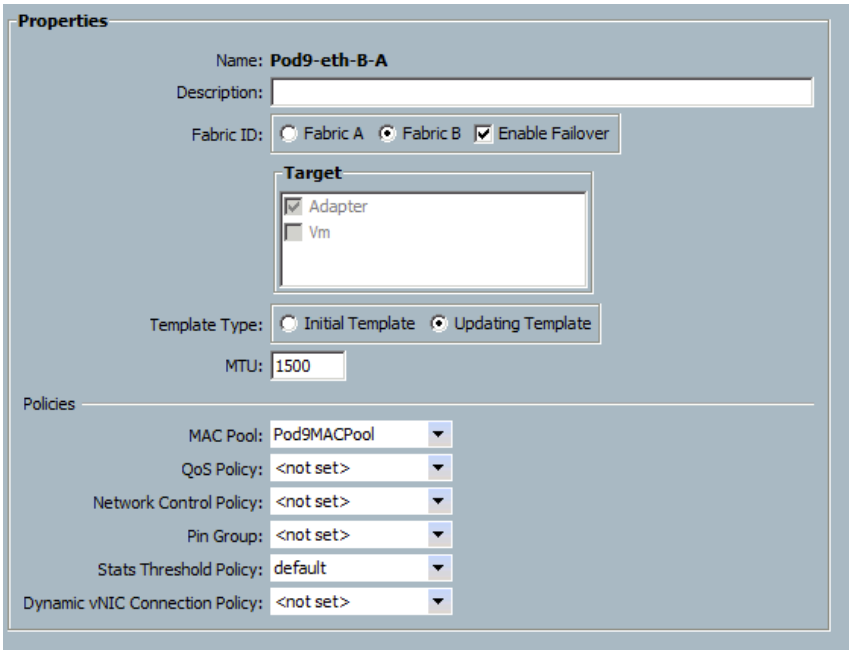


Step 5 Create a second **updating** vNIC template named "PodX-eth-B-A" (X is your Pod#) like the one before but attach it to fabric B with failover to A.

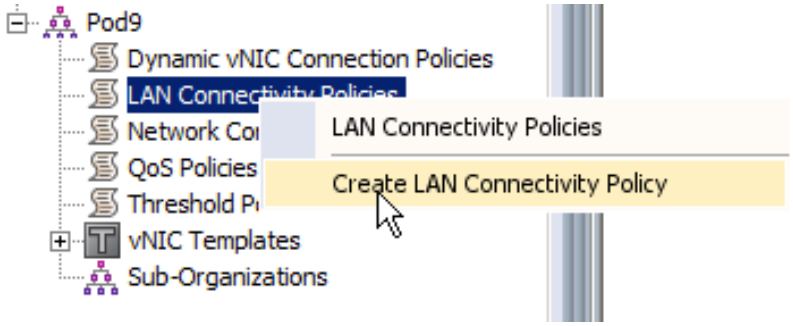
Step 6 Click on both vNIC templates and check your configuration. If necessary adjust the configuration and click "Save Changes"



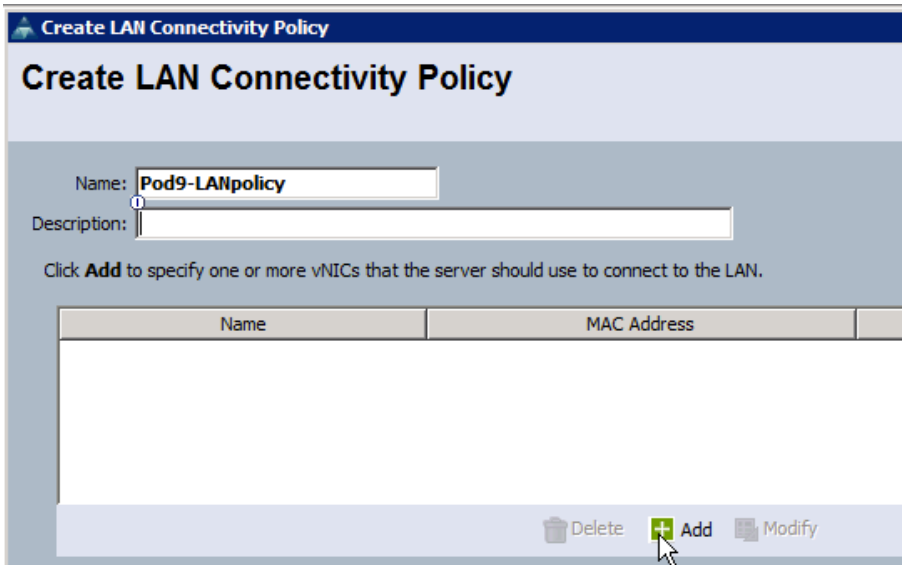




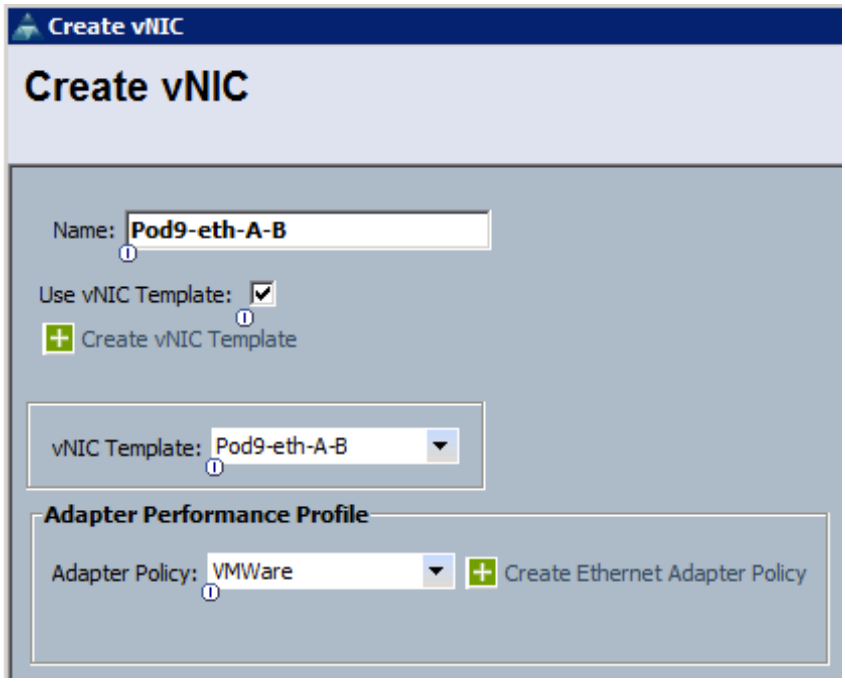
Step 7 Inside your Organization right-click “LAN Connectivity Policies” and click “Create LAN Connectivity Policy”



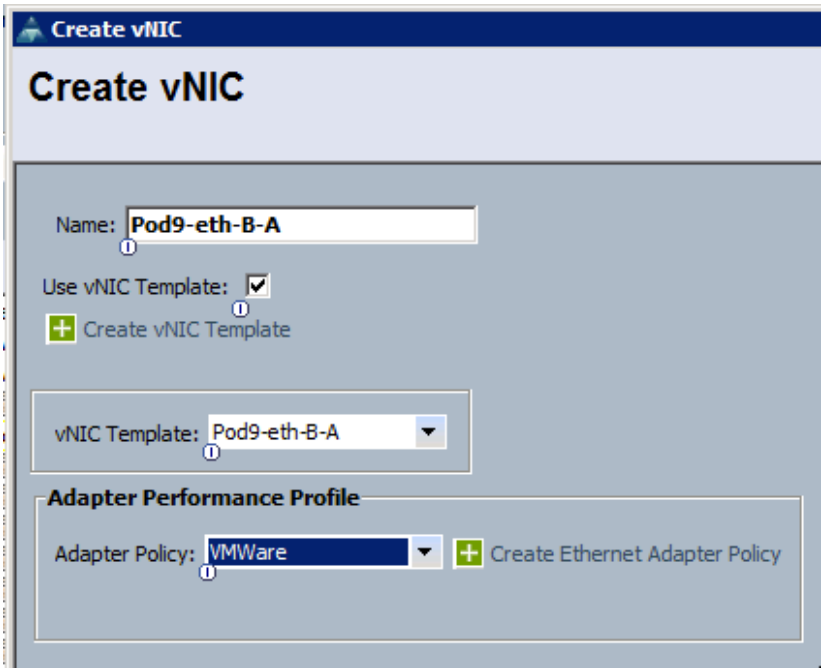
Step 8 Name your policy “Pod#-LANpolicy”, then click “Add” to add NICs



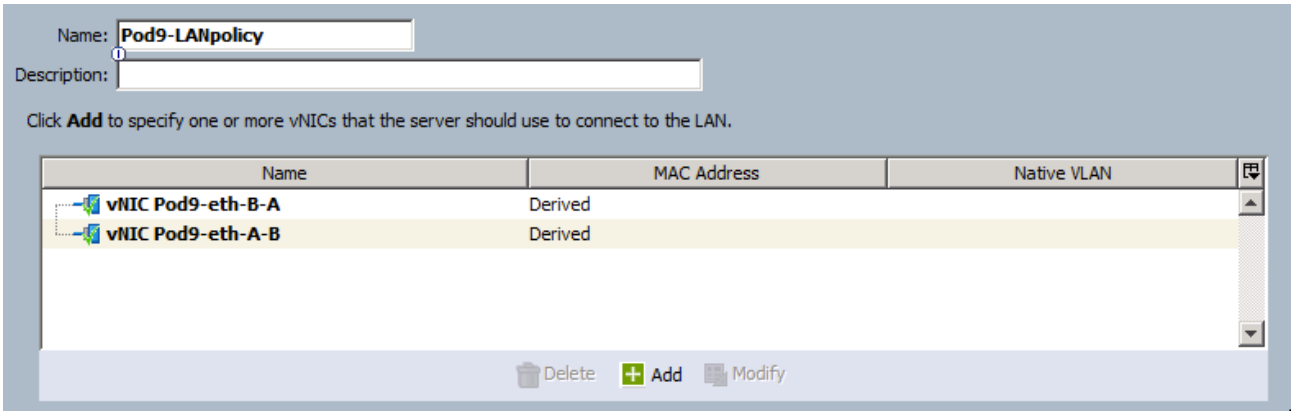
Step 9 Name your first card “Pod#-eth-A-B” (# is your Pod#), click “use vNIC Template”, select your Pods A-B template and the “VMWare” Adapter Performance Profile, then click OK.



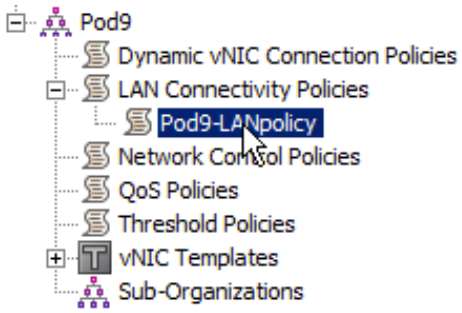
Step 10 Create a second vNIC named “Pod#-eth-B-A” (# is your Pod number) using template B-A.

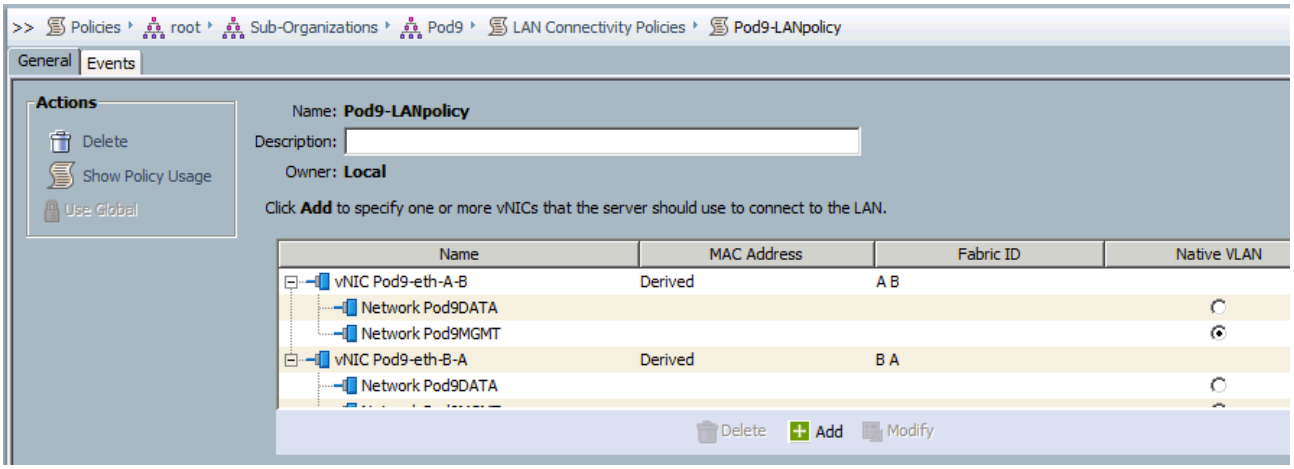


Step 11 Check your LAN policy configuration, then click “OK”



Step 12 Select the the policy you just created and the check the configuration.





Task 4: Create vHBA templates and Connectivity Policies

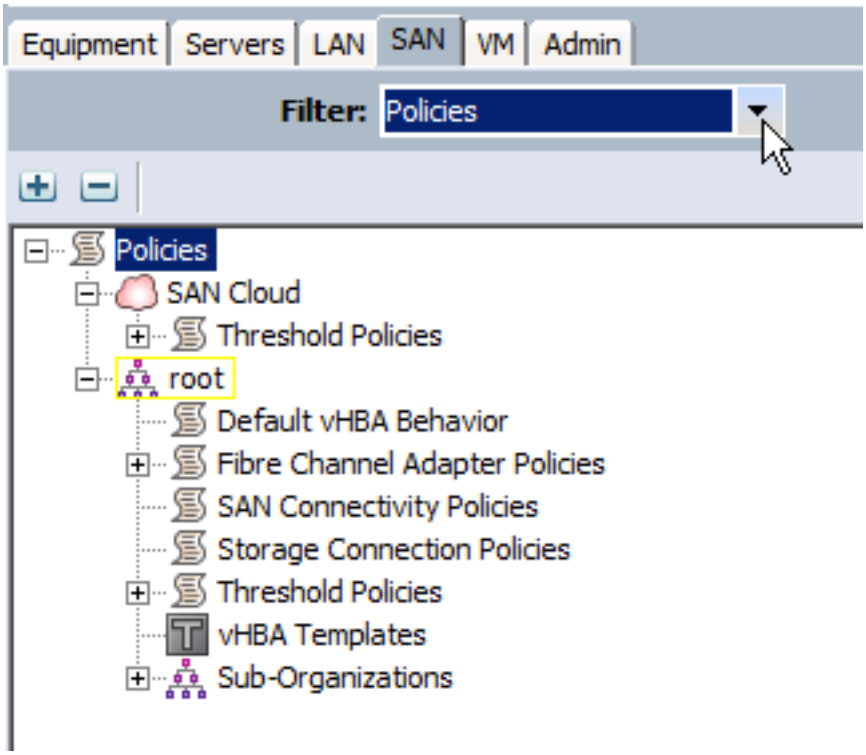
In this task, you will create templates and Connectivity Policies for vHBAs. This can save a lot of work because may servers have very similar requirements for HBAs.

Activity Procedure

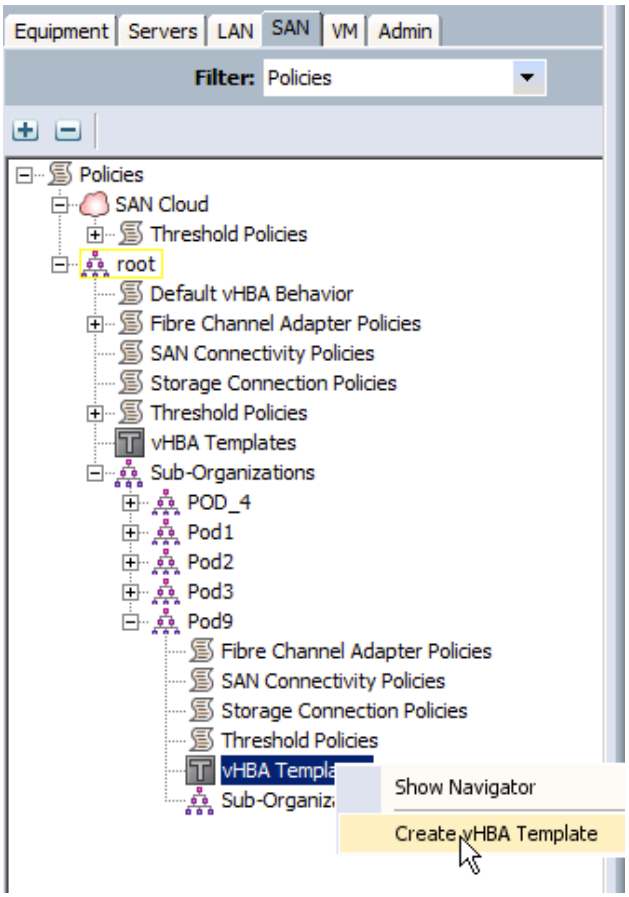
Complete these steps:

Step 1 Log into Cisco UCS Manager if necessary.

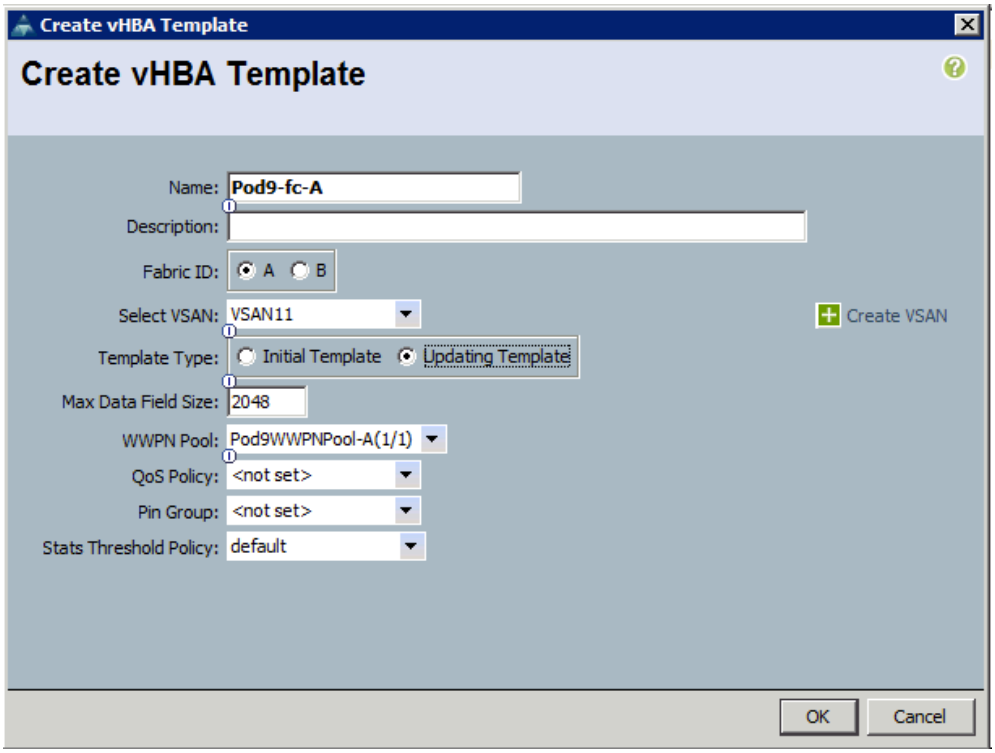
Step 2 In the navigation pane, choose the **SAN** tab. It may be helpful to set the **Filter** field to **Policies** for the following steps.



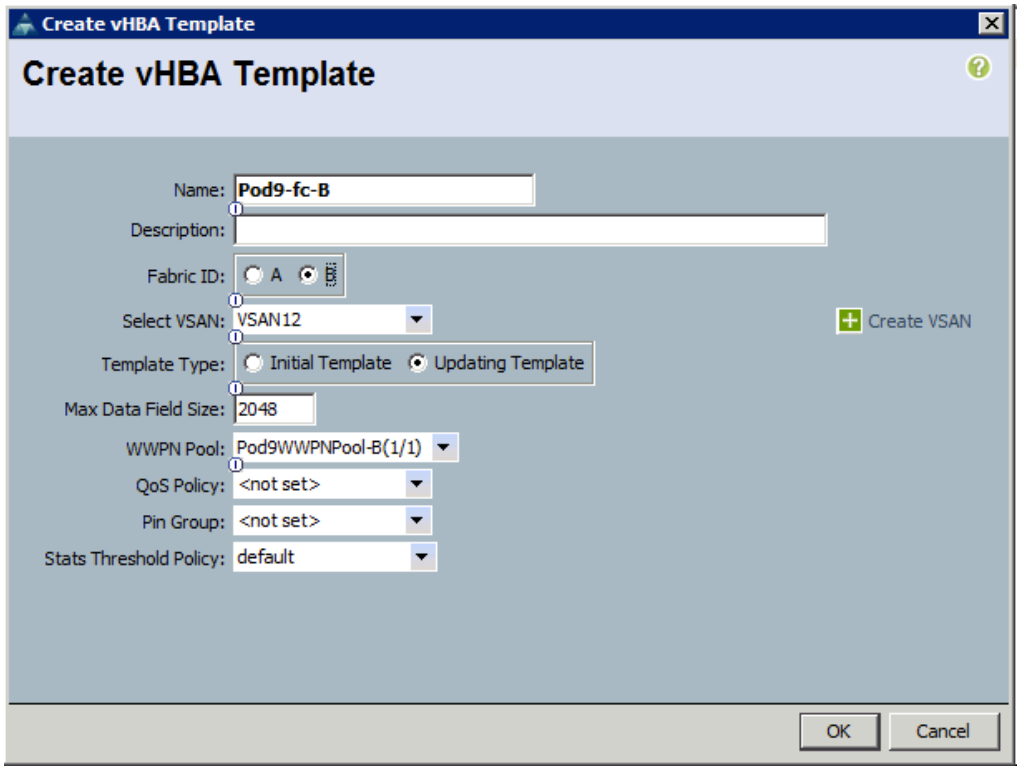
Step 3 Expand your organization, right-click “vHBA Templates” to create a new vHBA template INSIDE your Organization.



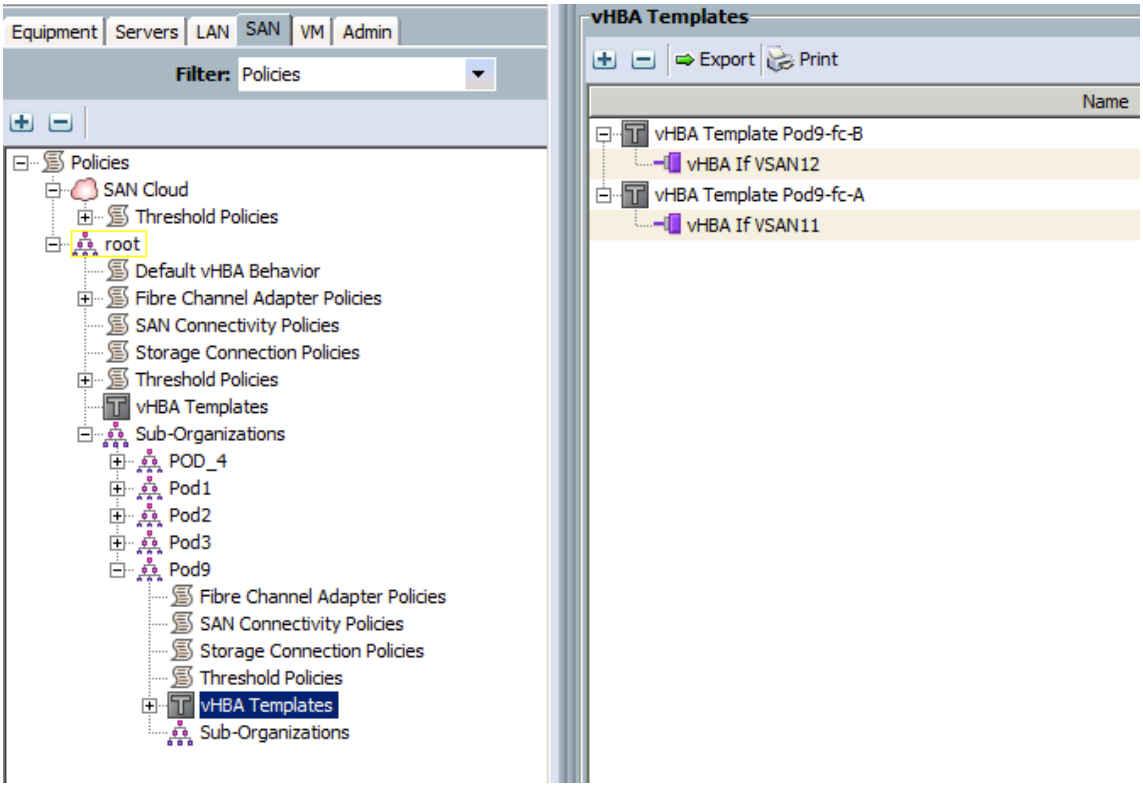
Step 4 Name your updating template "PodX-fc-A" (X is our Pod#) using Fabric A and VSAN 11 (all Pods MUST use VSAN11 here or boot/install will fail!) Make sure to select the –A WWPN Pool!



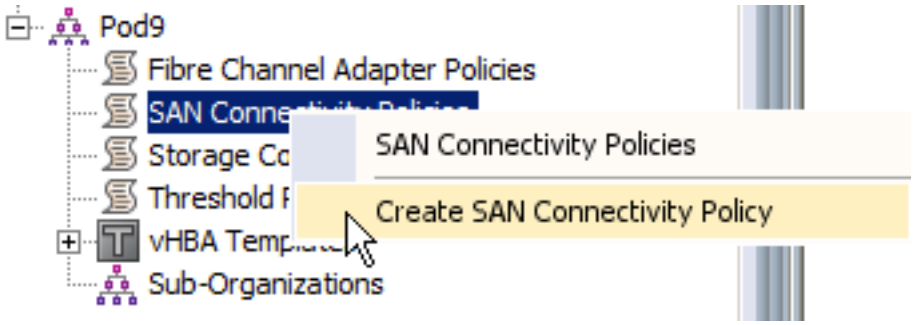
Step 5 Create a second updating template named "PodX-fc-B" (X is your Pod #) using Fabric B and VSAN 12. Make sure to select the –B WWN Pool



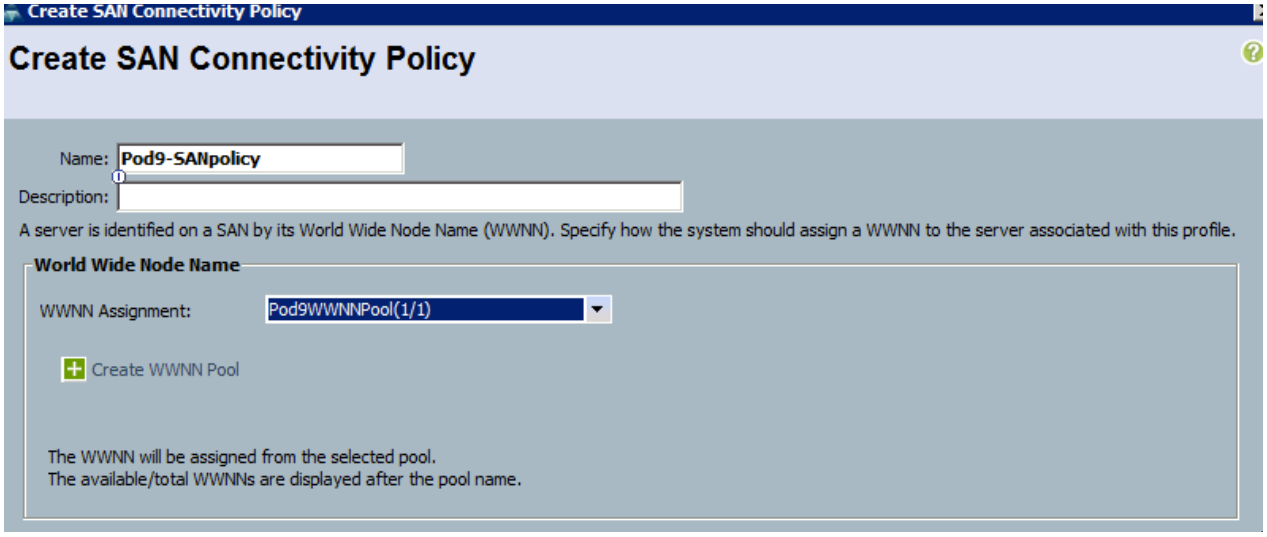
Step 6 Check your configuration by clicking vHBA templates in the navigation pane in your organization and expand the two vHBA templates in the left pane



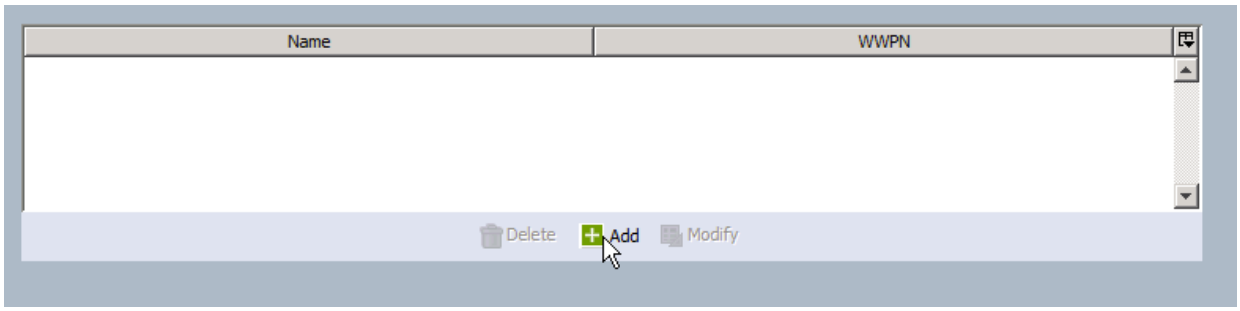
Step 7 Inside your organization right-click “SAN Connectivity Policies” and select “Create SAN Connectivity Policy



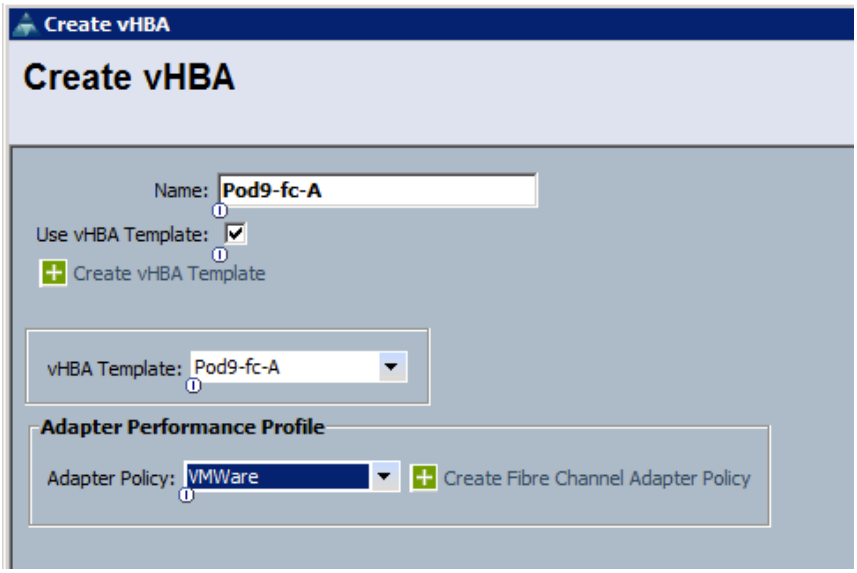
Step 8 Name your Policy Pod#-SANpolicy (# is your Pod number) and select the WWNN Pool you created earlier.



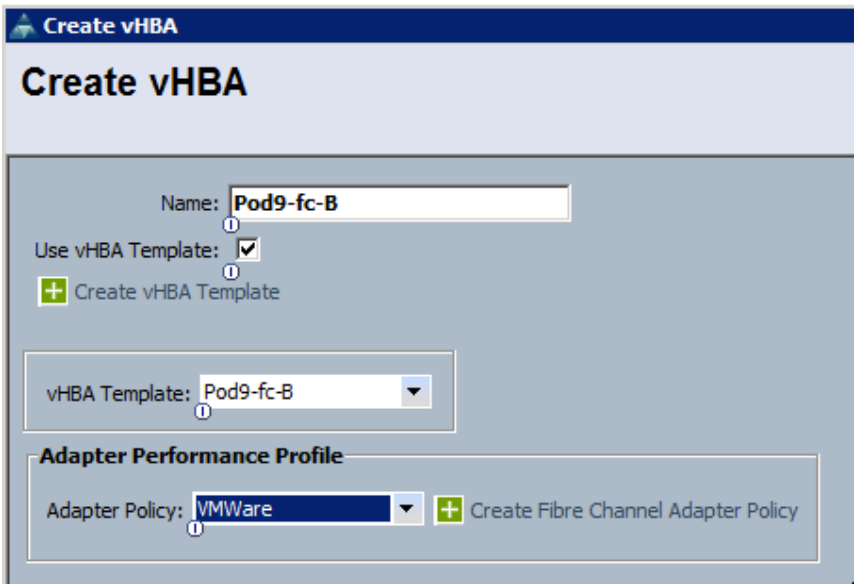
Step 9 Click "Add" to add a vHBA



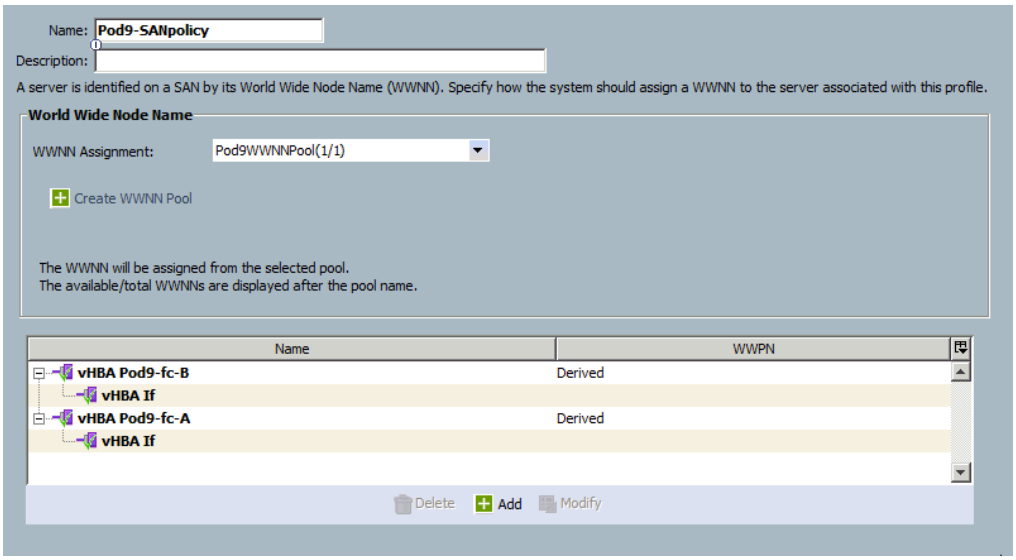
Step 10 Name your first vHBA "Pod#-fc-A", use the template for A you created earlier and use the "VMWare" performance profile, then click OK



Step 11 Click “Add” again and create a second HBA named “Pod#-fc-B” (# is your Pod number) for Fabric B using the B template.

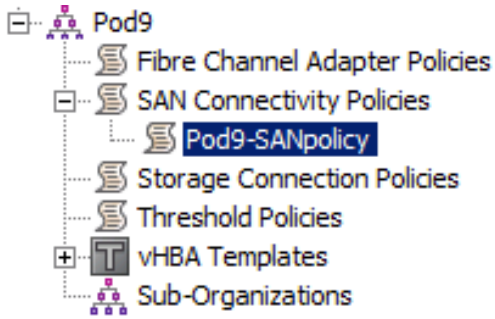


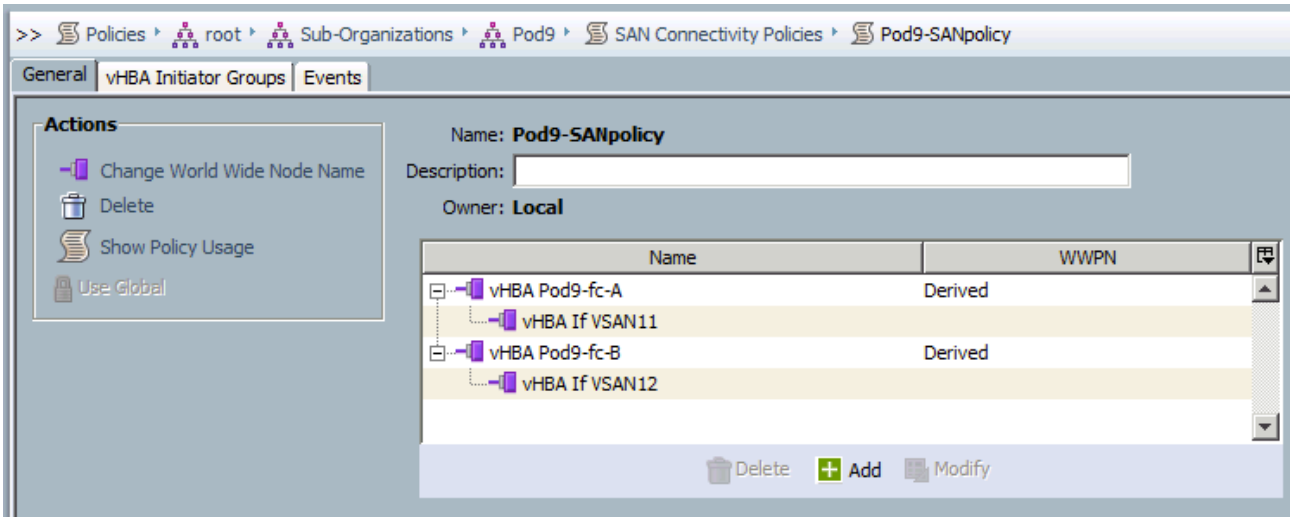
Step 12 Check your configuration, then click OK



Step 13 Click OK to confirm your SAN Connectivity Policy

Step 14 Select your newly created policy and confirm the configuration





Task 5: Create a BIOS policy

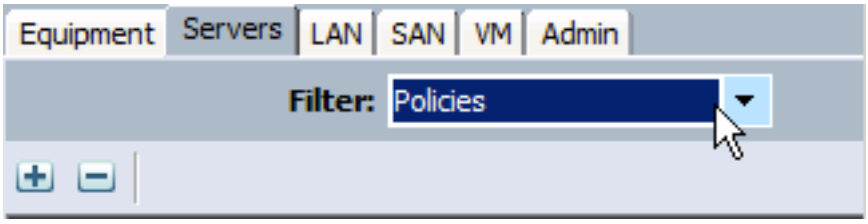
In this task, you will create a BIOS configuration.

Activity Procedure

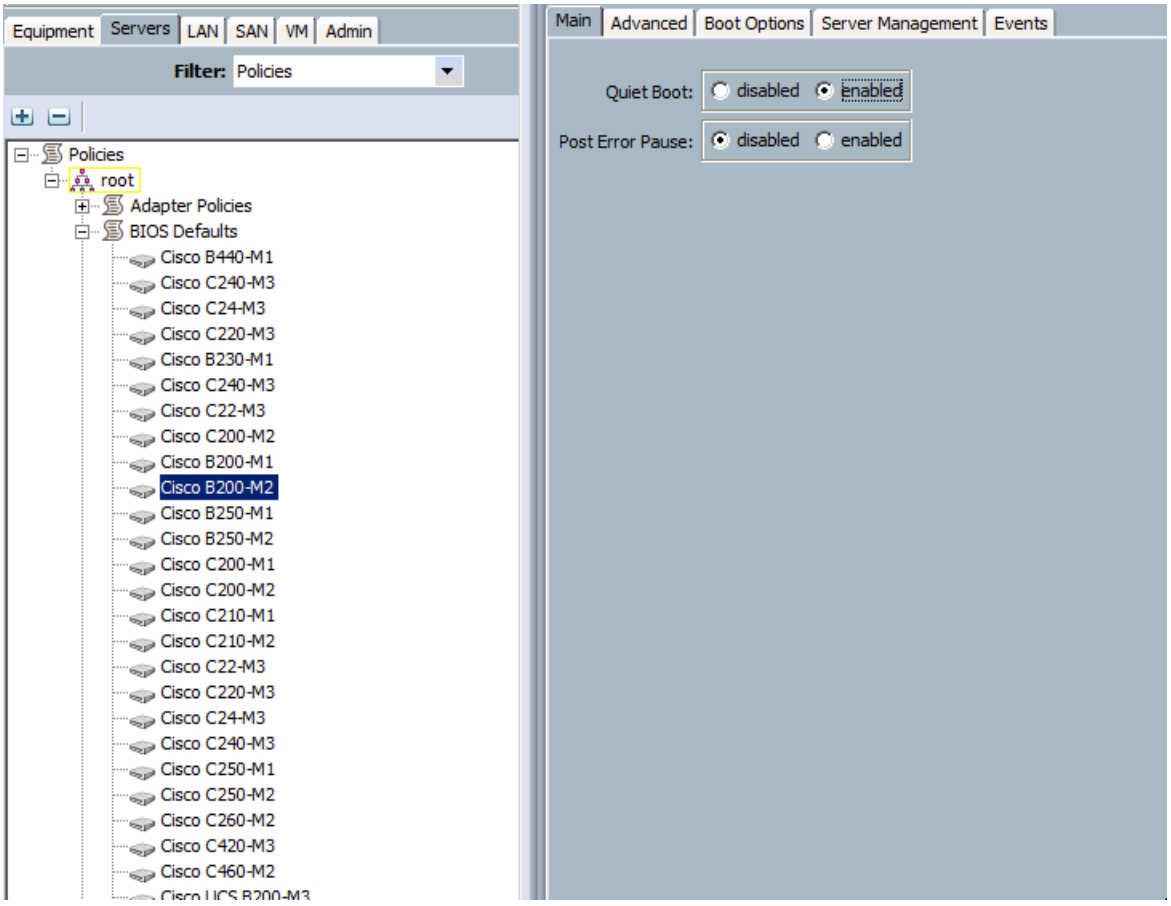
Complete these steps:

Step 15 Log into Cisco UCS Manager if necessary.

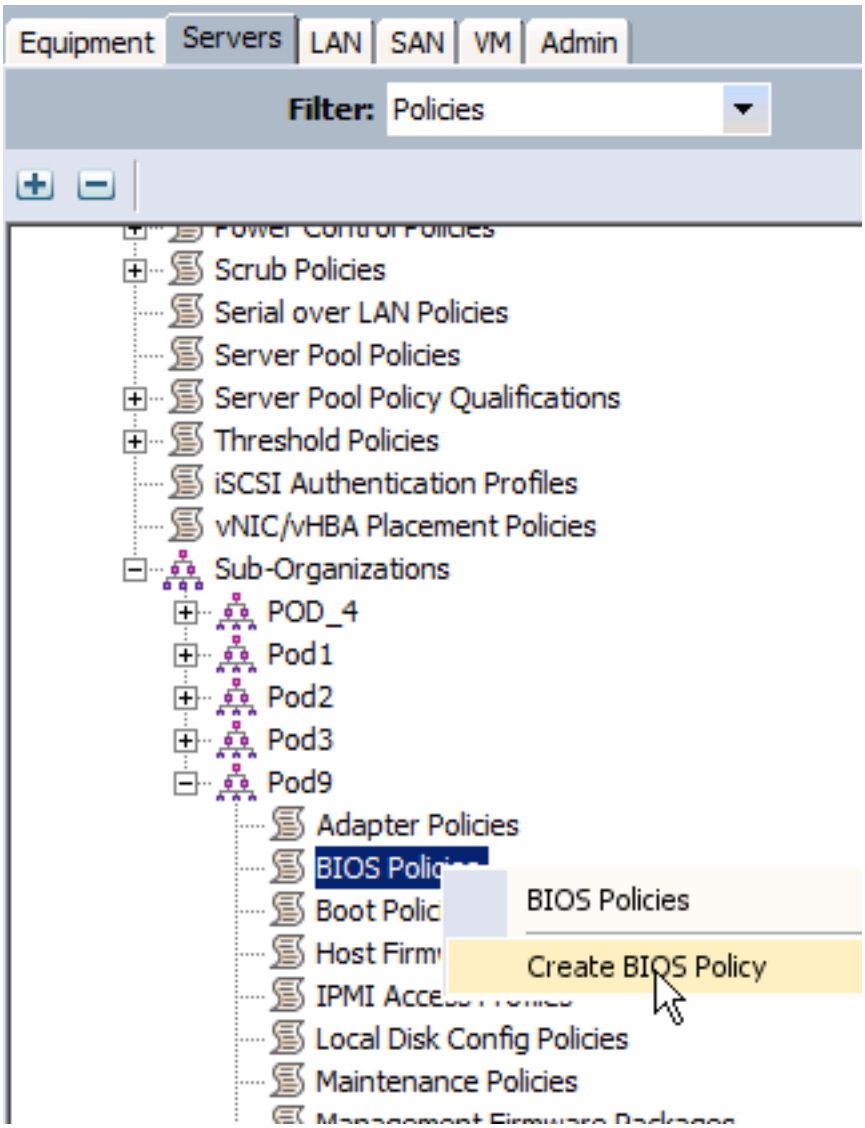
Step 16 In the navigation pane, choose the **Servers** tab. It may be helpful to set the **Filter** field to **Policies** for the following steps.



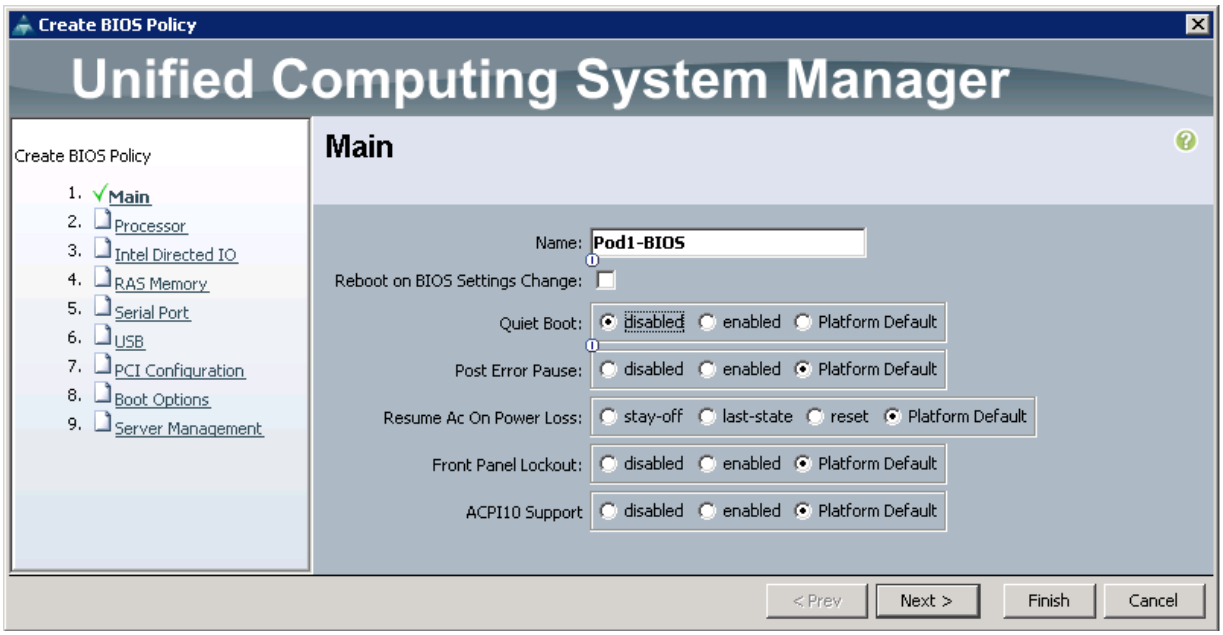
Step 17 Note there is a "BIOS Defaults" section ONLY in the root organization. Expand and select any Server. The right pane shows the "platform-default" settings, these will be used if NO BIOS-Policy is created. **Do NOT change any values!**



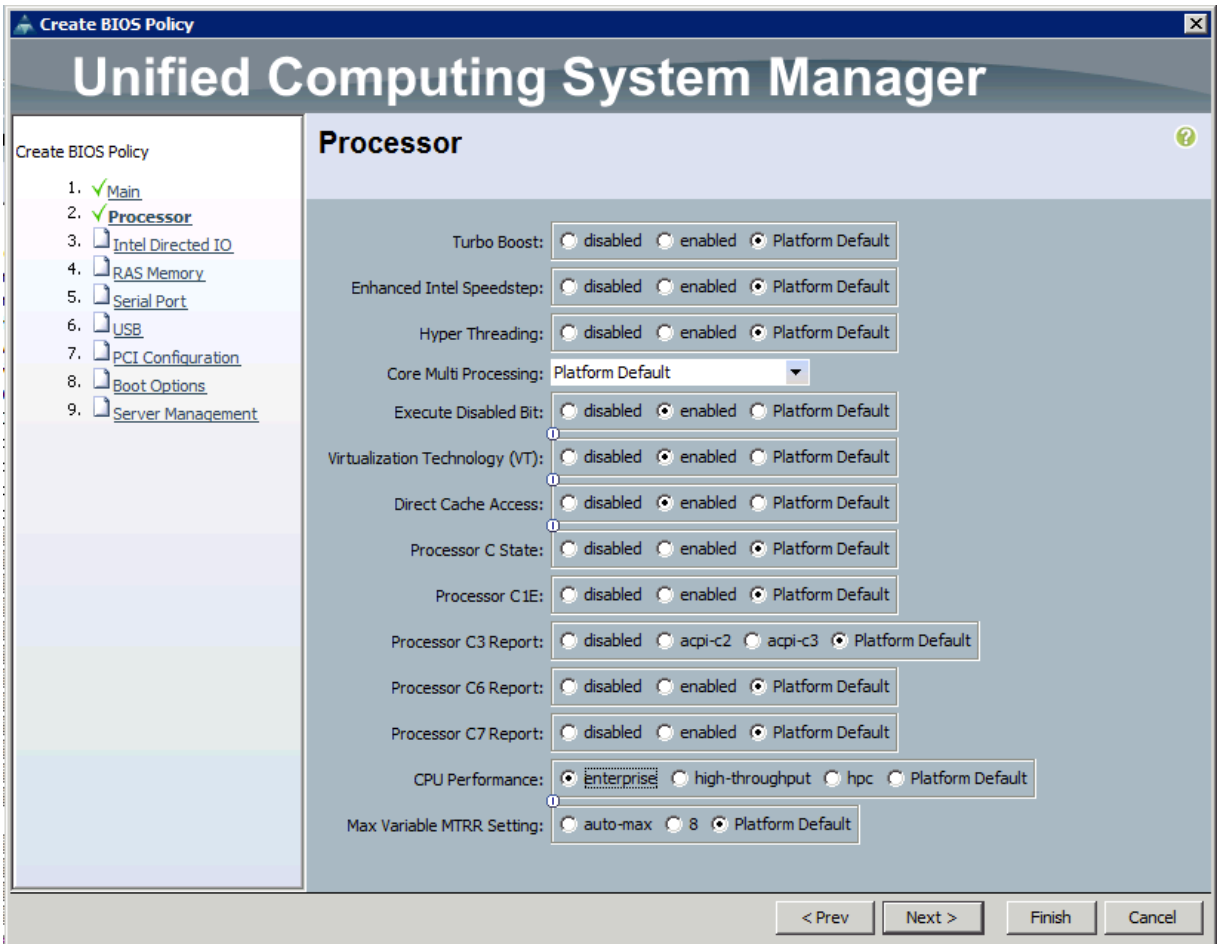
Step 18 Navigate to your Organization and right-click “BIOS polices” to create a new BIOS policy



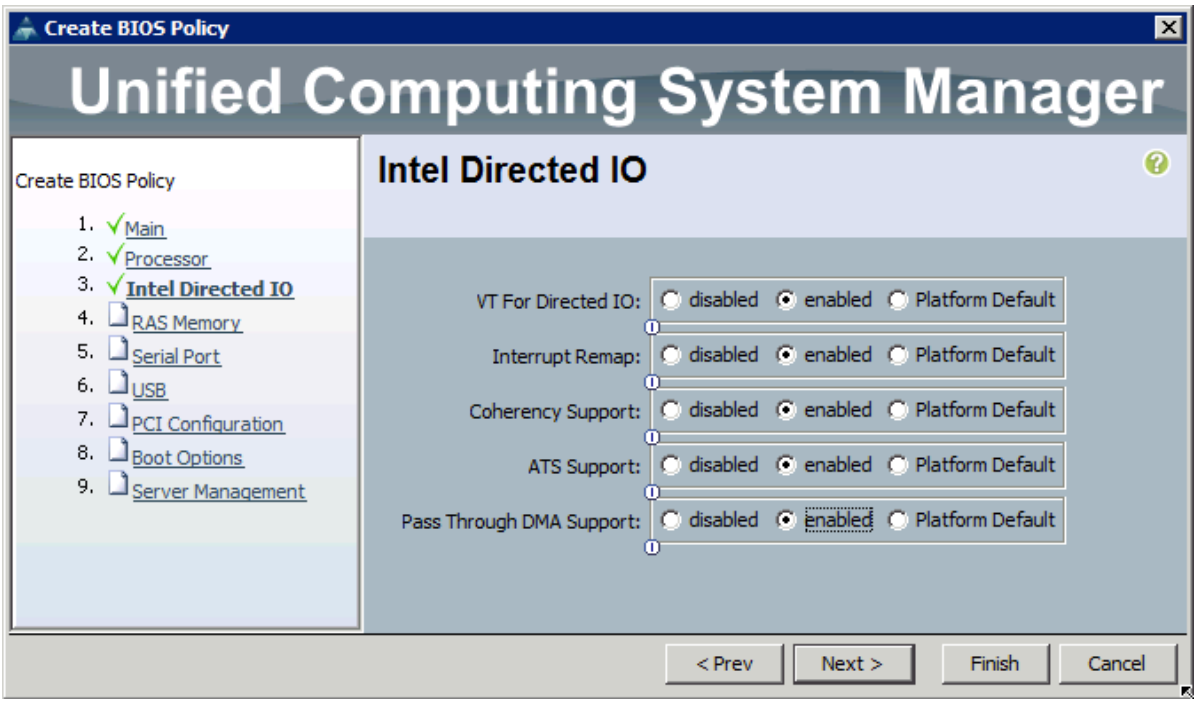
Step 19 Note this Wizard offers a LOT of options for all kinds of available servers. Name the BIOS policy and turn OFF quiet boot on the first page (“Main”). Note the default setting is “platform-default”, which we just reviewed.



Step 20 Turn ON VT support, "Direct Cache Access" and "Execute Disabled Bit" on the second page ("Processor").



Step 21 Turn ON ALL VT-directed IO features on the third page (“Intel directed IO”).



Step 22 Click “Finish” or review the remaining pages.

Task 6: Create a Boot Policy

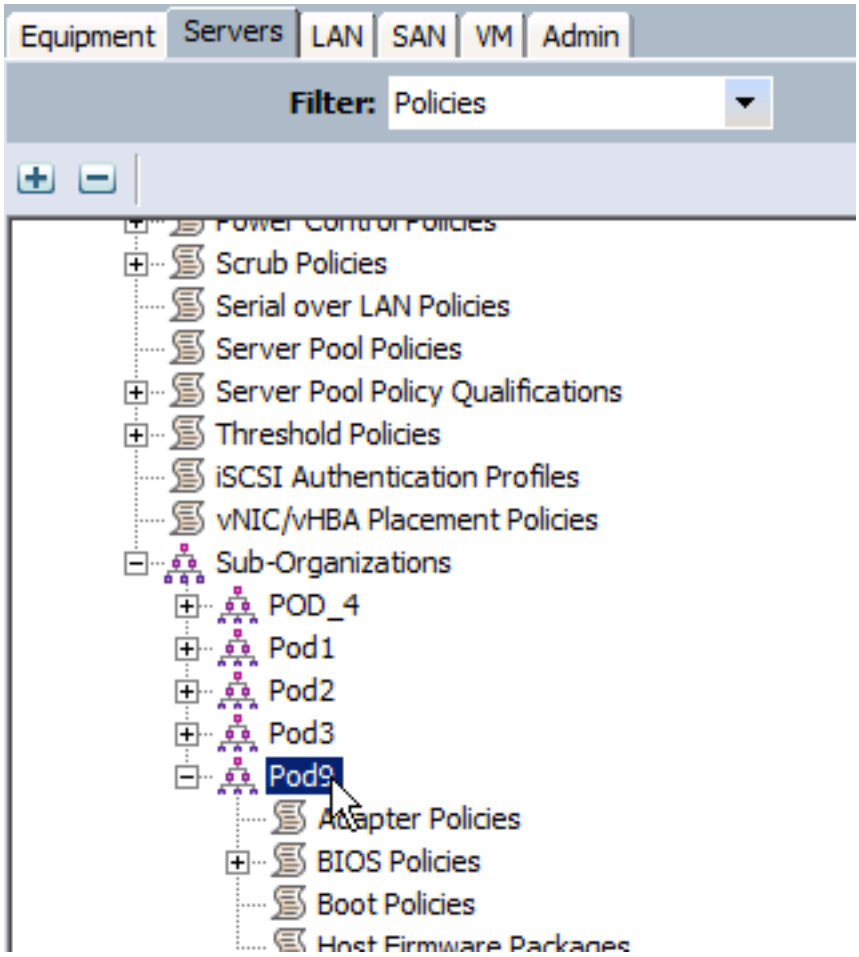
In this task, you will create a policy for SAN boot.

Activity Procedure

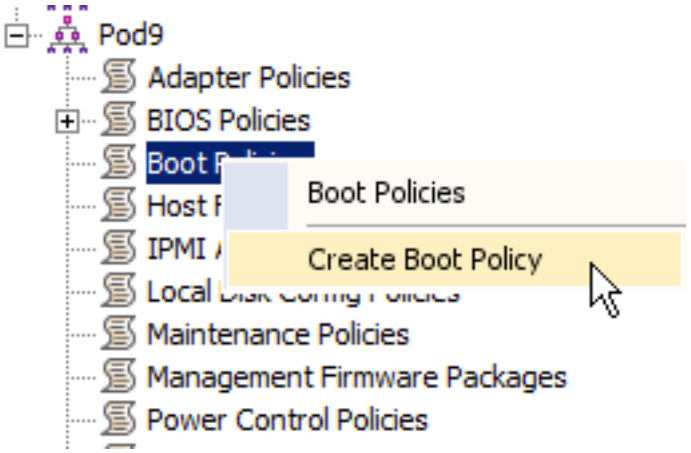
Complete these steps:

Step 1 Log into Cisco UCS Manager if necessary.

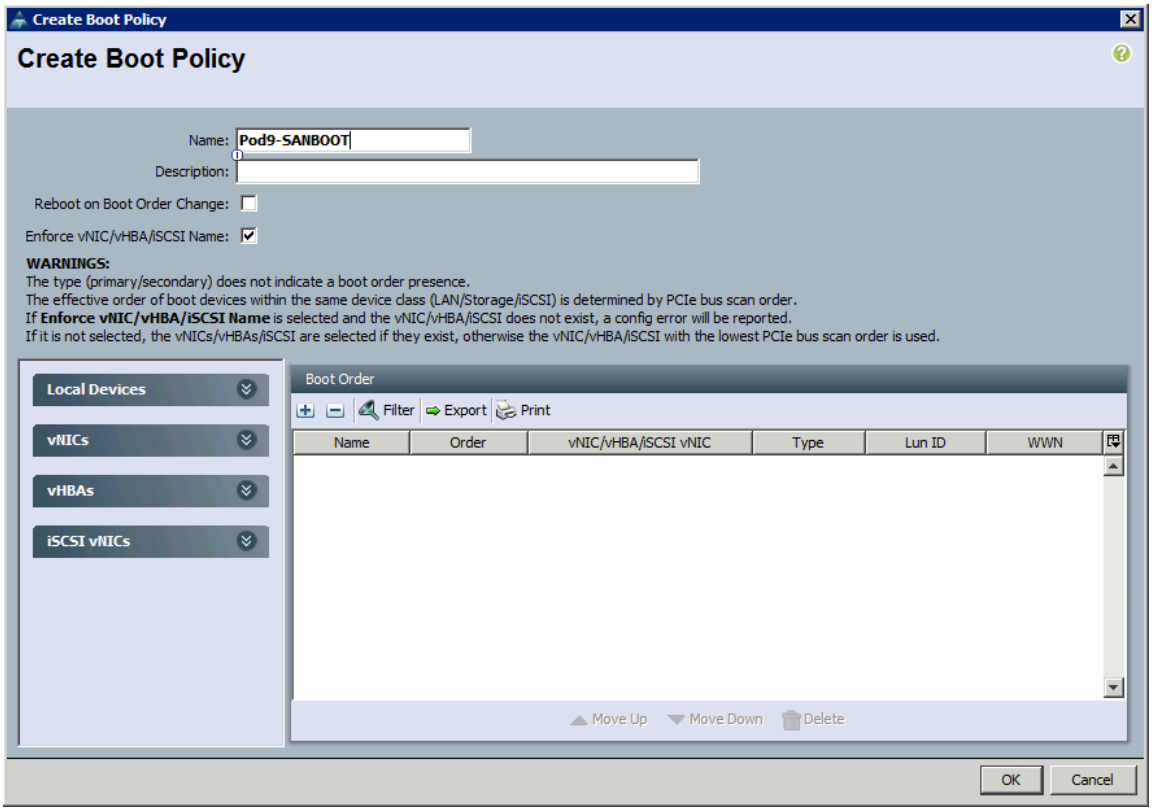
Step 2 In the navigation pane, choose the **Servers** tab. It may be helpful to set the **Filter** field to **Polices** for the following steps.



Step 3 Expand your organization and right-click “Boot Polices” to create a new Boot Policy



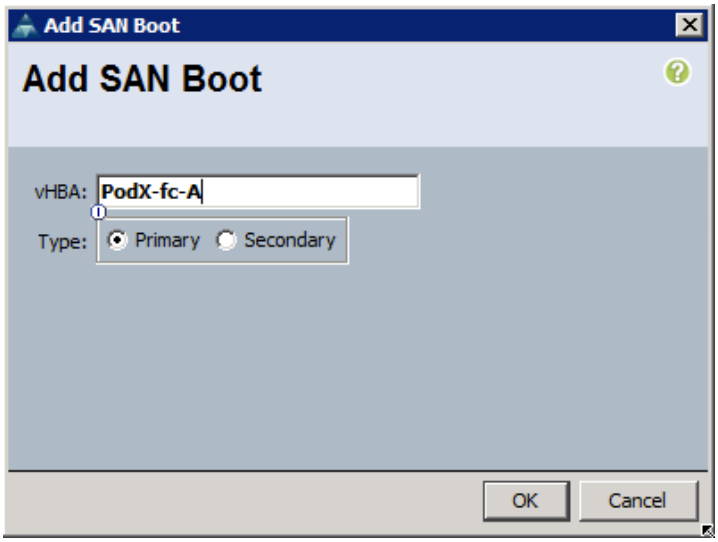
Step 4 Name your Boot Policy "PodX-SANBOOT" (X is your Pod#) and add a description if you want



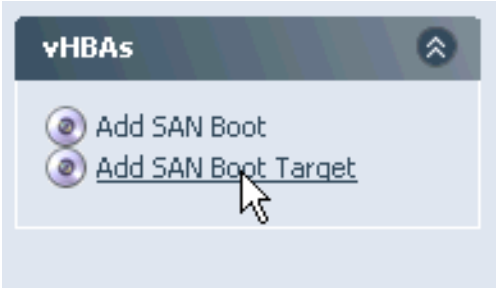
Step 5 Expand "local devices" and click "add CD-ROM" (this will be used for installation

Step 6 Expand "vHBAs" and click "add SAN Boot"

Step 7 Add "Pod#-fc-A" as the primary SAN Boot target (please note the name must match the case-sensitive vHBA name by default) – # is your Pod#

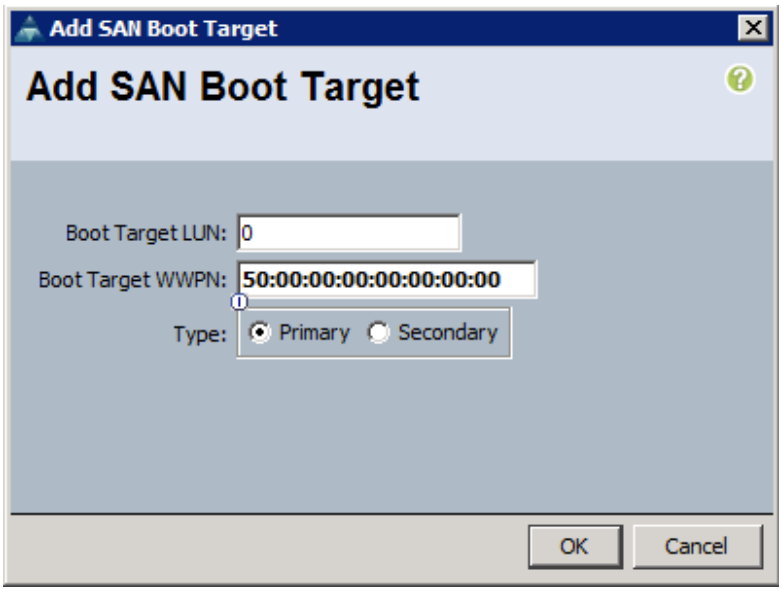


Step 8 Click “add SAN Boot Target” to add SAN boot target

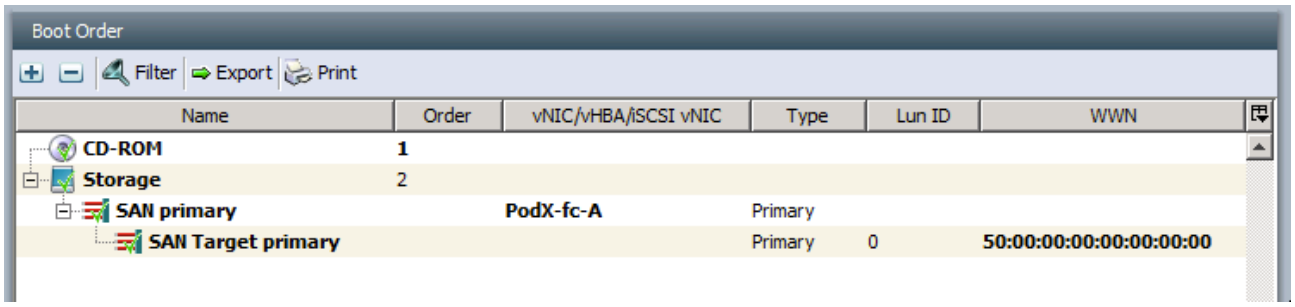


Step 9 Enter LUN 0 and use the table below to find the NetApp WWPN for your lab. Ask the instructor if unsure.
Using the wrong WWPN and/or LUN will result in boot and/or install failures.
NOTE THIS TABLE USES THE LAB ID, NOT THE POD#

Lab ID **NOT YOUR POD NUMBER!**	NetApp Storage PWWN in Fabric A
Lab 1	**50:0a:09:81:86:a9:fb:f1**
Lab 2	**50:0a:09:83:86:a9:fb:f1**
Lab 3	**50:0a:09:85:86:a9:fb:f1**
Lab 4	**50:0a:09:87:86:a9:fb:f1**
Lab 5	**50:0a:09:81:83:e1:00:86**
Lab 6	**50:0a:09:83:83:e1:00:86**
Lab 7	**50:0a:09:85:83:e1:00:86**



Step 10 Check your configuration, it should look like this.



Task 7: Create an updating Service Profile Template

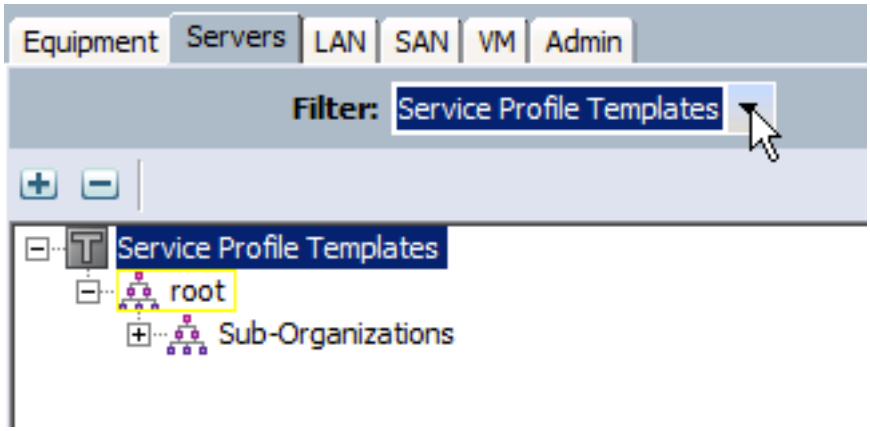
In this task, you will create a service profile template.

Activity Procedure

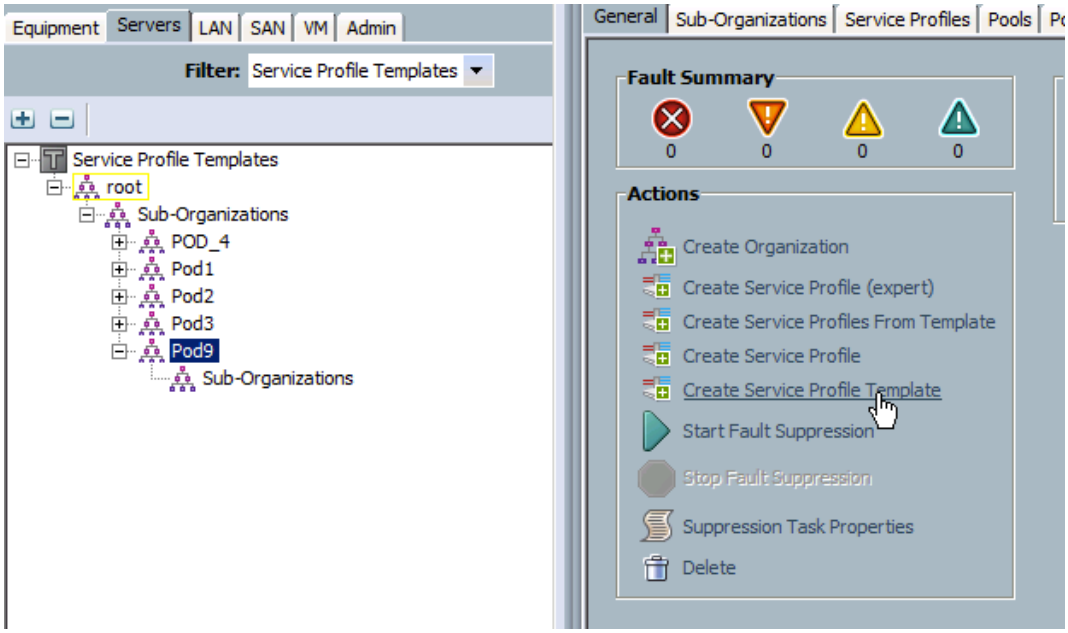
Complete these steps:

Step 1 Log into Cisco UCS Manager if necessary.

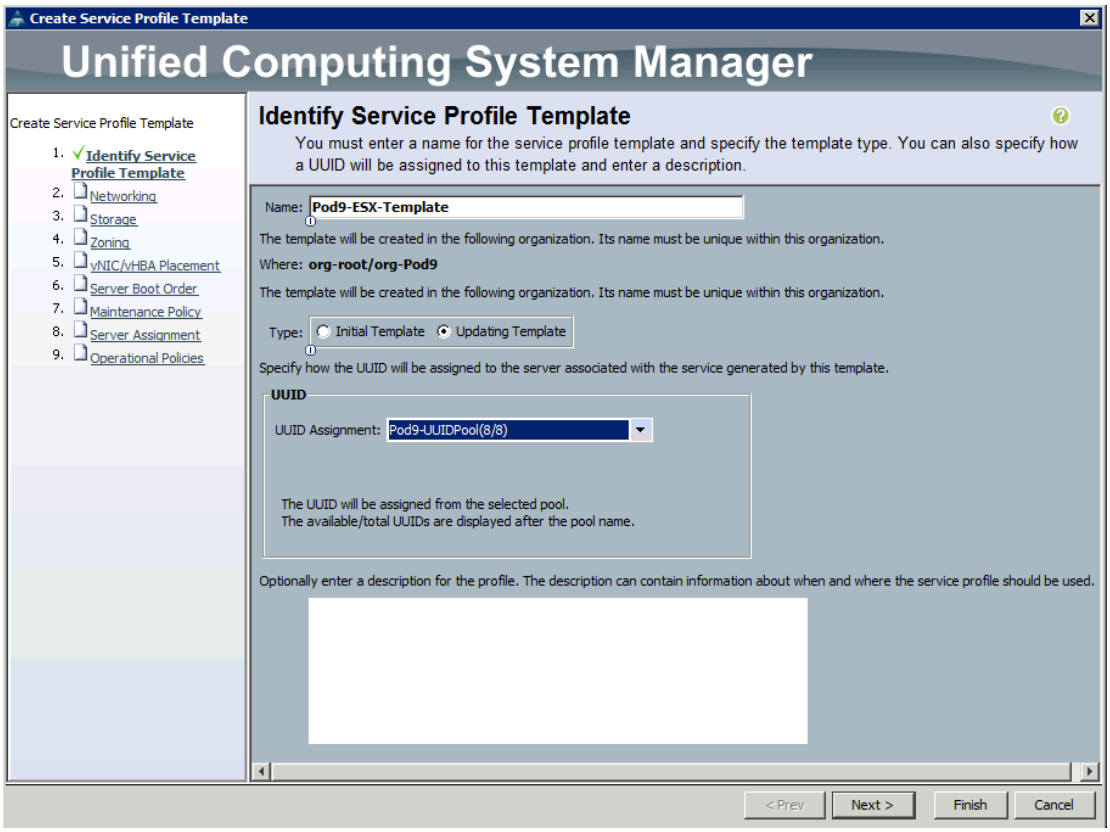
Step 2 In the navigation pane, choose the **Servers** tab. It may be helpful to set the **Filter** field to **Service Profile Template** for the following steps.



Step 3 Select your Organization and **Create Service Profile Template** on the Actions Pane. (you could also use the context menu)

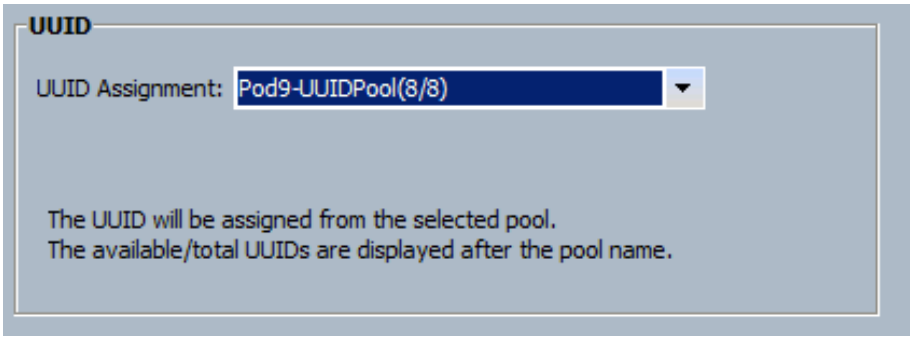


Step 4 Name your Template “Pod#-ESX-Template” (the # is your Pod#)

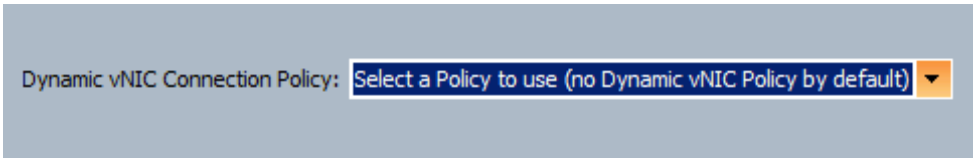


Step 5 Make sure you create an updating template

Step 6 Select your Pod UUID-Pool and click “Next>”



Step 7 Do NOT select any Dynamic vNIC.

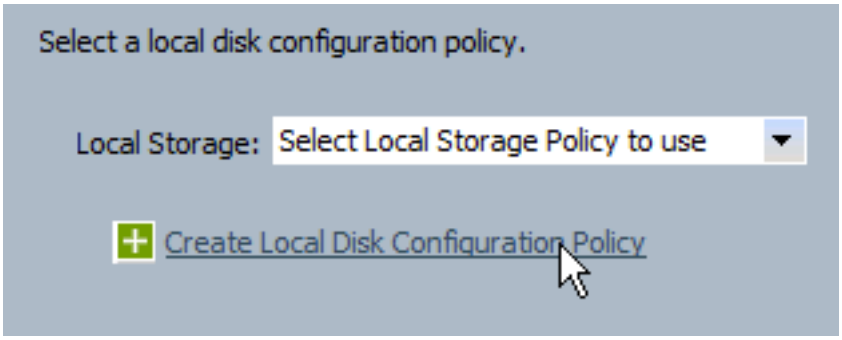


Step 8 Select “Use Connectivity Policy ” for LAN configuration

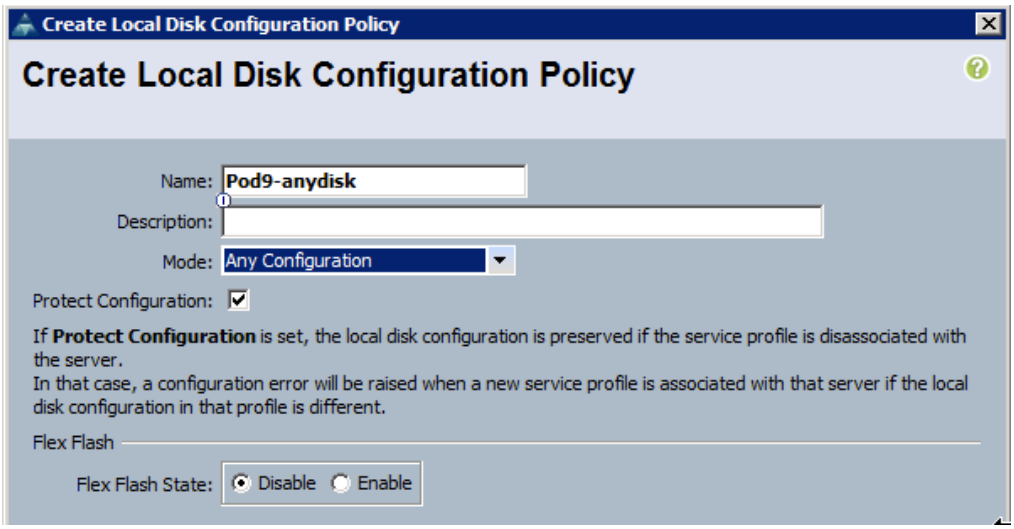
Step 9 Select the LAN Connectivity Policy you created earlier

Step 10 Click “Next>”

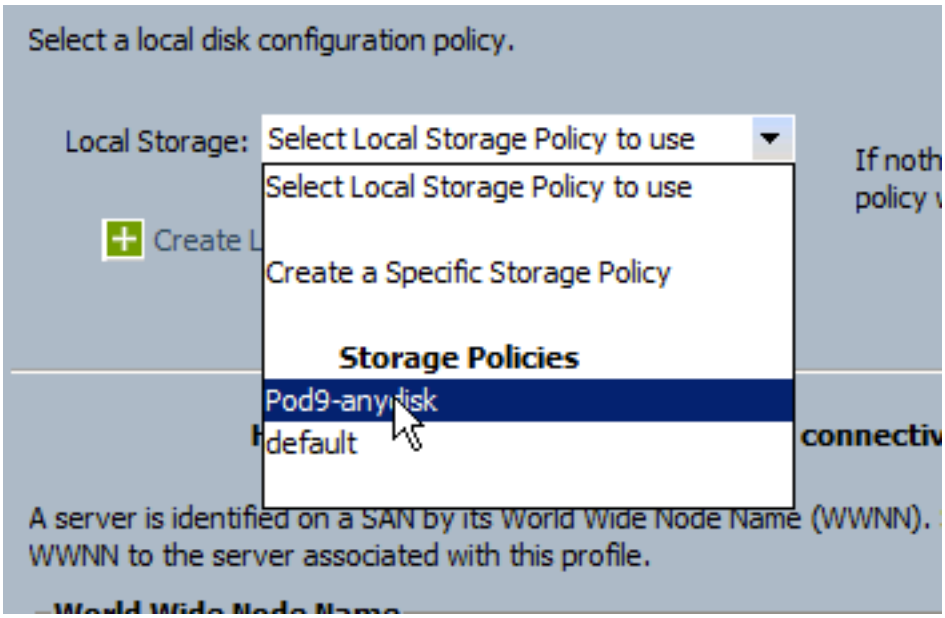
Step 11 Ooops, we haven’t created a local disk policy yet… but UCSM offers the opportunity to create new policies without exiting the wizard (and having to reconfigure)! Click “Create local Disk Configuration Policy”



Step 12 We don’t really care if there is a disk installed, so select “any configuration” for your Policy “PodX-anydisk” (X is your Pod# again), click OK when done.



Step 13 Do not forget to select the policy we just created ;)

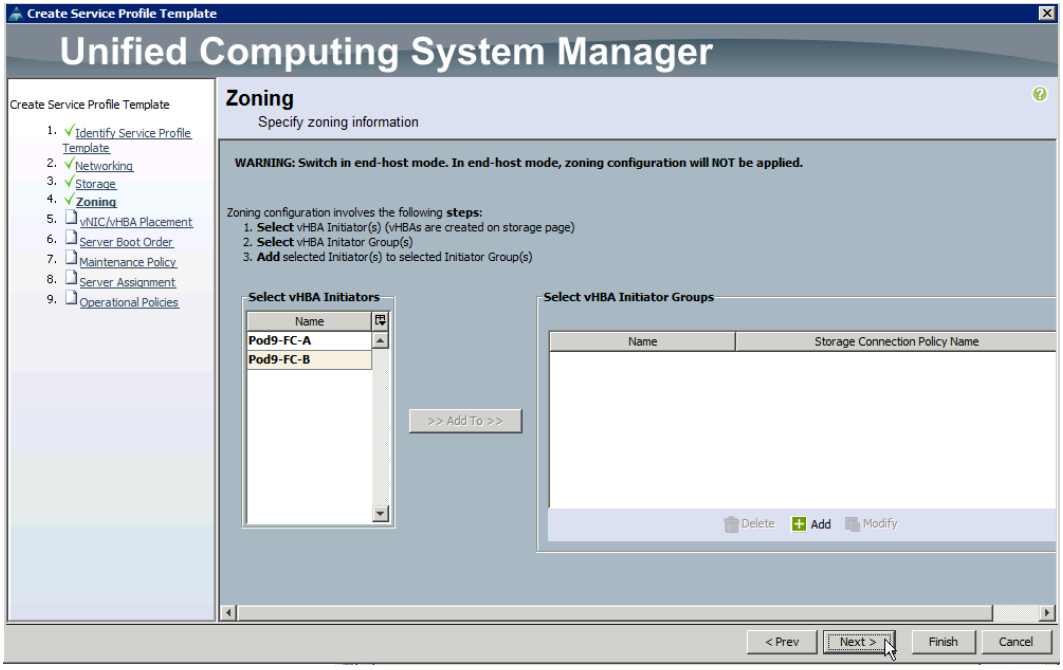


Step 14 Select "Use Connectivity Policy" for SAN

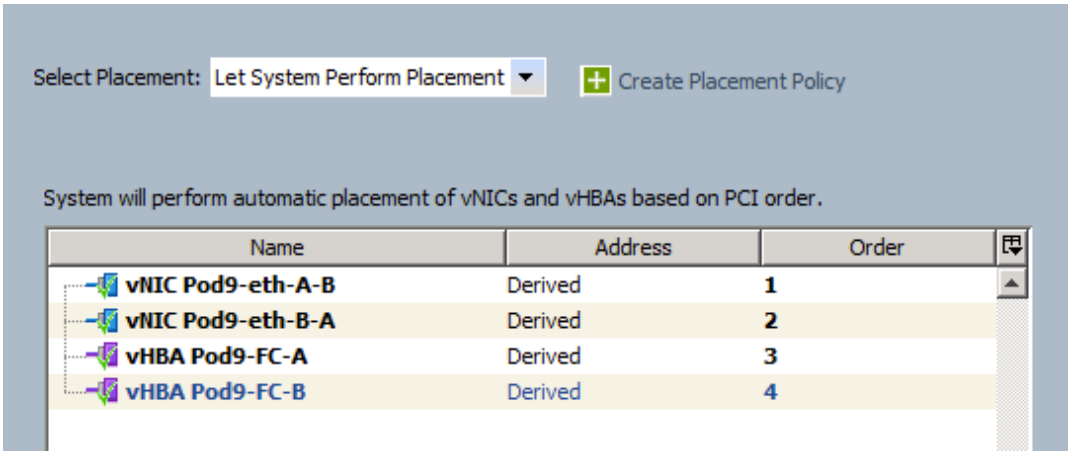
Step 15 Select the SAN Policy we created earlier.

Step 16 Click Next>

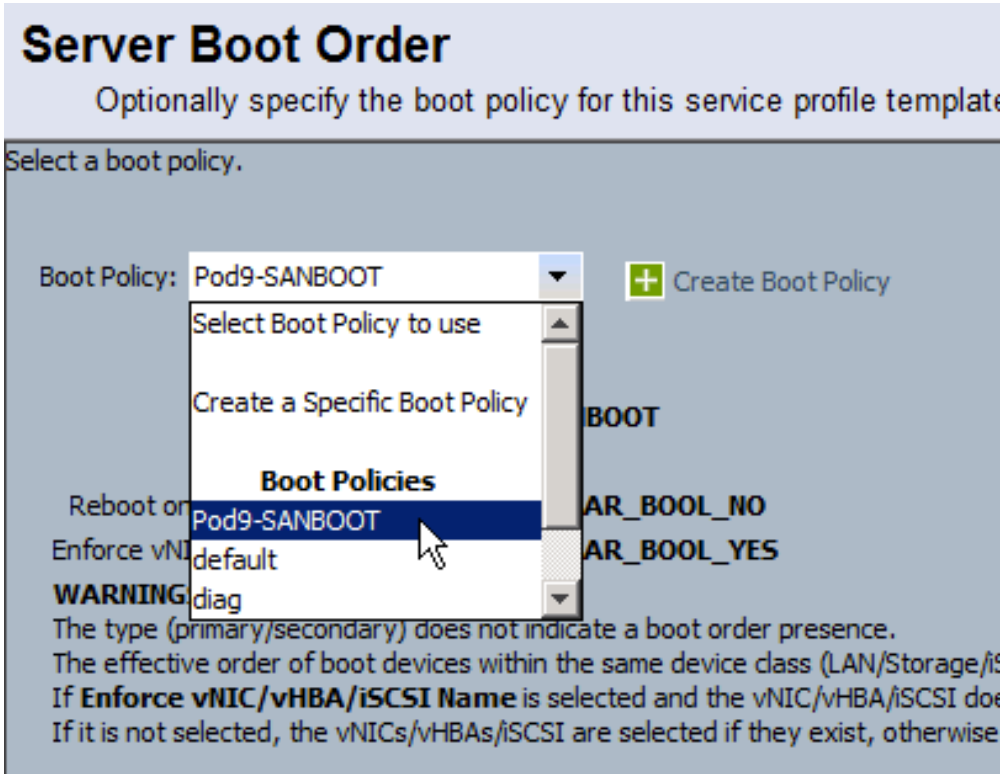
Step 17 Skip the Zoning configuration with "Next>" (Zoning is ONLY used in FC switching mode)



Step 18 Review the vNIC/vHBA placement configuration, don't change anything here. Click "Next>"

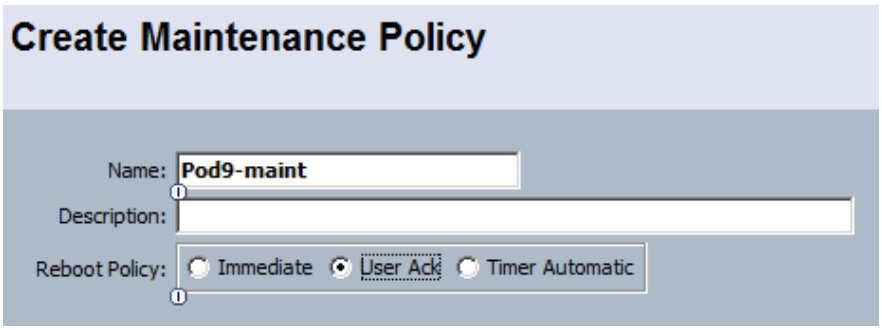


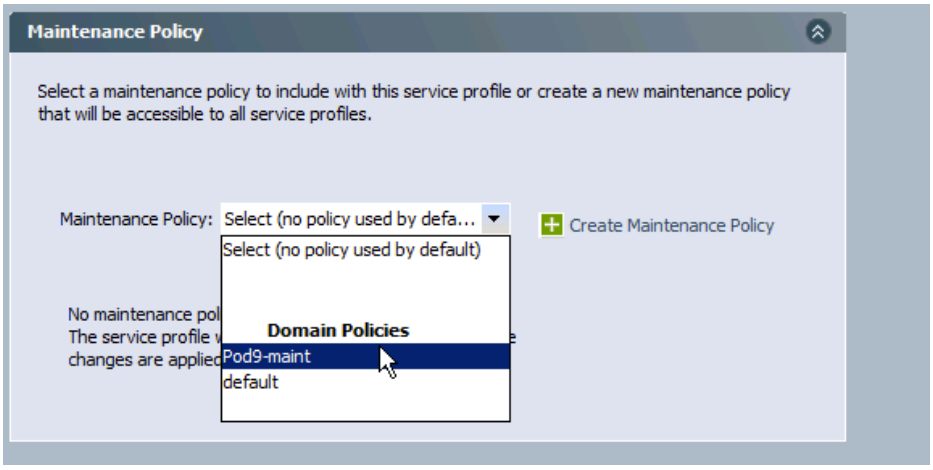
Step 19 Select the Boot Policy we created for SAN boot, review and click "Next>"



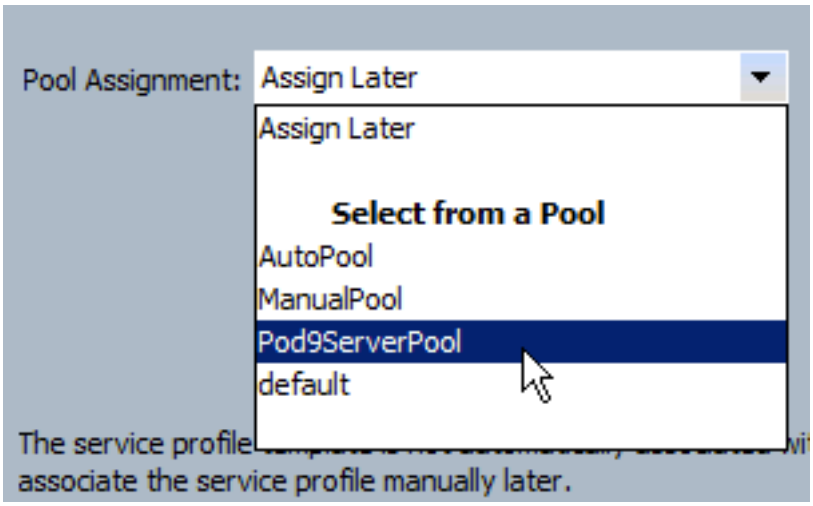
Step 20 We have not defined a maintenance policy. Some changes in templates/profiles require a reboot, by default the server is rebooted automatically to apply those changes. We certainly do NOT want that to happen to our ESXi server.

Step 21 Create a new maintenance policy named **Pod#-maint** , select "user-acknowledged" and apply it! **DO NOT forget to select the policy we just created!**

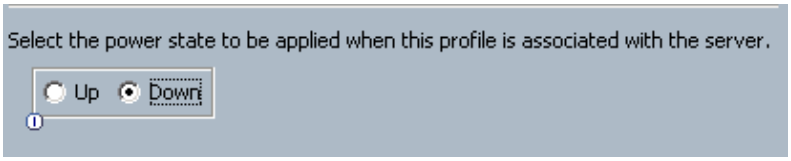




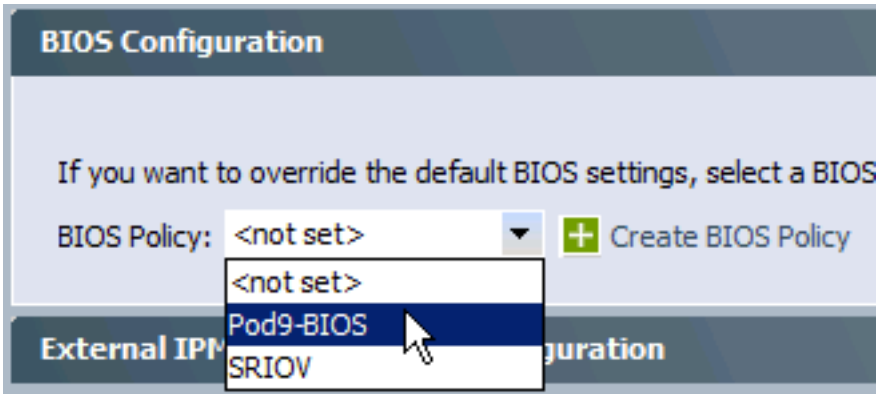
Step 22 Click "Next>". Select your Pods MANUAL Server pool.



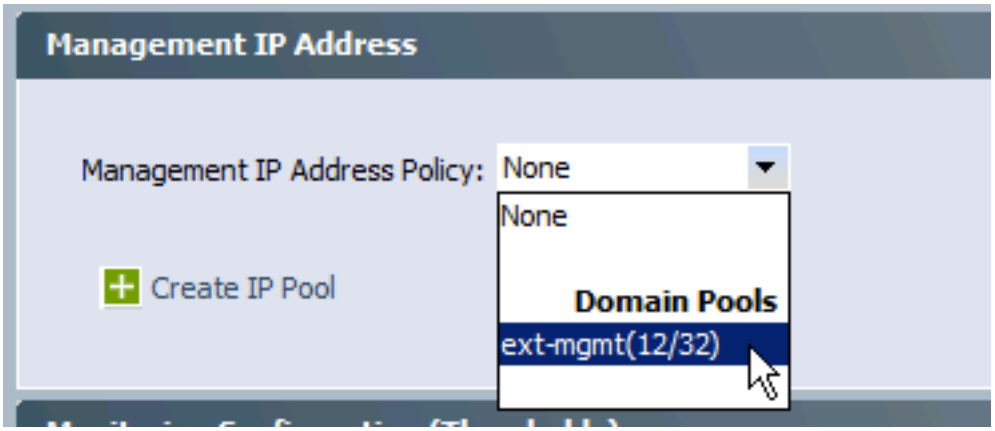
Step 23 Change the Power state to “down” (for the purpose of this lab), Click “Next>”



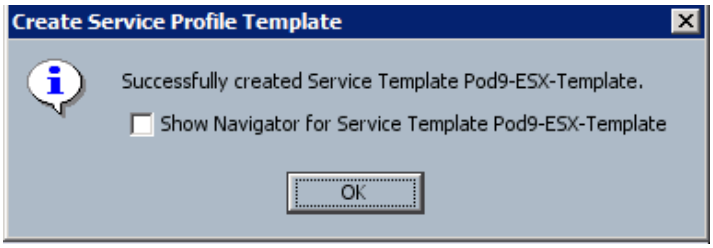
Step 24 Expand “BIOS policy” and assign the BIOS policy we created earlier



Step 25 Open “Management IP” and select the “Domain Pool”. This allows the management IP (for IPMI,SOL etc.) to move with the service profile)



Step 26 Click “Finish”



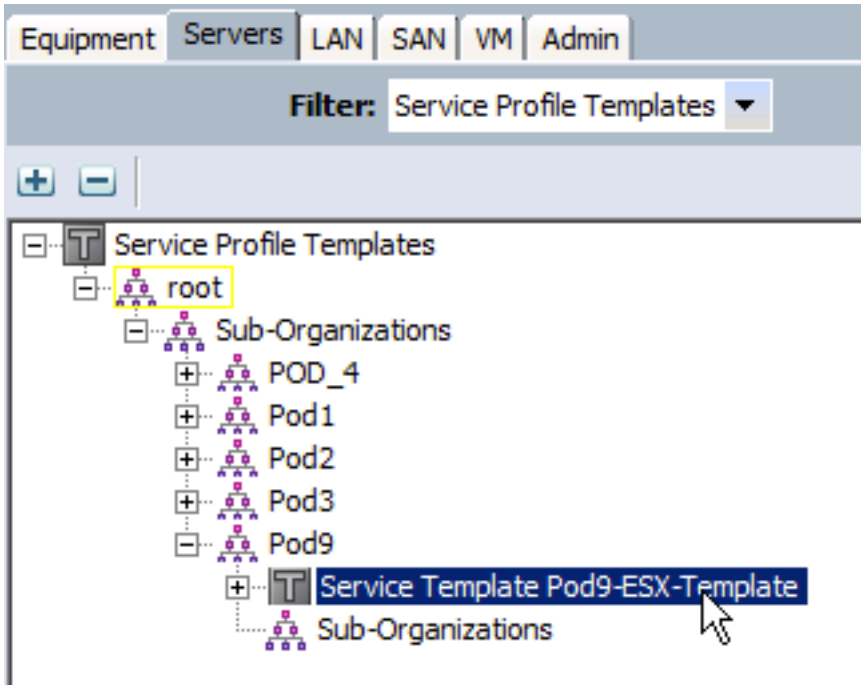
Task 8: Create a Mobile Service Profile from a Template

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

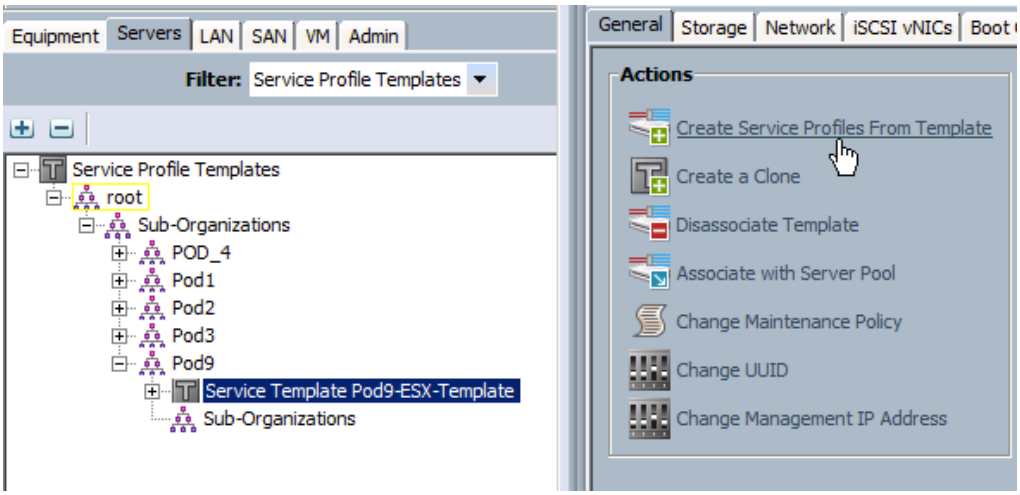
Activity Procedure

Complete these steps:

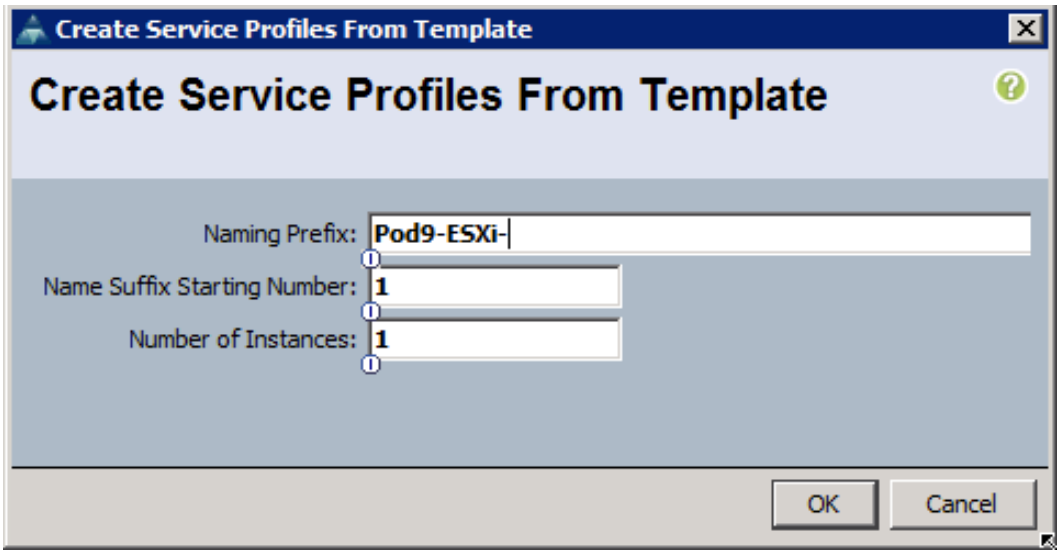
Step 1 In the navigation pane, choose the **Servers** tab. It may be helpful to set the **Filter** field to **Service Profile Template** for the following steps. (you could also use **Service Profile** and create from there…



Step 2 Select your Service Profile Template and click “Create Service Profiles from template”



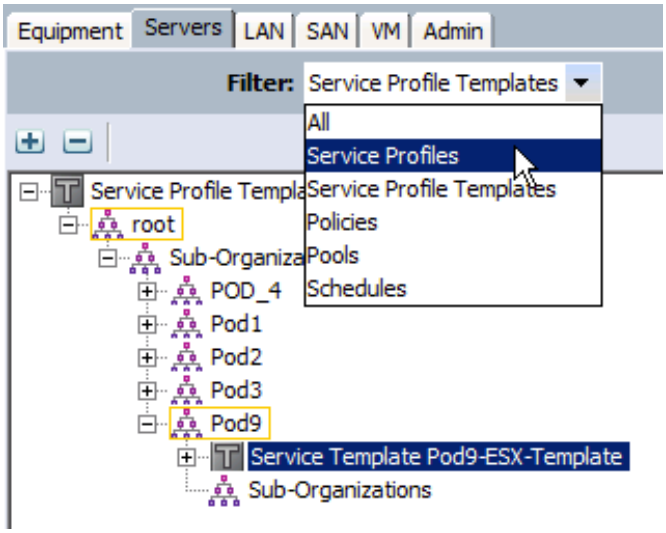
Step 3 Name your Profile Pod#-ESXi- (#is your Pod#) and create ONE profile starting from number 1.



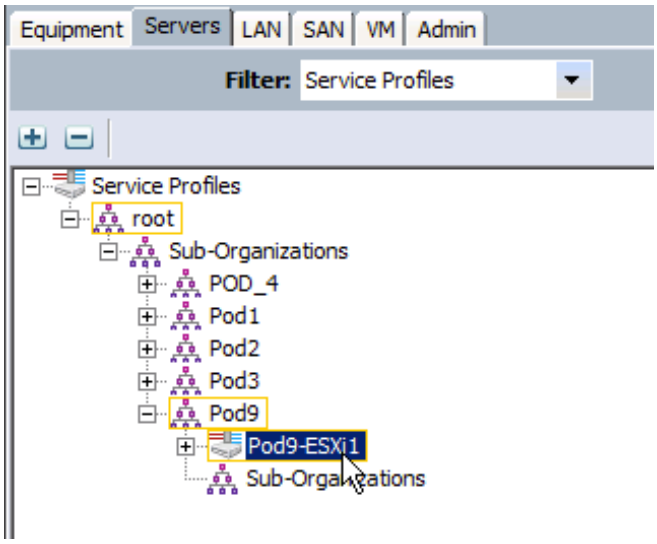
Note	Since every Pod has their own org we could use the same name.

Step 4 Click OK and you are done!

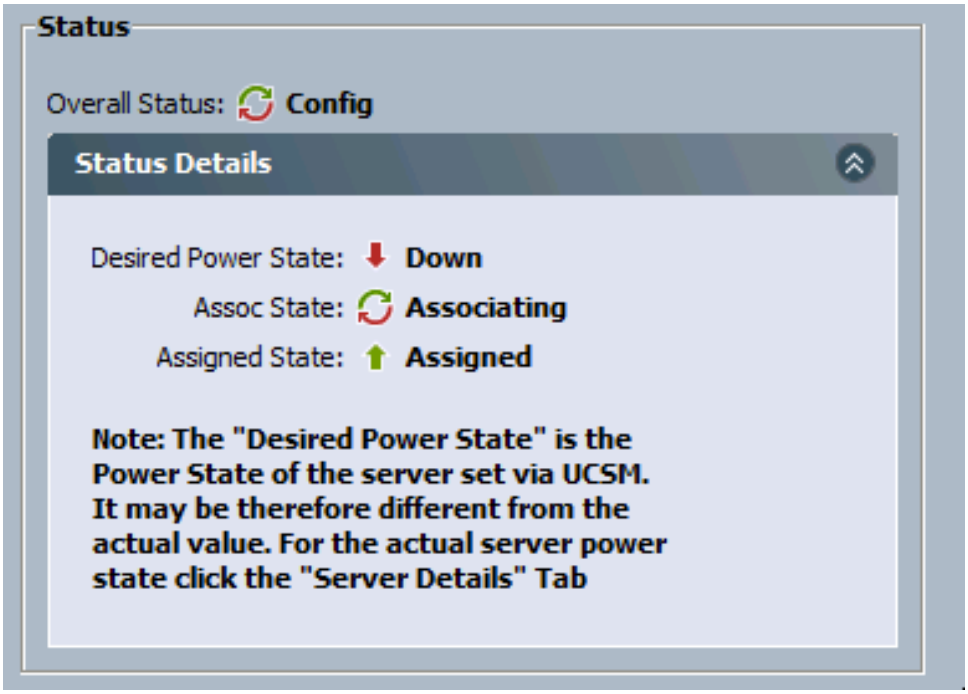
Step 5 Change the filter to “Service Profiles”



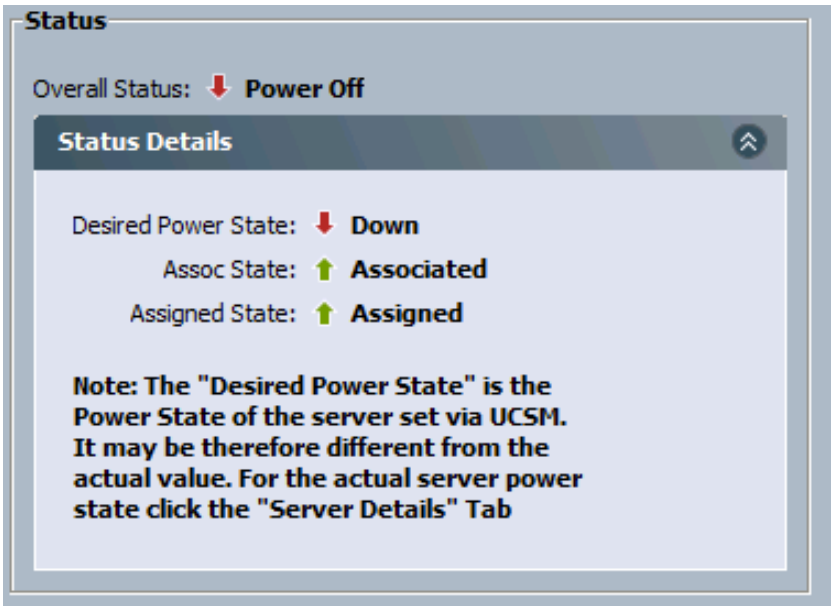
Step 6 Expand your Organization and select your newly created service profile



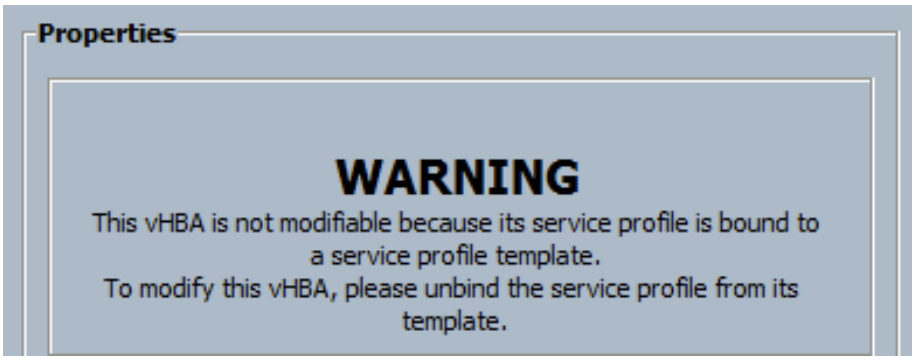
Step 7 **Check the state of the newly created Service Profile.**



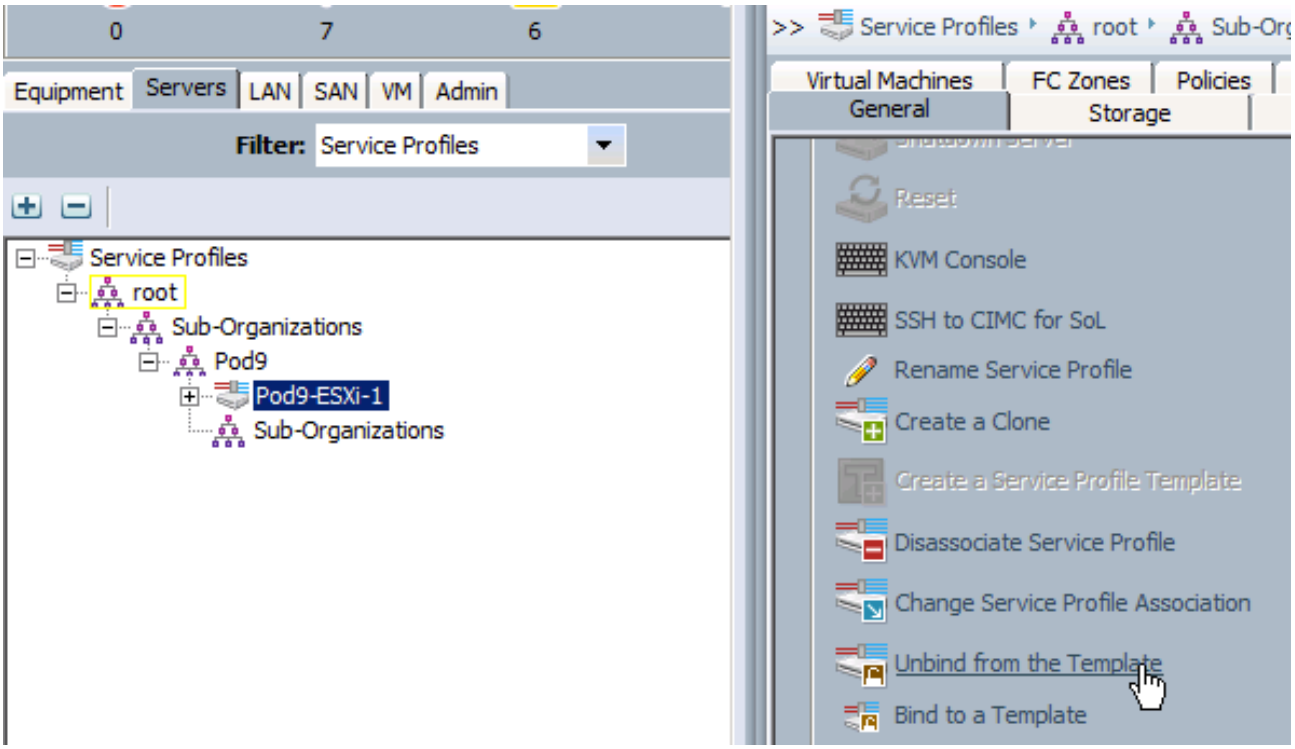
Step 8 Wait for your Service profile to be associated.



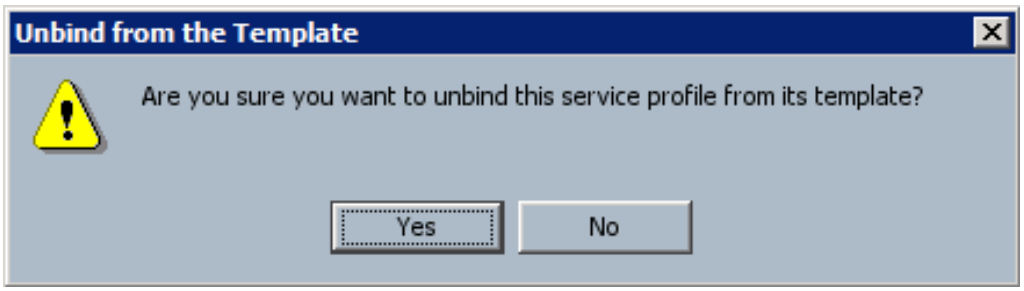
Step 9 If you try to change anything in your service profile you will notice all add/delete/modify buttons are greyed-out. This is because the Service Profile was created from a template.



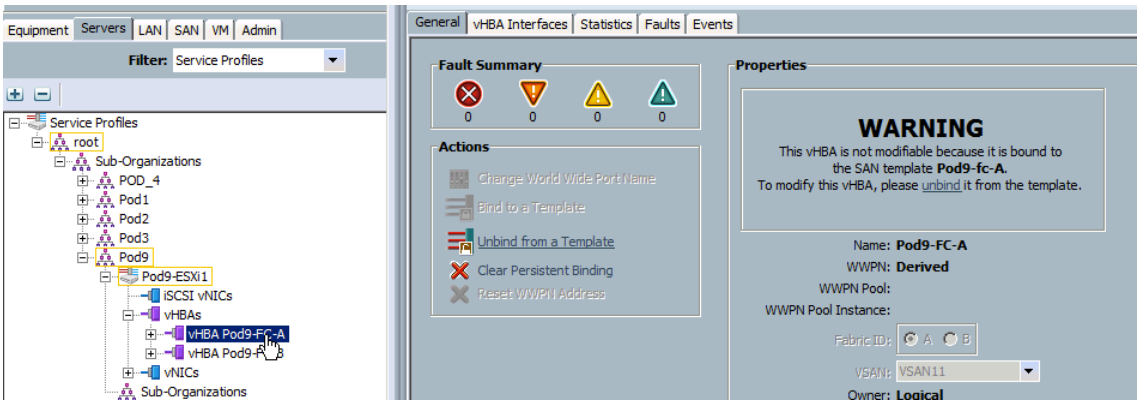
Step 10 Click “unbind” in the “General” of the Service Profile to remove the connection between the profile and the template.



Step 11 Acknowledge you really want to unbind the profile from the template.

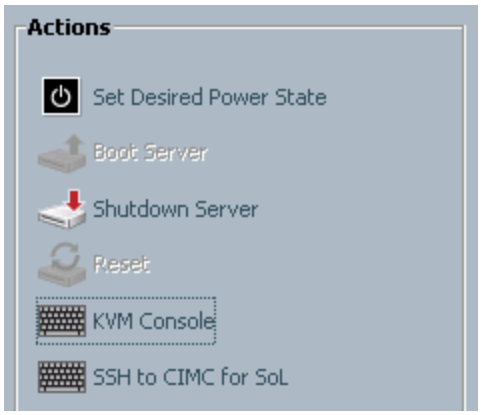


Step 12 If you try to change the vHBA settings for your first HBA and you'll notice the vHBA is still linked with the vHBA template.

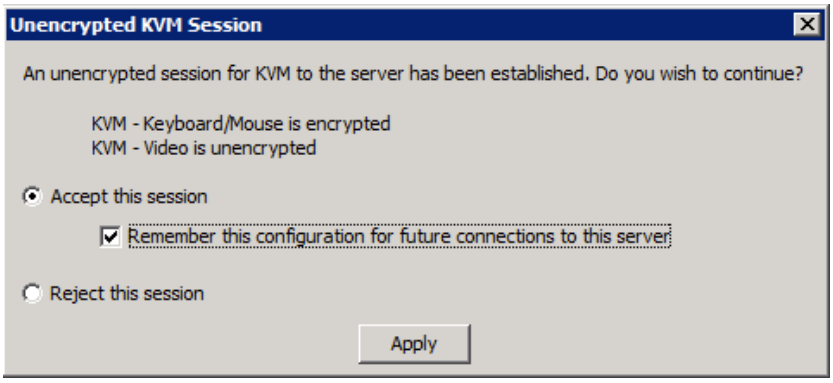


Step 13

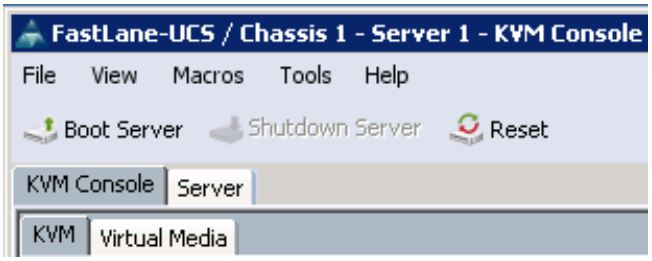
Step 14 Open KVM from the service profile actions box and confirm all following security warnings.



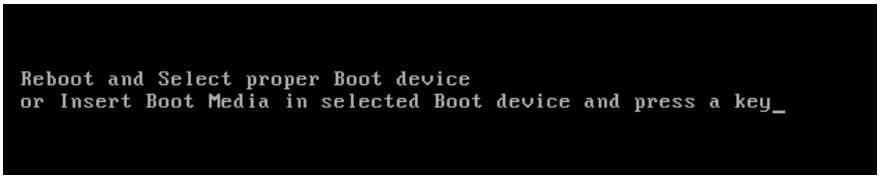
Step 15 Confirm unencrypted KVM video.



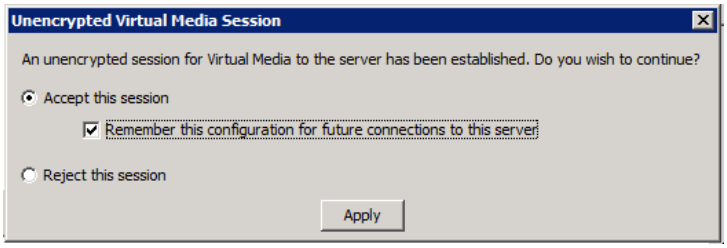
Step 16 You have to click the "Boot Server" Button in KVM (you can also use the action pane from the service profile) after the UUOS has been started

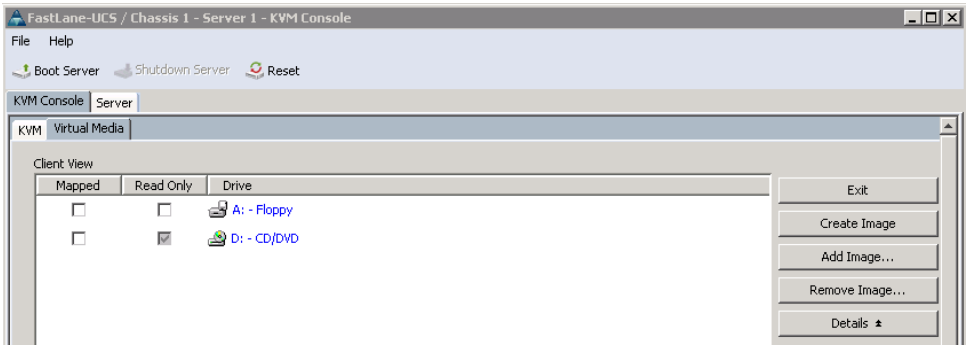


Step 17 After a "successful" boot (if you look carefully you can see the NetApp disk already) the server will complain about the missing OS. This may take a while and your server may reboot multiple times to apply all settings.

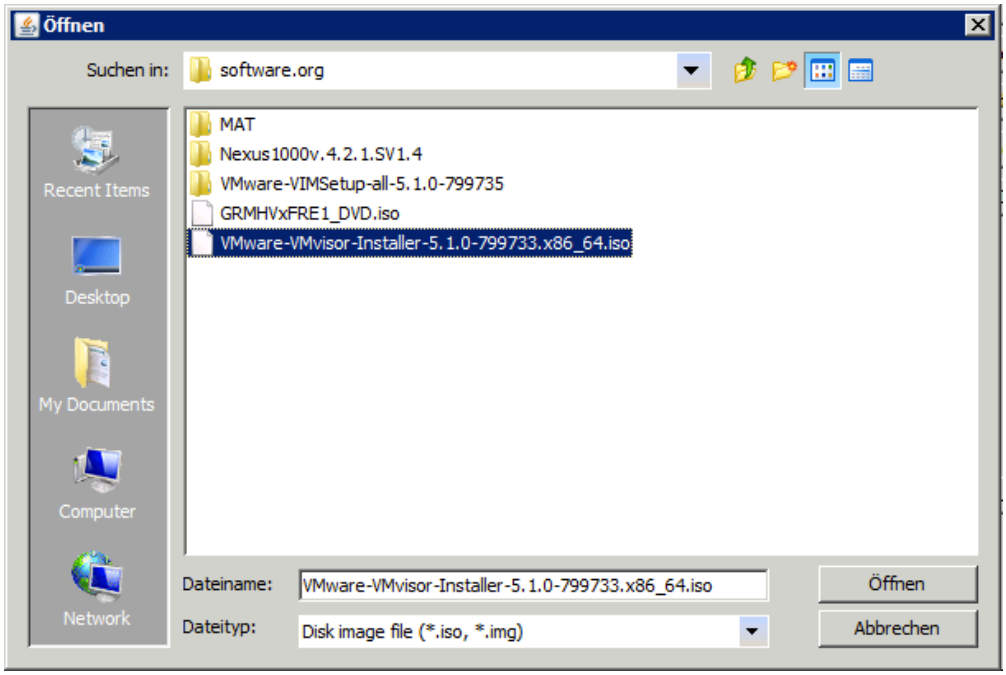


Step 18 We configured the Boot Profile to boot from CDROM, so let's insert a (virtual) CDROM… Open the Virtual Media Tab and confirm unencrypted transport for virtual media.

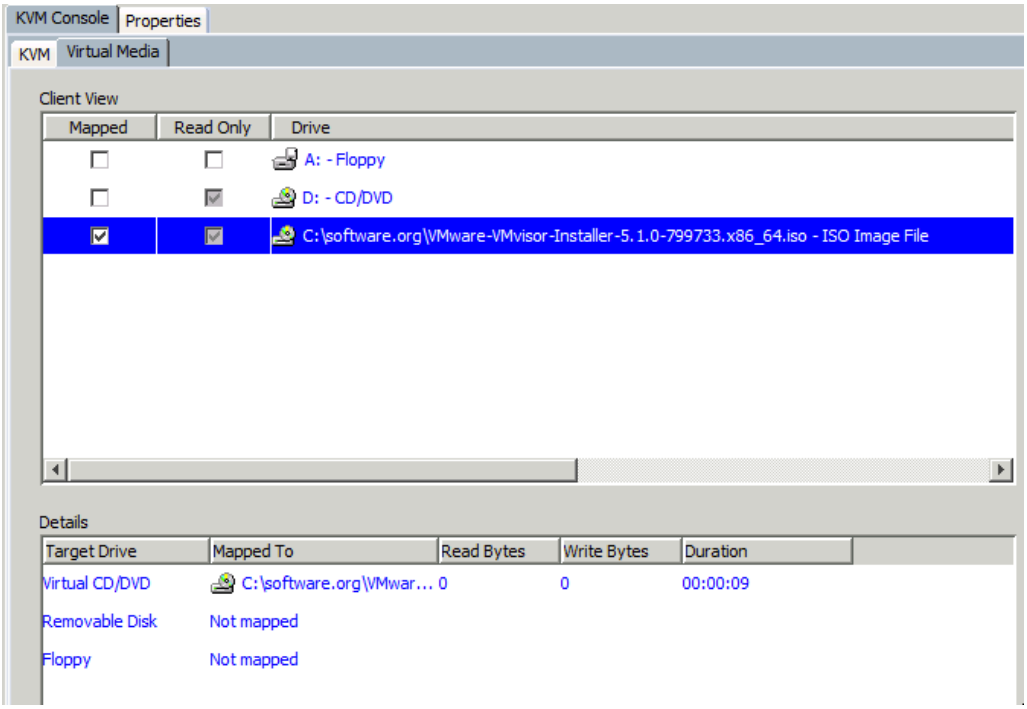




Step 19 Click “add Image”, navigate to c:/software.org and select the 5.1.0 VMVisor ISO file.



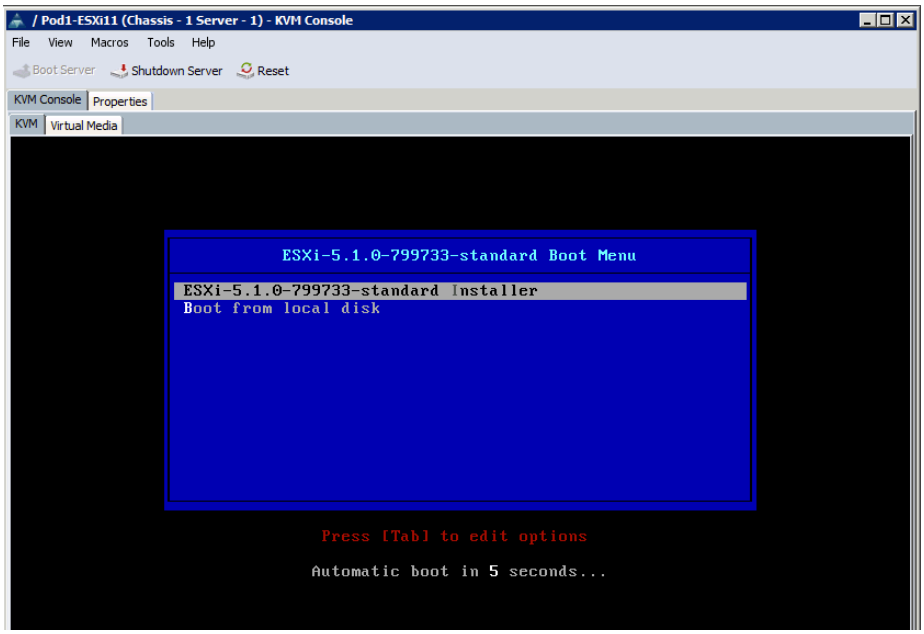
Step 20 Click the “mapped” checkbox to connect the virtual CD to the server..



Step 21 Click into the KVM window and press a key, ESXi install will boot from the virtual CDROM

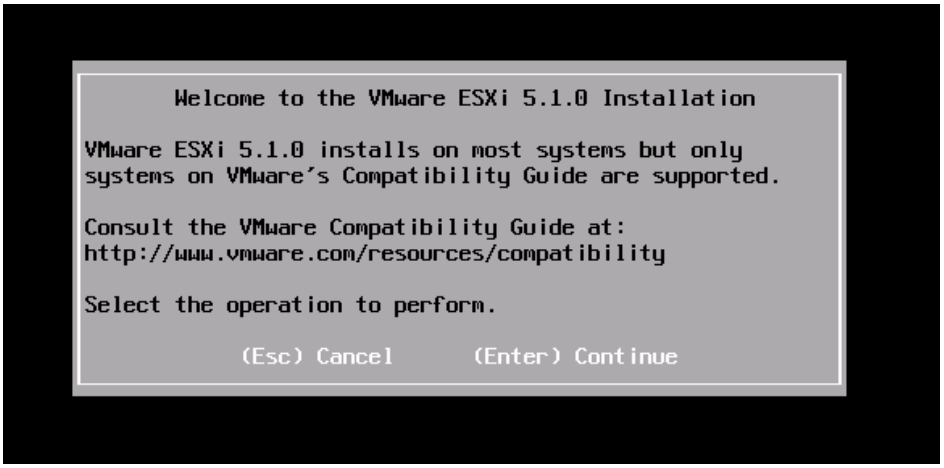
Note If the media is not recognized it may be necessary to reset the server.

Step 22 Press Enter to start installation

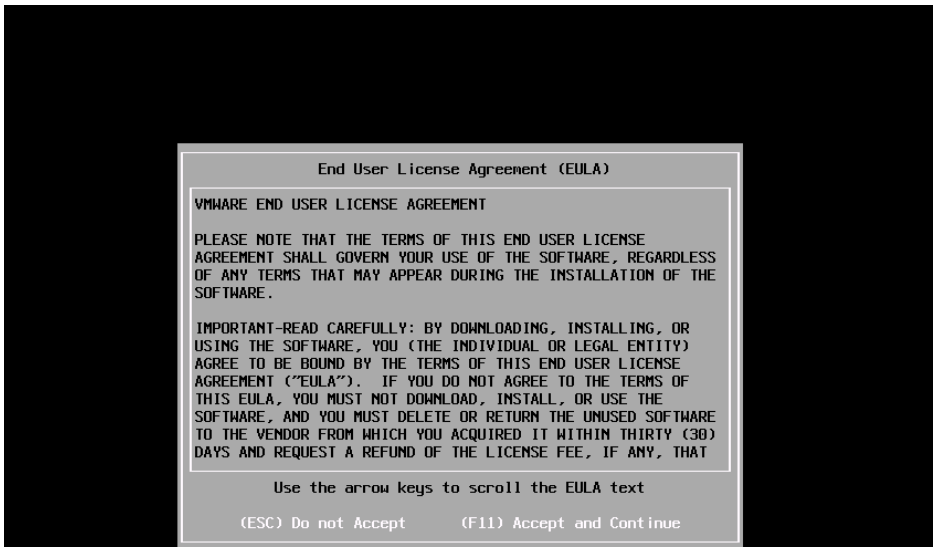


Step 23 Wait for the ESXi installer to fully load.

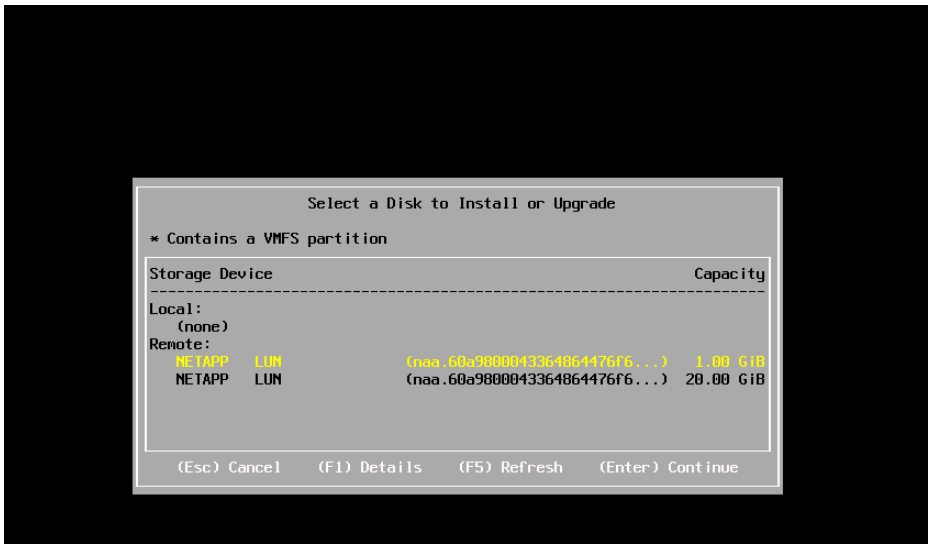
Step 24 Press Enter to start the installer.



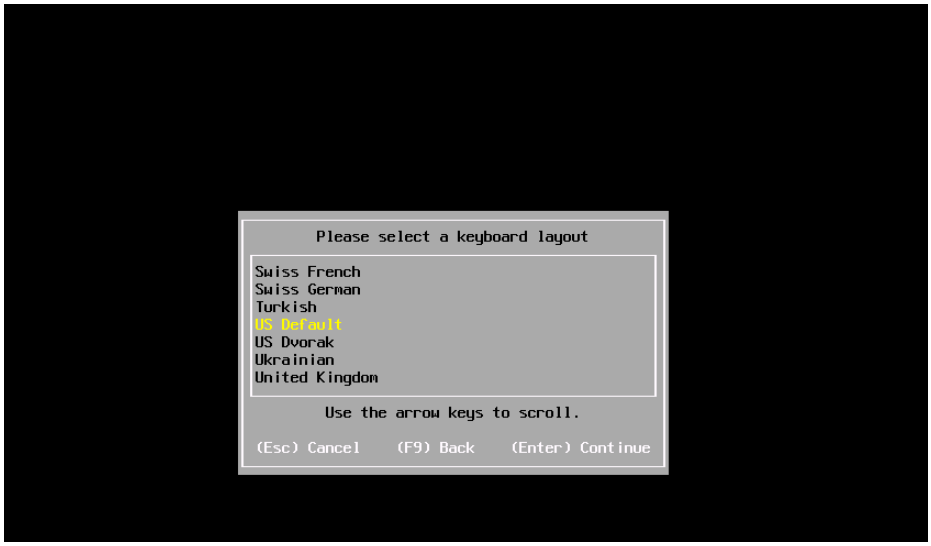
Step 25 Press F11 to accept the EULA



Step 26 Select the **1GB NETAPP Disk** for Installation, **DO NOT USE THE 20GB DISK or the local HDD if one is installed**.

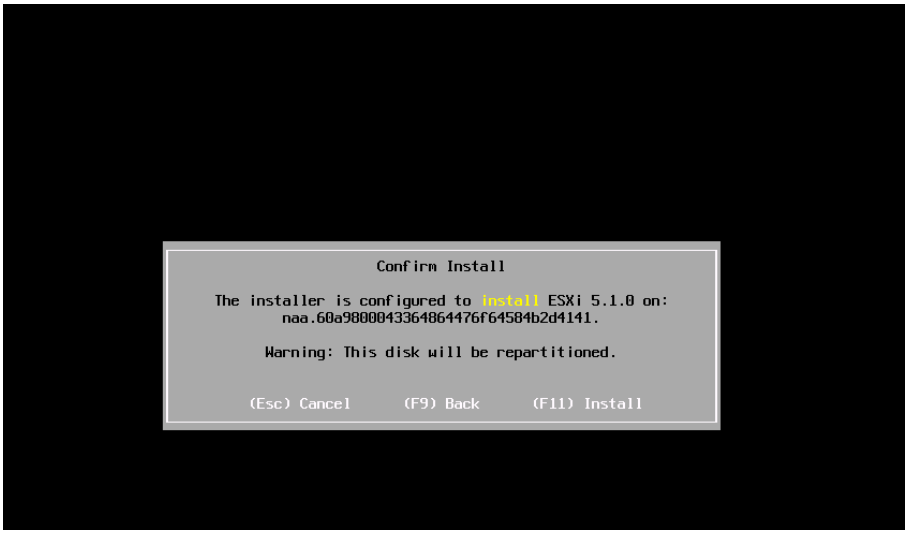


Step 27 Select your local keyboard layout



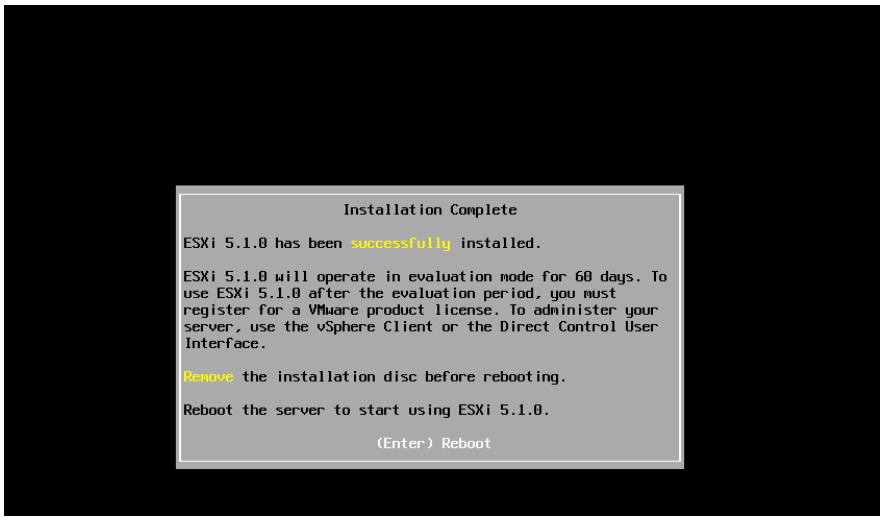
Step 28 Configure "1234QWer" as the root password.

Step 29 Start the installation by confirming the installation disk with F11.

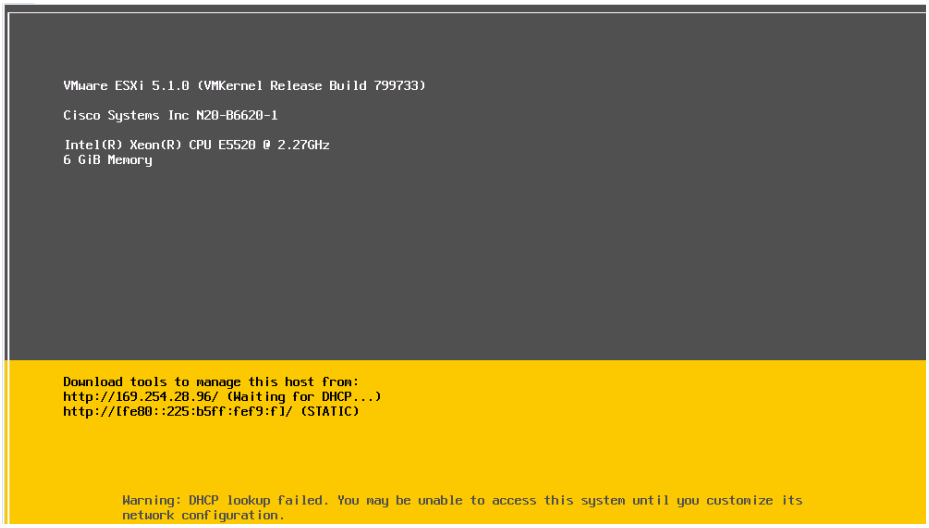


Step 30 The complete installation will take just 4-5 Minute including the final reboot.

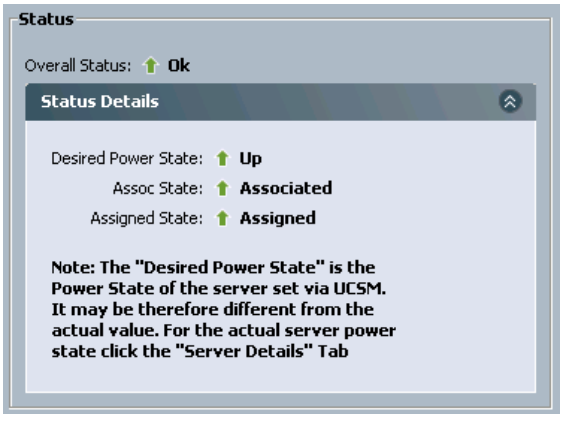
Step 31 When the installation is finished press enter to reboot.



Step 32 ESXi is installed and running! (do NOT configure anything yet)



Step 33 Notice the service profile status: up, associated and powered on.



Note	Do not configure the ESXi server, this will be done in a later exercise

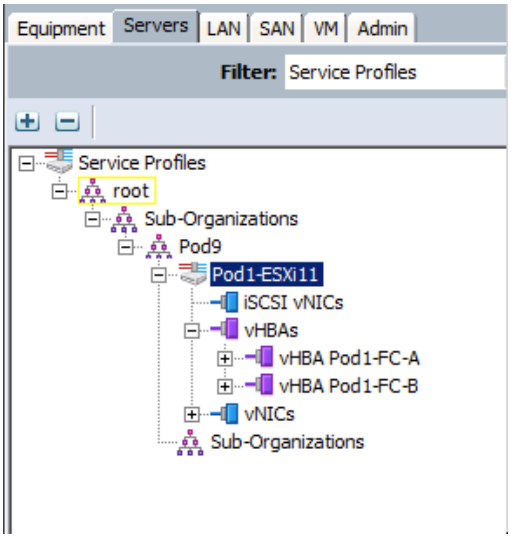
Task 9: Move a Mobile Service Profile

In this task, you will boot the mobile service profile and then move it to another physical server. This is possible because we have not used any local components like HDDs. Please note we are NOT moving a virtual machine but a server, so this will be disruptive, there is NO way to move a REAL (non-virtual) Server to another hardware while running.

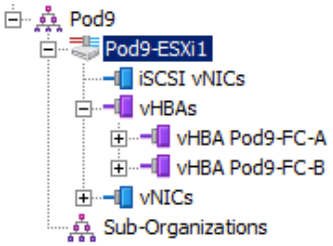
Activity Procedure

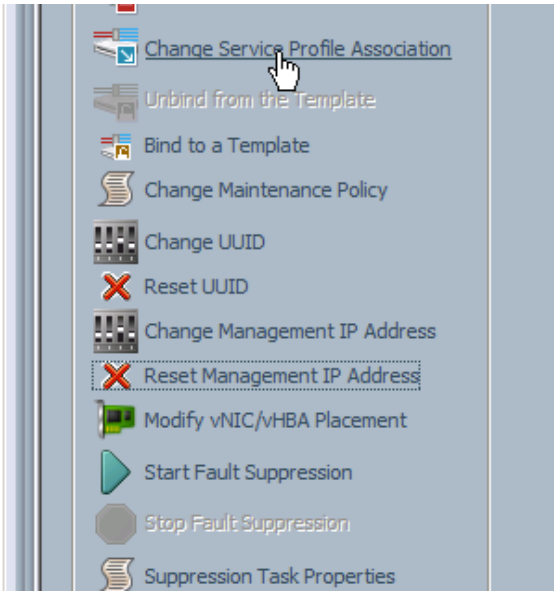
Complete these steps:

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 Pod's ESXi mobile profile you created in the previous lab.

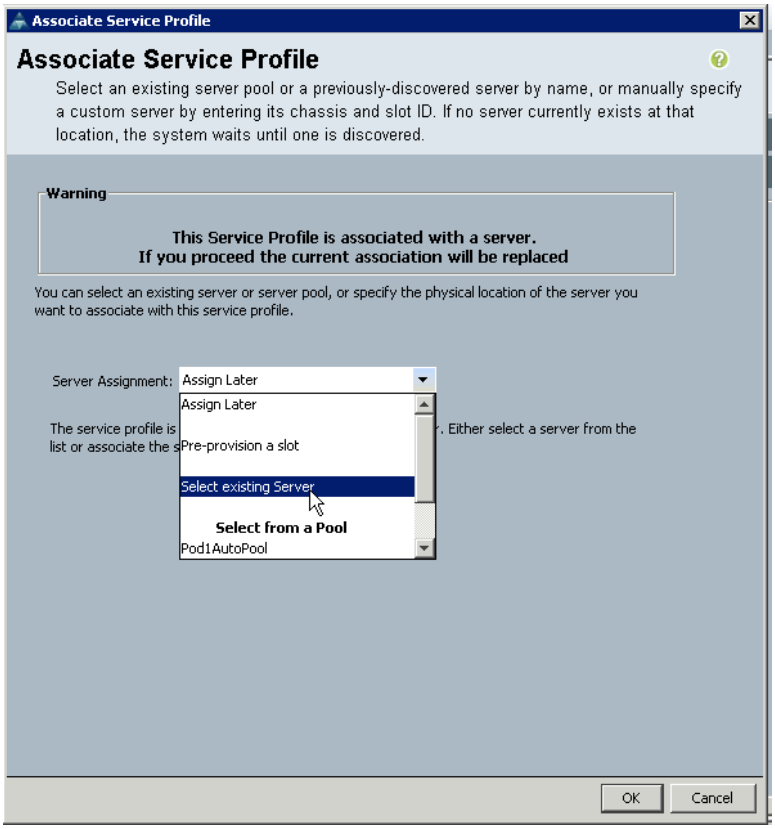


Step 2 Click "Change Service Profile Association" (you could also disassociate and associate manually, "Change Service Profile Association" does both you.)

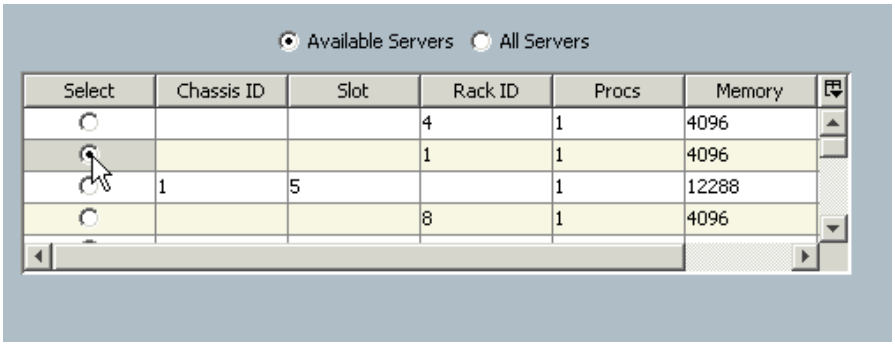




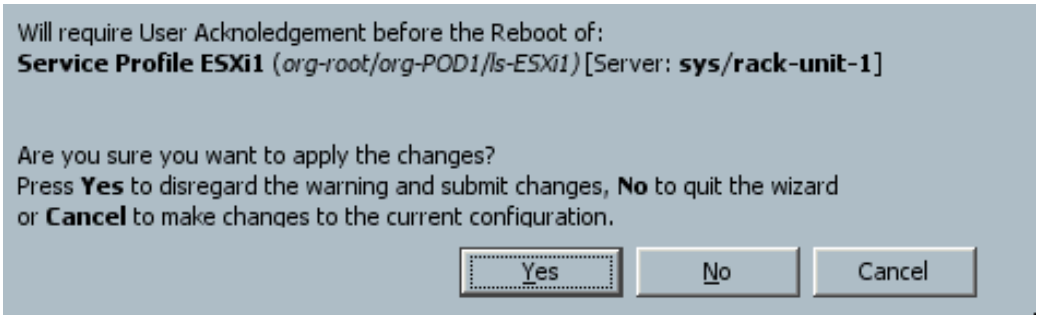
Step 3 Select "Select existing Server"



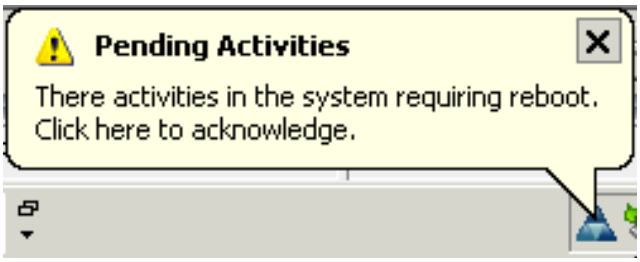
Step 4 Select the Rackmount-Server with your Pod# and click OK



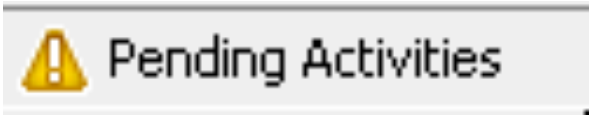
Step 5 Note the warning message.



Step 6 Notice the "Pending Activities"Alarms all over UCSM (and even in Windows). They show up because we specified in the Maintenance Policy the reboot (which is required for the move) needs to be acknowledged.



and in UCSM

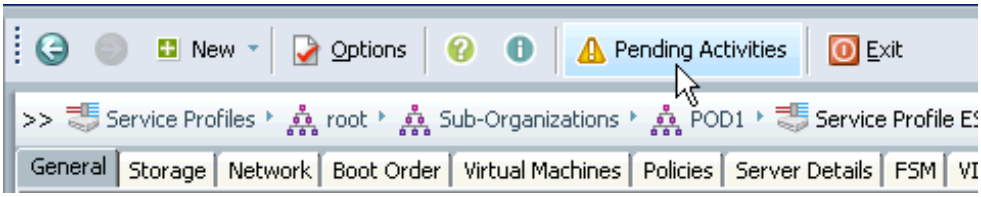


Step 7 Moving the profile requires rebooting the server. It is highly recommended to do a clean OS shutdown. Connect to the ESXi KVM console.

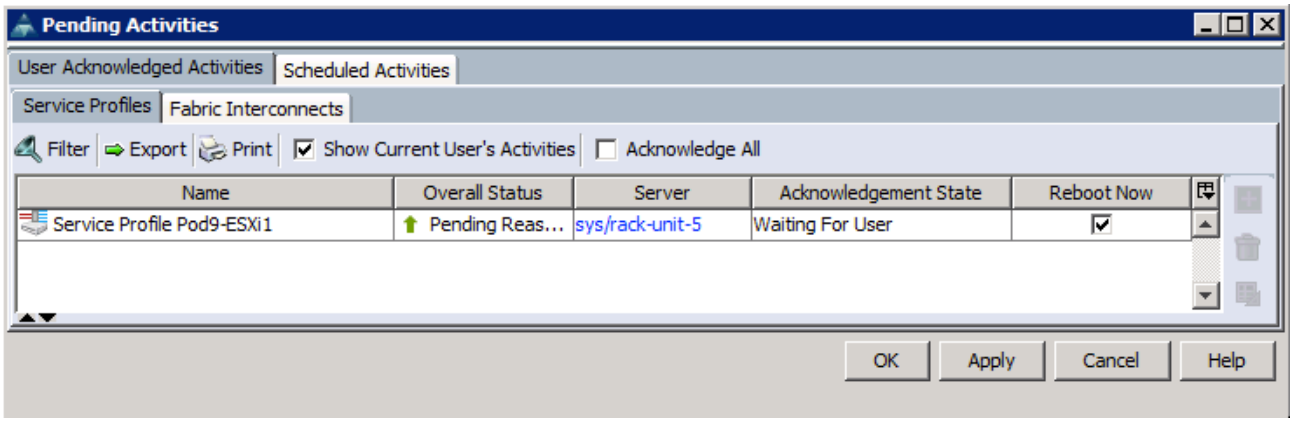
Step 8 Press F12 to shutdown the ESXi host and login with user “root” and password “1234QWer”

Step 9 Press F2 to shutdown the host, wait until “NO SIGNAL” appears.

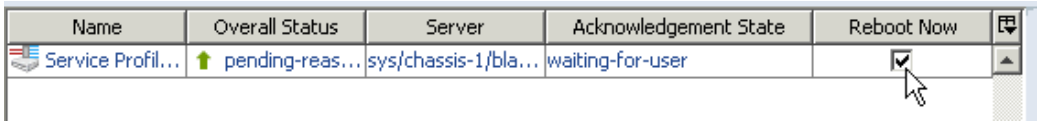
Step 10 Open the “Pending Activities” Window by clicking at “Pending activities” on the top toolbar.



Step 11 Check the pending activities by clicking on an event. Keep in mind some of these events may be from other Pods in the lab

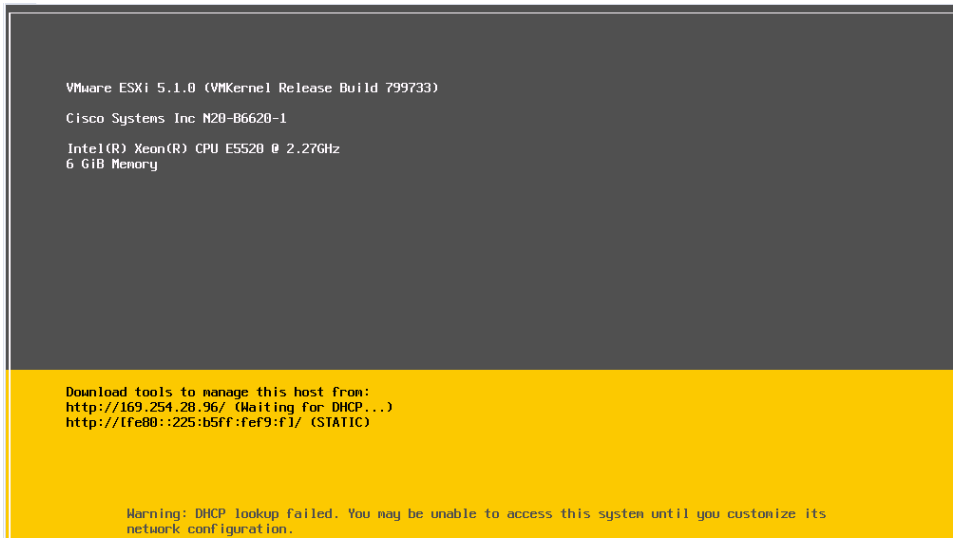


Step 12 Make sure to select ONLY YOUR Profile and klick “reboot now” and “Apply”



Step 13 Observe the move of the service profile to the Rackserver, UUOS will deconfigure the blade, configure the Rackserver and start the service profile on the new platform.

Step 14 Note the different CPU and memory on the ESXi welcome screen.



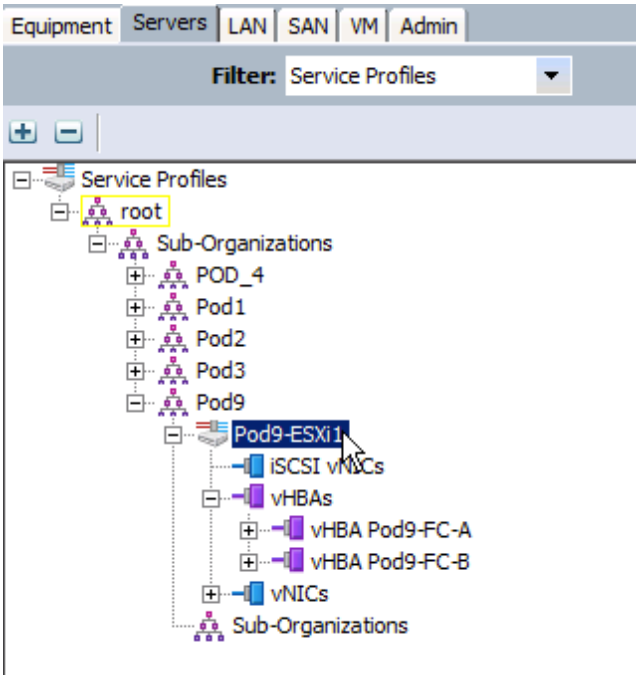
Task 10: Clone and reconfigure a Mobile Service Profile

In this task, you will clone an existing profile and change parameters.

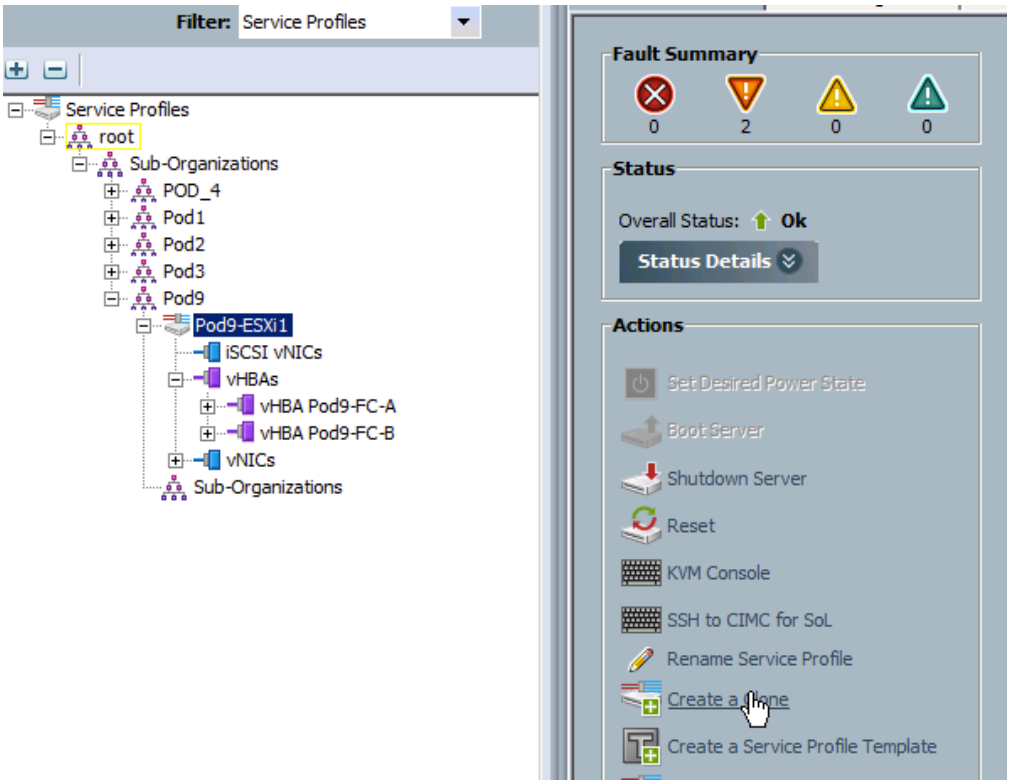
Activity Procedure

Complete these steps:

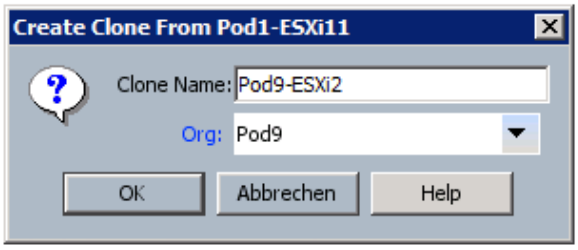
Step 1 In the navigation pane, choose the **Servers** tab. It may be helpful to set the **Filter** field to **Service Profiles** for the following steps. Choose your Pod's service mobile profile you created in the previous lab.



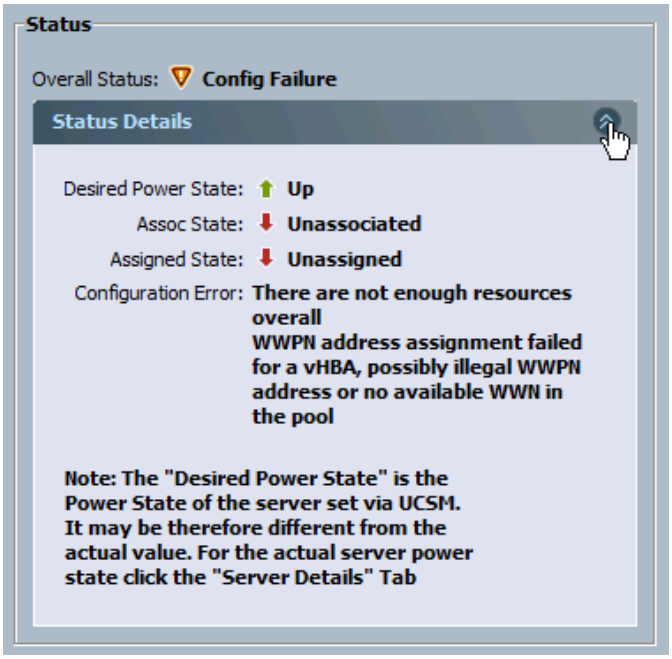
Step 2 Select your (running) ESXi service profile and use the action box or the context menu to create a clone of your Server.



Step 3 Use name "Pod#-ESXi2" and your Organization. Click OK to create.

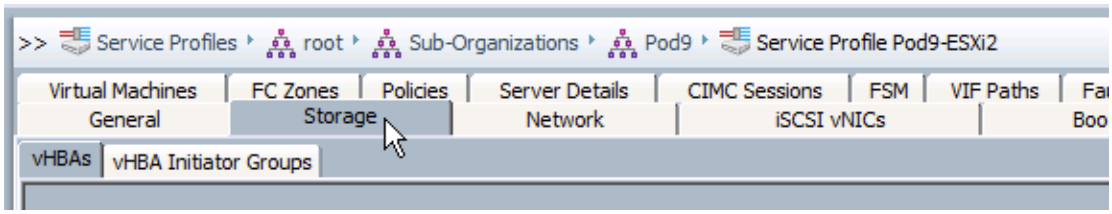


Step 4 Click the newly created service profile and note it has a "Config Failure" – expand the Status Details the find out more.

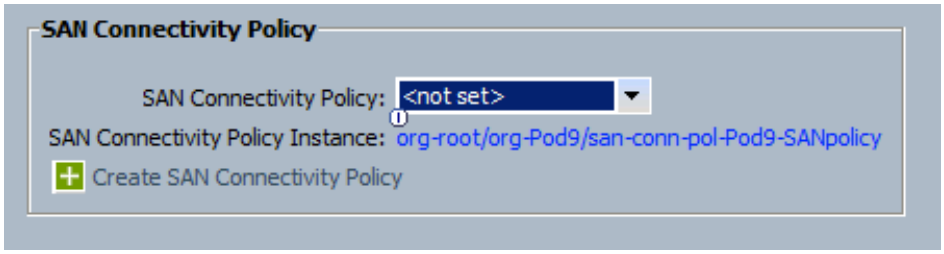


Step 5 The pools we created just contained ONE address each for Fibre Channel (WWNN and WWPN) so we exhausted these pools.
In this lab we will change the configuration for this Service Profile and use iSCSI instead of Fibre Channel.

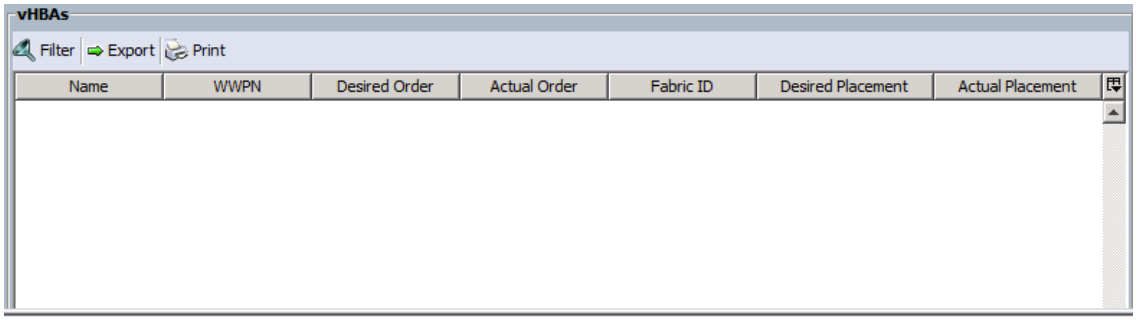
Step 6 We are going to delete the FC HBAs first.
Click the "Storage" Tab of your service profile.



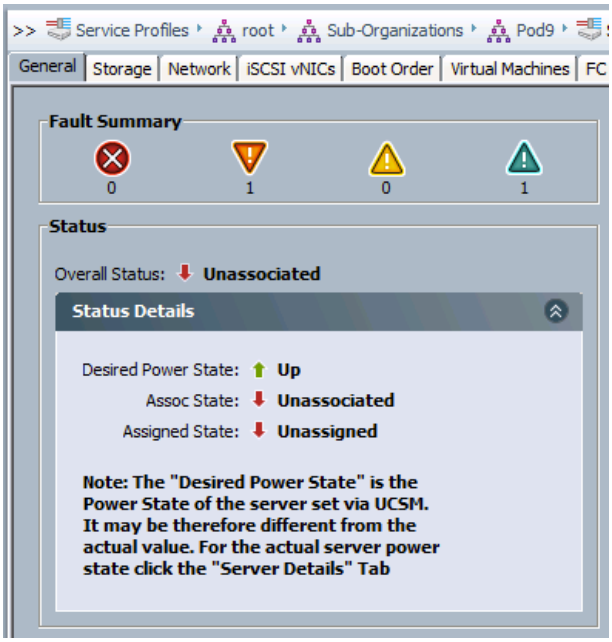
Step 7 Select "<not set>" as your SAN connectivity Policy and click "Save Changes"



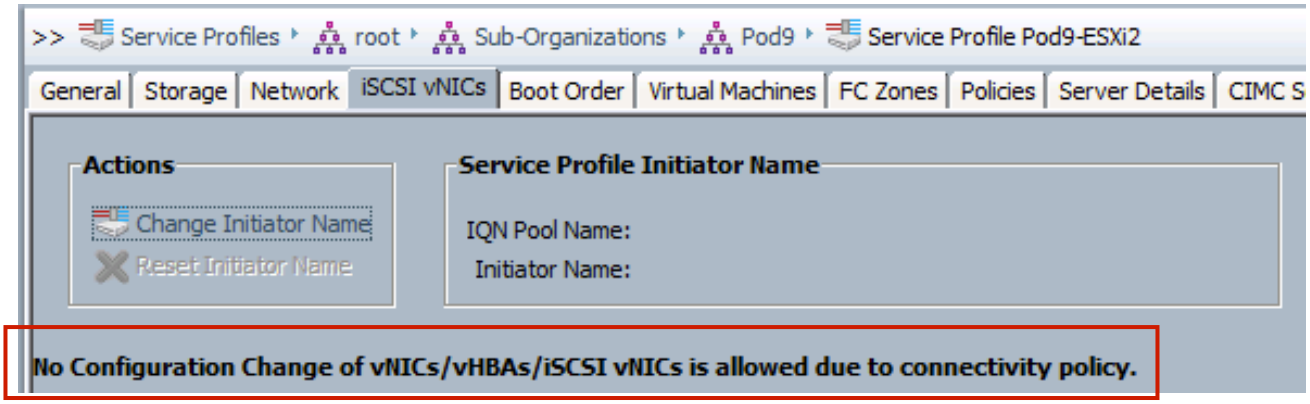
Step 8 Note the vHBAs are gone…



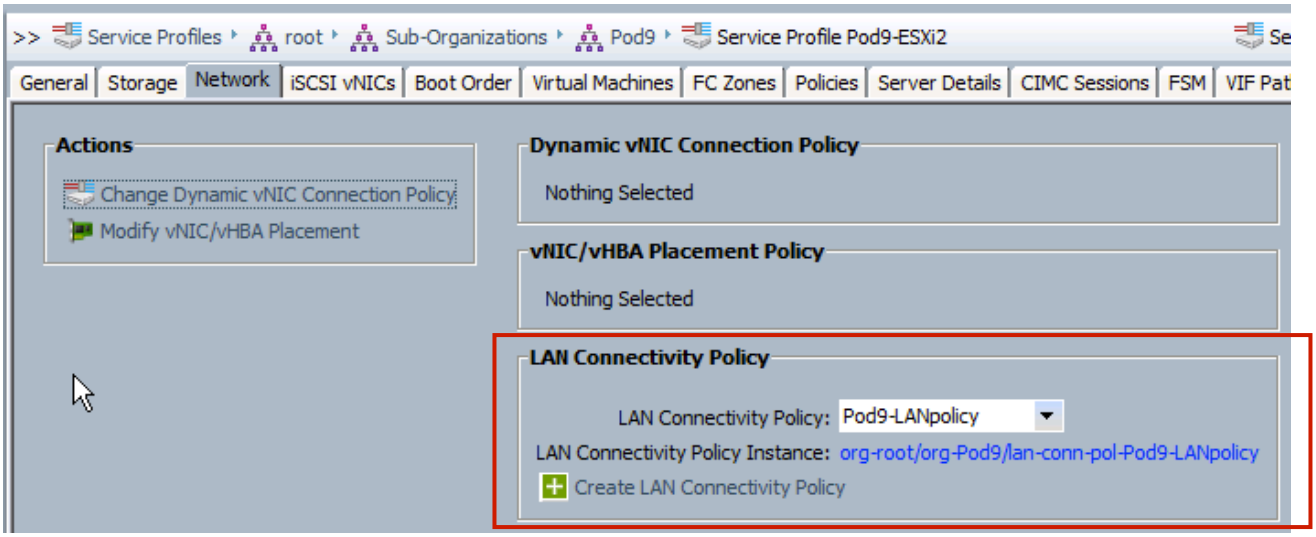
Step 9 Select the "General" Tab of your service profile - Notice the Status is now "Unassociated"



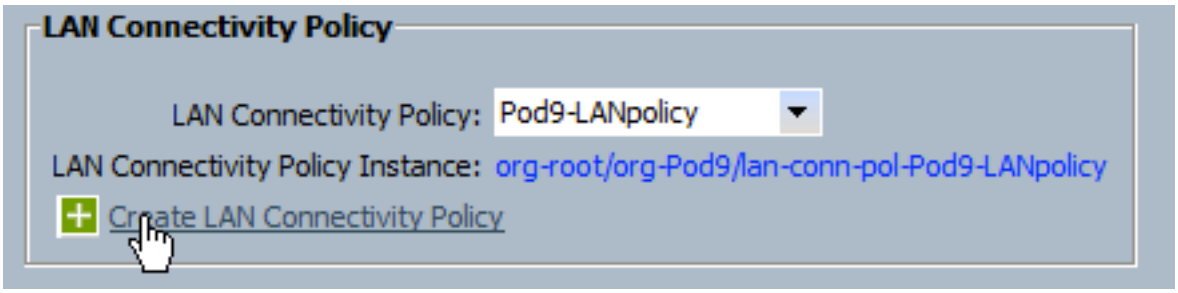
Step 10 Click the "iSCSI vNICs" Tab and notice the message – NIC cannot be configured because we use a Connectivity Policy.



Step 11 Click the Network Tab and notice our Connectivity Policy.

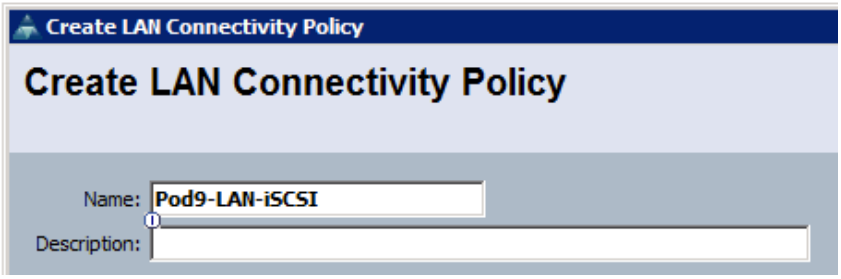


Step 12 Click "Create LAN Connectivity Policy" to create a new LAN Connectivity Policy.

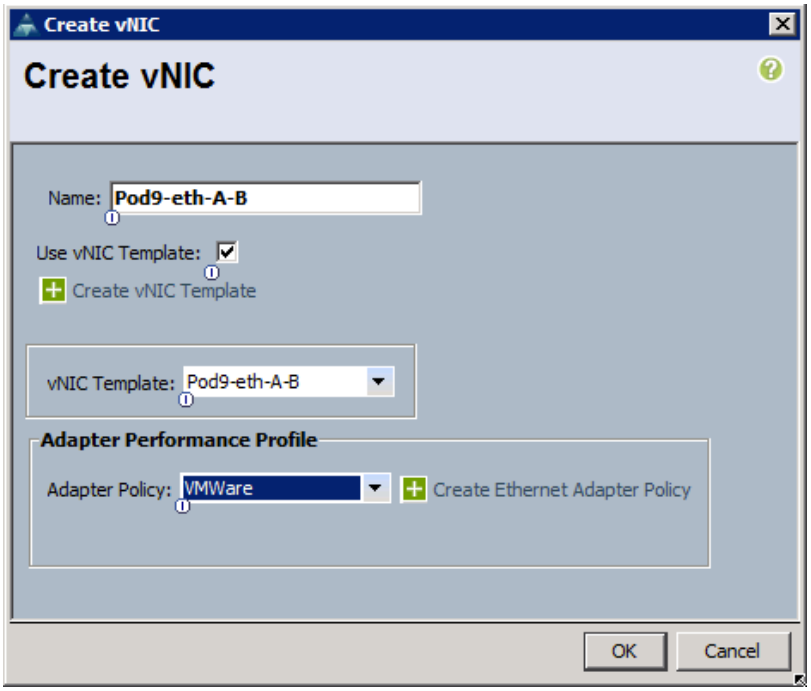


Note There is no way in the GUI to copy a LAN Connectivity Policy so we will create a new one.

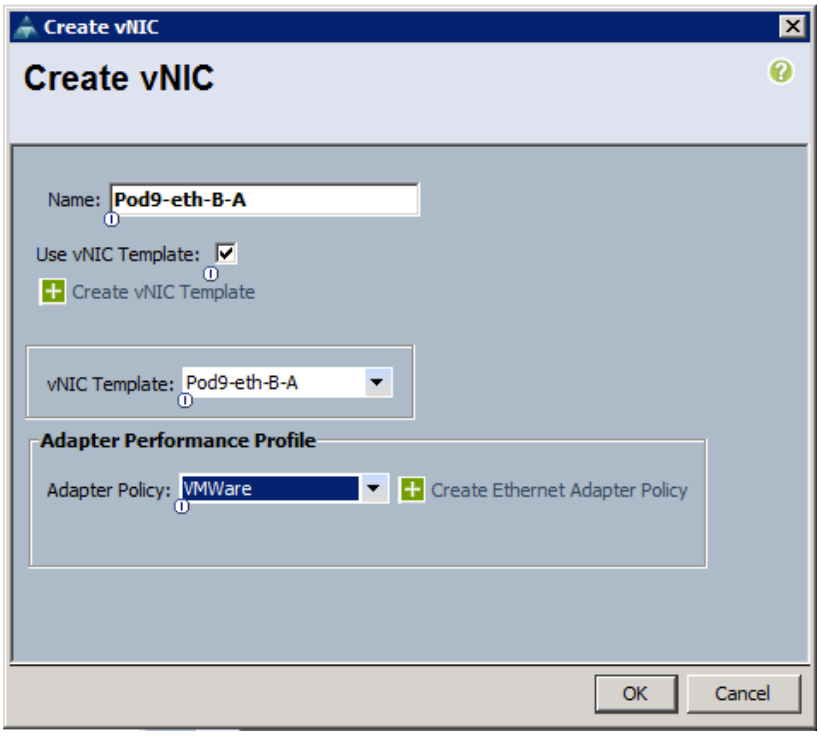
Step 13 Name your new Connectivity Policy "Pod#-LAN-iSCSI" (# is your Pod number)



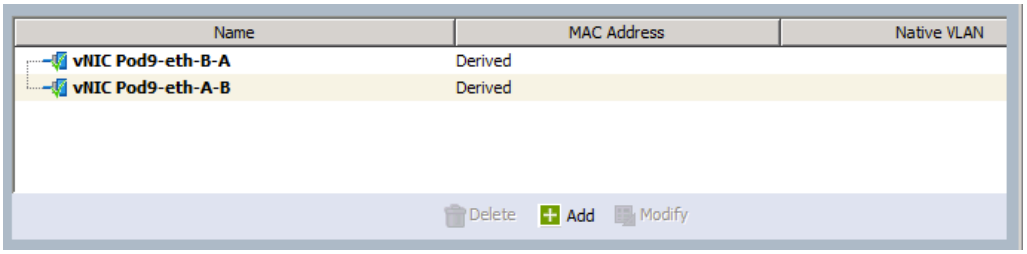
Step 14 Click “Add” to add the first A-B vNIC like we did with the first LAN Connectivity Policy (now you understand why Templates were created and used ;))



Step 15 Create the second vNIC (B-A) from the other template.



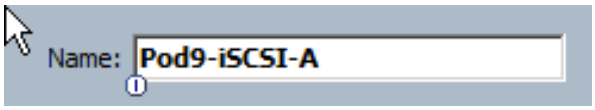
Step 16 Check your vNIC configuration.



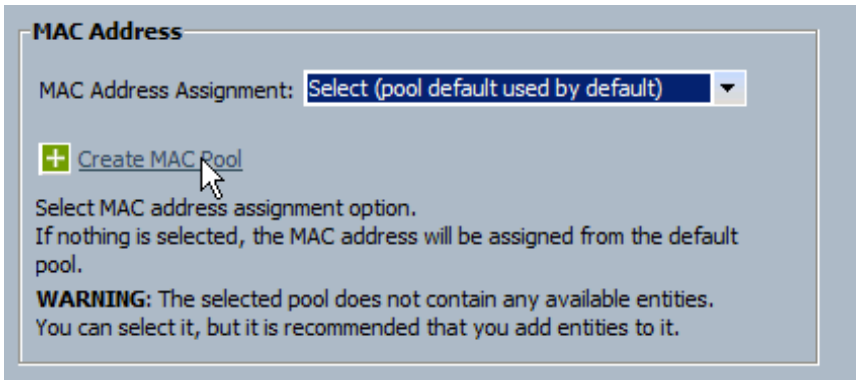
Note We could just add the iSCSI VLANs to the existing vNICs but were are going to create extra vNICs.
(iSCSI does NOT support Hardware Failover (which does not make any sense anyway for iSCSI) and the iSCSI VLAN needs to be native for iSCSI boot)

Step 17 Click "Add" to add an extra vNIC for iSCSI.

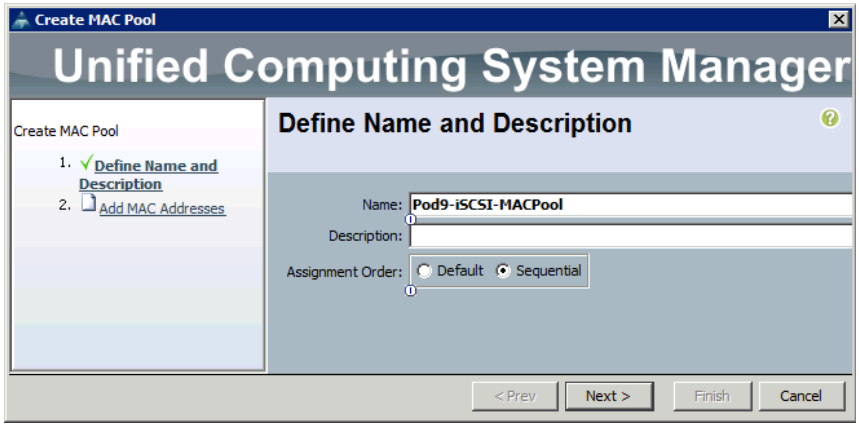
Step 18 Name the vNIC "Pod#-iSCSI-A" (# is your Pod Number)



Step 19 Click "Create MAC Pool" to create a new MAC Pool.

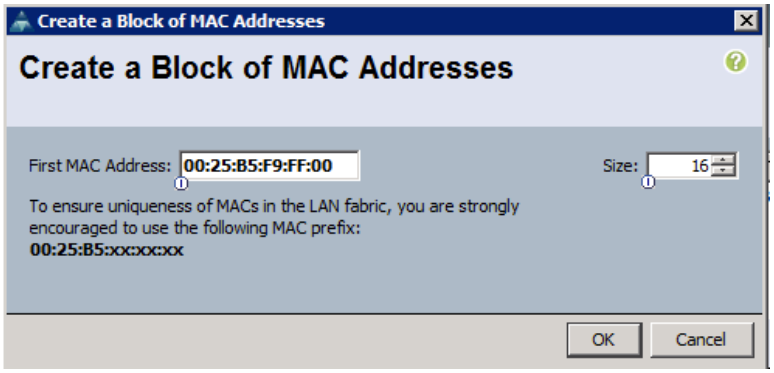


Step 20 Name your Pool "Pod#-iSCSI-MACPool" and select "Sequential", then click Next>



Step 21 Click "Add" to add a MAC address range.

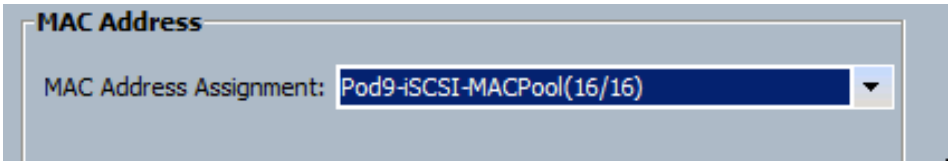
Step 22 Configure 16 MAC addresses starting from ***00:00:25:b5:LP:FF:00*** (L is the Lab ID P is your Pod number)



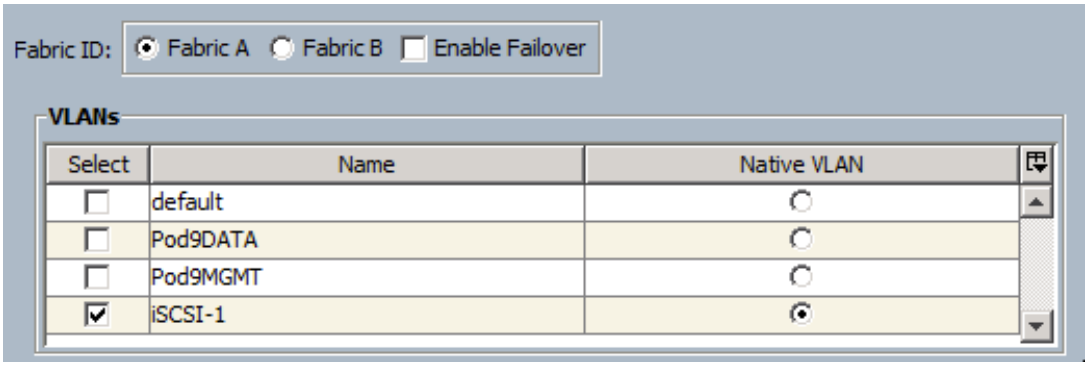
Step 23 Click OK and Finish.

Note The FF inside the MAC address makes it a lot easier to recognize these “special” NIC cards in VMWare.

Step 24 Make sure to select the Pool you just created.



Step 25 Select Fabric A, do NOT select Failover and select ONLY VLAN iSCSI-1 and mark it as native!



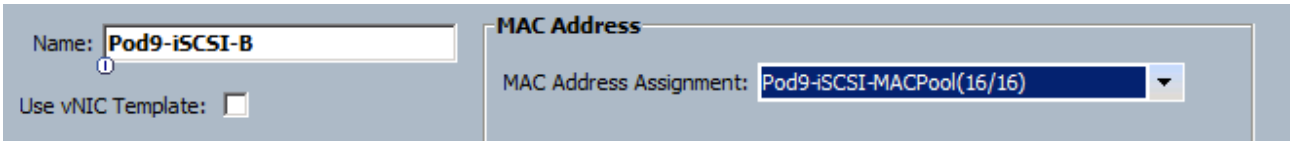
Caution Make sure iSCSI-1 is used!! Do NOT use the VLAN your created.

Caution Do not change the MTU size. Additional configuration (not covered in this lab guide) would be required.

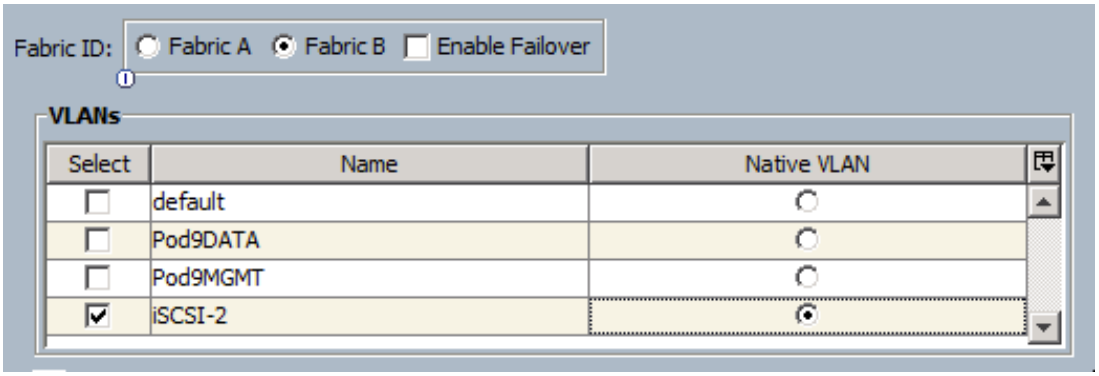
Step 26 Click OK to create the vNIC.

Step 27 Click “Add” to create a second vNIC

Step 28 Name the vNIC “Pod#-iSCSI-B” (# is your Pod Number), select the iSCSI-MAC-Pool we created in this section



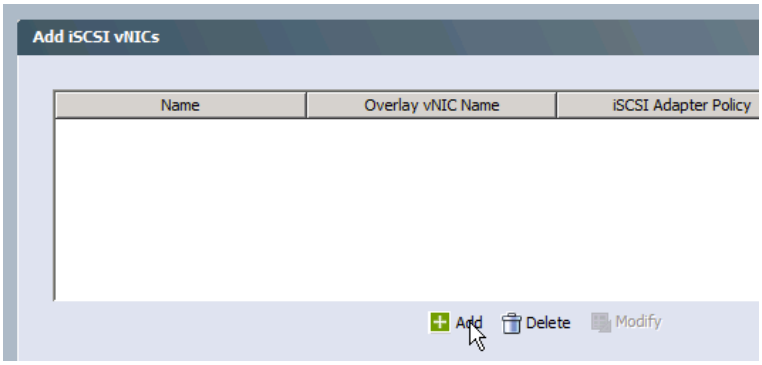
Step 29 Select Fabric B with NO failover, VLAN iSCSI-2 as native.



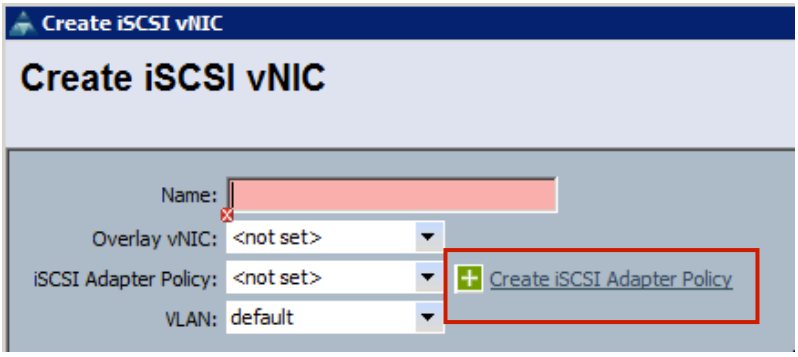
Caution Make sure iSCSI-2 is used!! Do NOT use the VLAN your created.

Caution	Do not change the MTU size. Additional configuration (not covered in this lab guide) would be required.

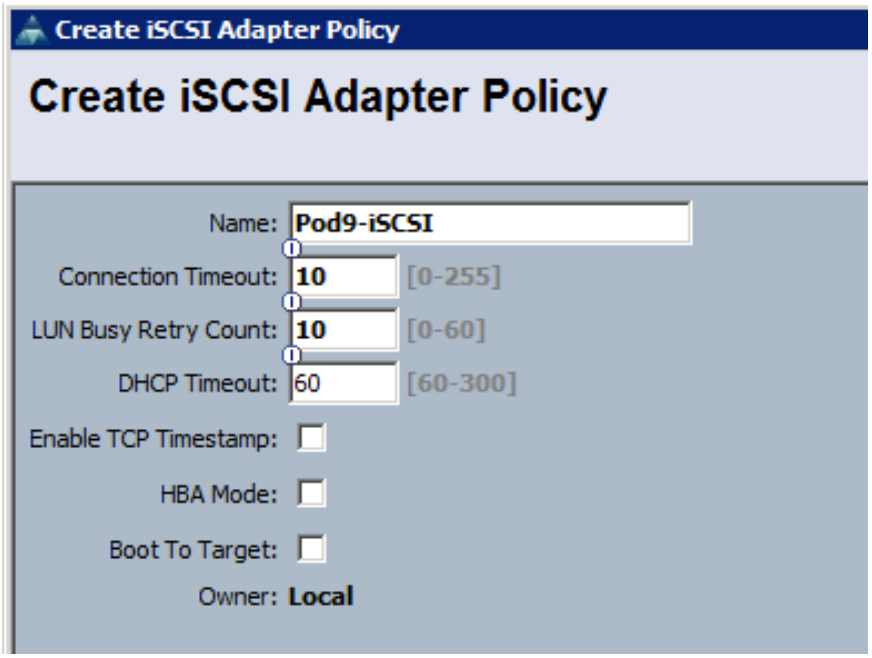
Step 30 Click “Add” at the “Add iSCSI vNICs” to add an iSCSI NIC.



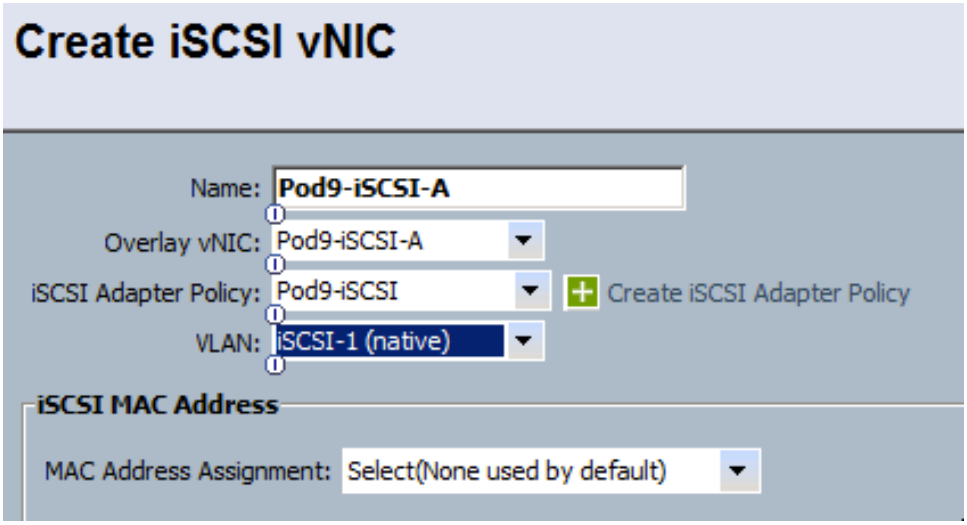
Step 31 Click “Create iSCSI Adapter Policy”



Step 32 Name your Policy “Pod#-iSCSI” (# is your Pod number), set the Connection Timeout to 10, the LUN Busy retry to 10 and verify NO options are checked.

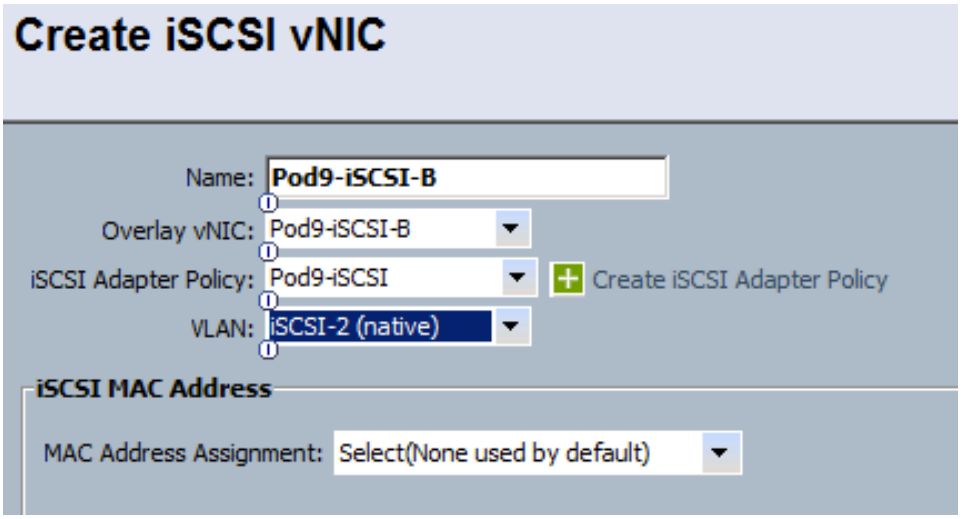


Step 33 Name your iSCSI-vNIC “Pod#-iSCSI-A” (# is your Pod number), select the iSCSI-A NIC as the overlay NIC, the iSCSI Adapter Policy we just created and VLAN iSCSI-1 (verify it is tagged as NATIVE) – DO NOT select a MAC address!

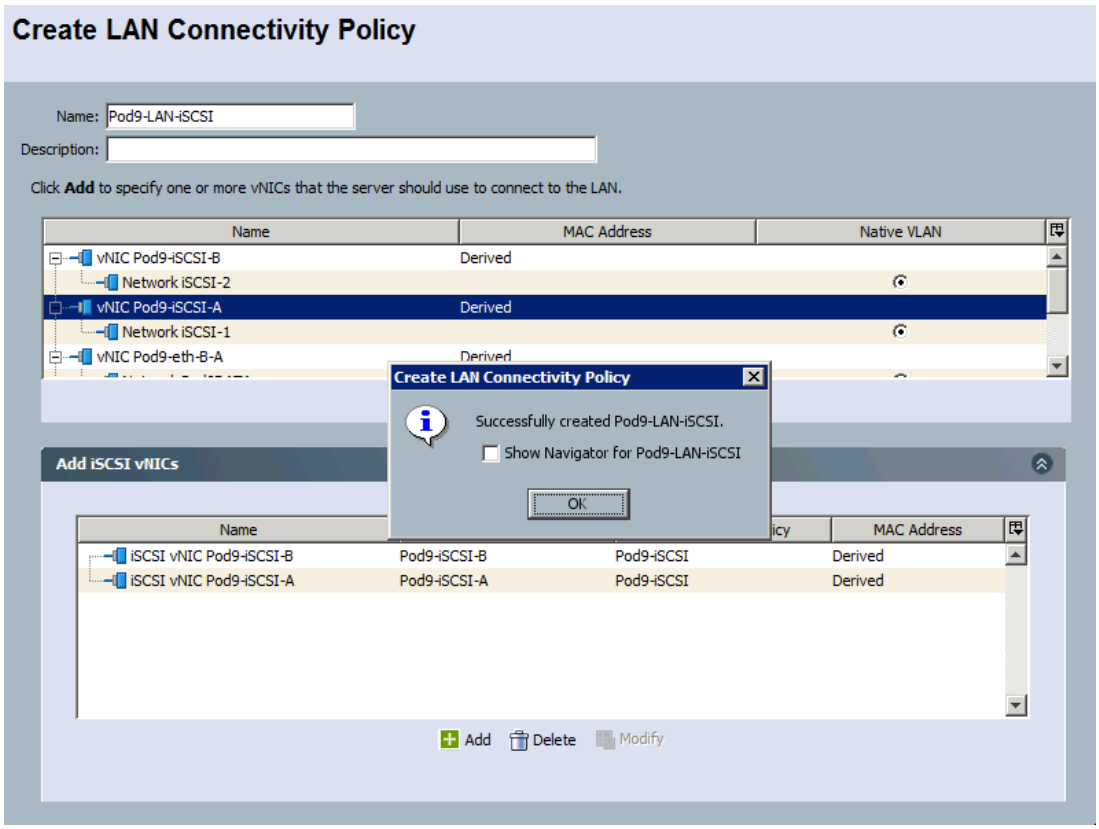


Step 34 Click OK.

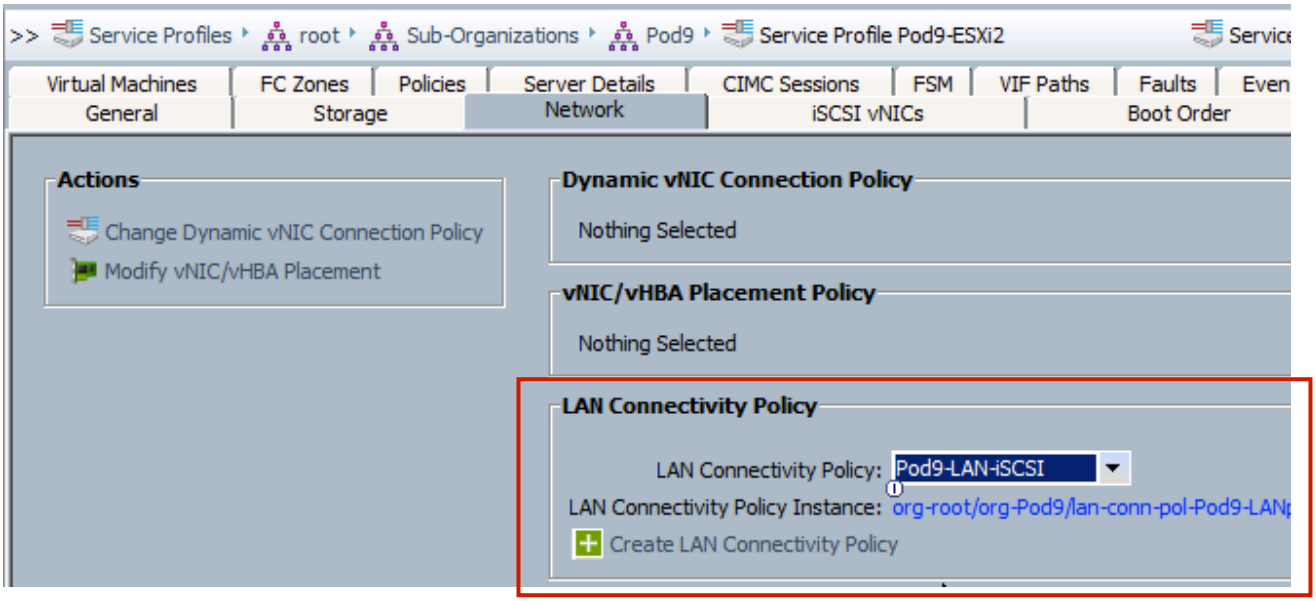
Step 35 Click "Add" to add a second iSCSI vNIC. (Make sure to use NATIVE VLAN iSCSI-2 and iSCSI-B as the Overlay NIC)



Step 36 Check your Configuration, then Click OK to create your LAN Connectivity Policy

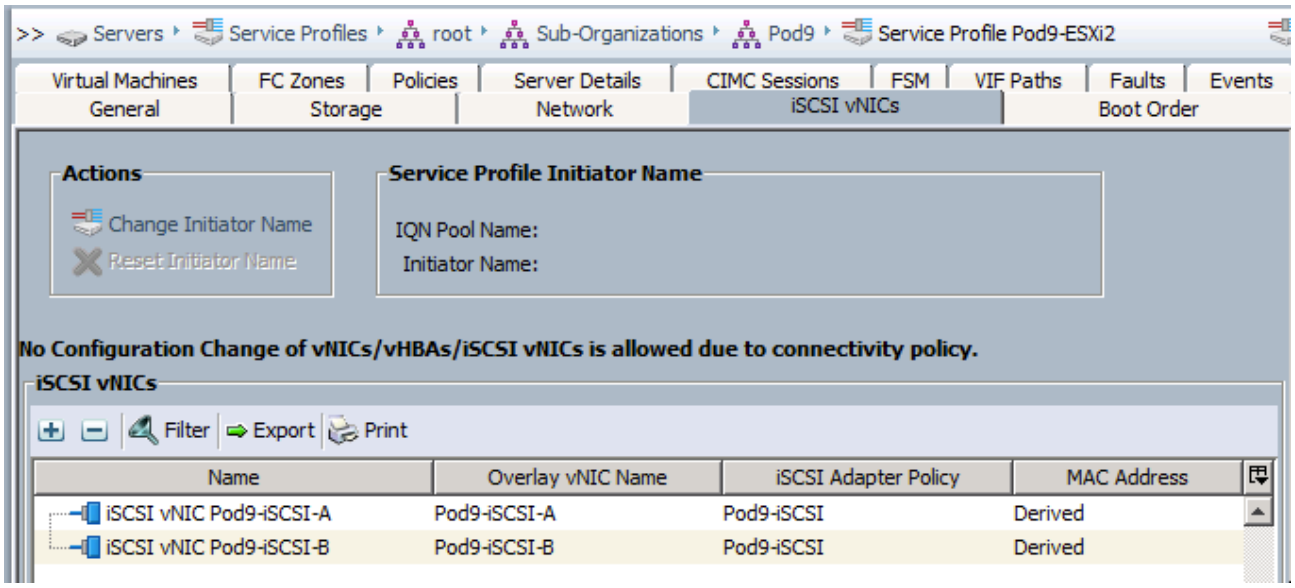


Step 37 Assign the new LAN Connectivity Policy to your Service Profile.

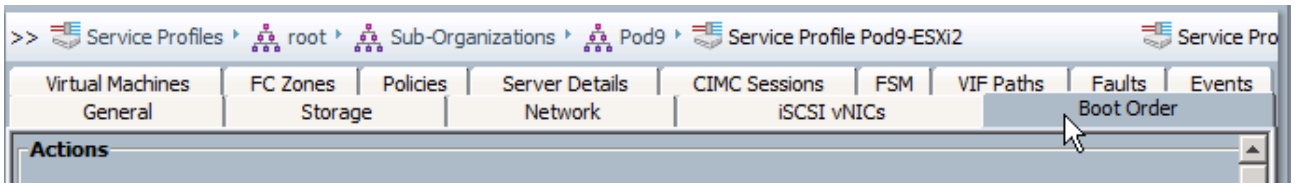


Step 38 Click “Save Changes”

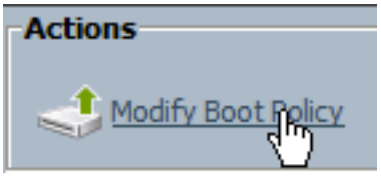
Step 39 Click on the “iSCSI vNICs” Tab in your service profile to validate.



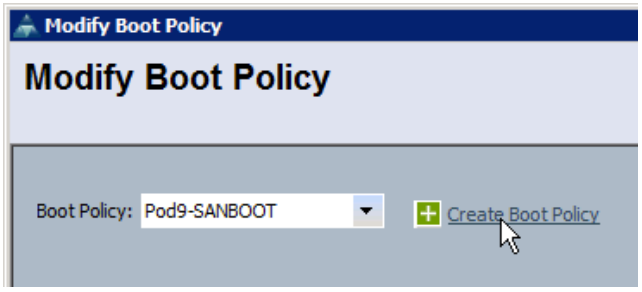
Step 40 Click the "Boot Order Tab" to enable iSCSI boot.



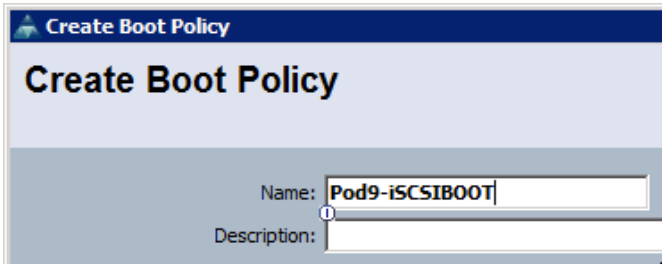
Step 41 Click "Modify Boot Policy"



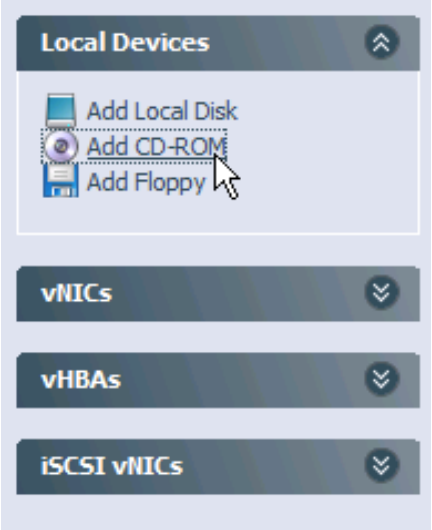
Step 42 Click "Create Boot Policy"



Step 43 Name your Policy "Pod#-iSCSIBOOT"

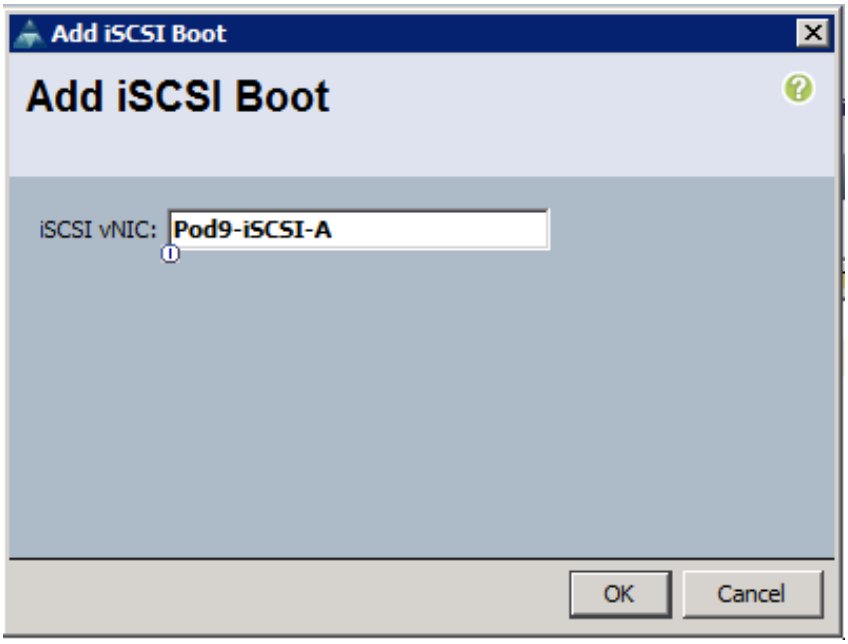


Step 44 Click Add CD-ROM"



Step 45 Click “Add iSCSI Boot”

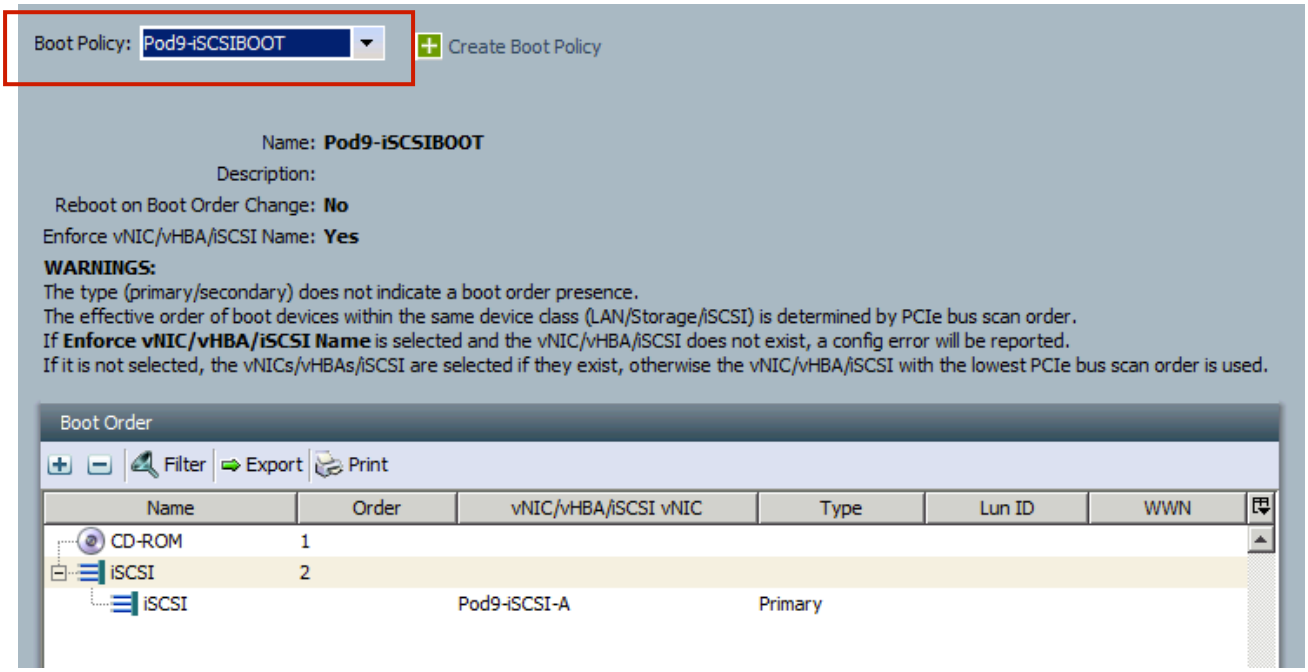
Step 46 Type your Adapter Name “Pod#-iSCSI-A” (# is your Pod#) and click OK



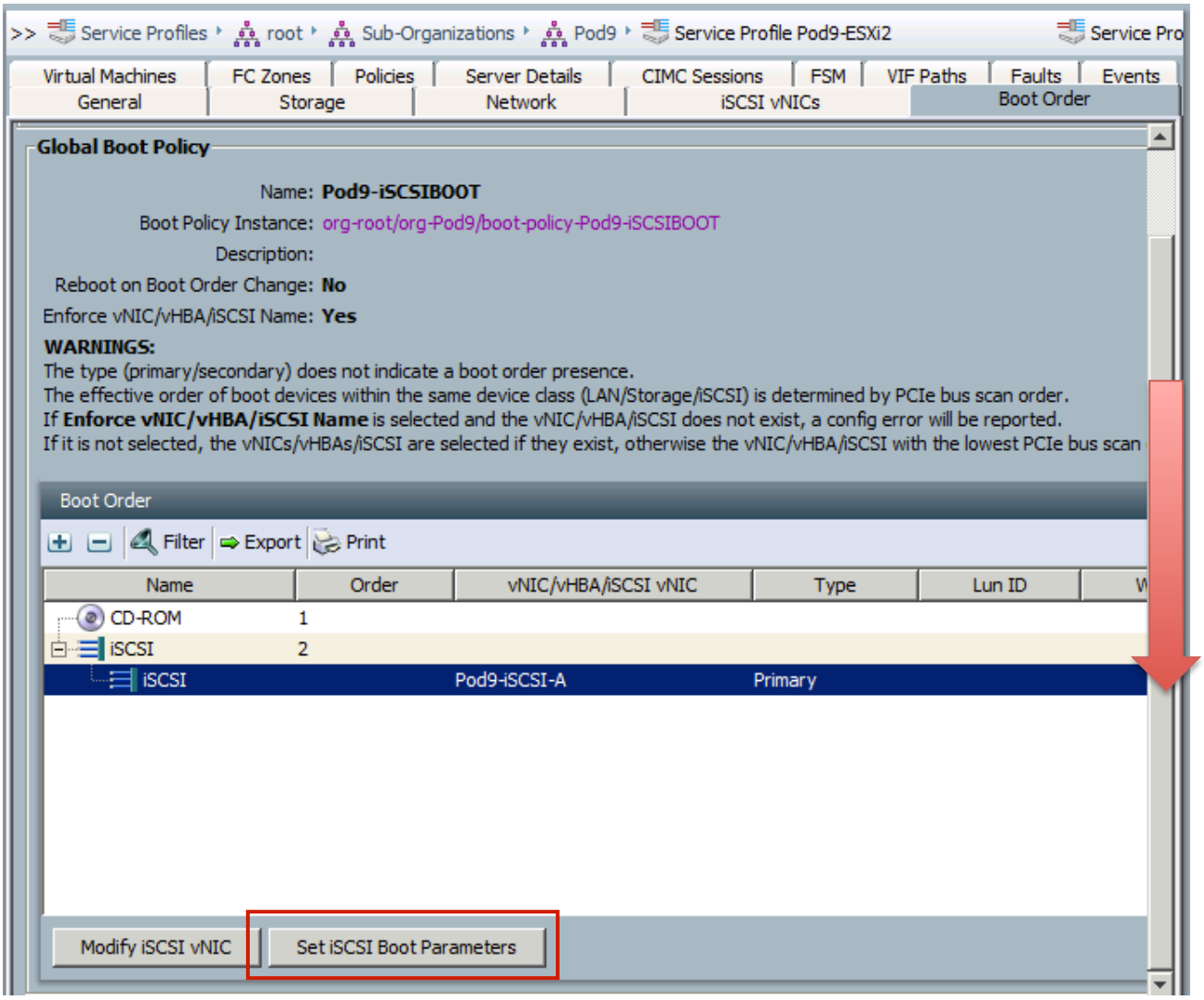
Caution This Parameter NEEDS to match your iSCSI vNIC name and is CASE-SENSITVE

Step 47 Click OK the create the Boot Policy

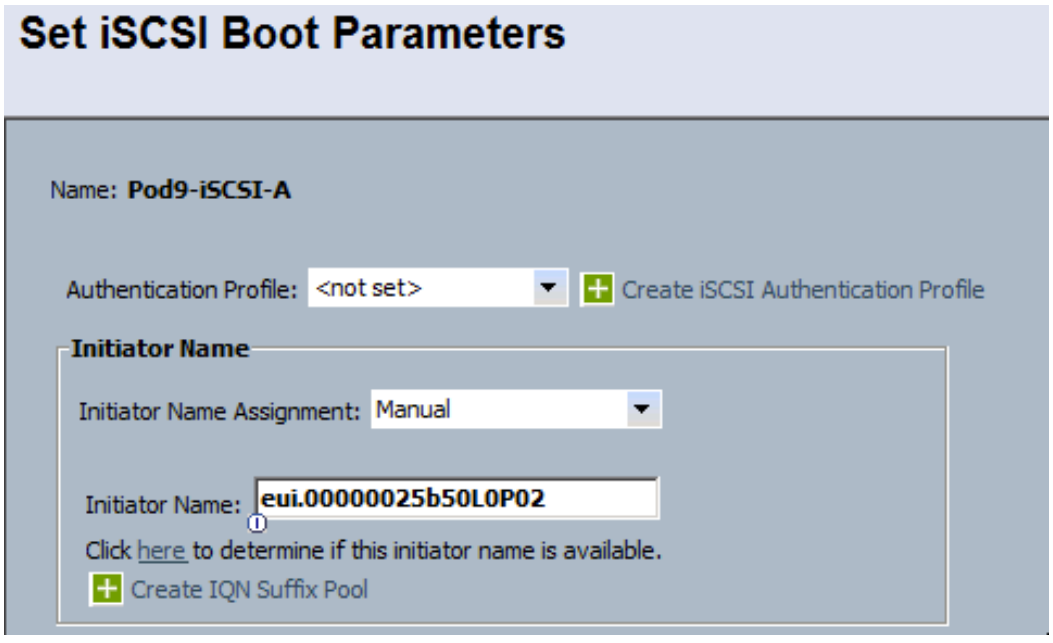
Step 48 Make sure to select the Boot policy we just created, then click OK in the "Modify Boot Policy" Window.



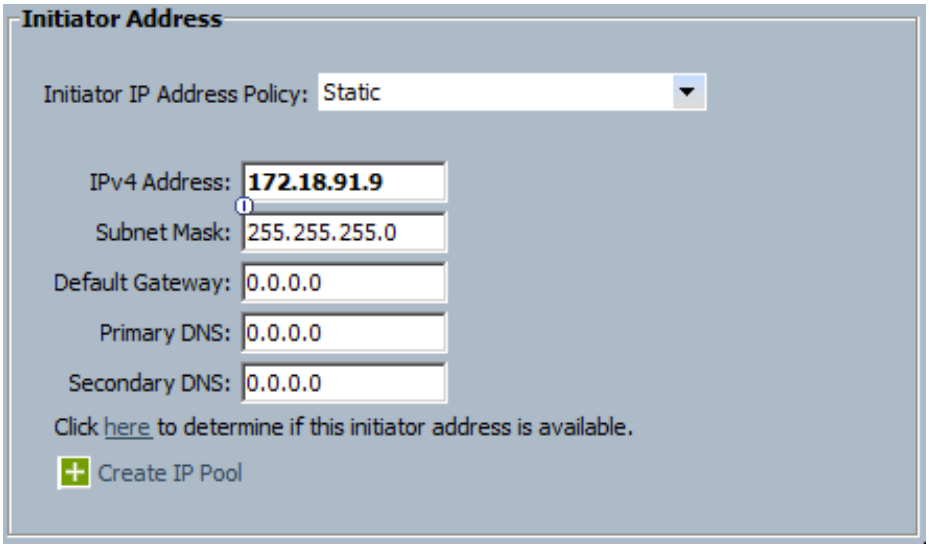
Step 49 Scroll to the buttom of the "Boot Order" Tab of your service Profile to reveal the "Set iSCSI Boot Parameters" Button



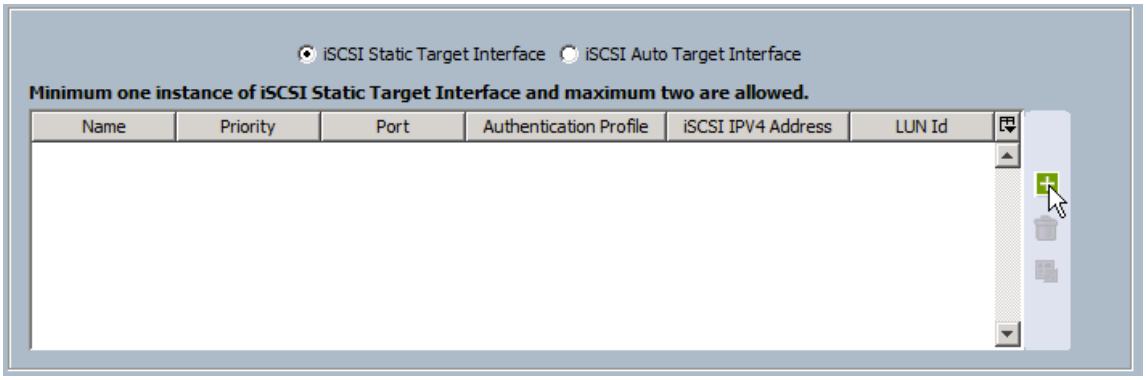
Step 50 Do NOT set an Authentication Profile, select "Manual" Initiator name Assignment, Initiator name is ***eui.00000025b50L0P02*** (**replace L and P:** L is the Lab ID, P is your Pod Number).



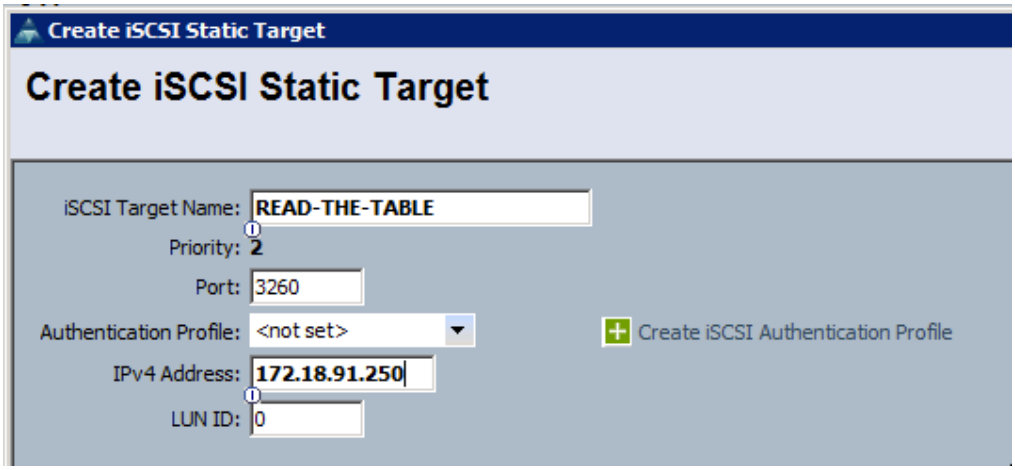
Step 51 Select "Static" as your IP Address Policy and assign ***172.18.L1.P (L is the Lab ID, P is your Pod number)*** as your IP address, Subnet Mask 255.255.255.0. Leave all other parameters at 0.0.0.0



Step 52 Select "iSCSI Static Target Interface" and click "+" to add a target.



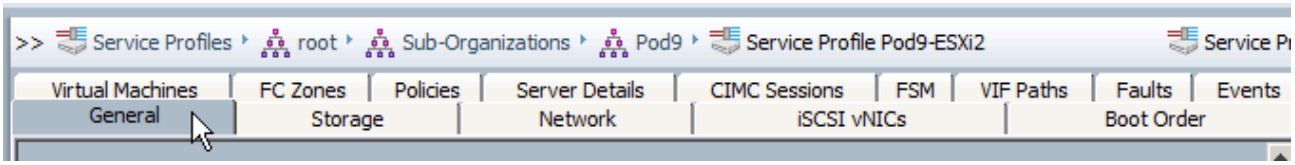
Step 53 Enter the value from the table below as the iSCSI Target Name and configure IP Address 172.18.L1.250 (L is the Lab ID) as the IPv4 Target address. (port 3260 and LUN 0 are correct), then click OK.



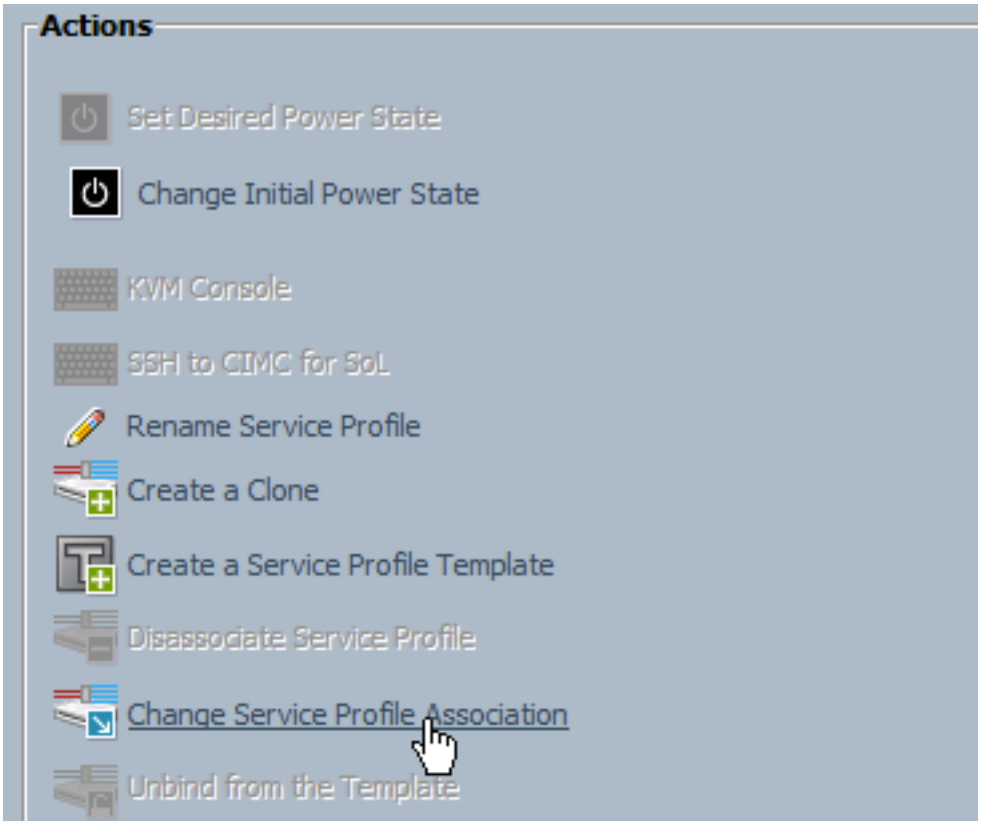
Lab ID (NOT YOUR POD NUMBER)	Target IQN
1-4	iqn.1992-08.com.netapp:sn.101317617
5-7	iqn.1992-08.com.netapp:sn.50397318

Step 54 Click OK to close the “Set iSCSI Boot Parameters” Window.

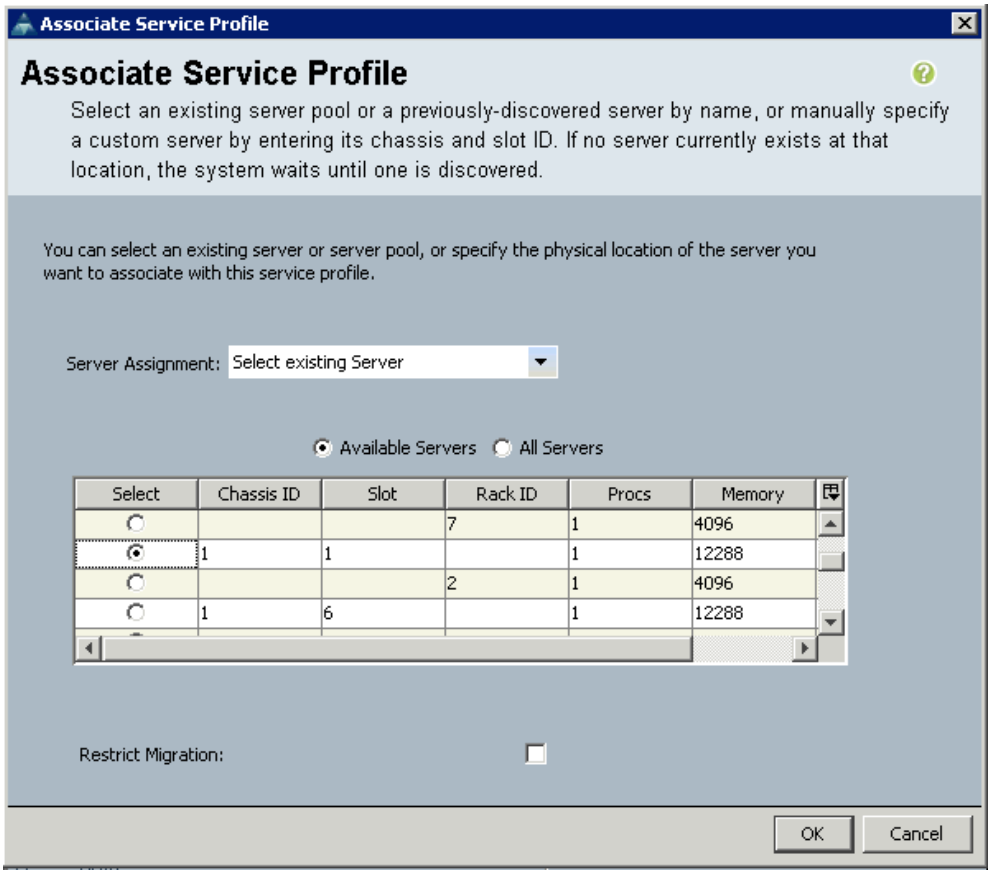
Step 55 Return to the “General” Tab of your Service Profile.



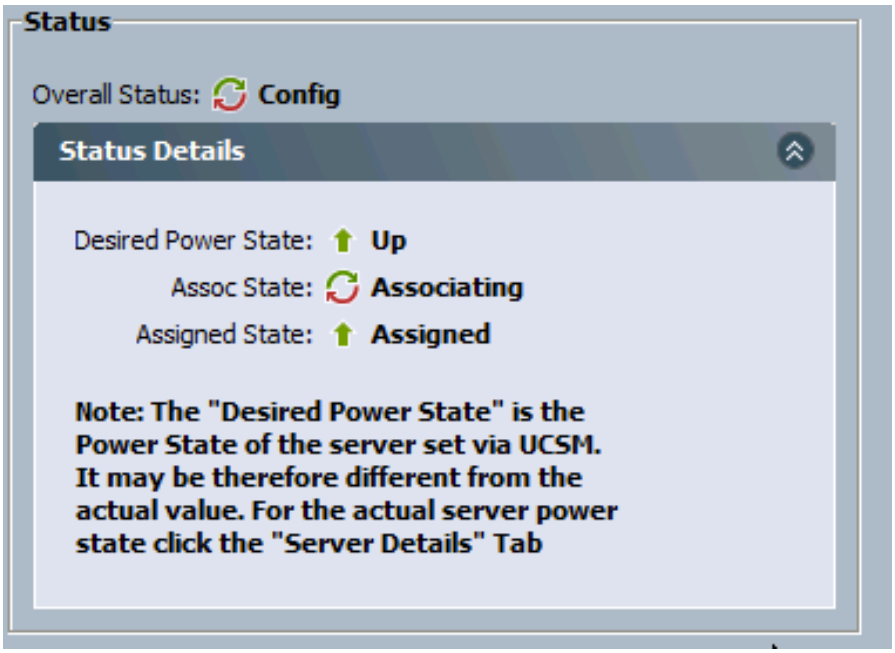
Step 56 Click the “change Service Profile Association” Action item.



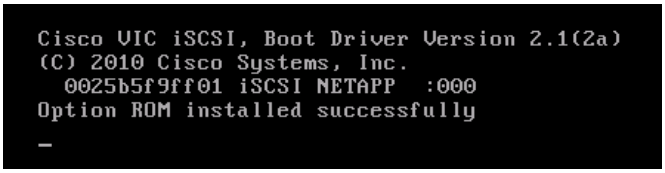
Step 57 Select “select existing server” and select your blade server (chassis 1, slot# is your pod#). Click OK.



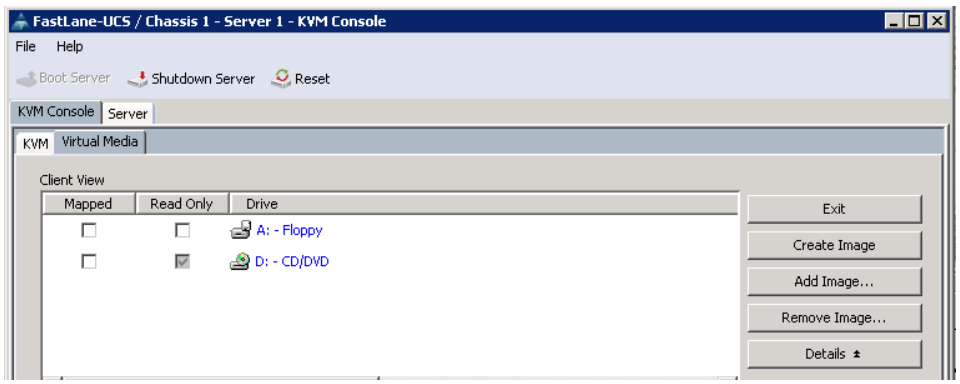
Step 58 Notice your Server is in "Config" state.



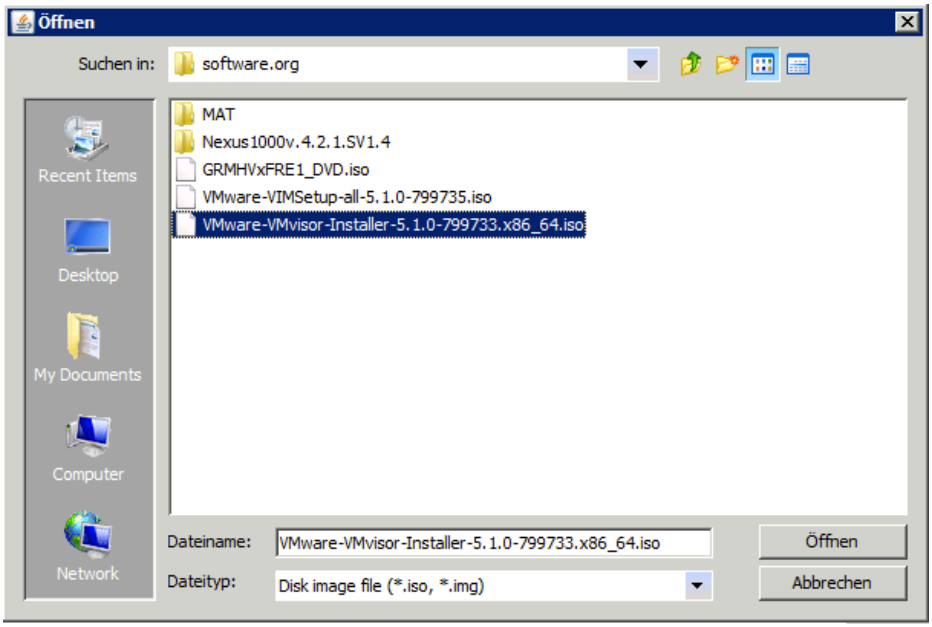
Step 59 After a successful boot (if you look carefully you can see the NetApp disk already) the server will complain about the missing OS.



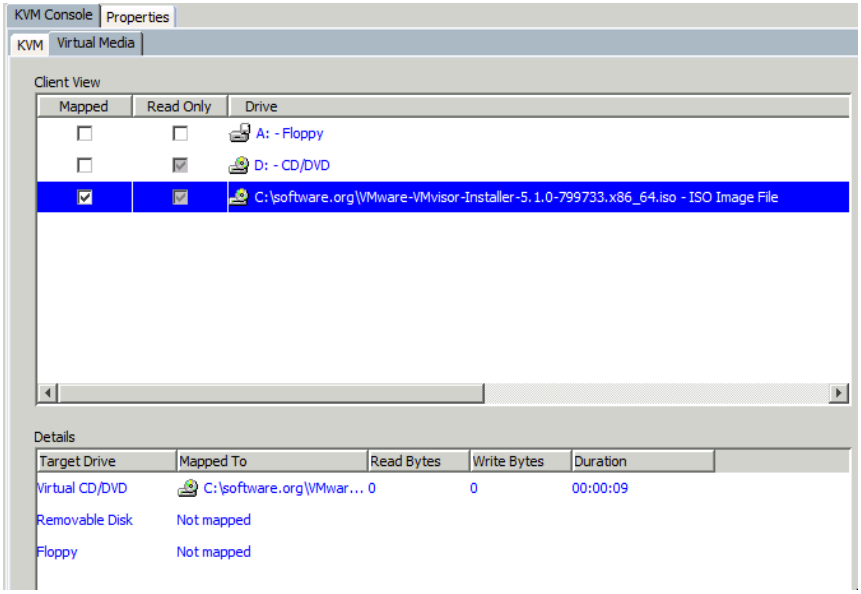
Step 60 We configured the Boot Profile to boot from CDROM, so let's insert a (virtual) CDROM… Click "Tools" in KVM and select "virtual Media".



Step 61 Click "add Image", navigate to c:/software.org/VMWare and select the 4.1.0 VMVisor ISO file.

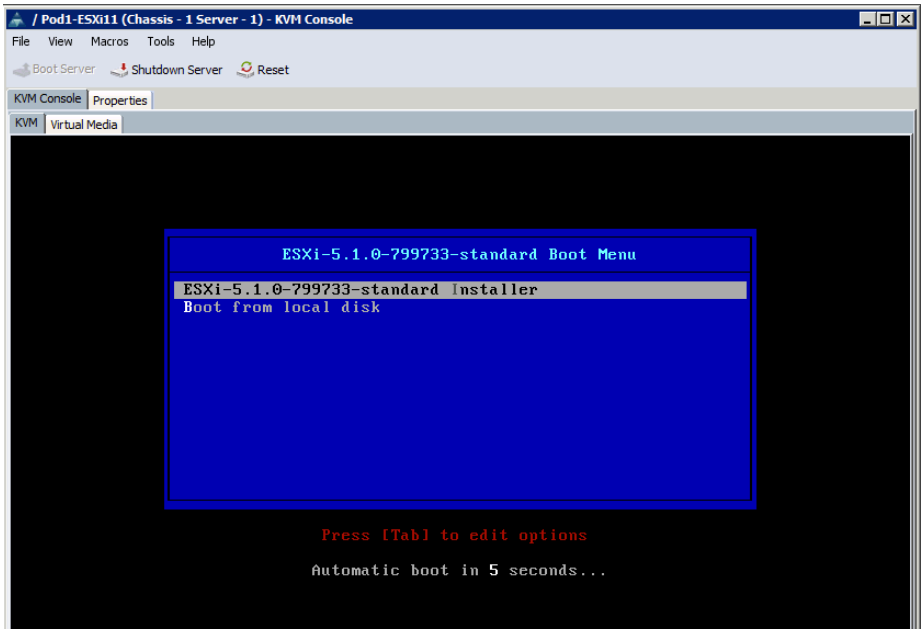


Step 62 Click the "mapped" checkbox to connect the virtual CD to the server. DO NOT close the VirtualMediaSession-Window as that will break the connection.



Step 63 Click into the KVM window and press a key, ESXi install will boot from the virtual CDROM.

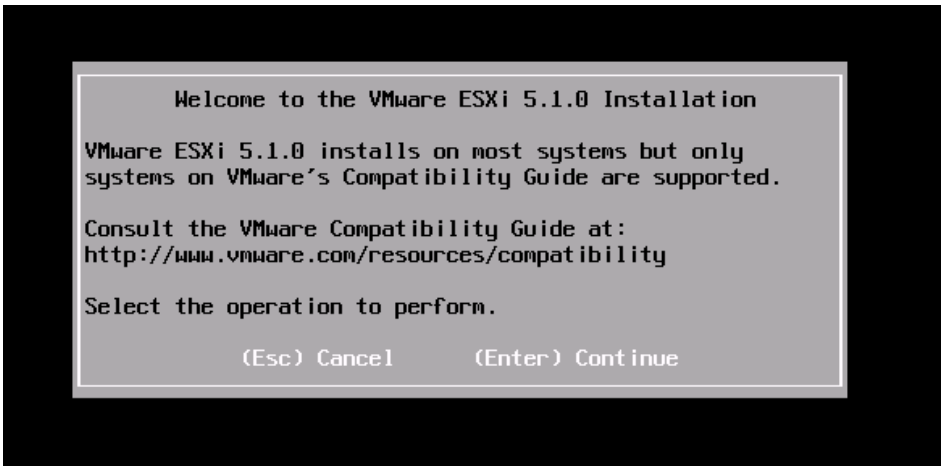
Step 64 Press Enter to start installation



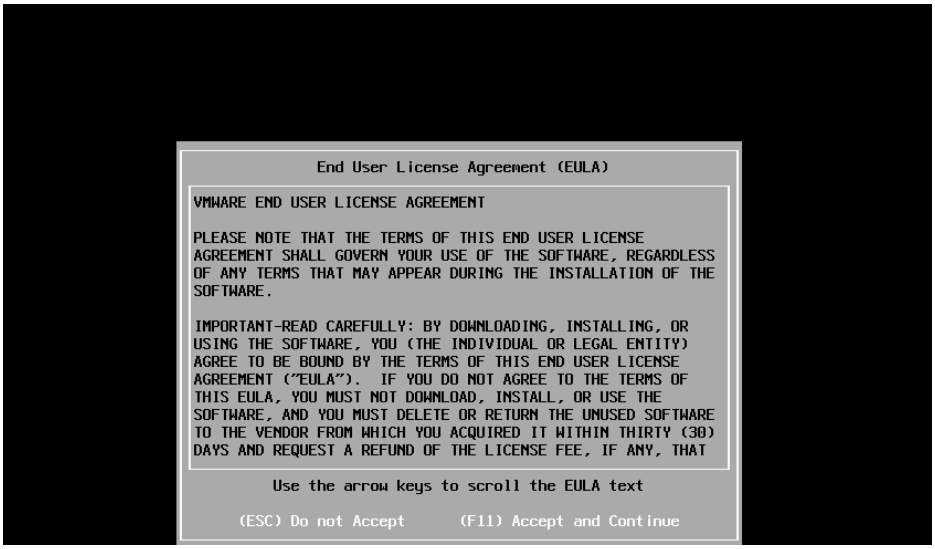
Step 65 Wait for the ESXi installer to fully load.

Note The vmkibft, iscsi_vmk and vmw_vaaip_netapp modules will take a while to load.

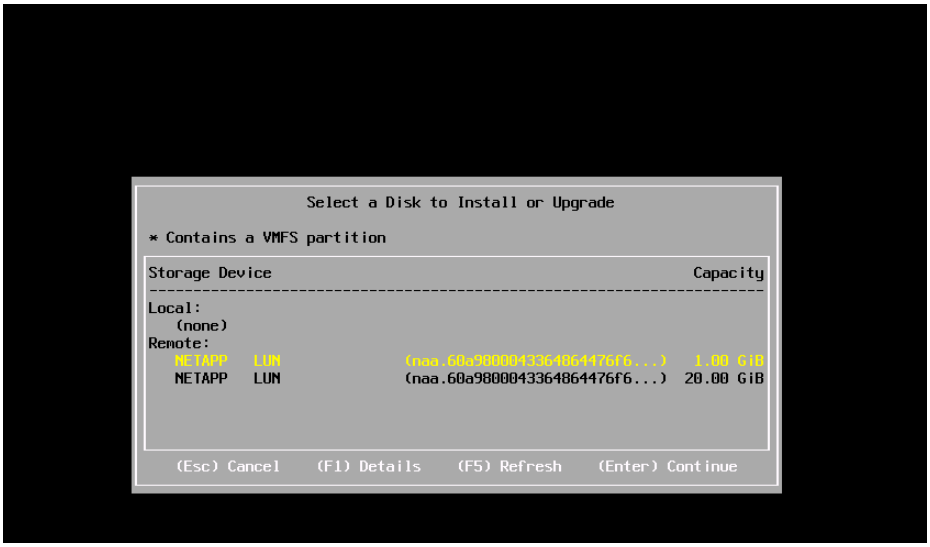
Step 66 Press Enter to start the installer.



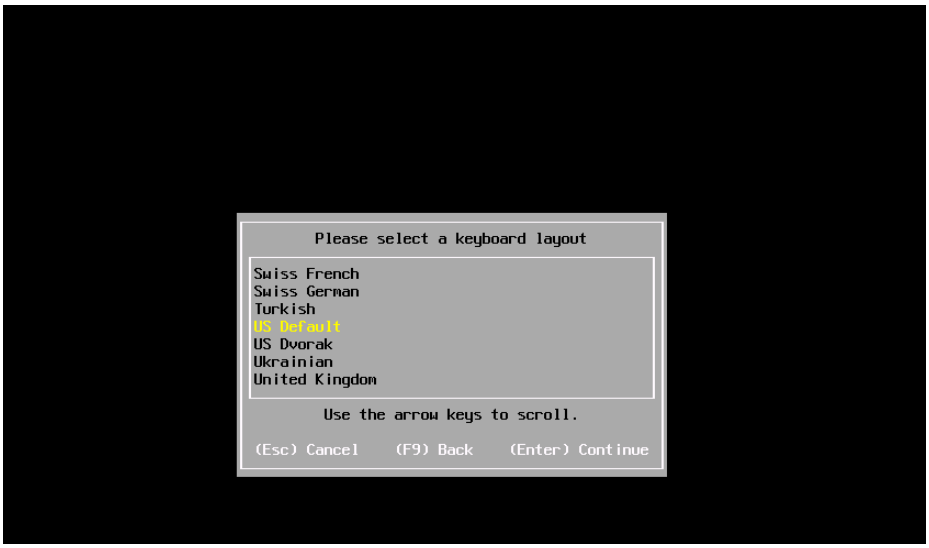
Step 67 Press F11 to accept the EULA



Step 68 Select the **1GB NETAPP Disk** for Installation, **DO NOT USE THE 20GB DISK or the local HDD if one is installed**.

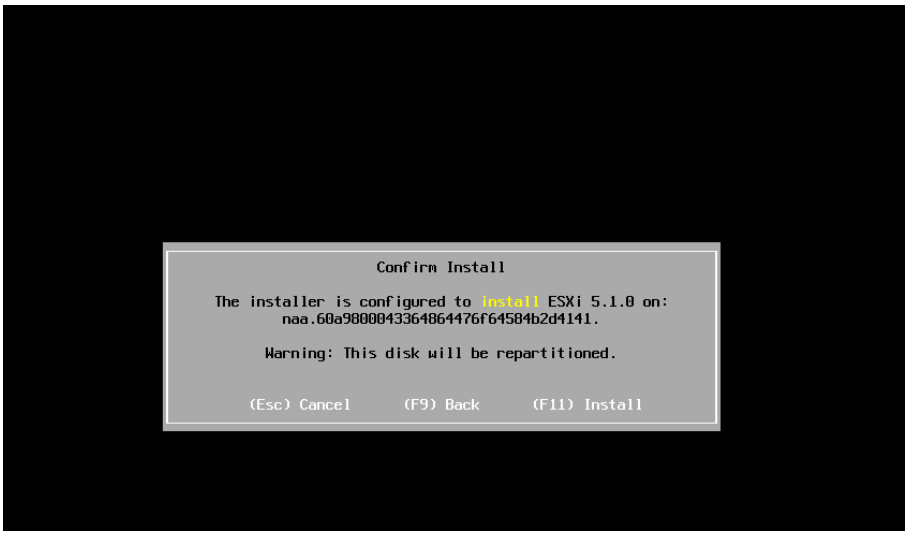


Step 69 Select your local keyboard layout

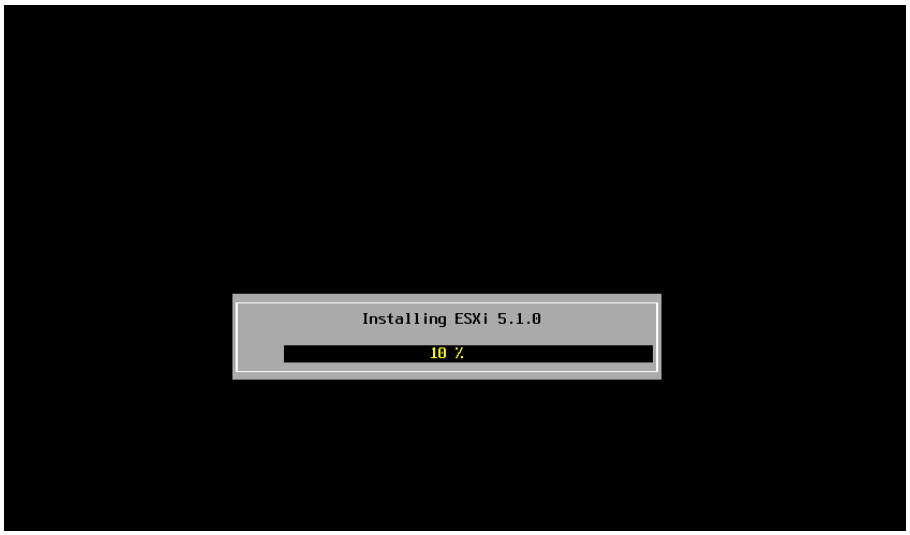


Step 70 Configure “1234QWer” as the root password.

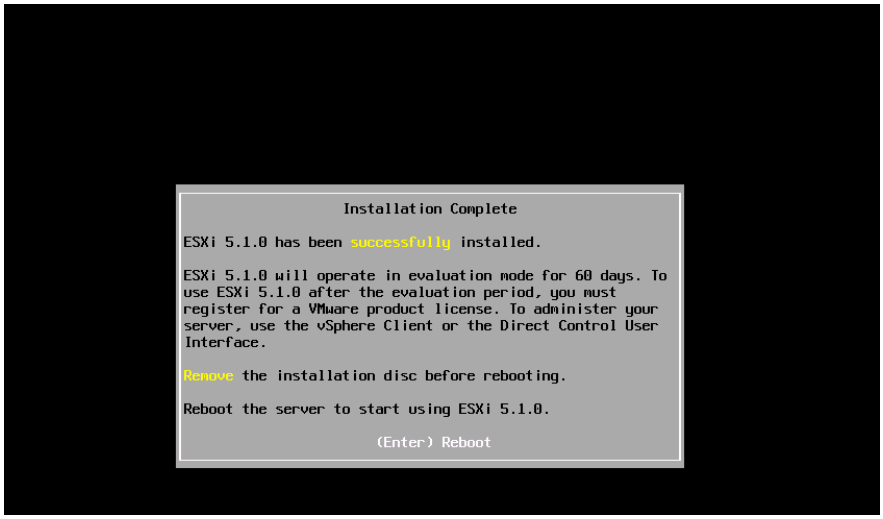
Step 71 Start the installation by confirming the installation disk with F11.



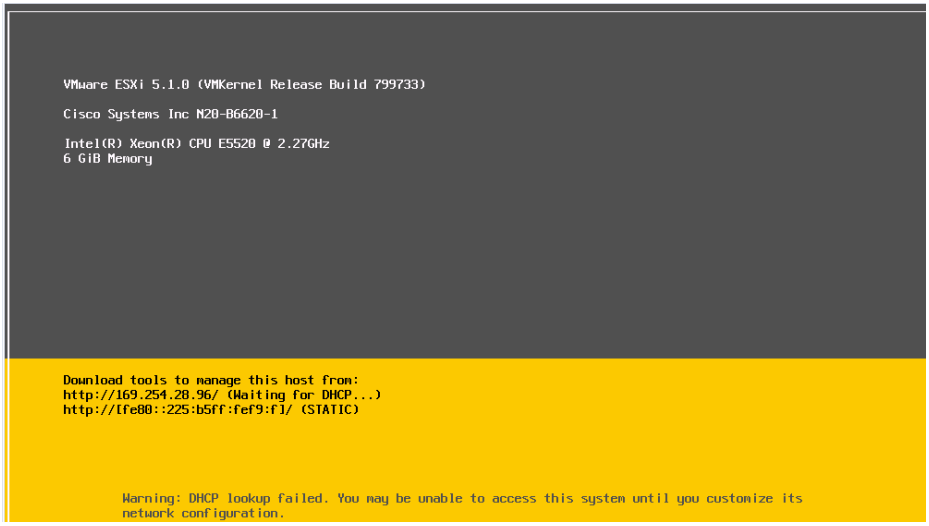
Step 72 The complete installation will take just 4-5 Minute including the final reboot.



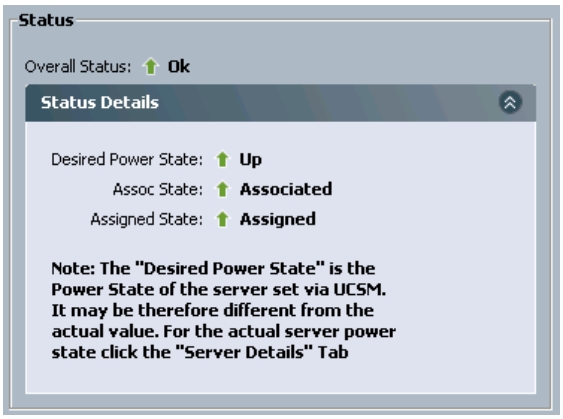
Step 73 When the installation is finished press enter to reboot.



Step 74 ESXi is installed and running! (do NOT configure anything yet)



Step 75 Notice the service profile status: up, associated and powered on.



Task 11: 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

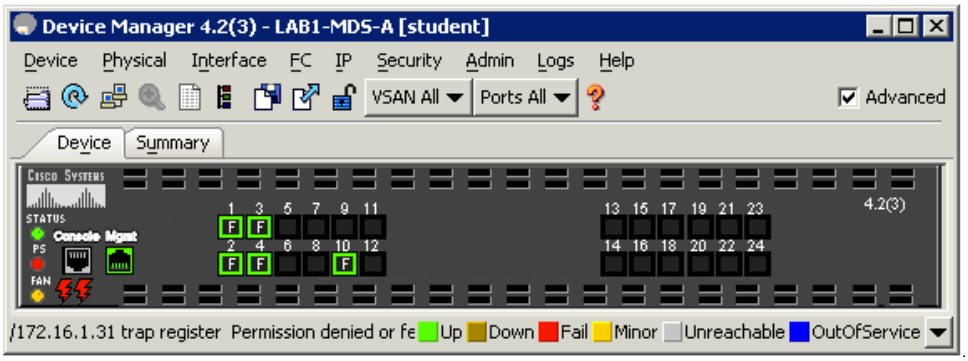
Complete these steps:

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

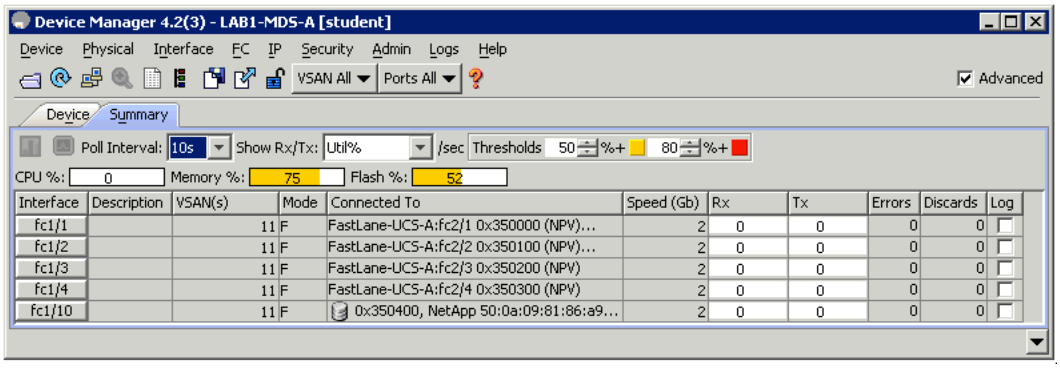
Note If Cisco Device Manager is not installed or the wrong version is installed: Open http://172.16.1.31 and install Cisco device manager directly from the MDS.

Step 2 Enter IP address 172.16.1.31, use username “student” and password “1234QWer”, and click **Open**.

MDS device manager will open up.

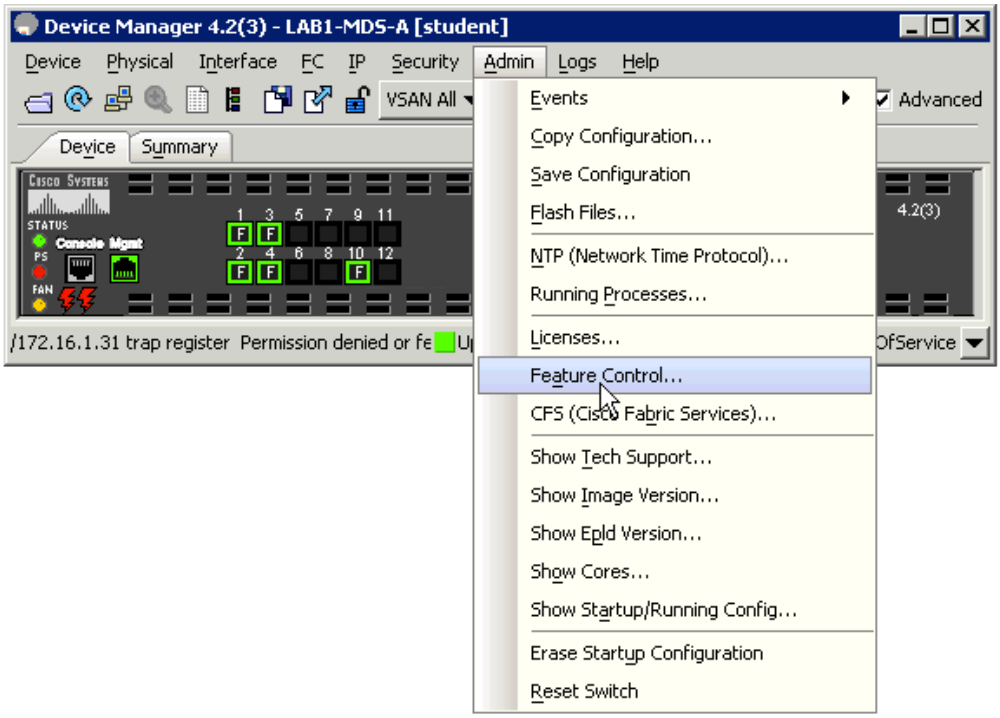


Step 3 Click the Summary tab. Note connected interfaces. Specifically, note that the MDS switch is reporting which Fabric Interconnect is visible, and the ports are running in NPV mode. When you are finished on this tab, return to the Device tab.

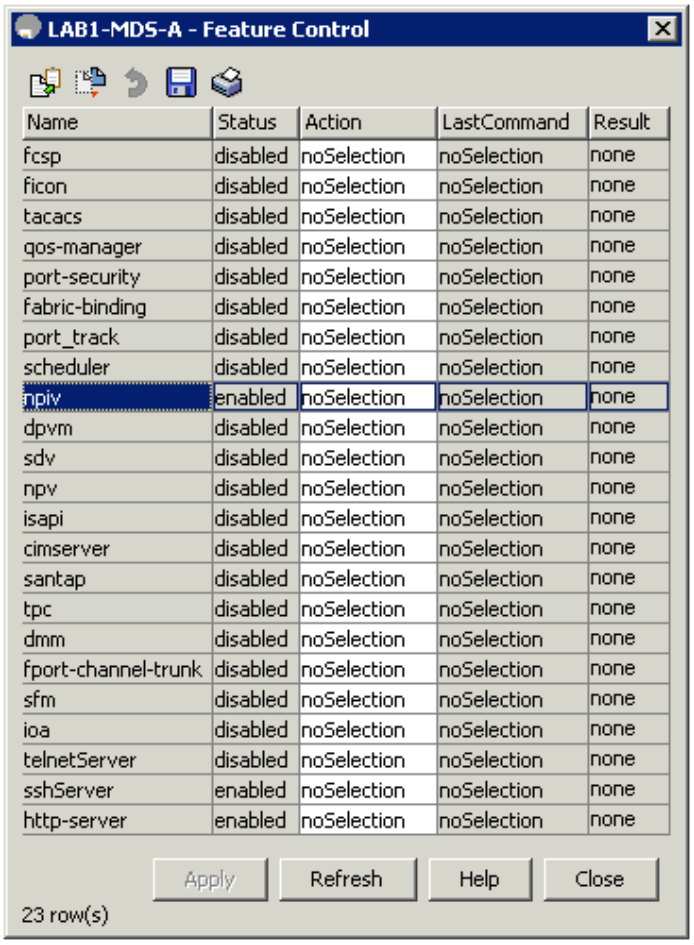


Note The text in the "Connected To" field for the Fabric Interconnects is being returned by the Fabric Interconnect during the login process. This is useful information for mapping connections or troubleshooting connection problems.

Step 4 Click **Admin** and **Feature Control**.

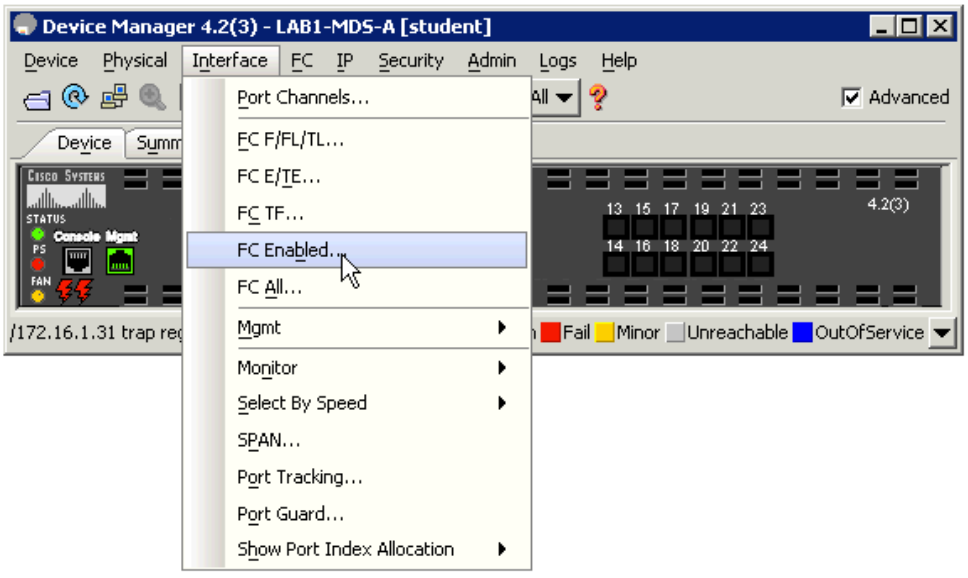


Step 5 Find the line **npiv**. NPIV is the feature on the MDS switch that supports multiple Fibre Channel devices logging in through the same physical port. Note that the feature is enabled.

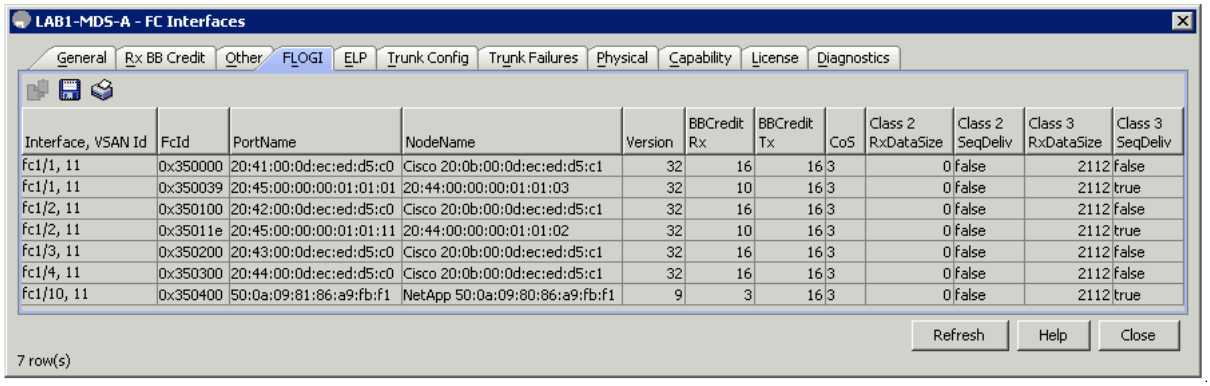


Step 6 Close the **Feature Control** window.

Step 7 Click **Interface** and **FC Enabled**.

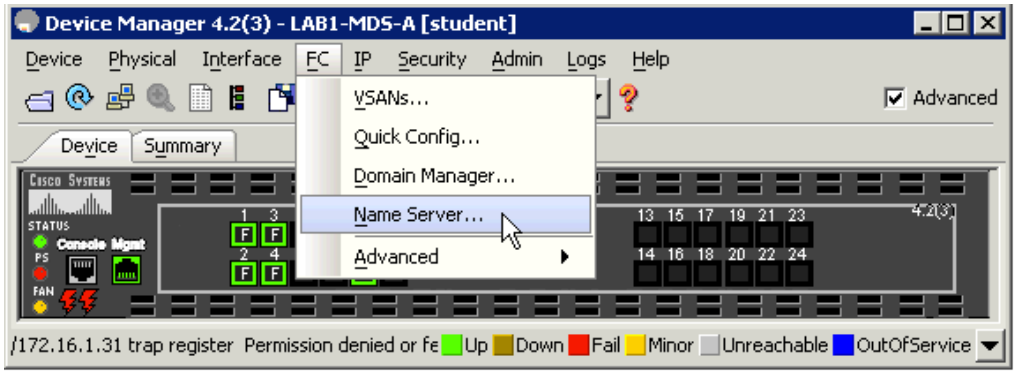


Step 8 Choose the **FLOGI** tab. Find your server's virtualized WWPN and WWNN and note the physical interface that it is logged into. There may be several other Pods that are WWNNs logged into the same physical interface. Click **Close**.

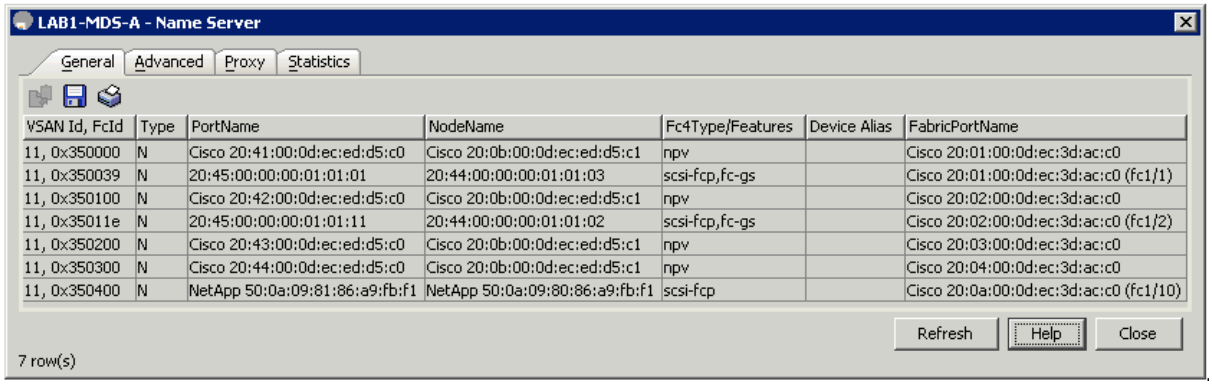


Interface, VSAN Id	FcId	PortName	NodeName	Version	BBCredit Rx	BBCredit Tx	CoS	Class 2 RxDataSize	Class 2 SeqDeliv	Class 3 RxDataSize	Class 3 SeqDeliv
fc1/1, 11	0x350000	20:41:00:0d:ec:ed:d5:c0	Cisco 20:0b:00:0d:ec:ed:d5:c1	32	16	16	3	0	false	2112	false
fc1/1, 11	0x350039	20:45:00:00:00:01:01:01	20:44:00:00:00:01:01:03	32	10	16	3	0	false	2112	true
fc1/2, 11	0x350100	20:42:00:0d:ec:ed:d5:c0	Cisco 20:0b:00:0d:ec:ed:d5:c1	32	16	16	3	0	false	2112	false
fc1/2, 11	0x35011e	20:45:00:00:00:01:01:11	20:44:00:00:00:01:01:02	32	10	16	3	0	false	2112	true
fc1/3, 11	0x350200	20:43:00:0d:ec:ed:d5:c0	Cisco 20:0b:00:0d:ec:ed:d5:c1	32	16	16	3	0	false	2112	false
fc1/4, 11	0x350300	20:44:00:0d:ec:ed:d5:c0	Cisco 20:0b:00:0d:ec:ed:d5:c1	32	16	16	3	0	false	2112	false
fc1/10, 11	0x350400	50:0a:09:81:86:a9:fb:f1	NetApp 50:0a:09:80:86:a9:fb:f1	9	3	16	3	0	false	2112	true

Step 9 Click **FC** and **Name Server**.



Step 10 Find your Pod's ESXi servers. Look at the PortName and NodeName fields.

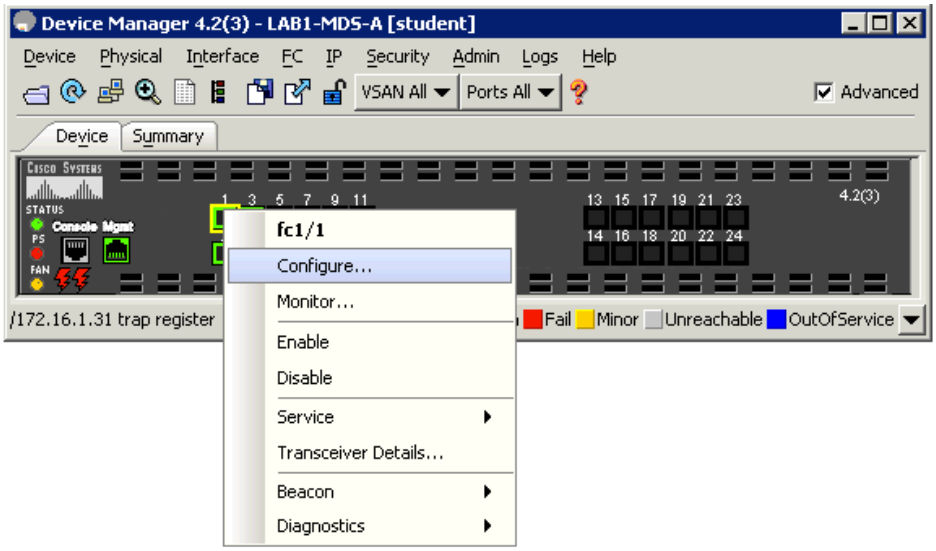


VSAN Id, FcId	Type	PortName	NodeName	Fc4Type/Features	Device Alias	FabricPortName
11, 0x350000	N	Cisco 20:41:00:0d:ec:ed:d5:c0	Cisco 20:0b:00:0d:ec:ed:d5:c1	npv		Cisco 20:01:00:0d:ec:3d:ac:c0
11, 0x350039	N	20:45:00:00:00:01:01:01	20:44:00:00:00:01:01:03	scsi-fcp,fc-gs		Cisco 20:01:00:0d:ec:3d:ac:c0 (fc1/1)
11, 0x350100	N	Cisco 20:42:00:0d:ec:ed:d5:c0	Cisco 20:0b:00:0d:ec:ed:d5:c1	npv		Cisco 20:02:00:0d:ec:3d:ac:c0
11, 0x35011e	N	20:45:00:00:00:01:01:11	20:44:00:00:00:01:01:02	scsi-fcp,fc-gs		Cisco 20:02:00:0d:ec:3d:ac:c0 (fc1/2)
11, 0x350200	N	Cisco 20:43:00:0d:ec:ed:d5:c0	Cisco 20:0b:00:0d:ec:ed:d5:c1	npv		Cisco 20:03:00:0d:ec:3d:ac:c0
11, 0x350300	N	Cisco 20:44:00:0d:ec:ed:d5:c0	Cisco 20:0b:00:0d:ec:ed:d5:c1	npv		Cisco 20:04:00:0d:ec:3d:ac:c0
11, 0x350400	N	NetApp 50:0a:09:81:86:a9:fb:f1	NetApp 50:0a:09:80:86:a9:fb:f1	scsi-fcp		Cisco 20:0a:00:0d:ec:3d:ac:c0 (fc1/10)

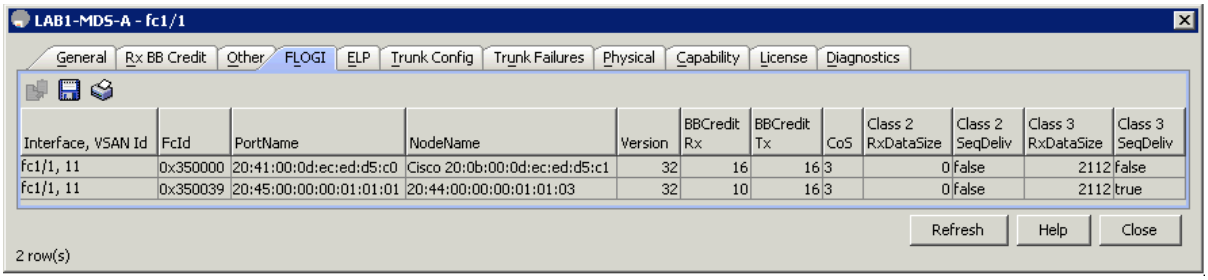
Step 11 When you have found your Pod's server, note the Fibre Channel ID (FcId, in the first column) that is assigned to your FC interface. This ID uniquely identifies your FC port in the Fibre Channel fabric.

Server	WWPN/PortName	FCID
ESXi1		
ESXi2		

Step 12 Find the physical port that you made note of in an earlier step, and right-click it in the Device view. Click **Configure**.



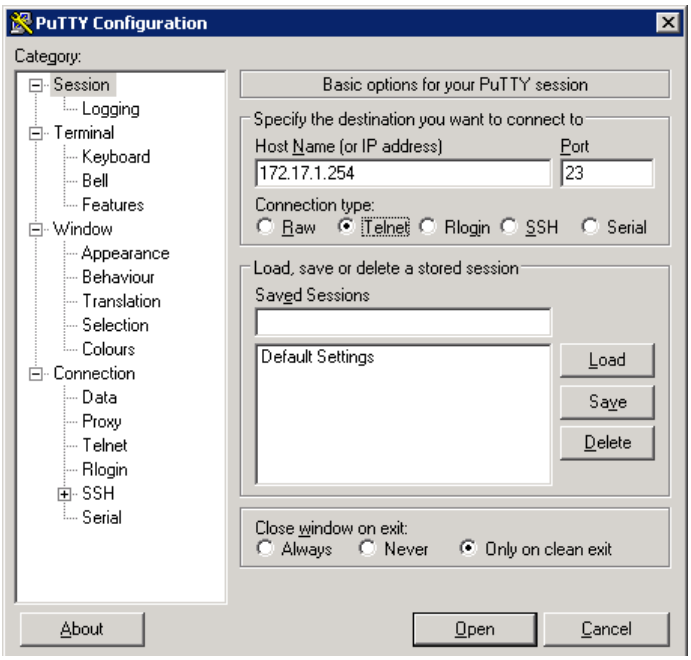
Step 13 Click the **FLOGI** tab. Note that you will see at least two logins to this port. One is the Fabric Interconnect port, and the other will be your vHBA port. Each logged-in device will have its own FcId, uniquely identifying the device on the Fibre Channel fabric. When you have completed reviewing the contents of the table, click **Close**.



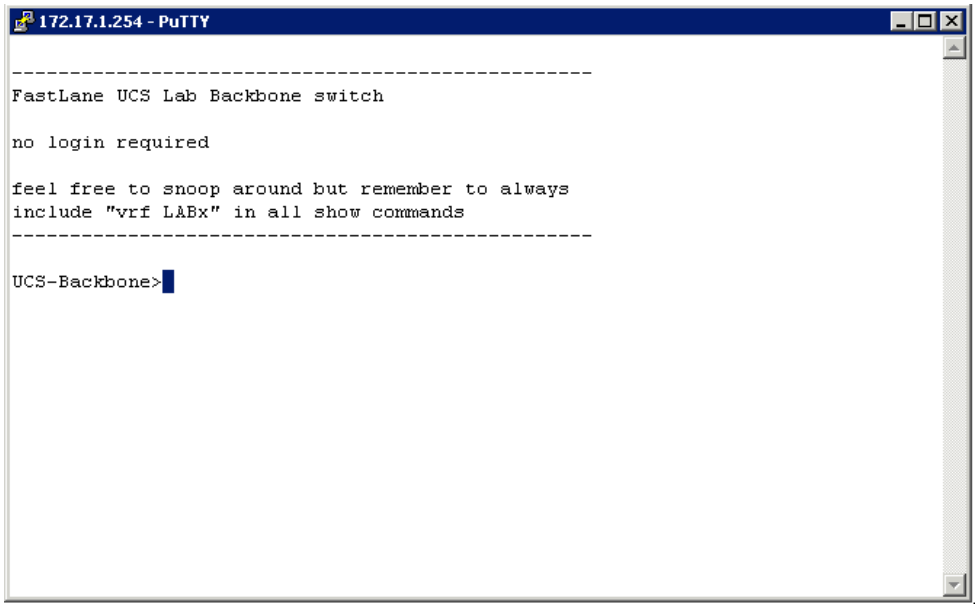
Step 14 Close the **Device Manager** window.

Step 15 Find and double-click the **putty.exe** icon on your student desktop.

Step 16 Enter the IP address 172.17.1.254, select “Telnet” and click **Open**.

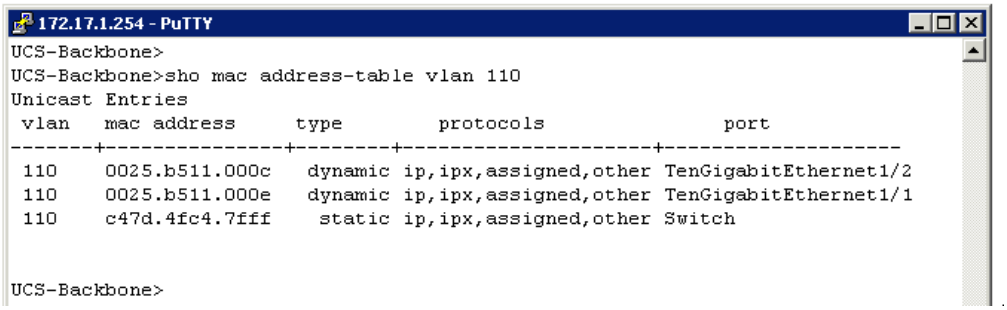


Step 17 The Switch in this lab does not require authentication. Since it is a shared resource we will use unprivileged mode only. (even your instructor does not have the enable password, so don’t bother to ask ;))



Step 18 Since our ESXi servers are not yet configured with IP addresses they ask for DHCP all the time, which makes sure they appear in the mac address tables.

Step 19 Enter **sh mac address-table vlan LP0**, replacing L with the Lab ID and P with your pod number.



Step 20 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. In this example, the address is 0025.b511.000c and 0025.b511.000e. You should also see a MAC address c47d.4fc4.7fff, that is the switch Layer3 interface (you can check with "sho int vlanLP0")

Step 21 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:

show interface *tengig x/y* (replacing x/y with the values from the previous step)

show mac address-table interface *tengig x/y*

Step 22 Type **exit** to log out of the switch and close the PuTTY window.

Step 23 Notify your instructor that you are done

Lab 5-1: Building a VMWare Infrastructure

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

Task 1: Configure your ESXi servers

In this task, you will configure your two ESXi servers.

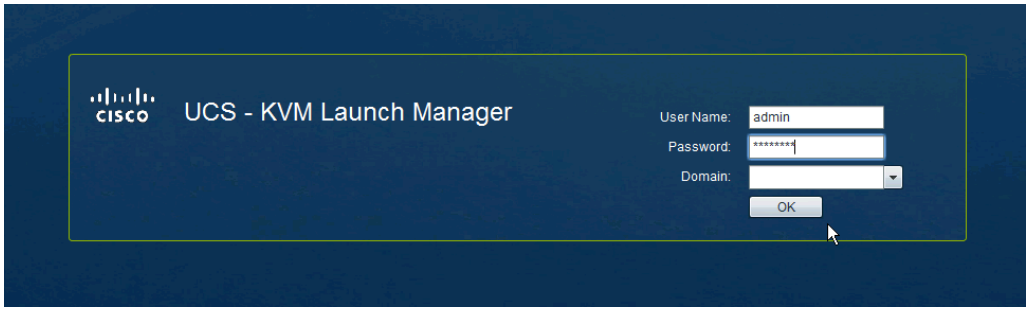
Activity Procedure

Complete these steps:

Step 1 Double-click the “UCS Manager” icon on your desktop.

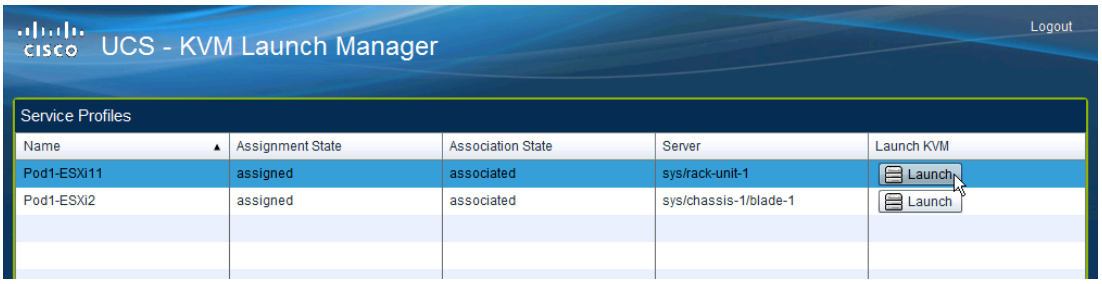
Step 2 Click on “Launch KVM Manager” and acknowledge all following warnings to bring up the KVM without using the UCS manager.

Step 3 Log into KVM Manager with “admin” and “1234QWer”

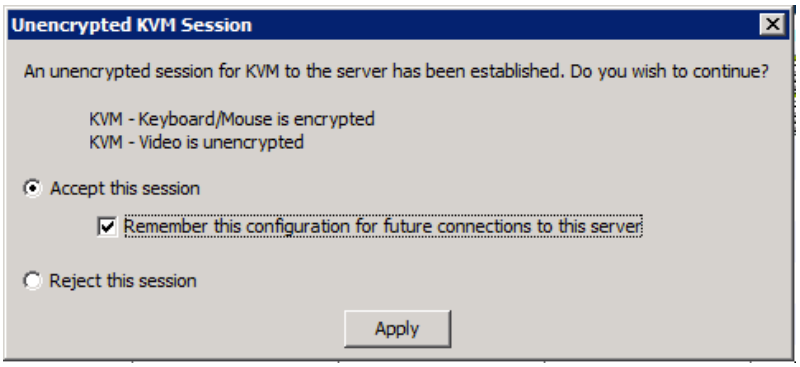


Note	In a real data center additional accounts would have been created in UCSM to allow server admins to use KVM but NOT log into UCSM.

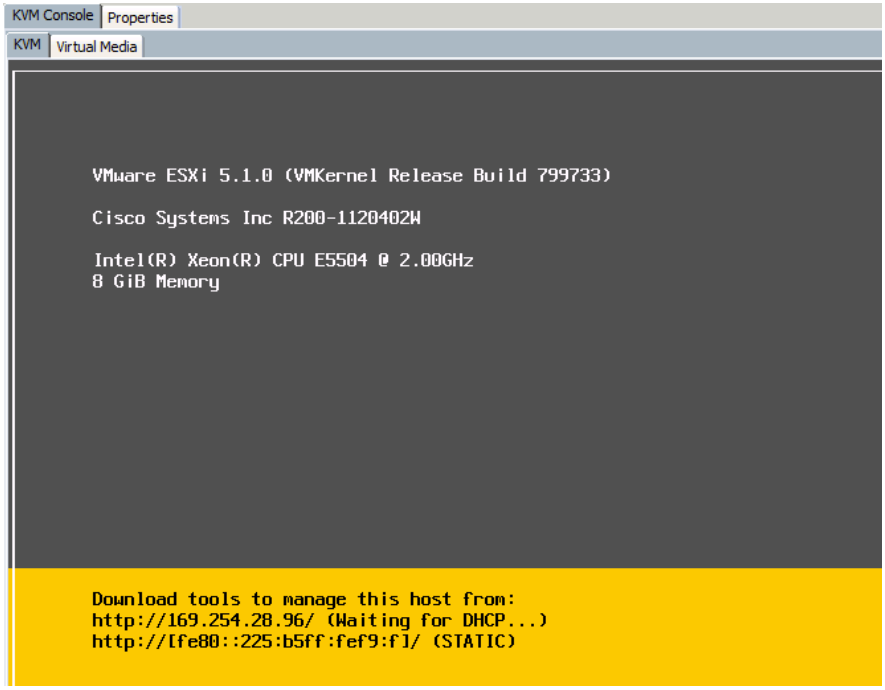
Step 4 Click on “Launch” on row ESXi1 to open a KVM session



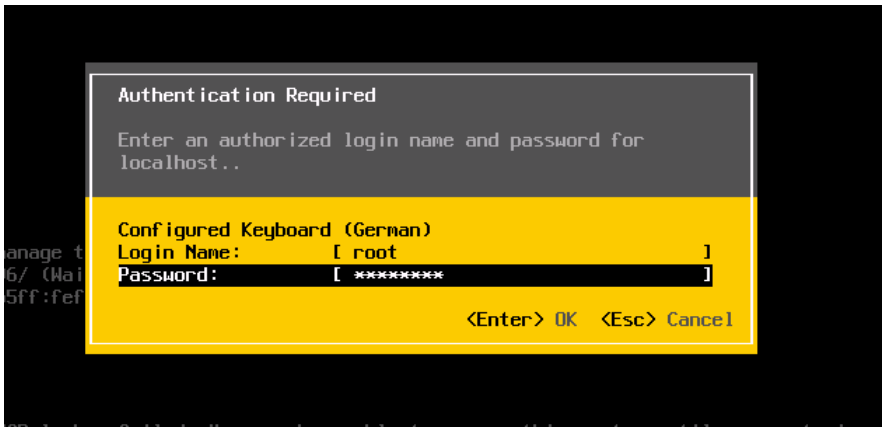
Step 5 Confirm unencrypted connectivity.



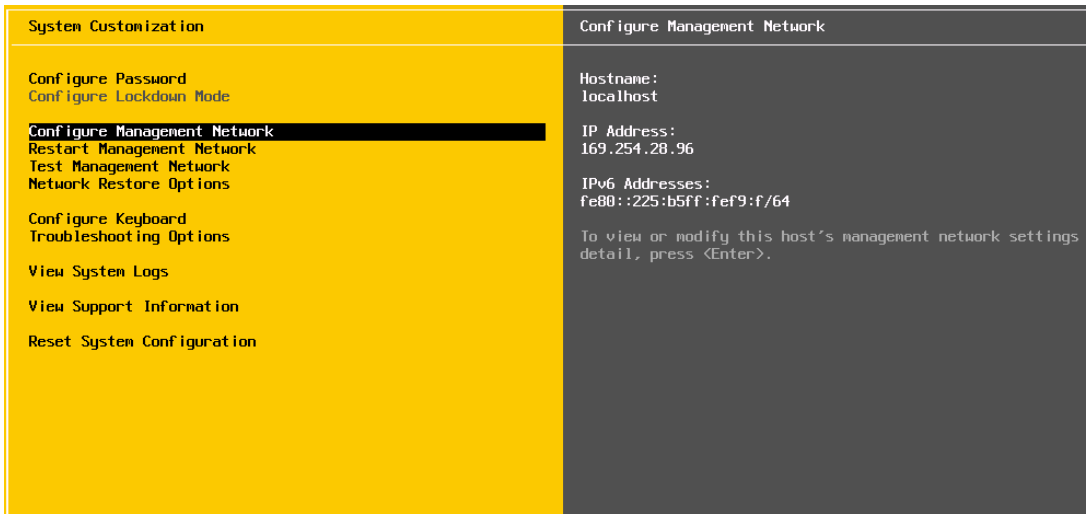
Step 6 Press F2 to get started (maybe twice)



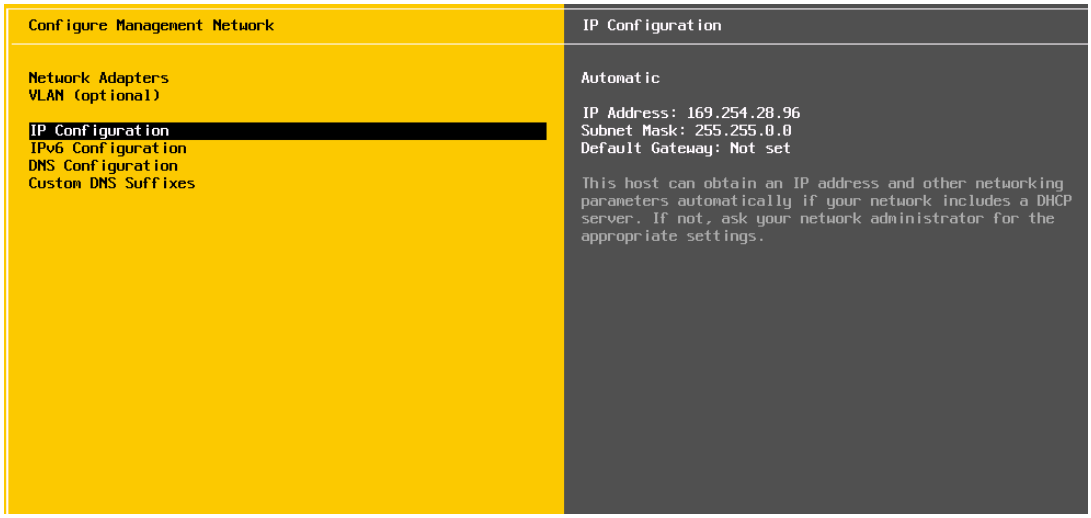
Step 7 Enter username “root” with password “1234QWer” to log in



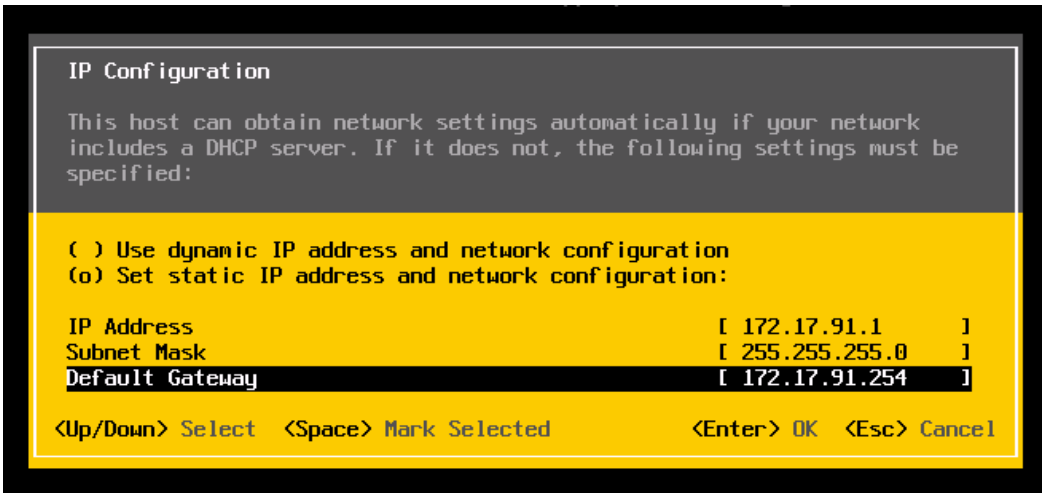
Step 8 Select “Configure Management Network”



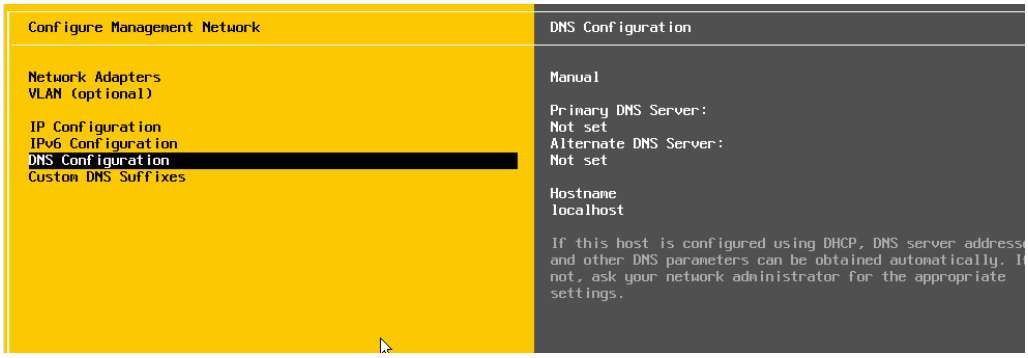
Step 9 Select “IP Configuration”



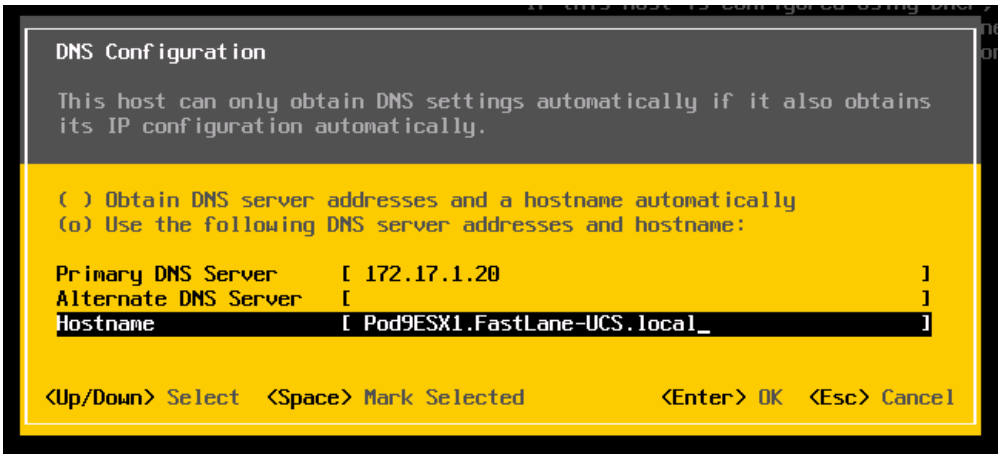
Step 10 Configure IP address **172.17.P1.1** with subnet mask 255.255.255.0 and default gateway **172.17.P1.254**



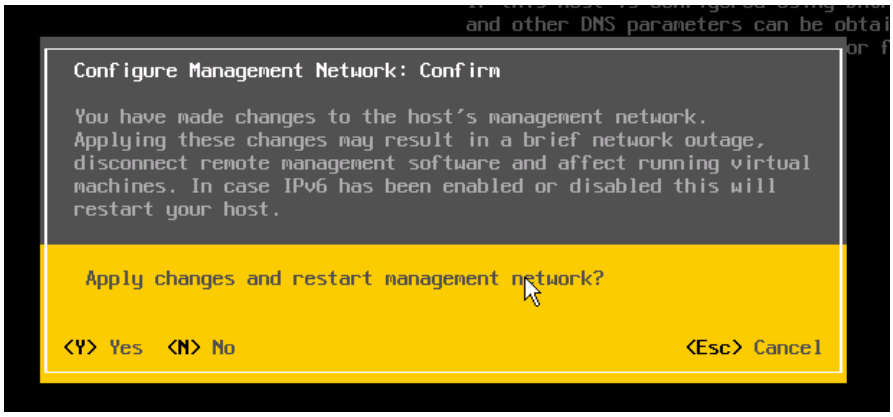
Step 11 Select “DNS Configuration”



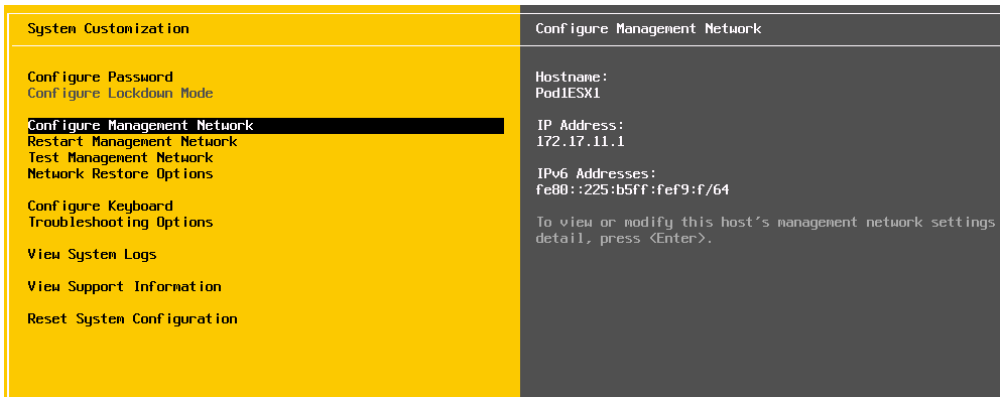
Step 12 Configure DNS server 172.17.1.20 and name **podPesx1.FastLane-UCS.local** as the hostname (P is your Pod#)



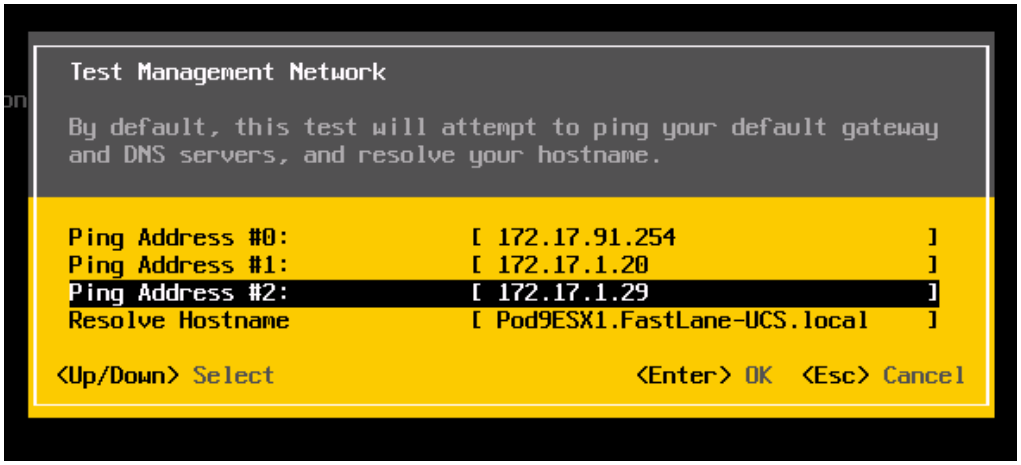
Step 13 Press “ESC” in the “Configure Management Network” screen. Press “Y” to confirm your changes (if you did not change the keyboard mapping this yould be Z or another key on your keyboard ;))



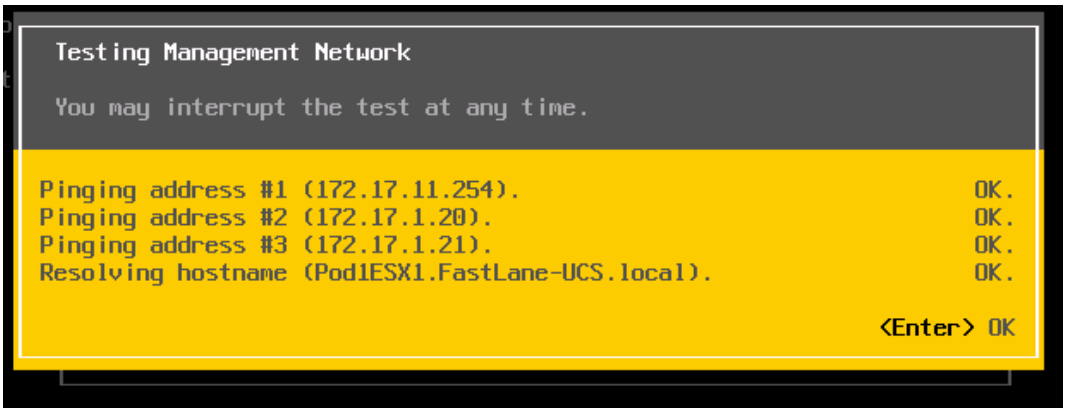
Step 14 Select "Test Management Network"



Step 15 Confirm the default Options (you can add your Student PC 172.17.1.2P (P is your Pod#) as Ping Address#2)



Step 16 Make sure the test result is "OK" for PINGs or we will run into problems with later labs. If you cannot fix the problem, ask your instructor for help.



Step 17 Close the KVM session.

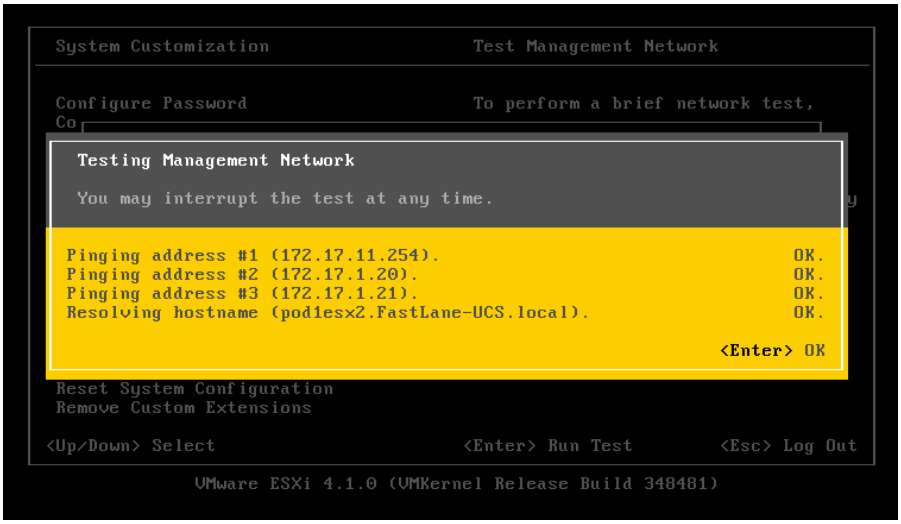
Step 18 Open a new KVM session from your KVM Manager, Connect to ESXi2.

Step 19 Press F2 to log in as “root” with password “1234QWer”.

Step 20 Configure IP address **172.17.P1.2/24** with default gateway **172.17.P1.254** (P is your Pod#)

Step 21 Configure DNS server **172.17.1.20** with local hostname **Pod#esx2.FastLane-UCS.local** (# is your Pod#)

Step 22 Test Management Network Connectivity. Once again we need 3x OK for PING! Ask your instructor for help if necessary.



Step 23 Close the KVM session.

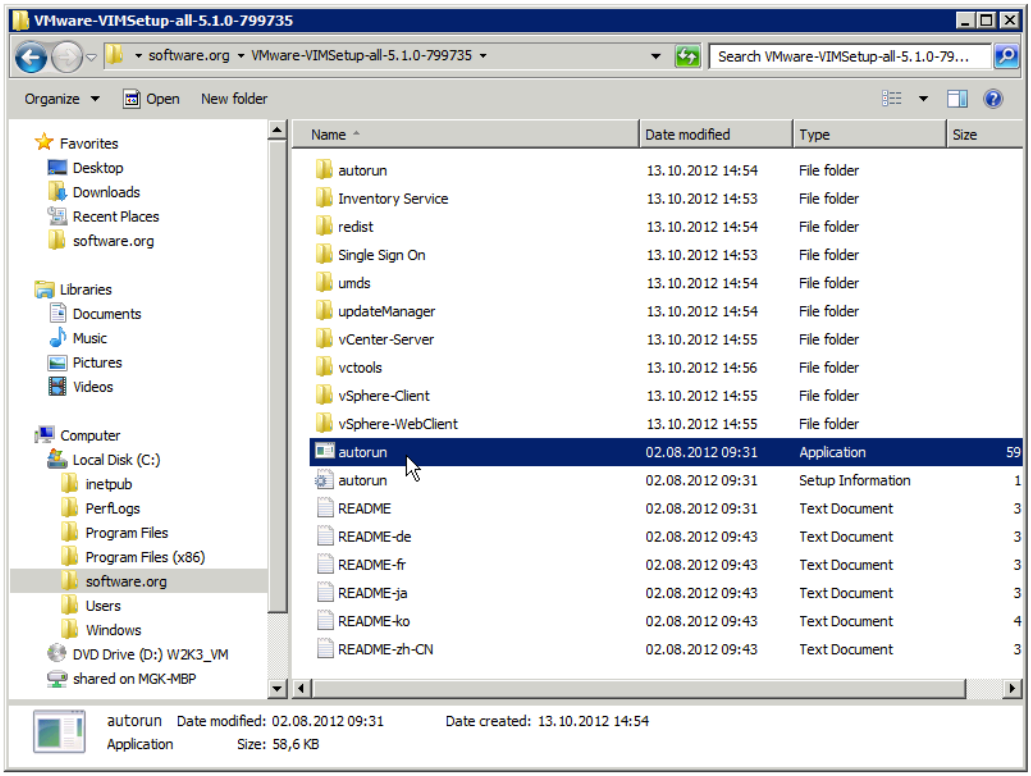
Task 2: Install vSphere / vCenter Server on your Student PC

In this task, you will configure your two ESXi servers.

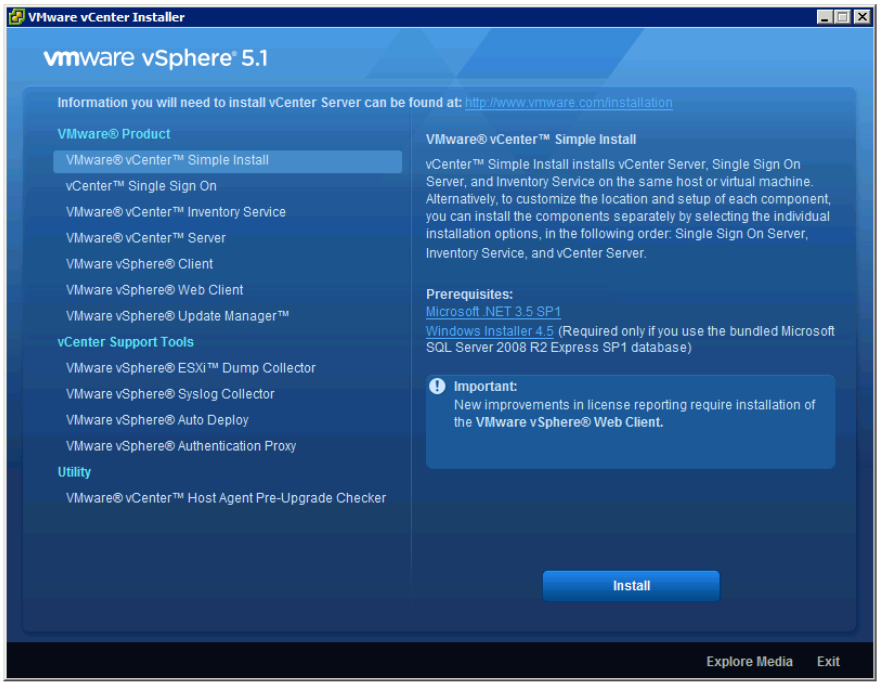
Activity Procedure

Complete these steps:

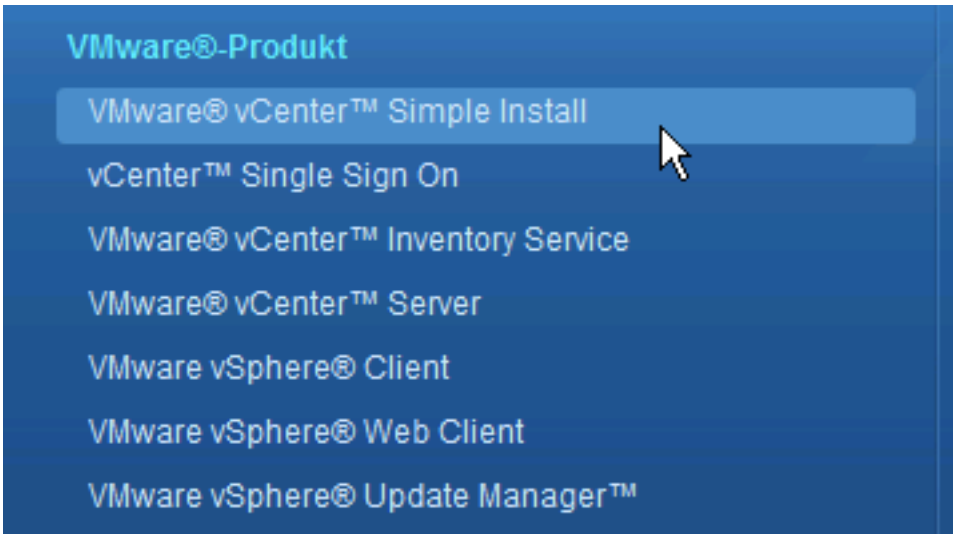
Step 1 Open Windows Explorer and navigate to “C:\software.org\VMware-VIMSetup-all-5.1.0-799735”.



Step 2 Click on “autorun.exe” to start the installation

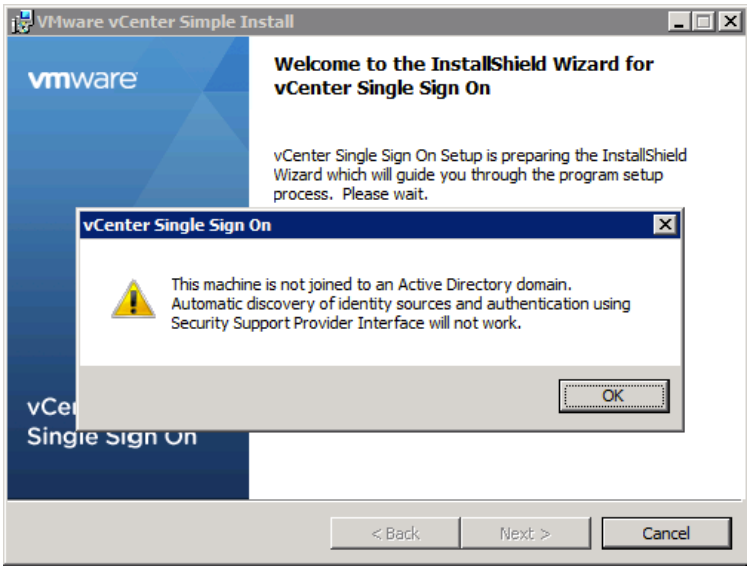


Step 3 Click “vCenter Server Simple Install” and Click “Install”

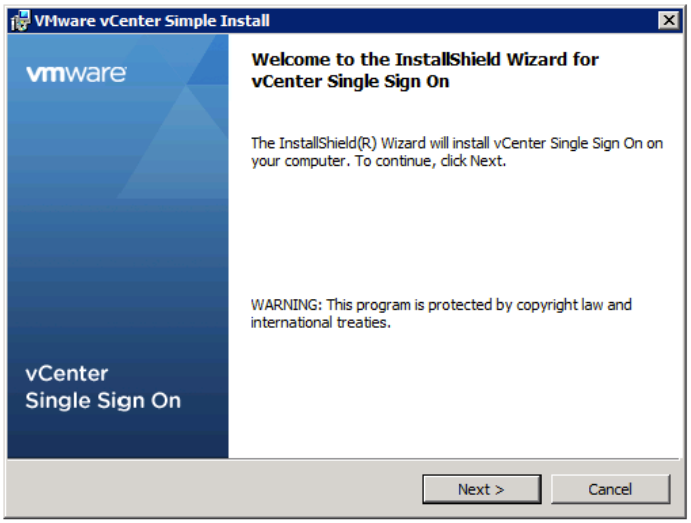


Step 4 vCenter Single Sign On will be installed first, wait for the installer to fully load.

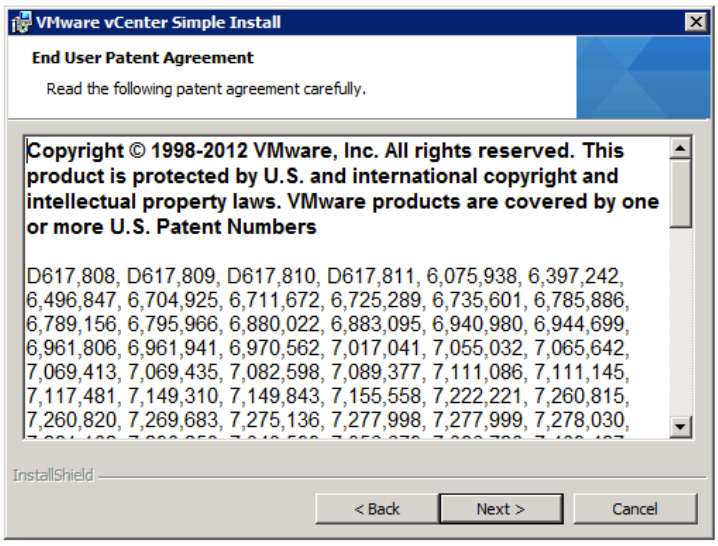
Step 5 Confirm that your student PC is not part of a AD domain.



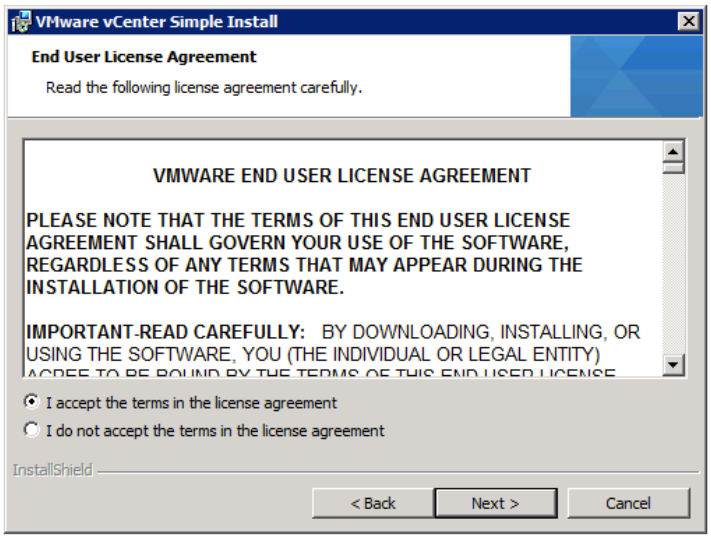
Step 6 Click “Next>” to start the installation.



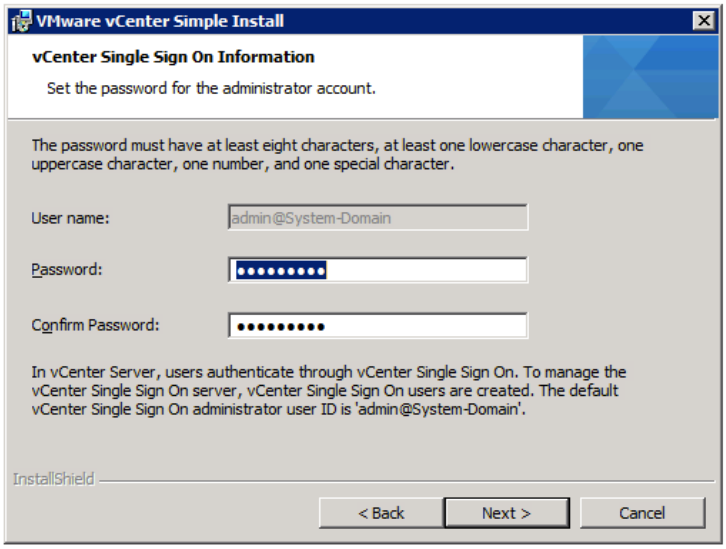
Step 7 Confirm the End User Patent Agreement.



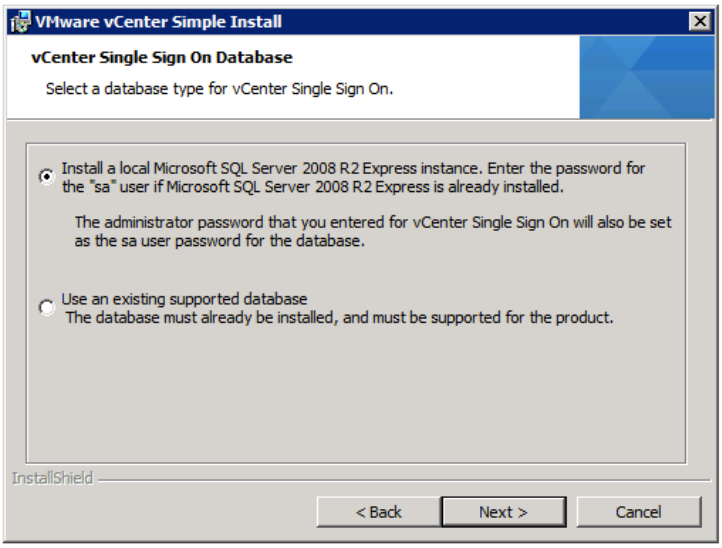
Step 8 Accept the License Agreement and click “Next>”



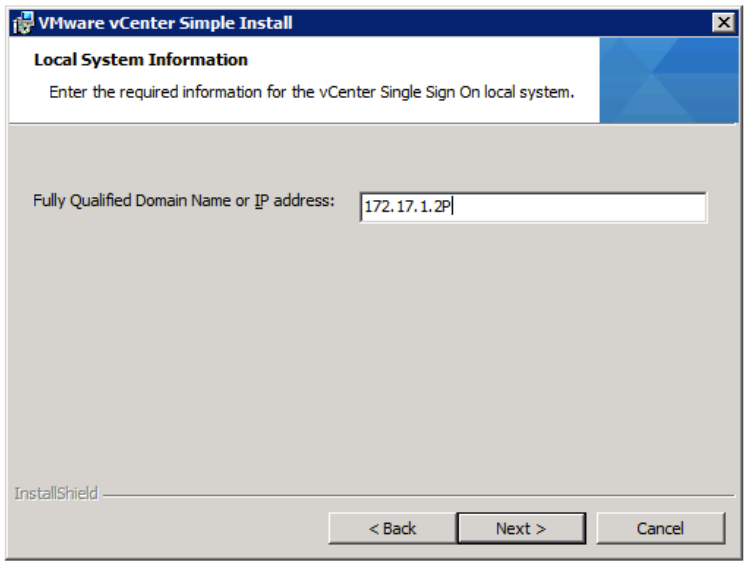
Step 9 Use “1234QWer!”as the password.



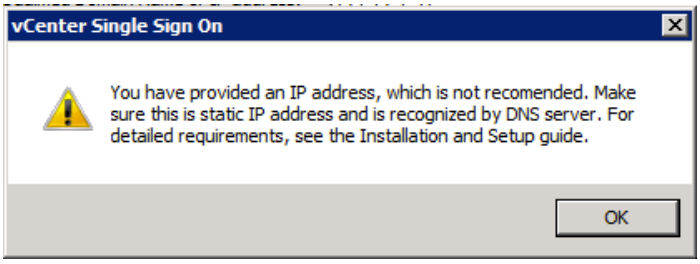
Step 10 Confirm local SQL Server Express installation by clicking ”Next>”



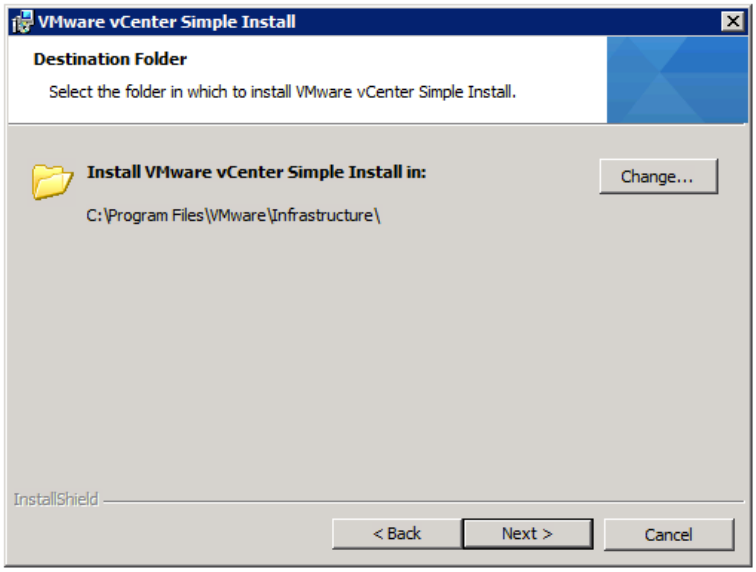
Step 11 Confirm “172.17.1.2#” (# is your pod#) as the IP address.



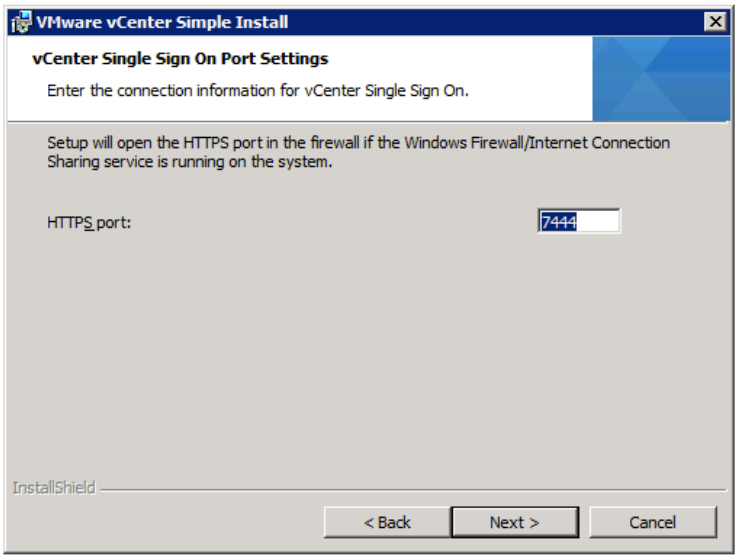
Step 12 Confirm usage of an IP address



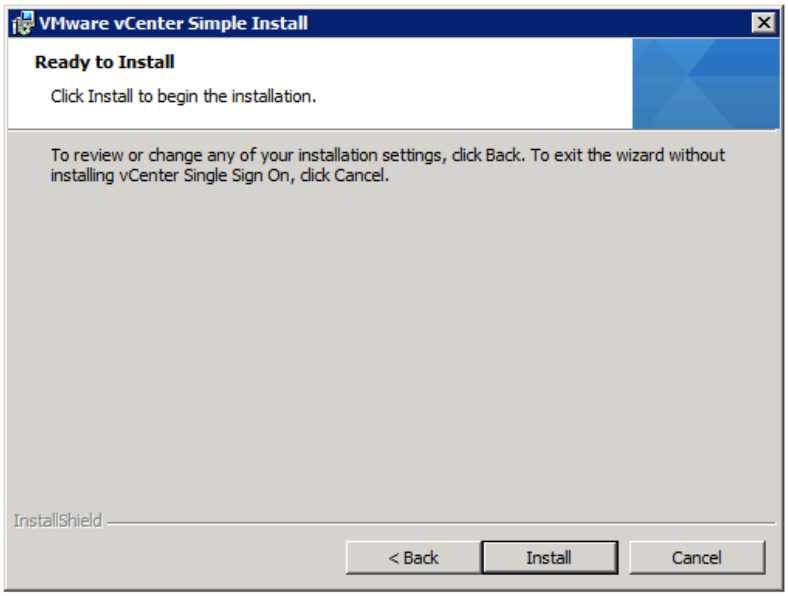
Step 13 Confirm the installation directory



Step 14 Confirm the SSO port settings.

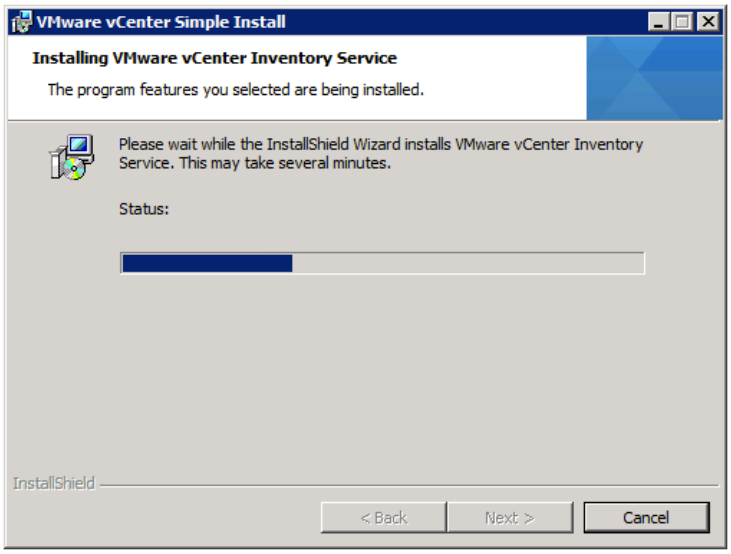


Step 15 Start the installer with “Install”.

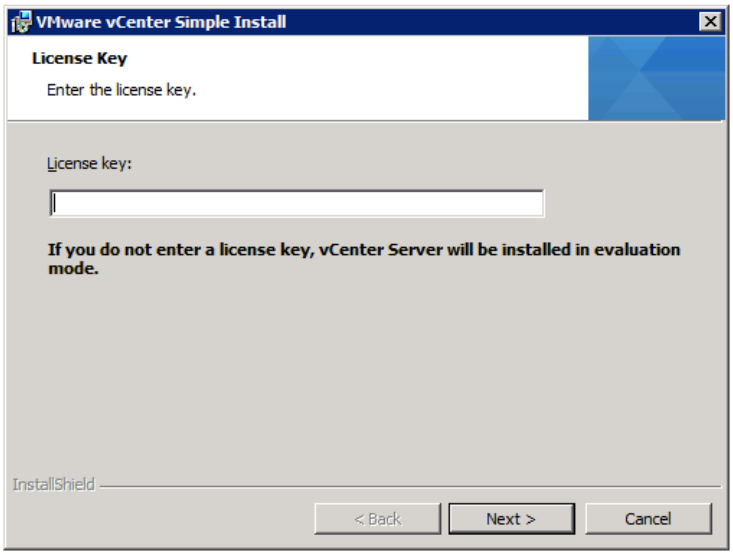


Step 16 Wait for the first Installer to complete. The installation (including SQL server) takes about 7 Minutes.

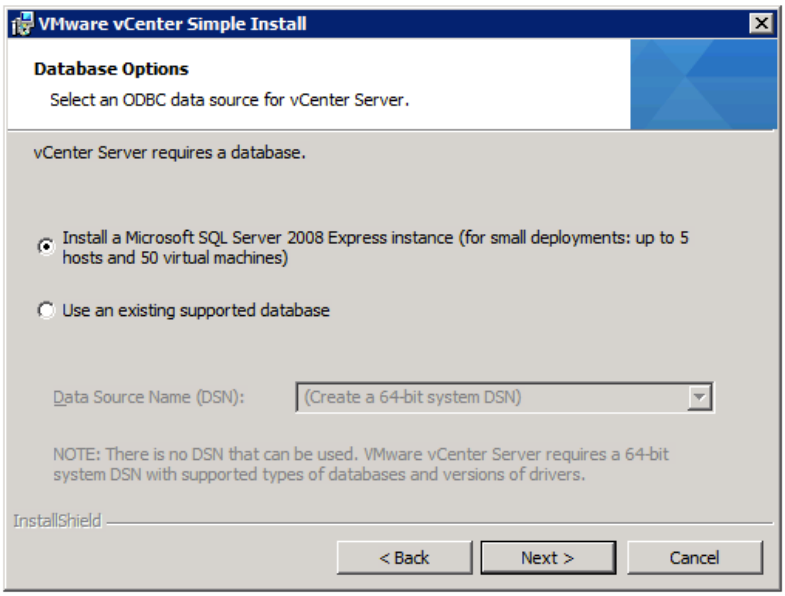
Step 17 vCenter Simple Setup continues automatically.



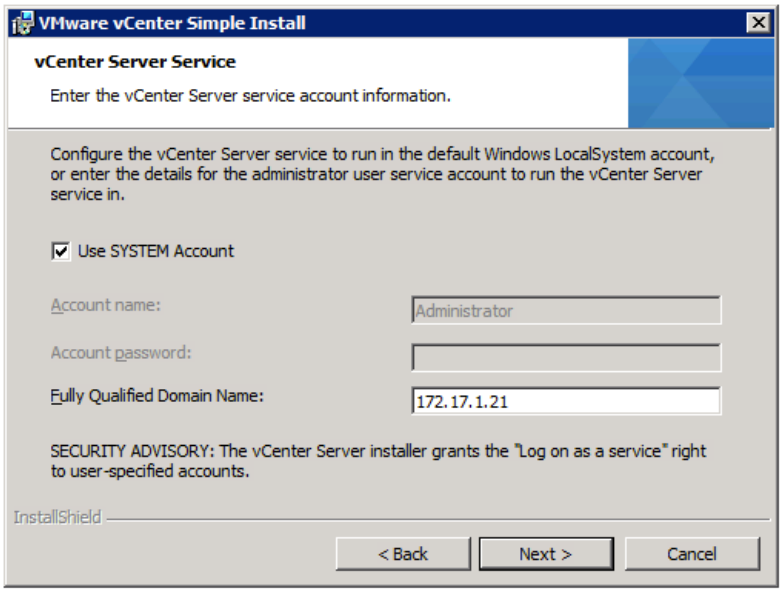
Step 18 Skip the License Key dialog by clicking “Next>”



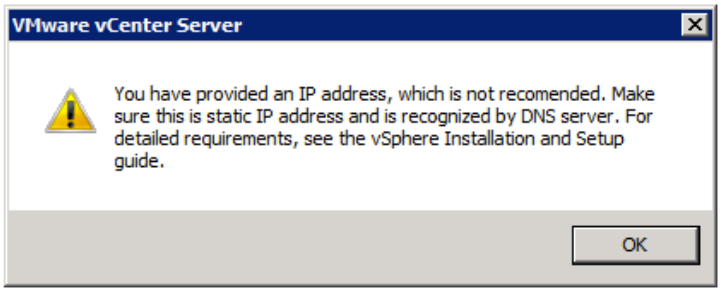
Step 19 Confirm the Microsoft SQL Server Express installation by clicking “Next>”



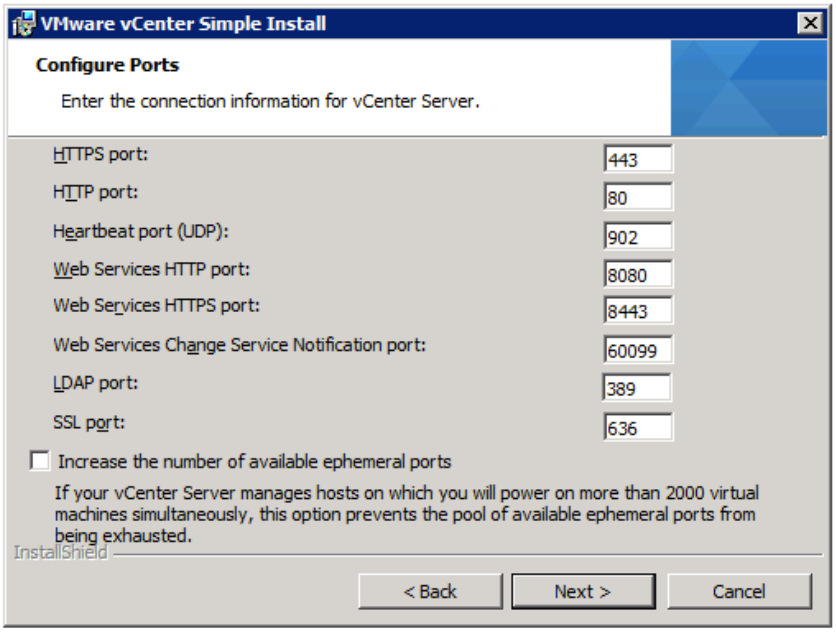
Step 20 Conform use of the SYSTEM account and make sure your FQDN is 172.17.1.2P (P is your Pod#), then click “Next>”



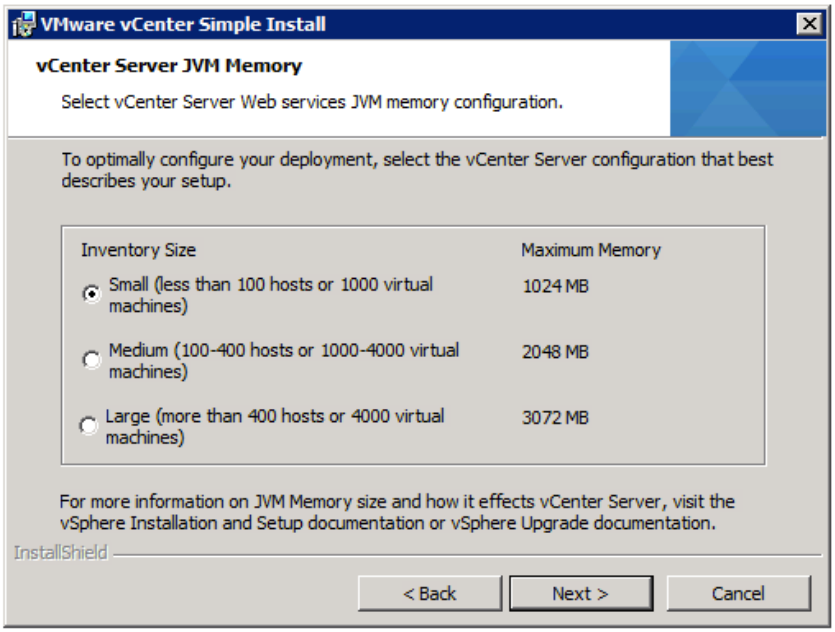
Step 21 Confirm use of an IP address



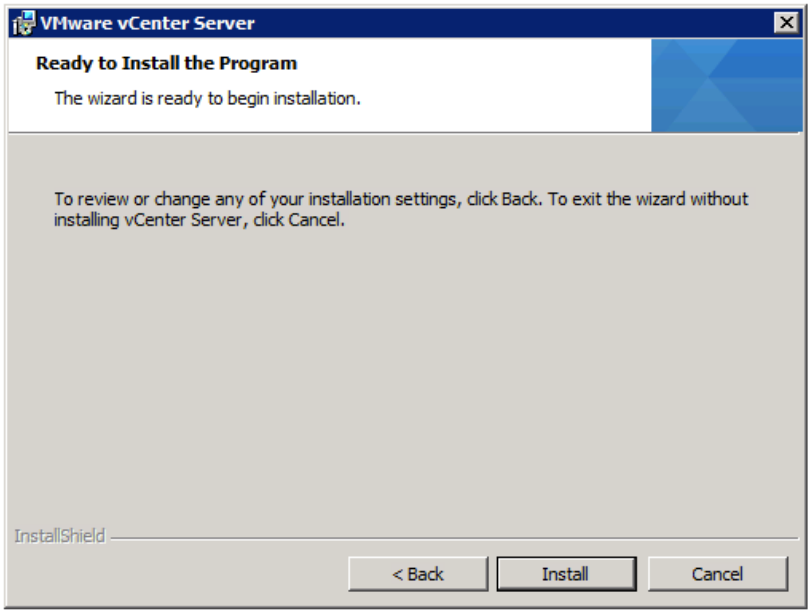
Step 22 Accept the default port numbers with “Next>”



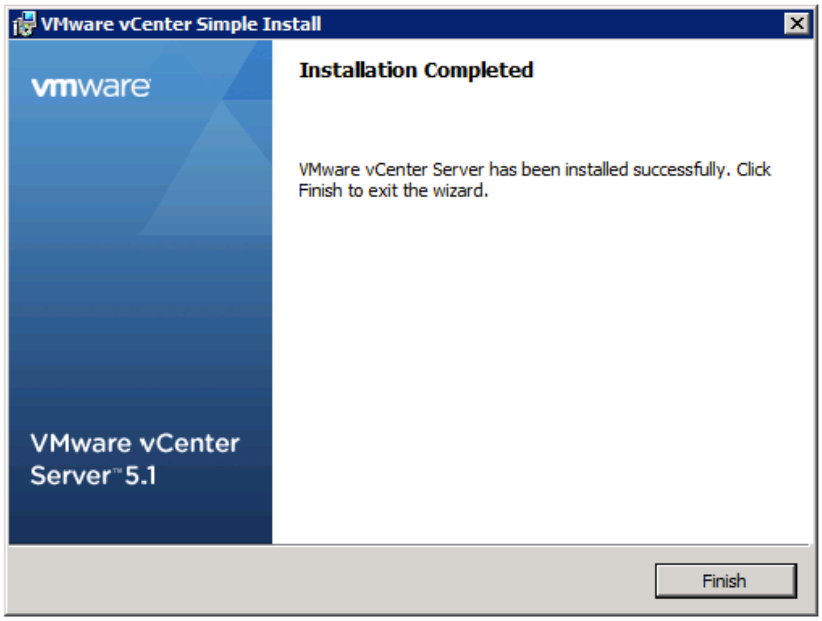
Step 23 Accept the default "small installation" JVM memory with "Next>"

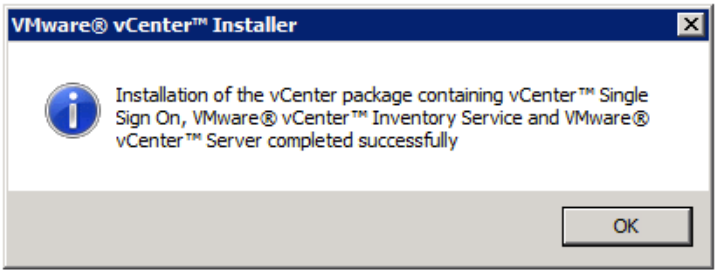


Step 24 Start the Installation with "Install". **The whole process will only take up to 8 minutes**.



Step 25 Click “Finish” to close the install wizard, do not close the main installer.





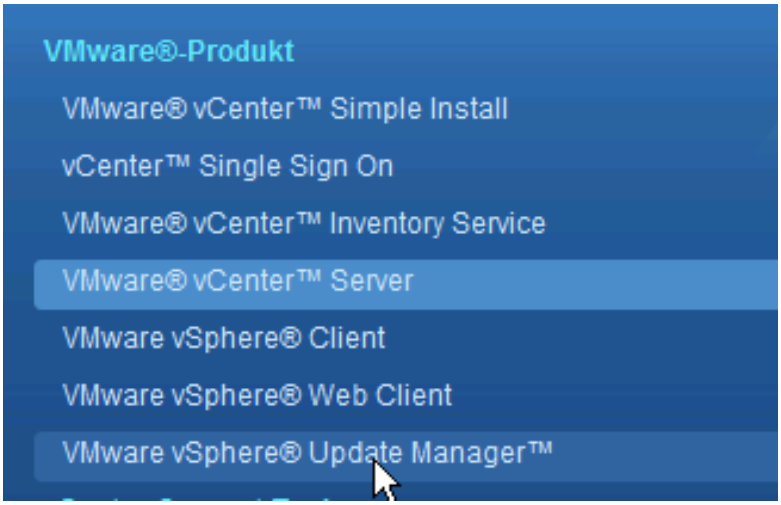
Task 3: Install VMWare Update Manager on your Student PC

In this task, you will configure your two ESXi servers.

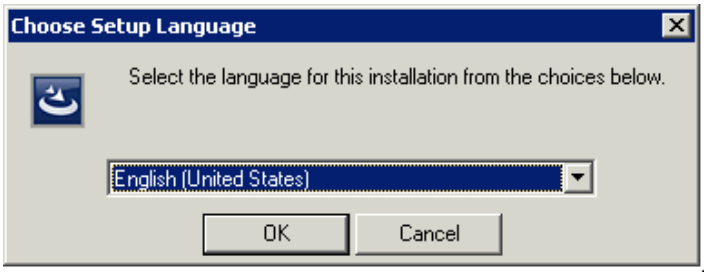
Activity Procedure

Complete these steps:

Step 1 Click “VMWare Update Manager” in the installer window

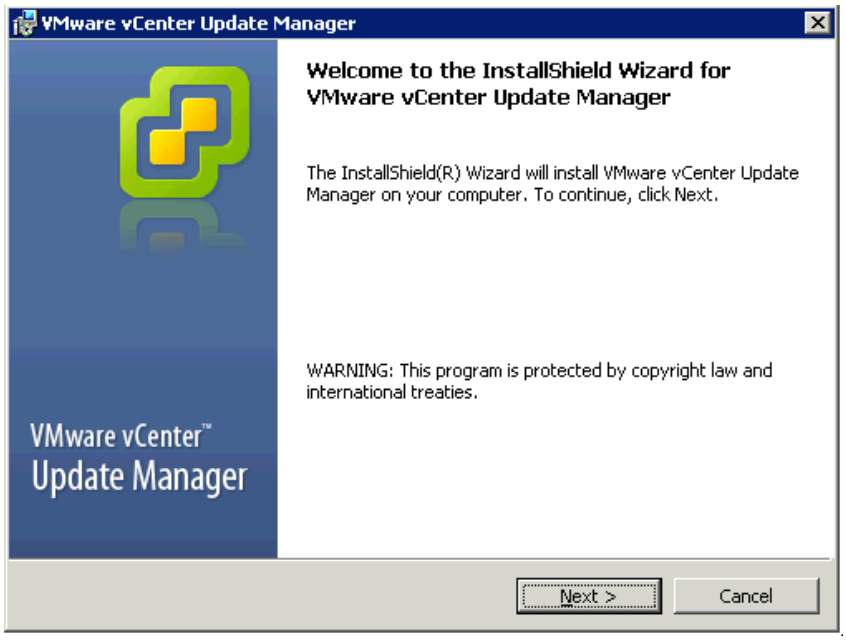


Step 2 Click OK to accept English (or change the language, but keep in mind this lab guide is based on the English installation)

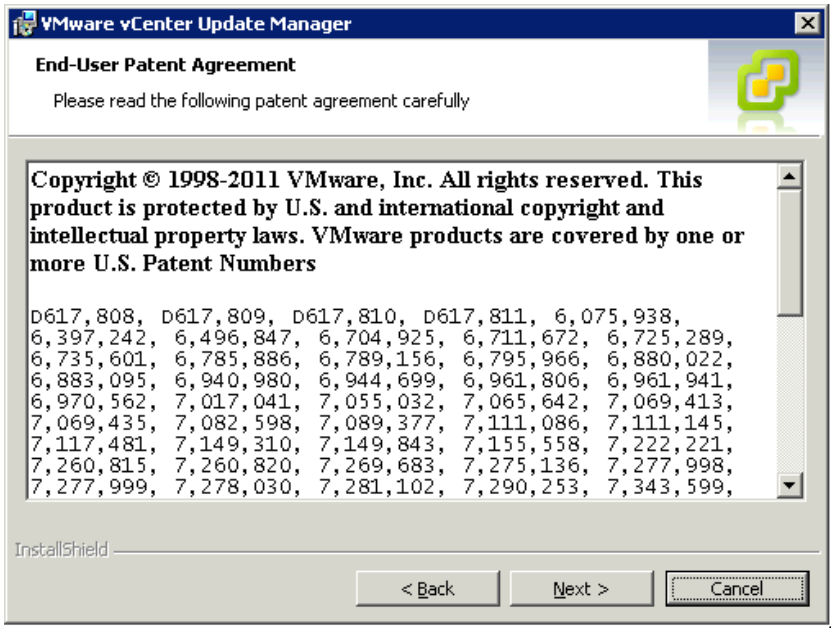


Step 3 Wait for the installer to load. This should take just a couple of seconds

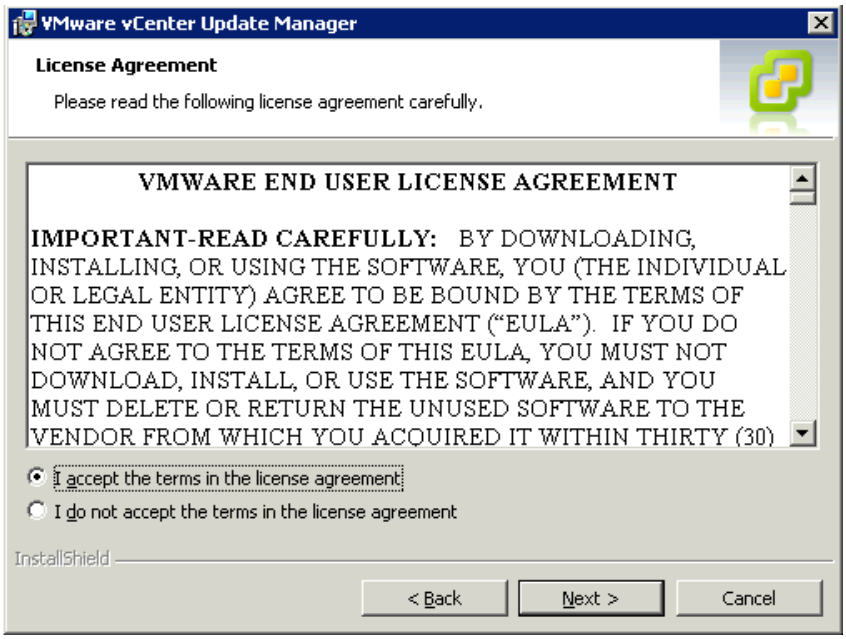
Step 4 Click “Next>” to start the Update Manager installation



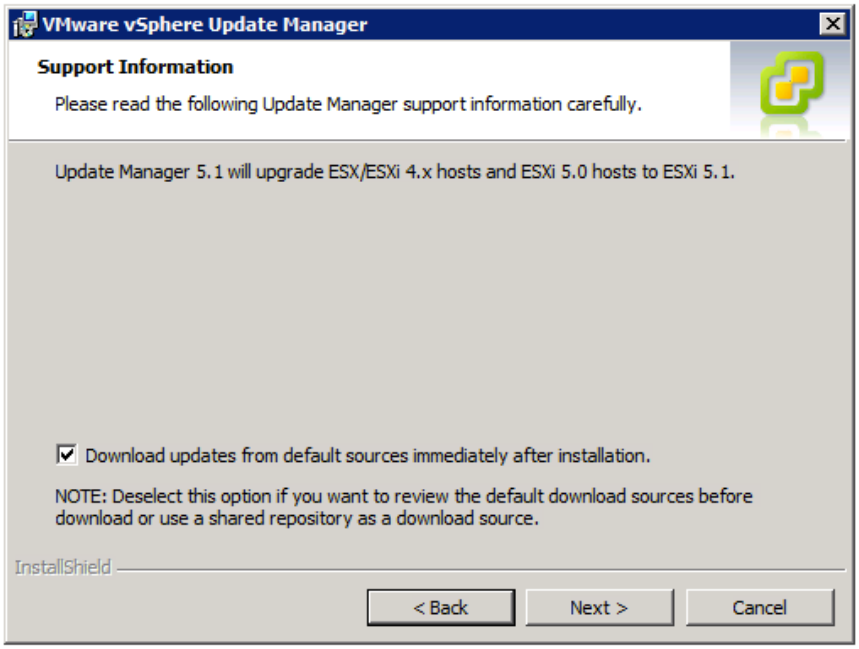
Step 5 Click “Next>” to acknowledge VMWares impressive patent number list…



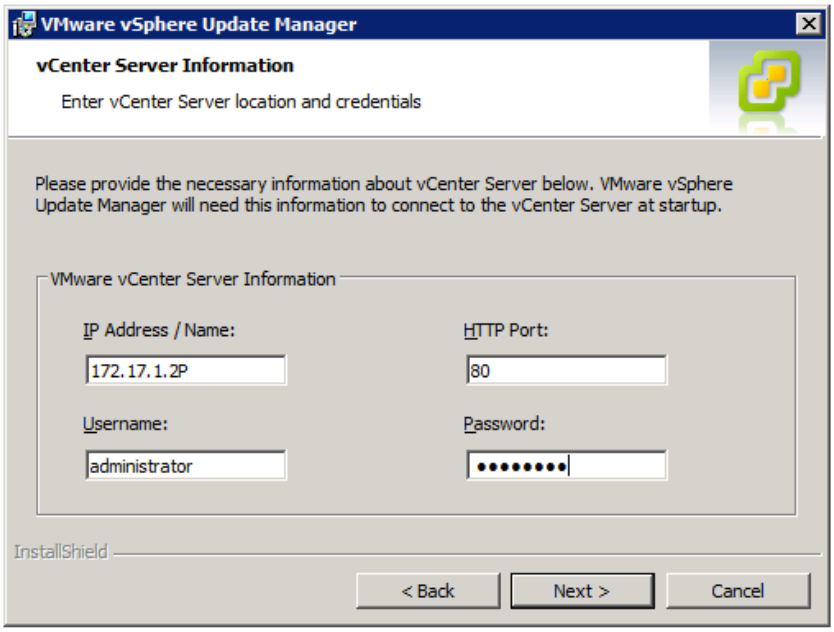
Step 6 Accept the EULA by clicking “I Agree…” and “Next>”



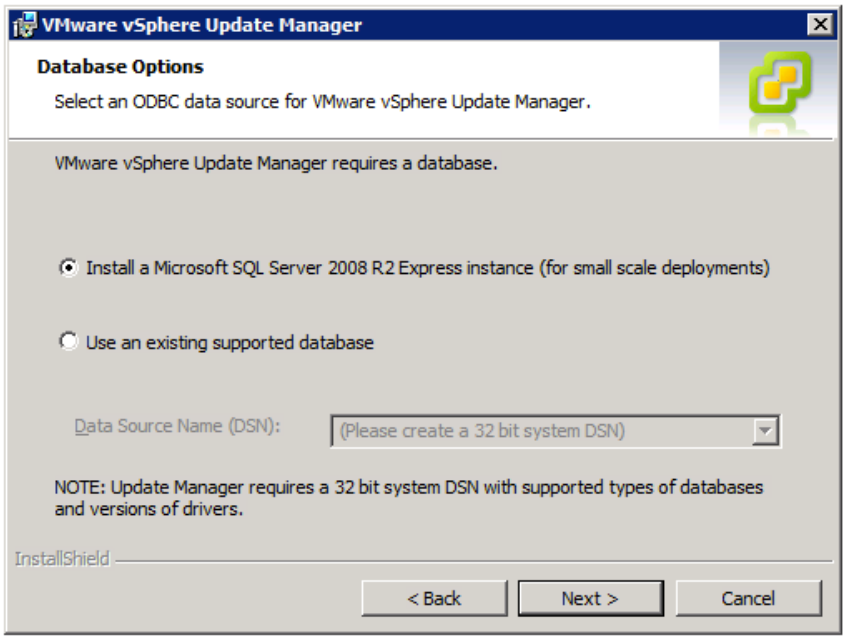
Step 7 Confirm the Support Information



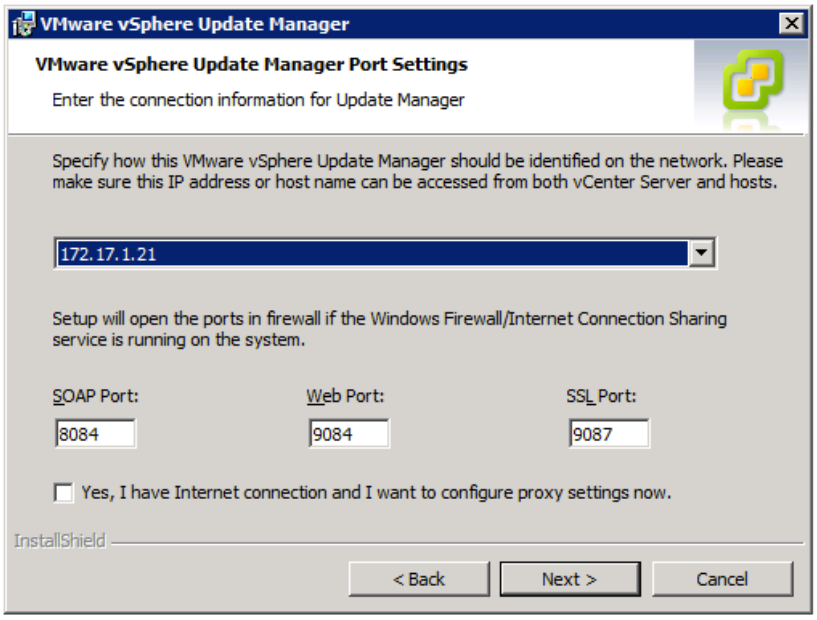
Step 8 Make sure the IP address of vCenter is 172.**17**.1.2P, username of your local PC is "administrator" and password is "1234QWer" and click "Next▷"



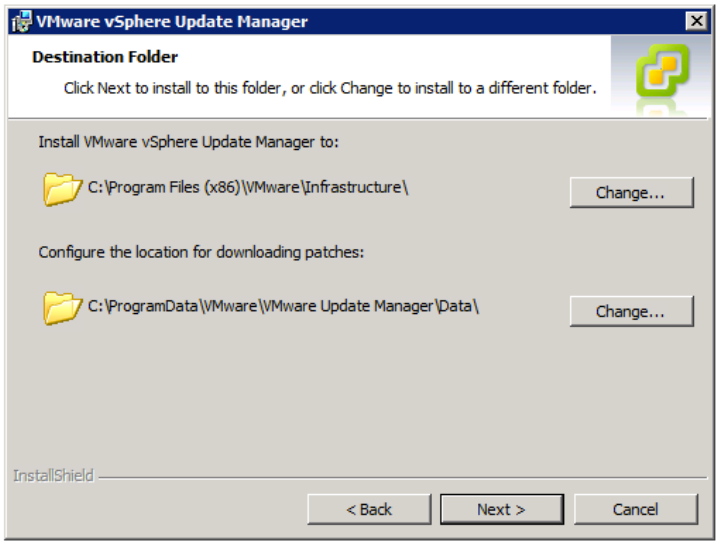
Step 9 Click on “Install a Microsoft SQL Server Express” (VUM is still 32-bit and requires an extra database) and click “Next>”



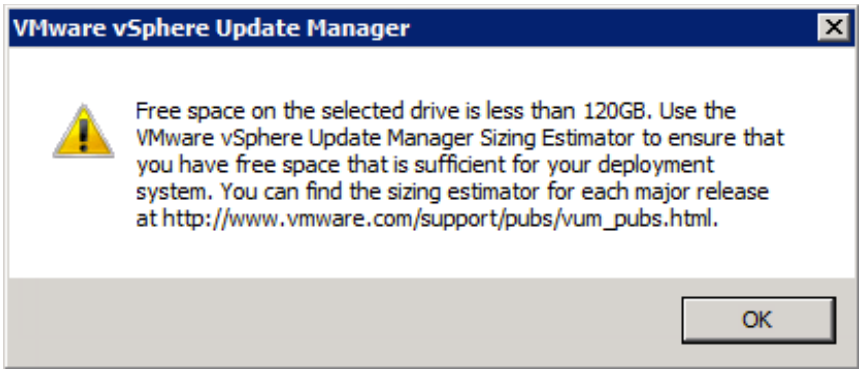
Step 10 Change the Network Ideitification to 172.17.1.2P and accept the default Ports with “Next>”



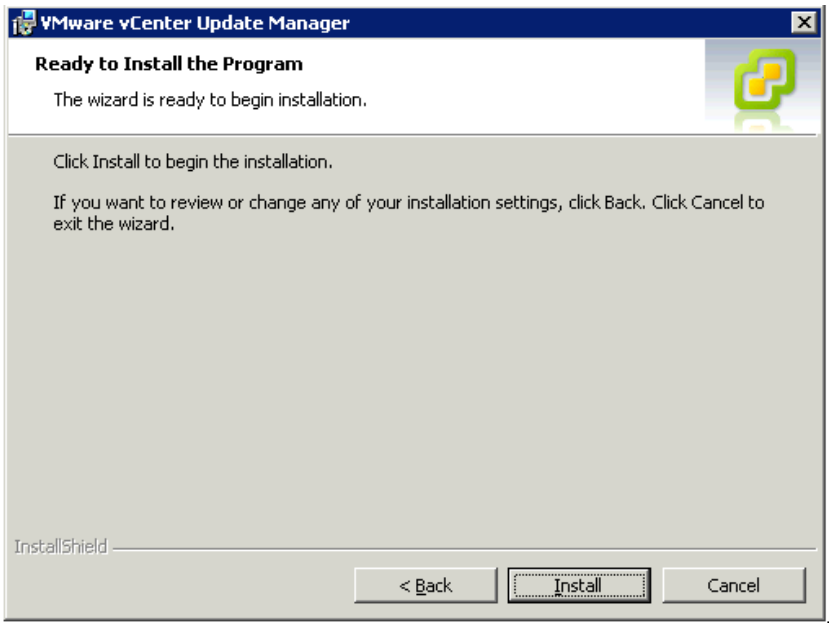
Step 11 Accept the default installation path with "Next>"



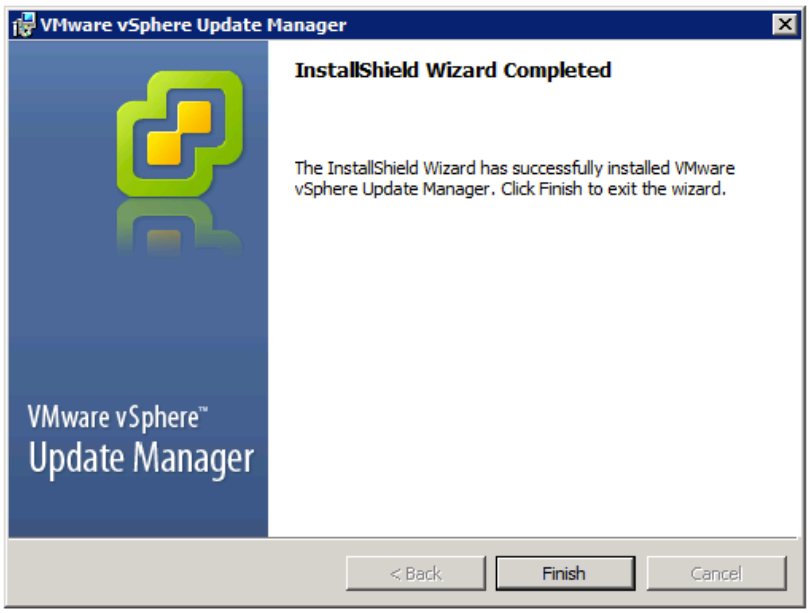
Step 12 Acknowledge the disk space warning (20GB are plenty for our lab)



Step 13 Click Install to start the installation. **This will take less than a minute.**



Step 14 Click “Finish” to close the installer



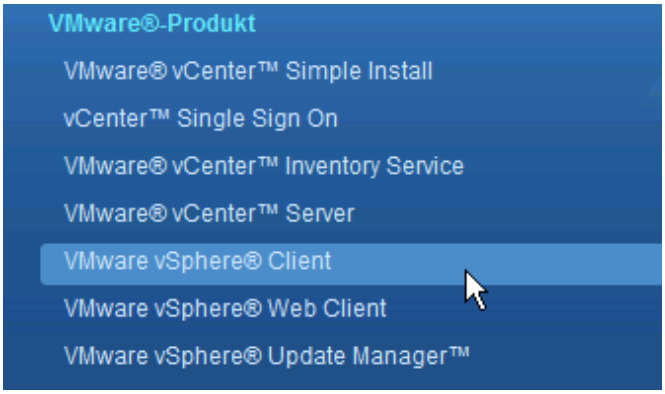
Task 4: Install vSphere Client

In this task, you will install vShere Client on your Student PC.

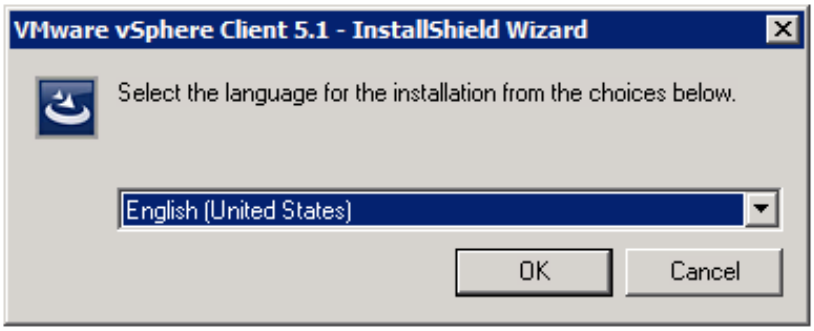
Activity Procedure

Complete these steps:

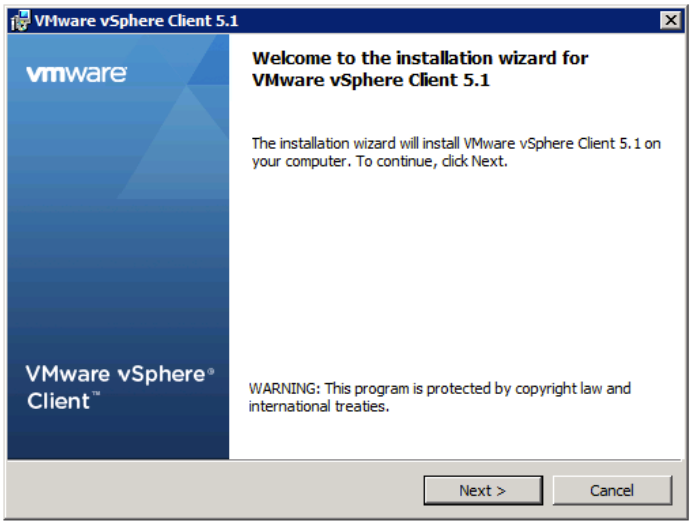
Step 1 Click “VMWare vSphere Client” and “install” in the vCenter installion program.



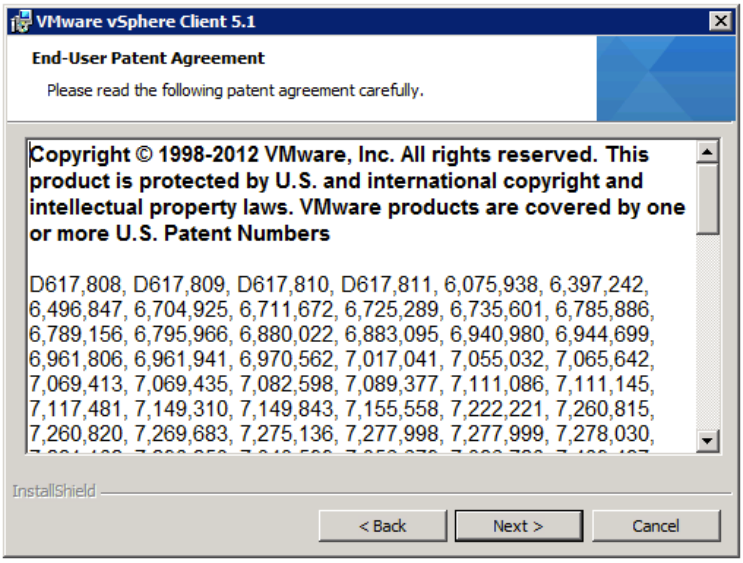
Step 2 Select the language vSphere Client will be installed in (keep in mind this lab guide uses English)



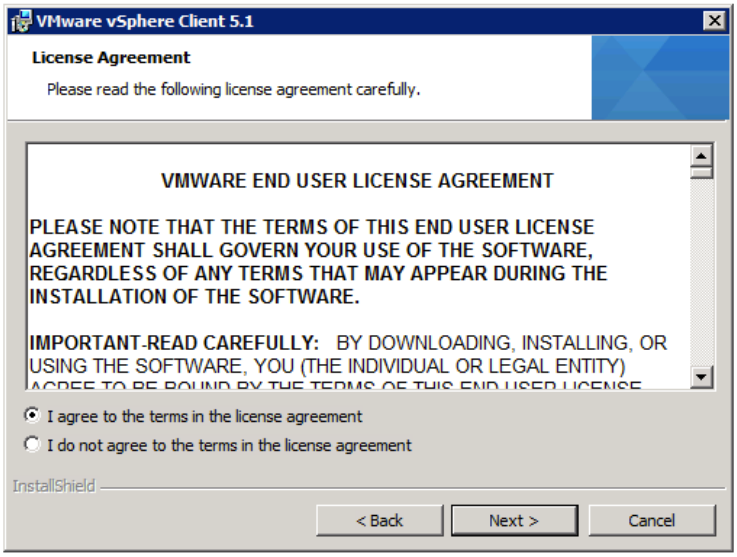
Step 3 Start the installer with “Next>”



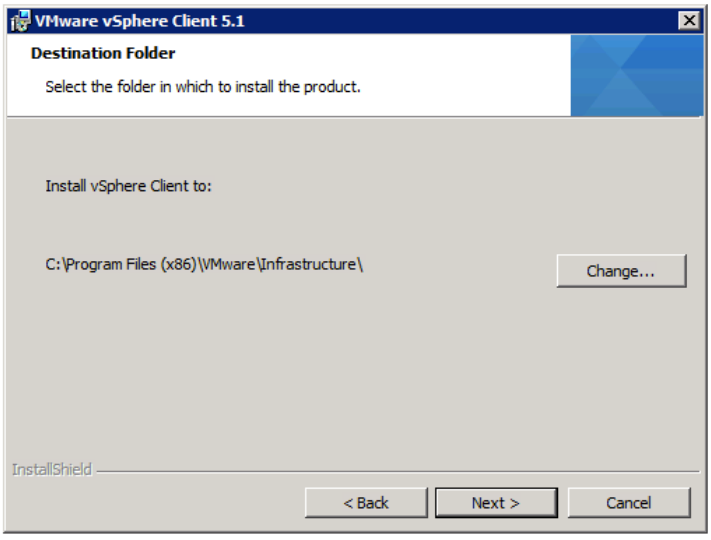
Step 4 Confirm the End User Patent agreement with “Next>”



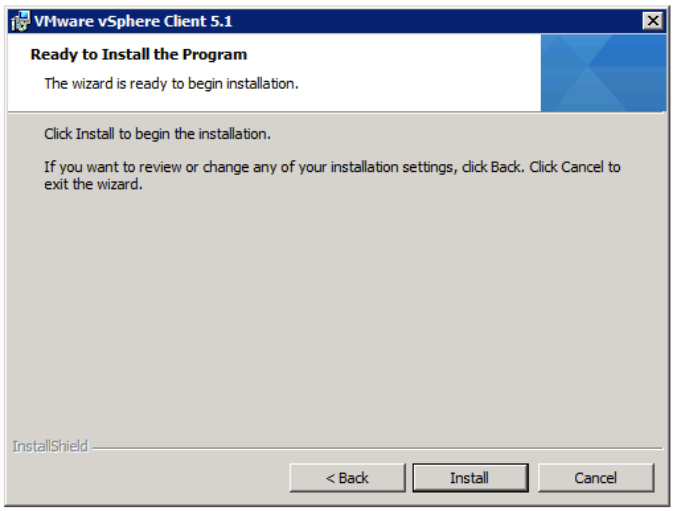
Step 5 Confirm the EULA and click “Next>”



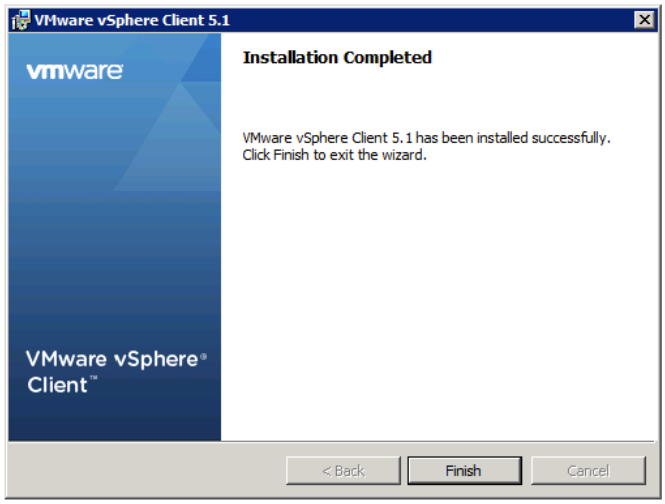
Step 6 Confirm the installation path with “Next>”



Step 7 Click “Install” to start the installation.



Step 8 Wait for the installation to complete and click “Finish” to close the installation Wizard.



Task 5: Build a VMWare Datacenter

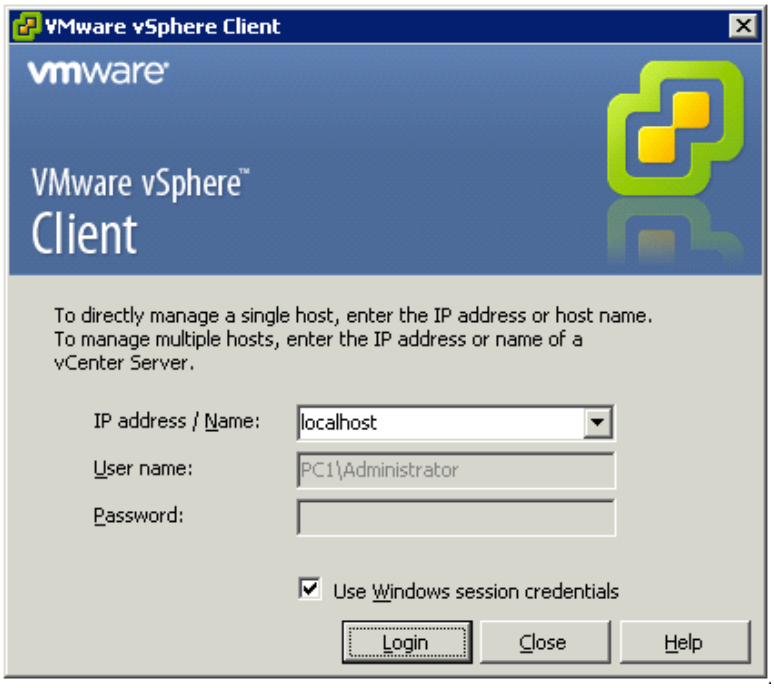
In this task, you will configure your two ESXi servers for vCenter Server.

Activity Procedure

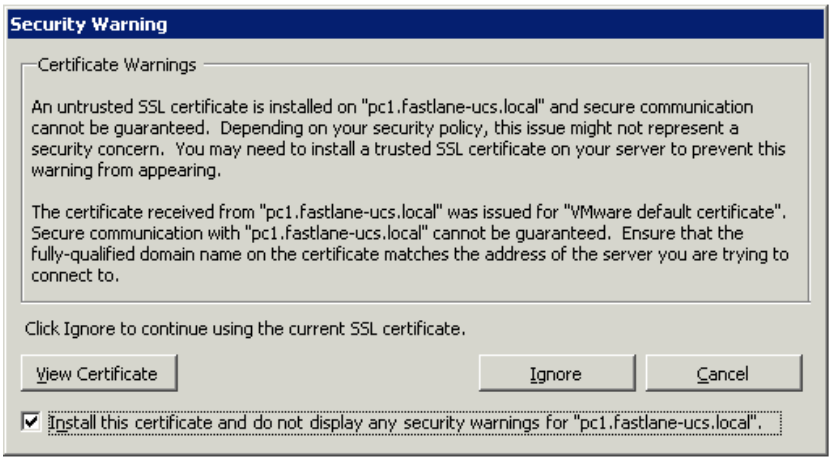
Complete these steps:

Step 1 Find the Icon for the vSphere Client and double-click to start

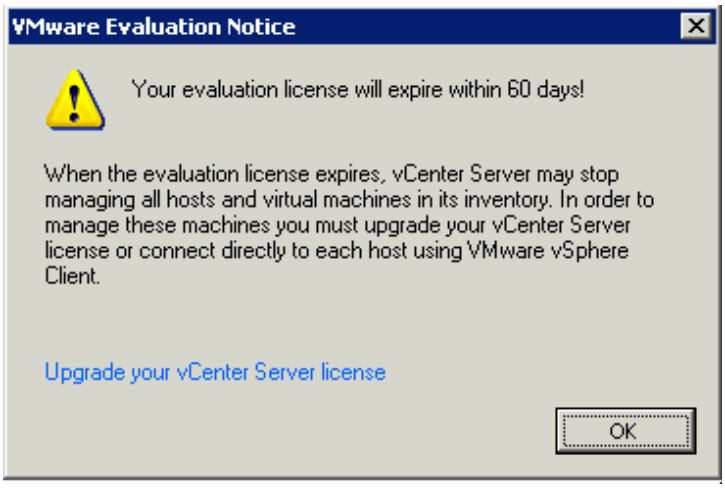
Step 2 Connect to host “localhost” (or 172.17.1.2P) and use Windows Session Credentials to log on.



Step 3 Click “Install this Certificate…” and “Ignore” to accept the vCenter certificate.

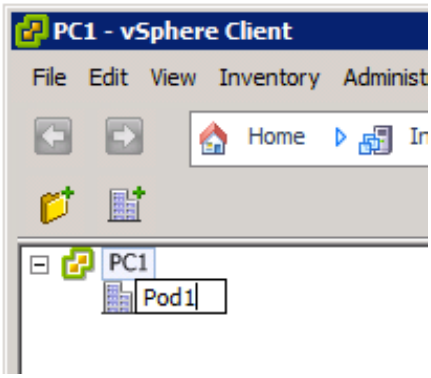


Step 4 Acknowledge the “Evaluation Warning” with “OK”

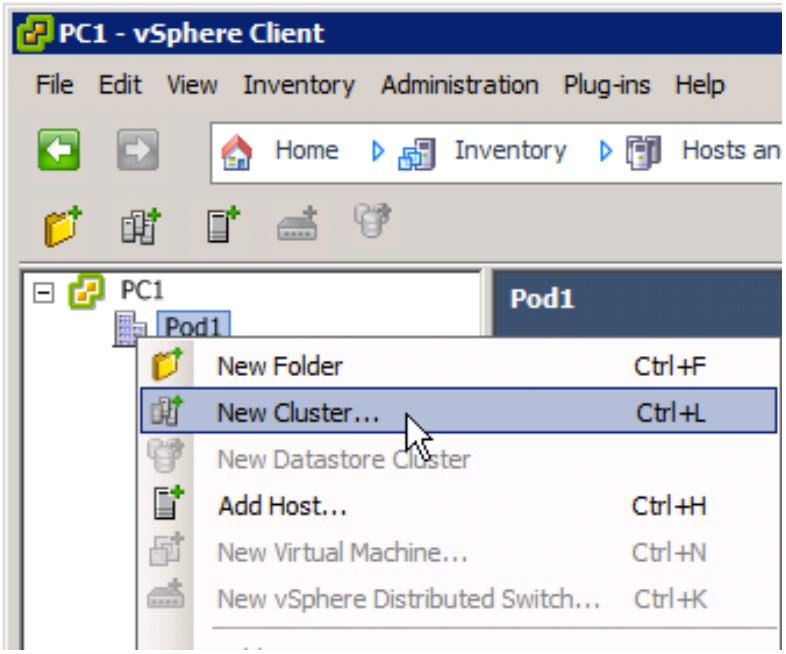


Step 5 Click “Create a DataCenter” in “Getting Started” Tab

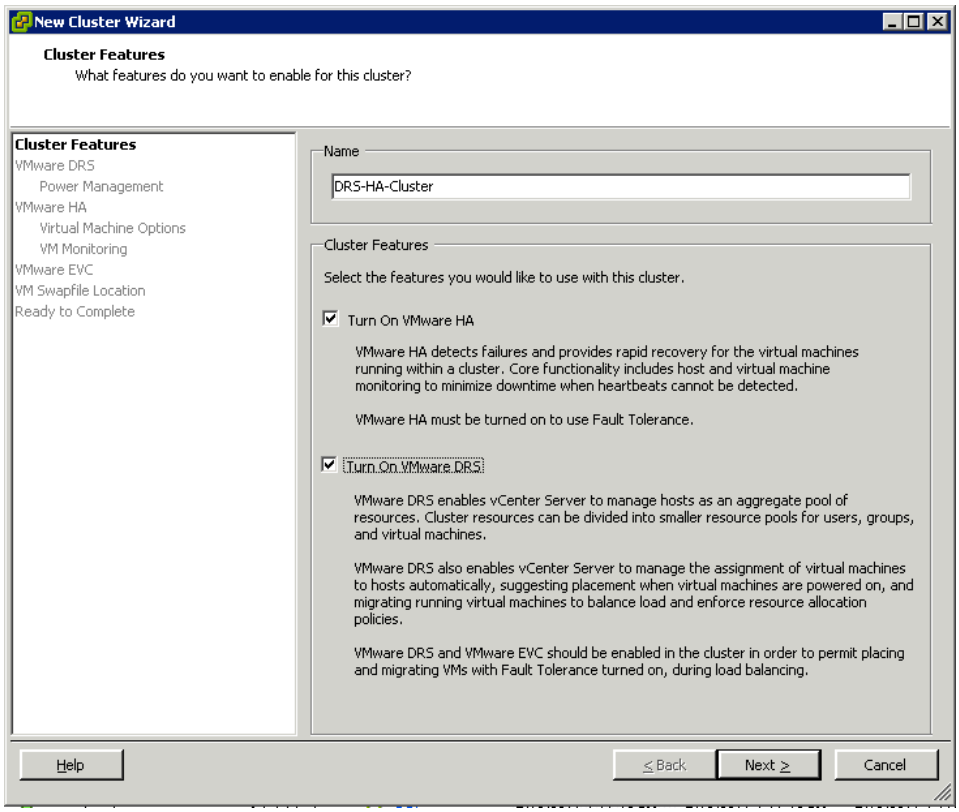
Step 6 Name your new DataCenter “Pod#” (# is your Pod#)



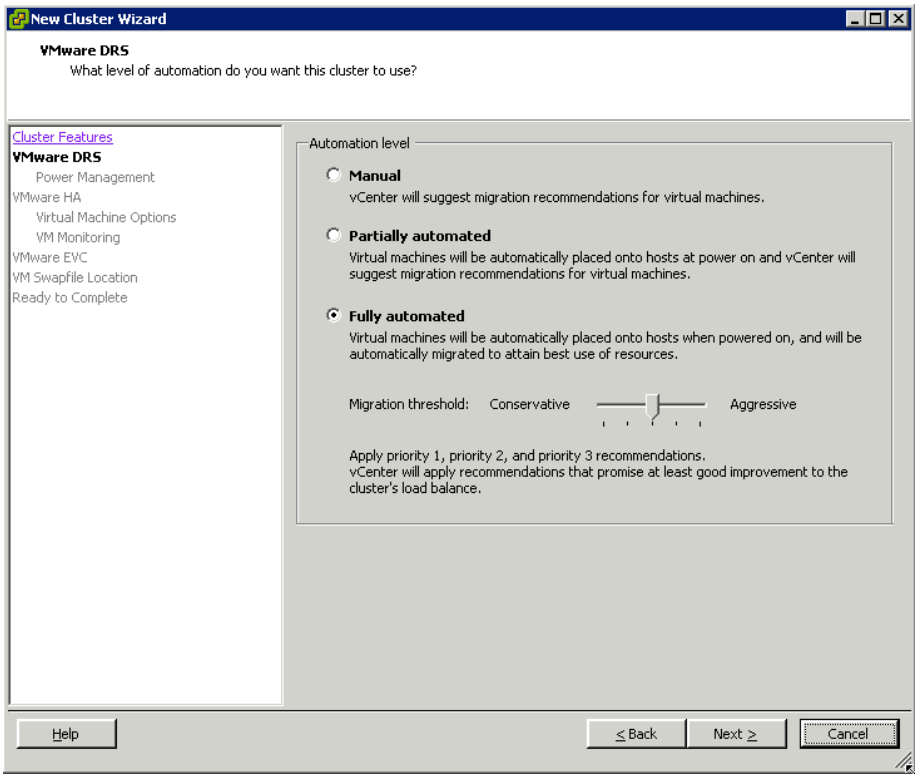
Step 7 DO NOT ADD a host! Right-click the DataCenter and click “New Cluster”



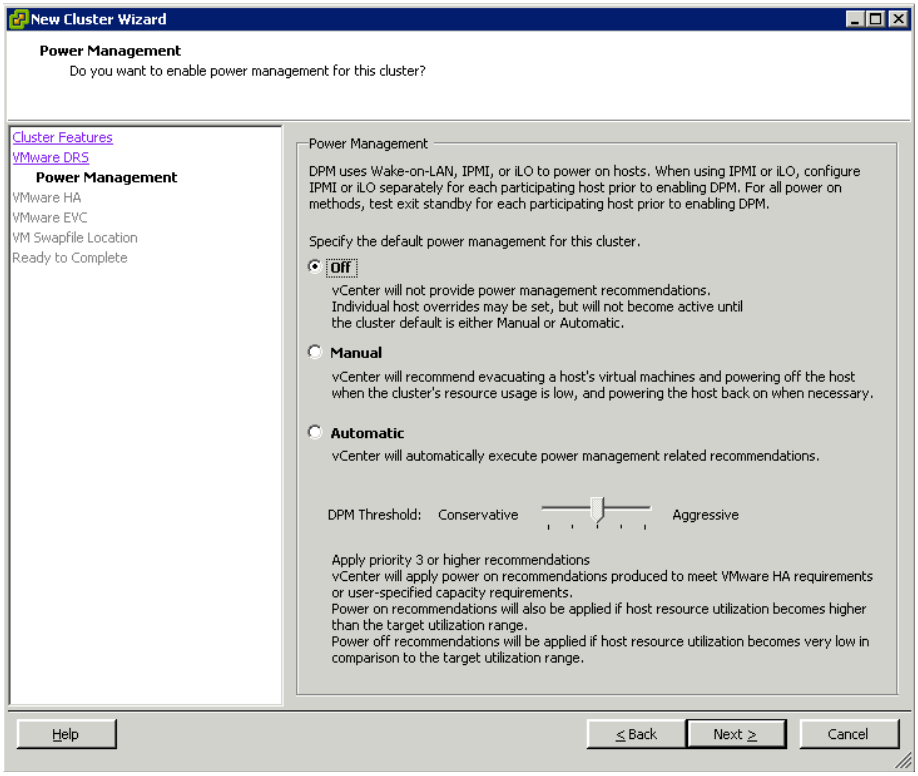
Step 8 Name your Cluster "DRS-HA-Cluster" and enable DRS and HA, click "Next>"



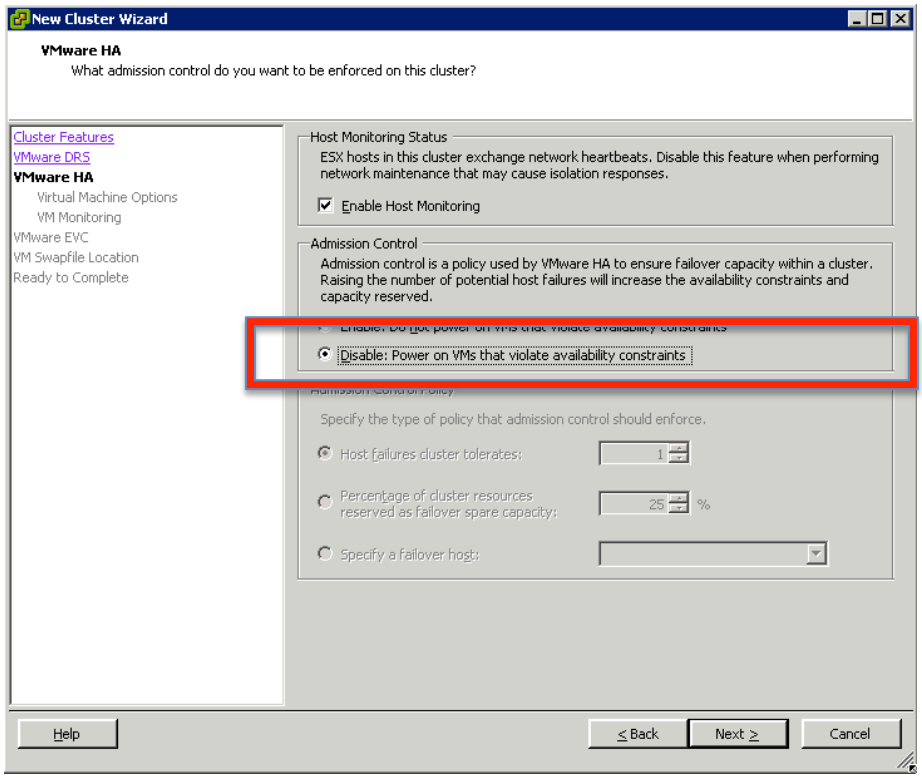
Step 9 Accept the default DRS configuration with "Next>"



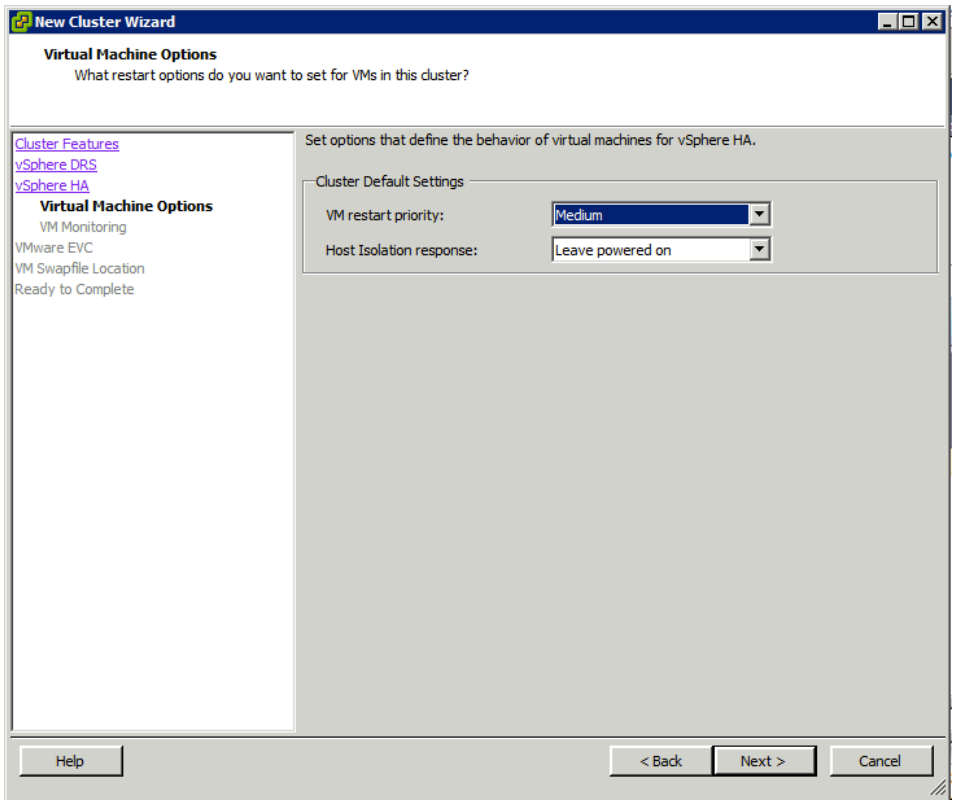
Step 10 Do not turn on Power Management (we don't want DPM to turn off servers in our lab), just click "Next>"



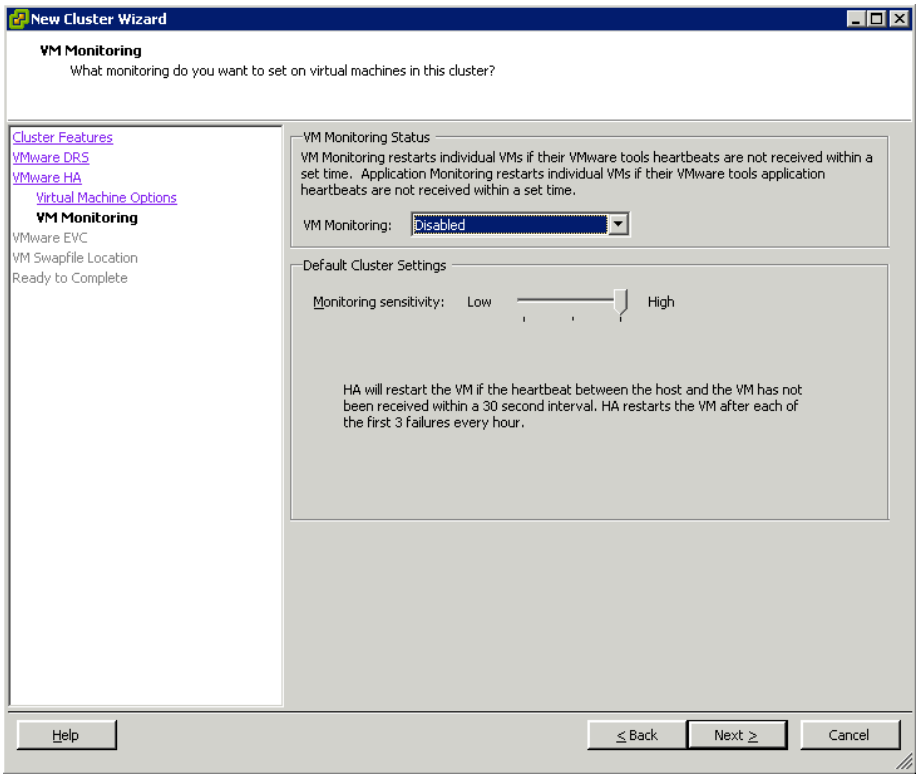
Step 11 **TURN OFF** Admission control, click "Next>"



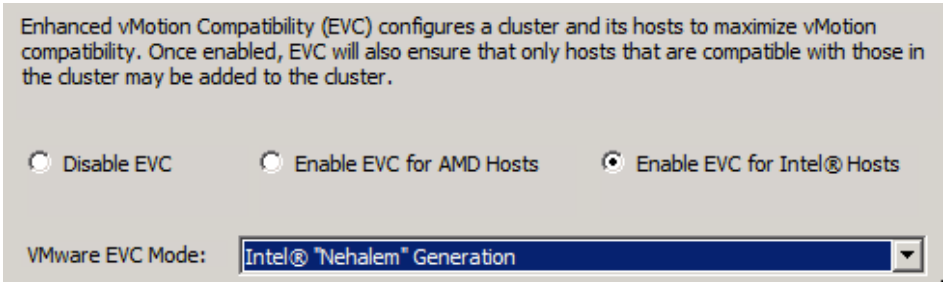
Step 12 Accept the HA virtual machine options defaults with "Next>"



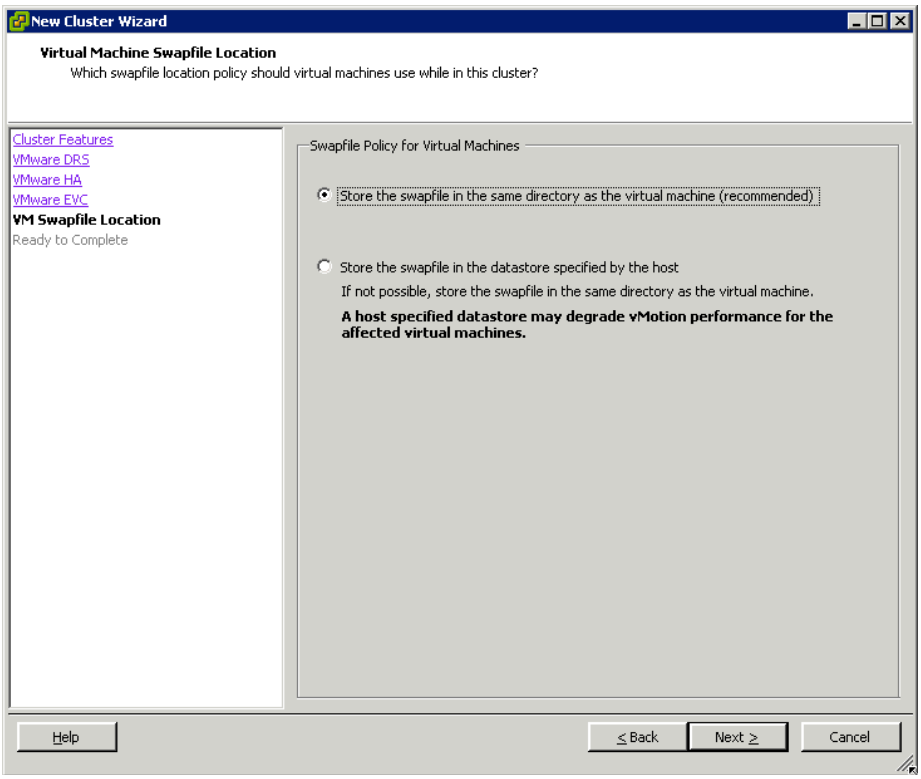
Step 13 Accept the HA VM Monitoring defaults with "Next>"



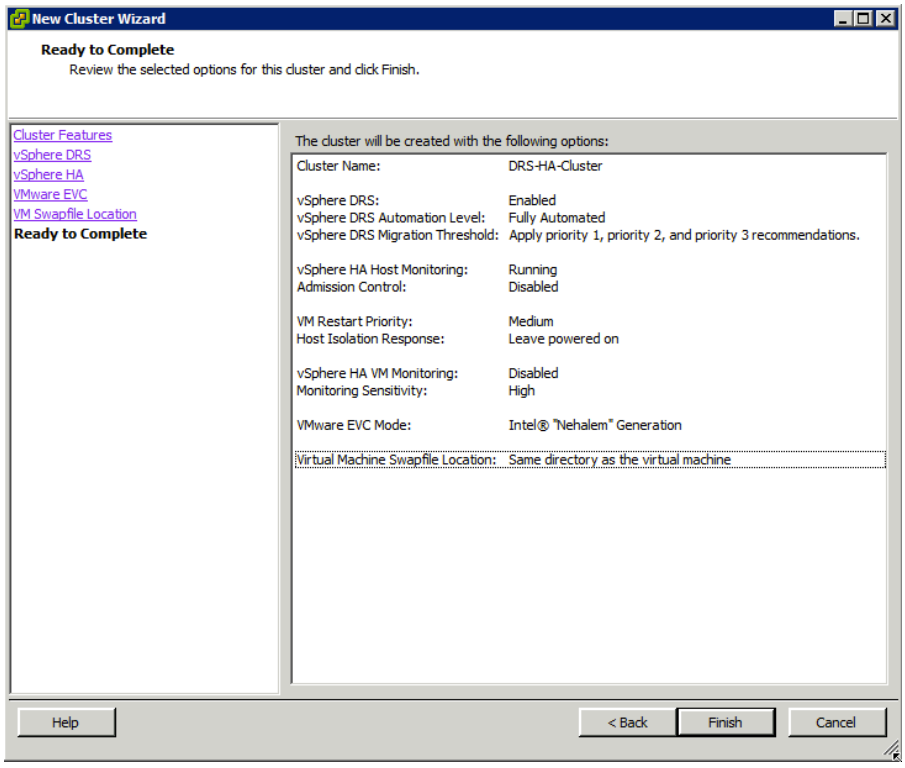
Step 14 Set EVC to ”Enable EVC for Intel®”, select the “Intel Nehalem Generation” and click “Next>”



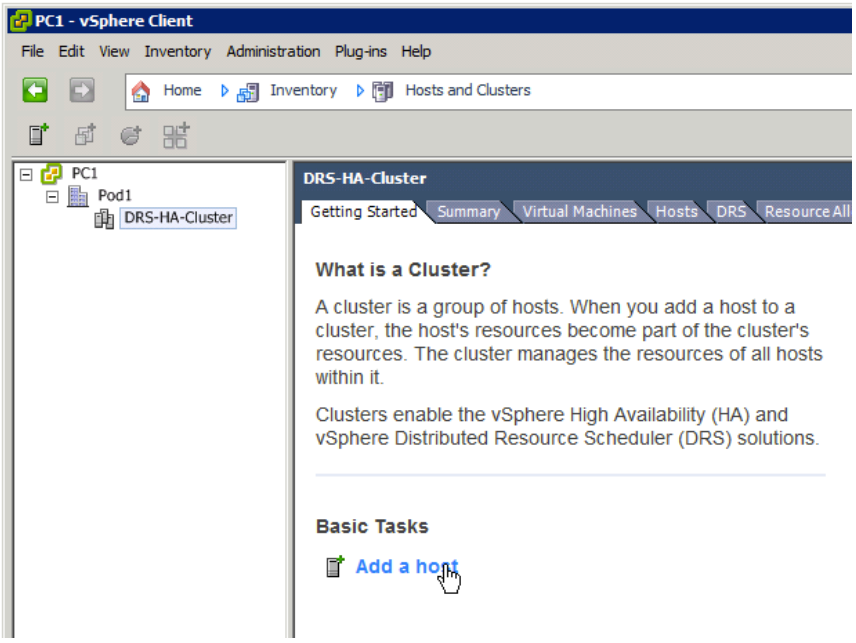
Step 15 Accept the default Swapfile configuration with “Next>”



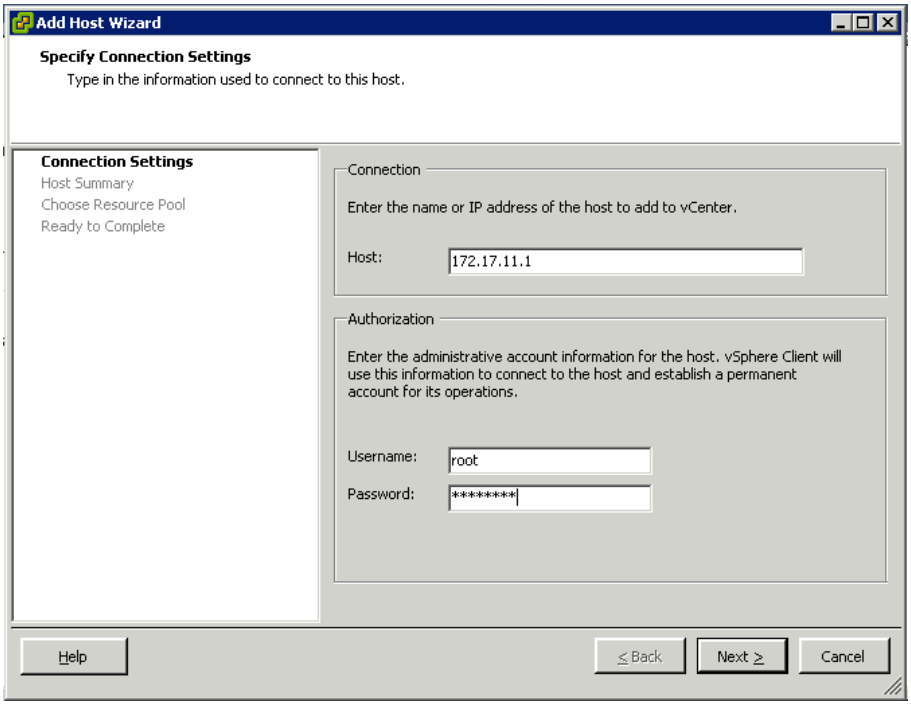
Step 16 Review the Cluster Configuration and click "Finish"



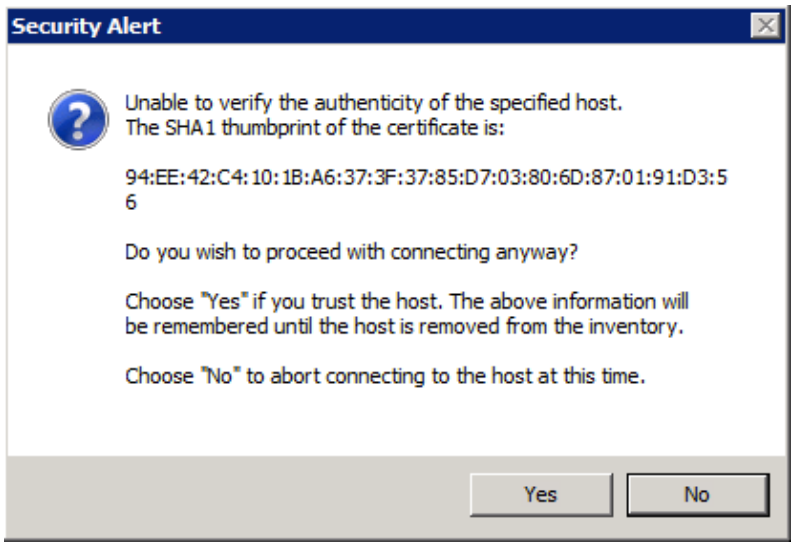
Step 17 **Select the newly created cluster** in the navigation pane and click “add host” in the “getting started” tab (you can also right-click the cluster and use the context menu)



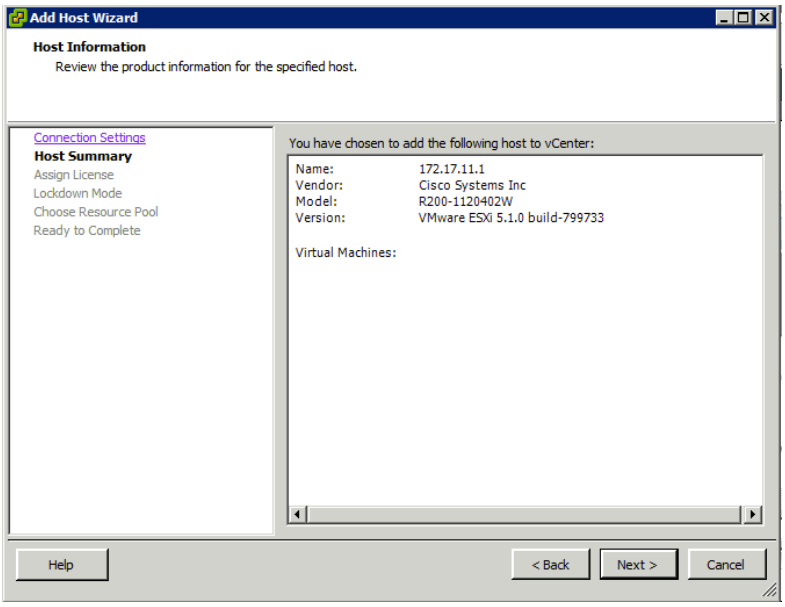
Step 18 Enter the IP address of ESXi1 (172.17.P1.1), username “root” password “1234QWer”, click “Next>”



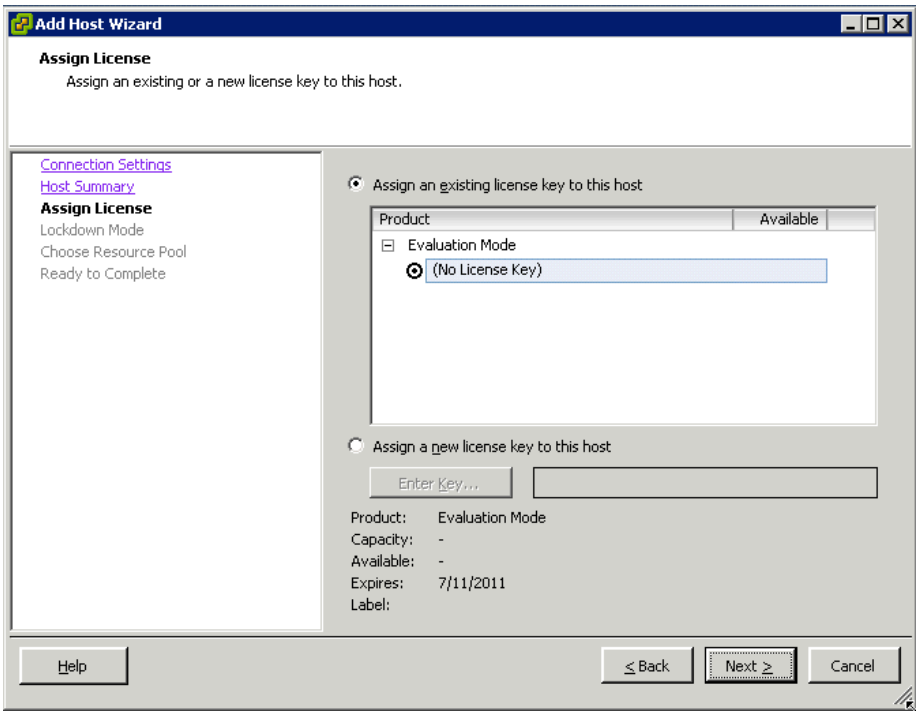
Step 19 Accept the SHA thumbprint by clicking “Yes”



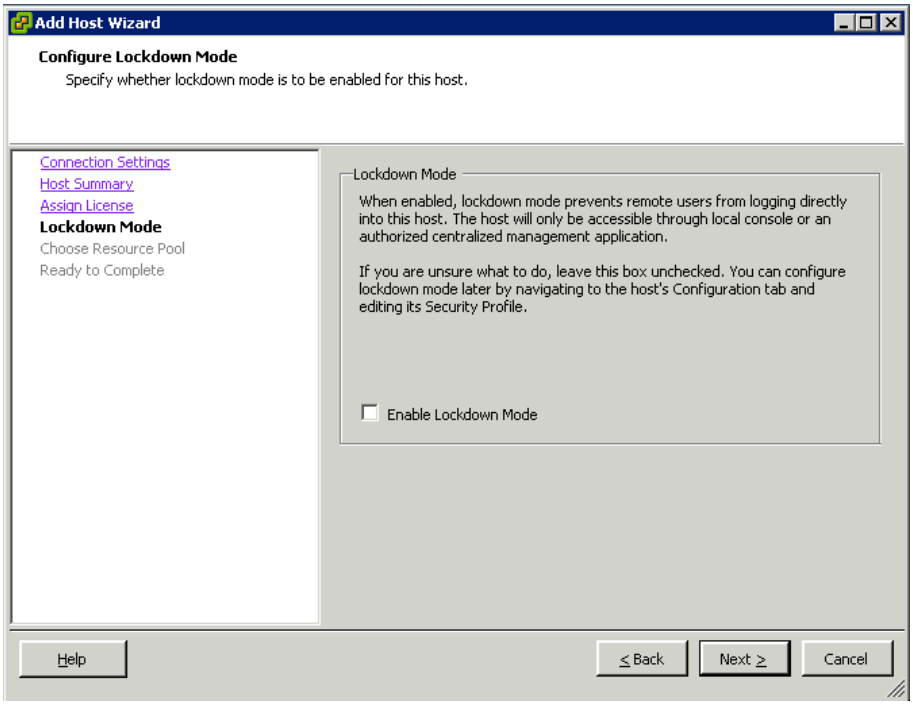
Step 20 Review the server information and click “Next>”



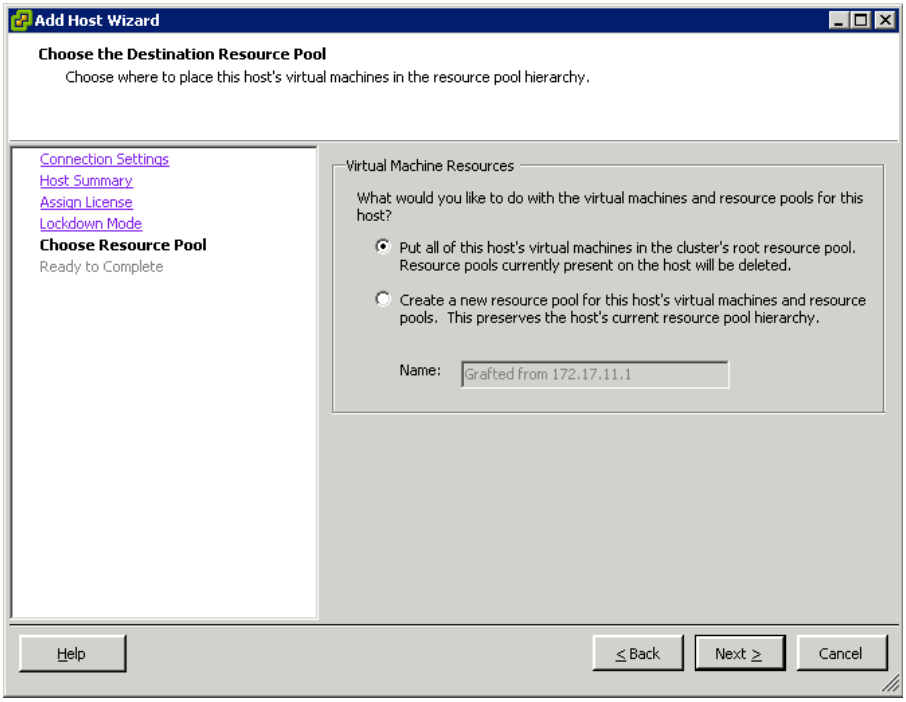
Step 21 We are going to use ESXi in Evaluation mode, just click “Next>”



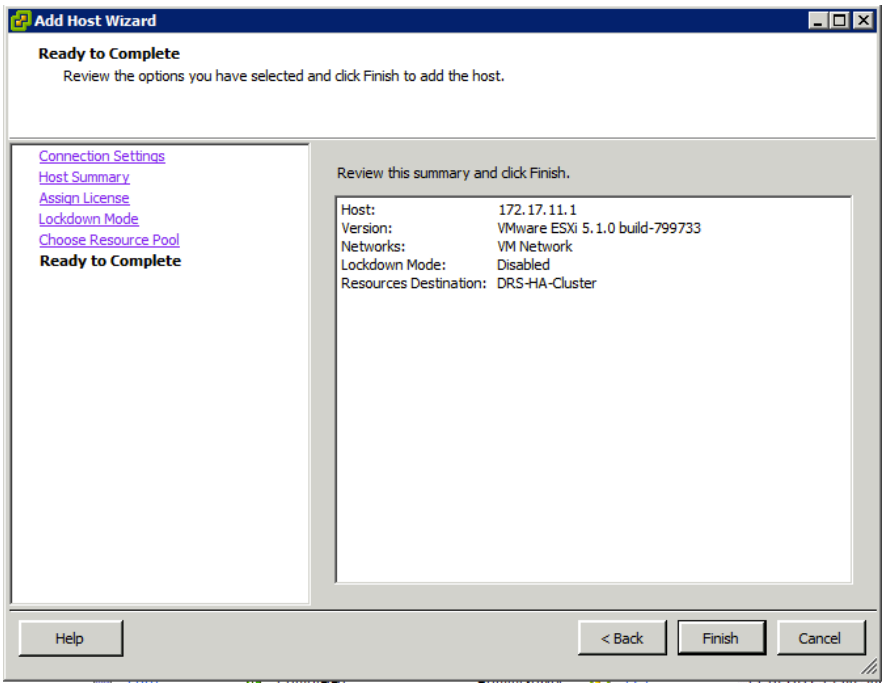
Step 22 Don't enable lockdown mode in this lab (in a real datacenter you would!!!), just click "Next>"



Step 23 Accept the Resource Pool configuration by clicking "Next>"

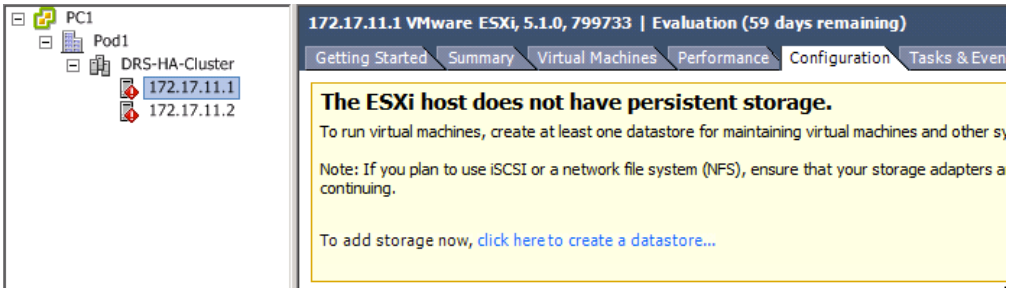


Step 24 Review and click "Finish" to add the host.

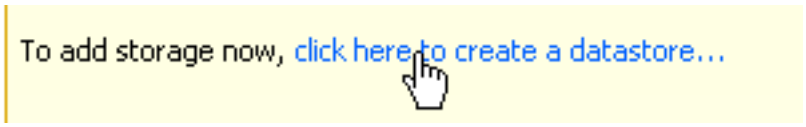


Step 25 Repeat Steps 17-24 for ESXi2 (172.17.P1.2)

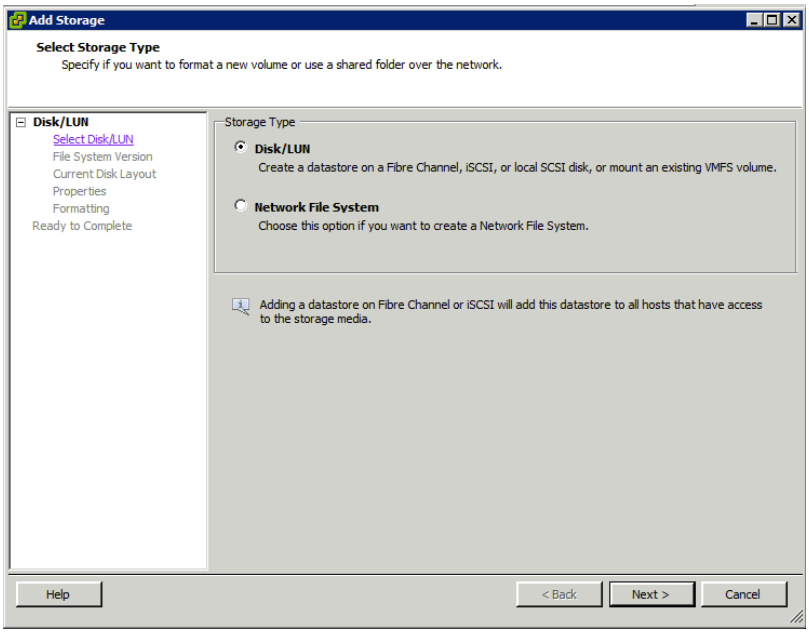
Step 26 Note there is a critical error on both servers, click on ESXi1.



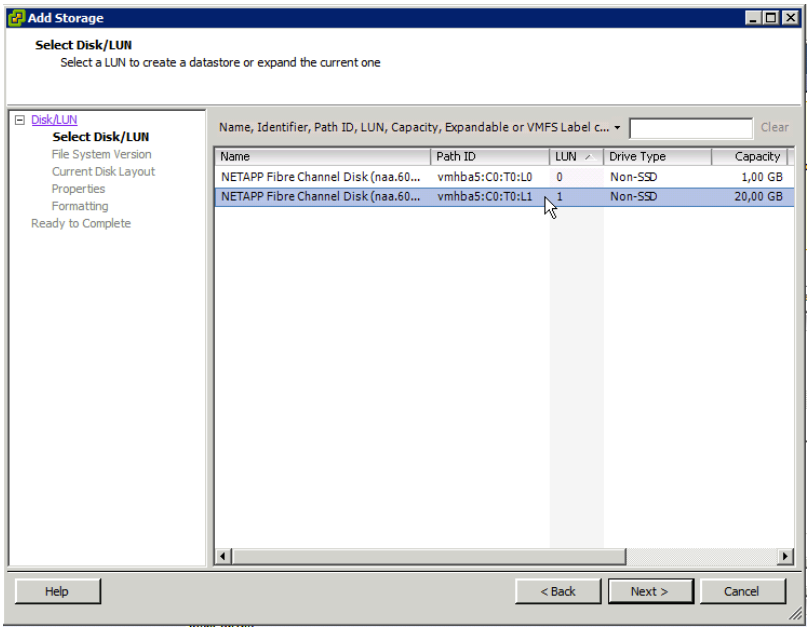
Step 27 Click “click here to create a datastore” to start creating a shared data store.



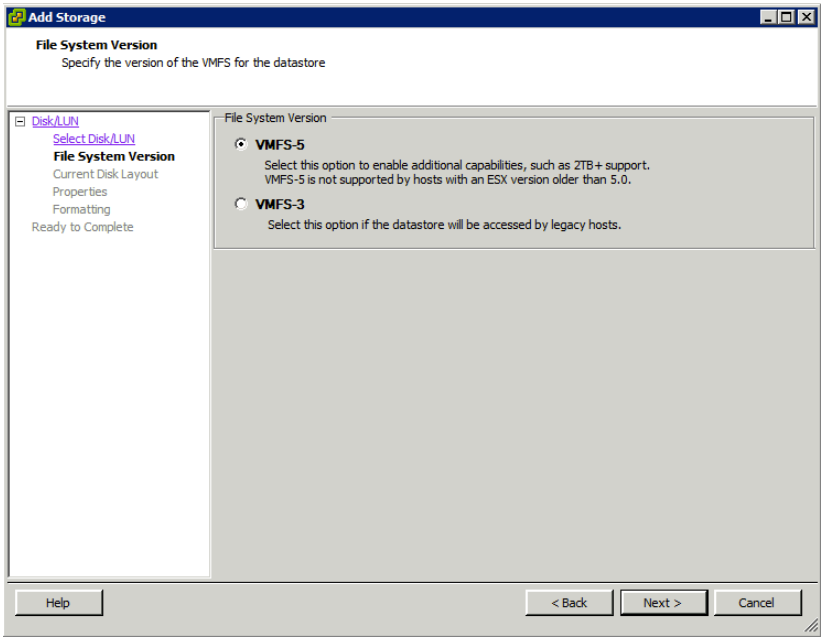
Step 28 Accept LUN (we are going to use the 20GB disk on the NetApp), click “Next>”



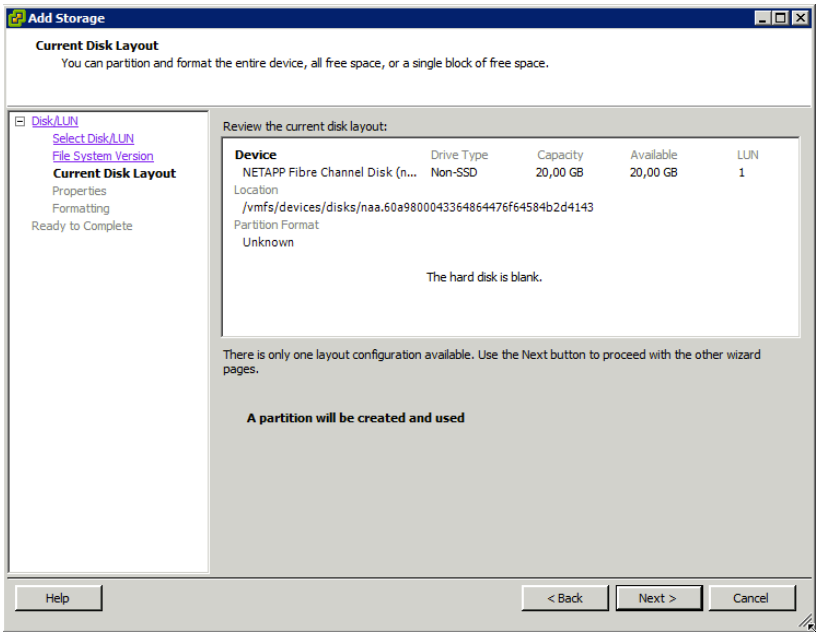
Step 29 **Select the 20GB NetApp disk** and click “Next>”



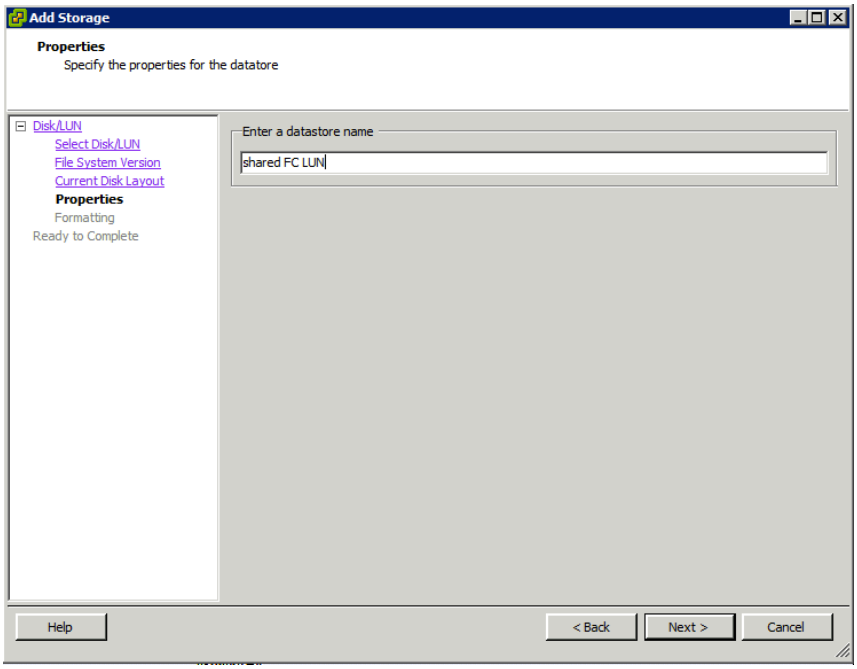
Step 30 Accept VMFS-5 as the file system (you can also use VMFS3, it does not make any difference in this lab)



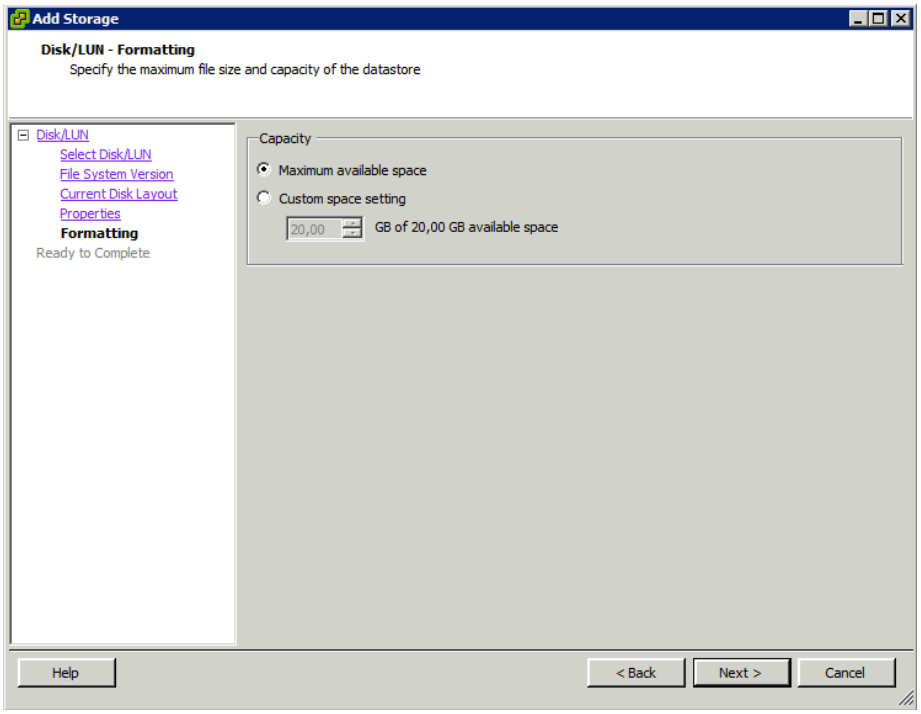
Step 31 There is nothing on that LUN, accept the partition scheme it by clicking “Next>”



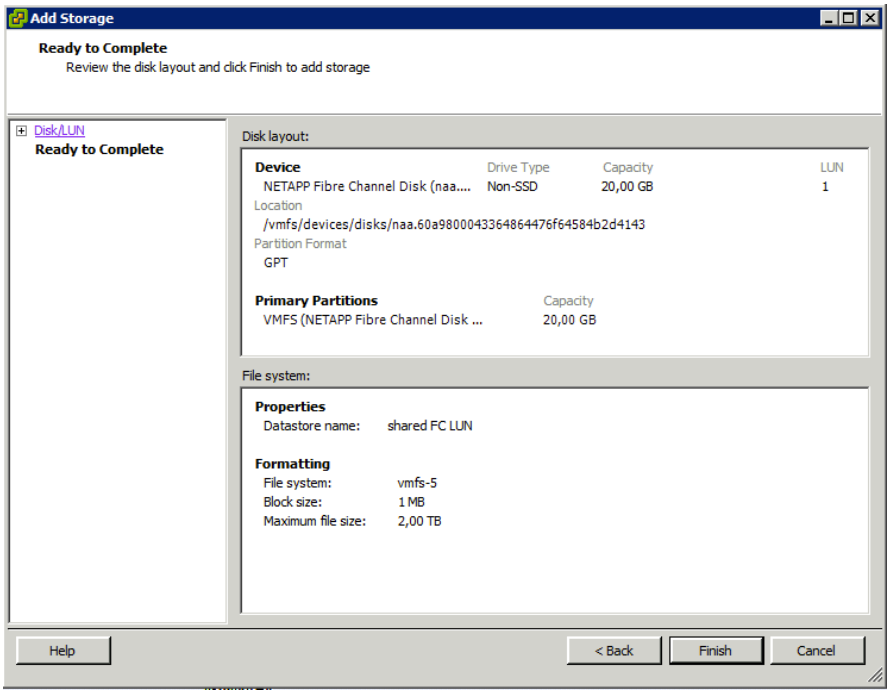
Step 32 Name the LUN “shared FC LUN” and click “Next>”



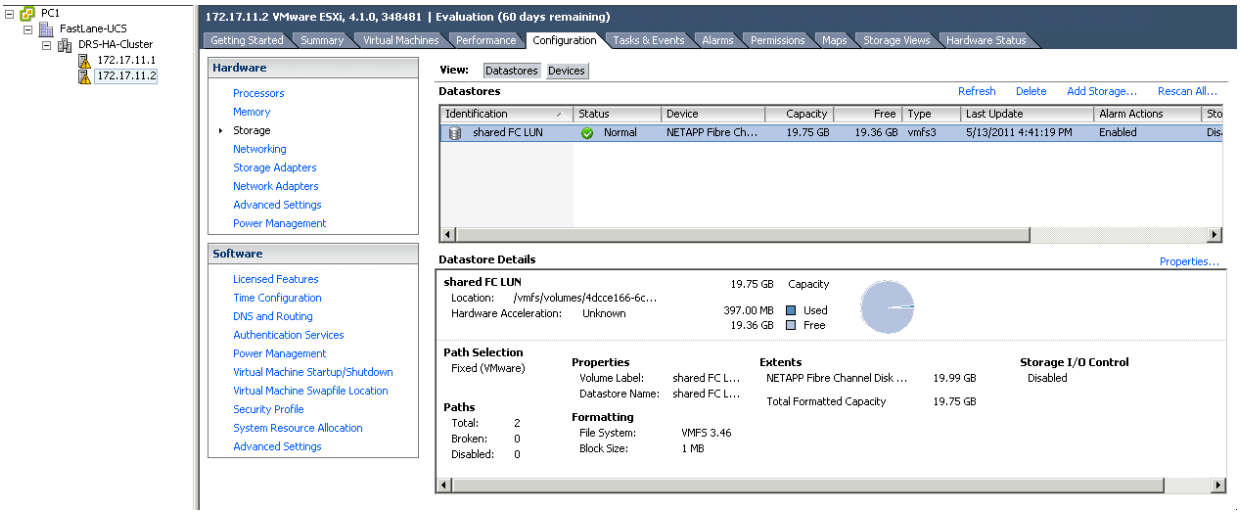
Step 33 Accept the default Capacity Options and click “Next>”



Step 34 Review and click “Finish” to create the shared storage



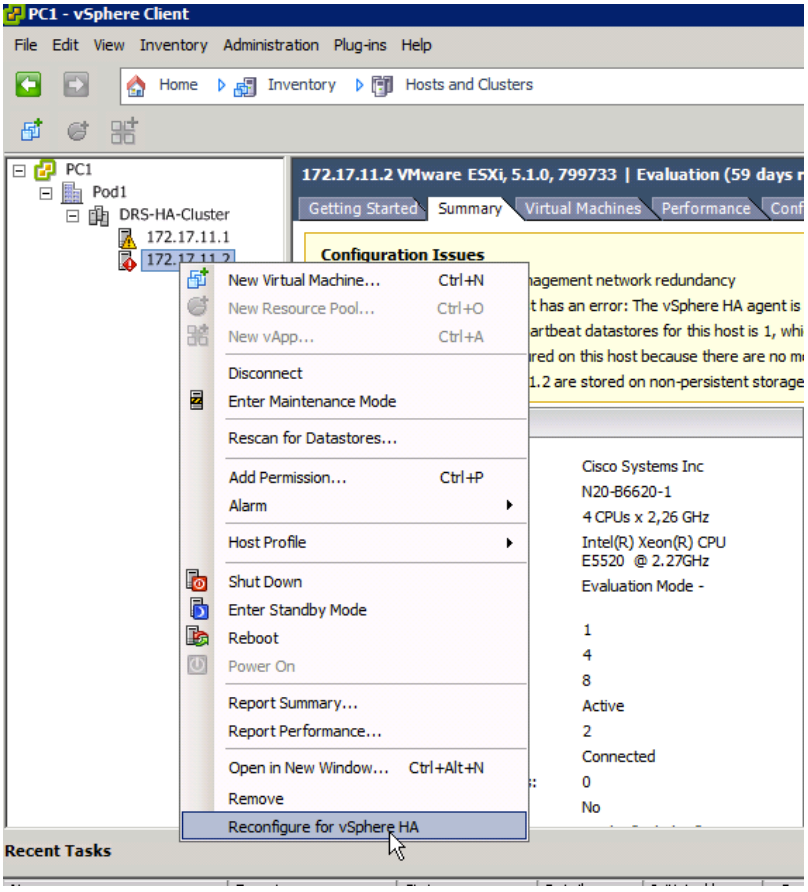
Step 35 Note vCenter automatically created the shared storage on both ESXi servers. Click ESXi2 in the navigation pane, select the "configuration" tab and click "storage" in the Hardware box, then select the LUN.



Note A warning message will appear at your hosts because VMWare thinks the ESXi servers have no management redundancy. Remember we are using VICs and we configured hardware redundancy.
You can disable the warning:
- Right-click the Cluster
- Click “Edit Settings…”
- Click “vSphere HA”
- Click “Advanced Options…”
- Click the first row, enter Option “das.ignoreRedundantNetWarning” with Value “true”

you need to reconfigure HA on your hosts to activate this settings, just right-click your host and select “reconfigure HA”

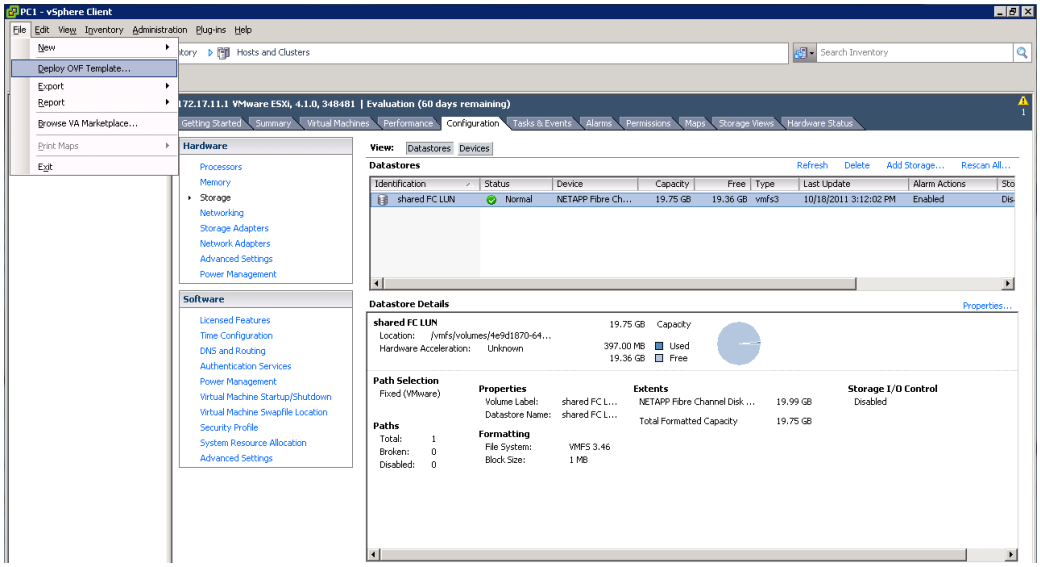
Step 36 Right-click ESXi1 and select “Reconfigure for VMWare HA”



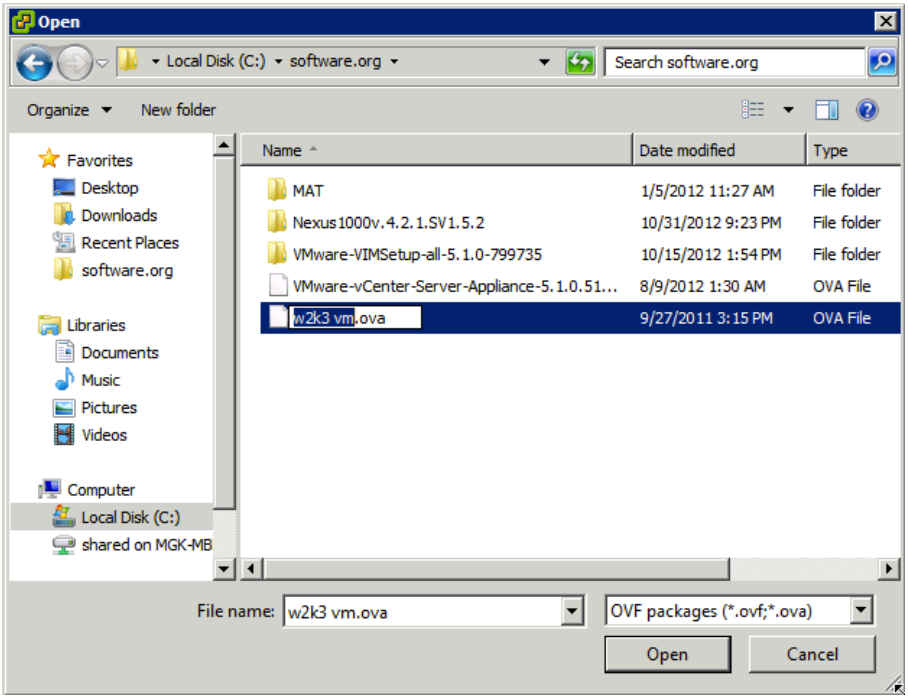
Step 37 Right-Click ESXi2 and select “Reconfigure for VMWare HA”

Note Ignore the warnings about non-persistent log storage and heartbeat datastores in this lab.

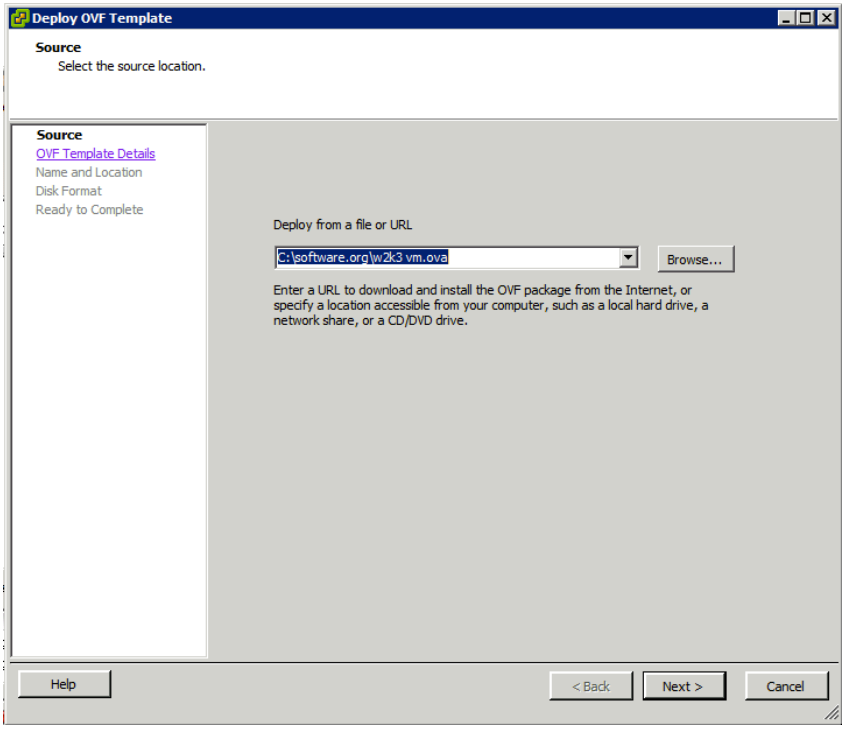
Step 38 Next we are going to deploy a virtual machine.
In vSphere Client click on File then “Deploy OVF Template”.



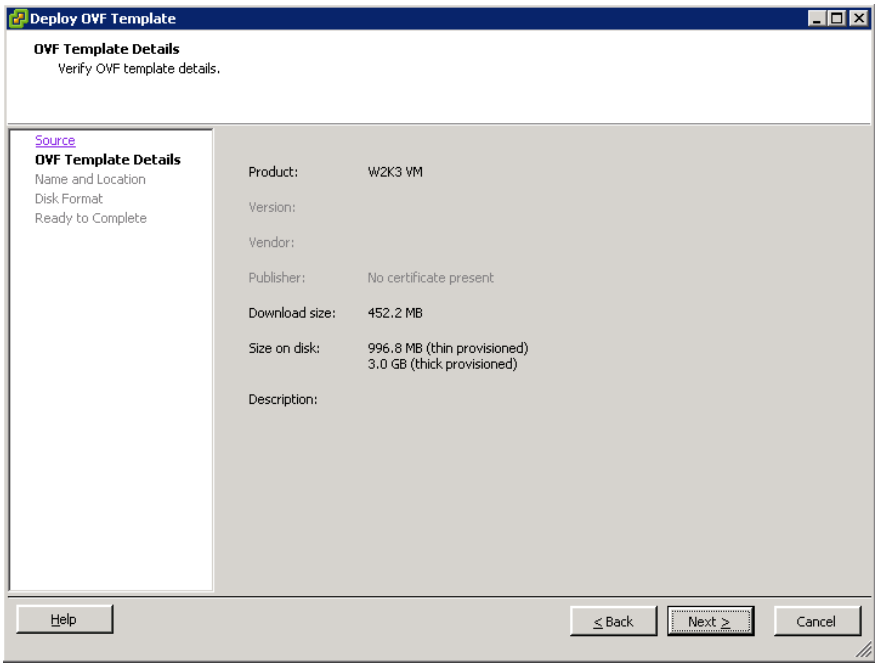
Step 39 Navigate to “c:\software.org” , select the file W2K3_VM.ova and click Open.



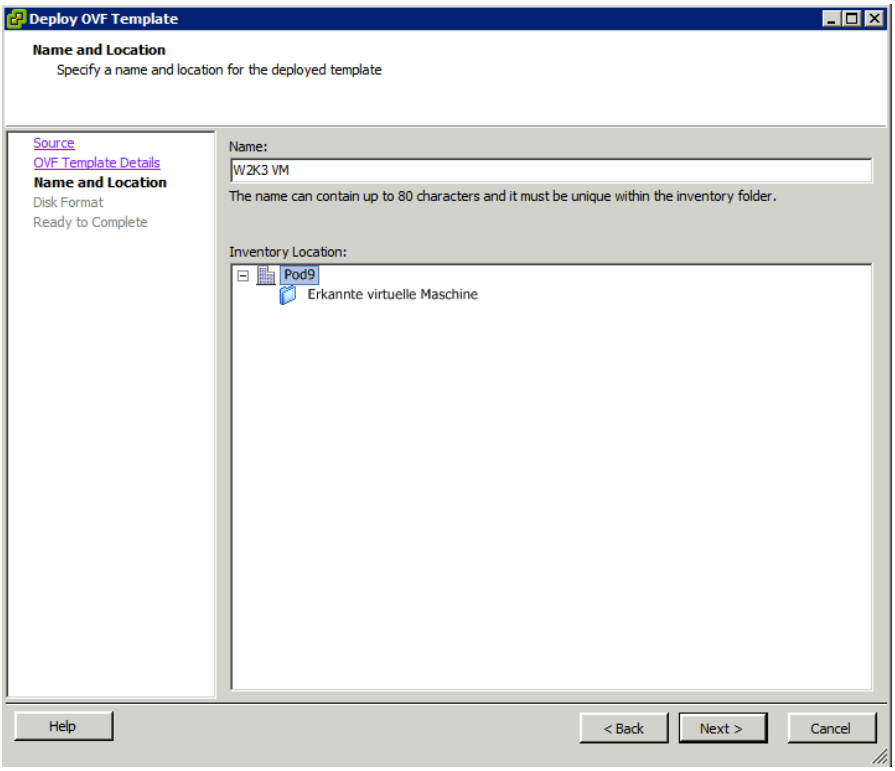
Step 40 Click next to accept the file as template source.



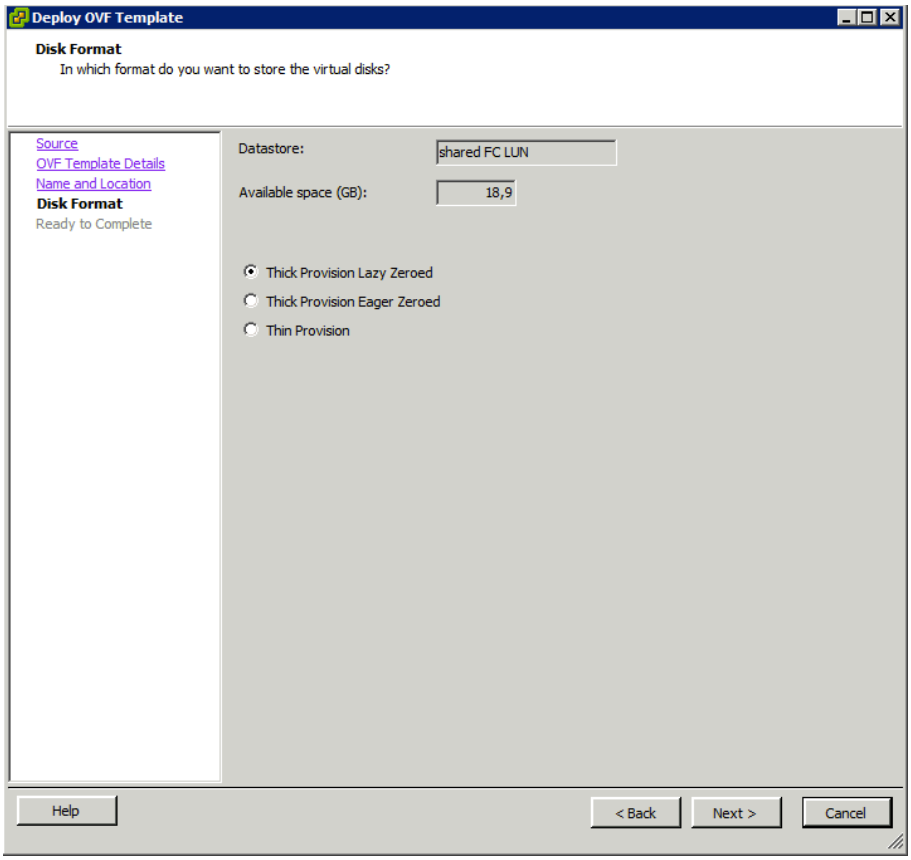
Step 41 Click next to accept the template details.



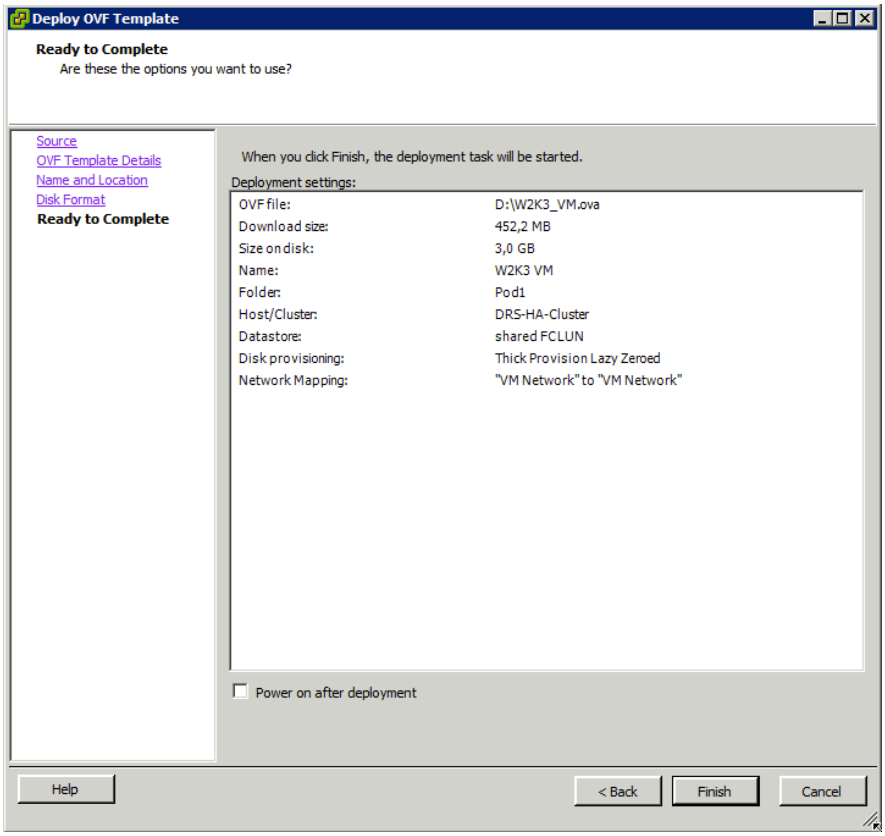
Step 42 Select your “Pod#”-DataCenter, click “Next>”



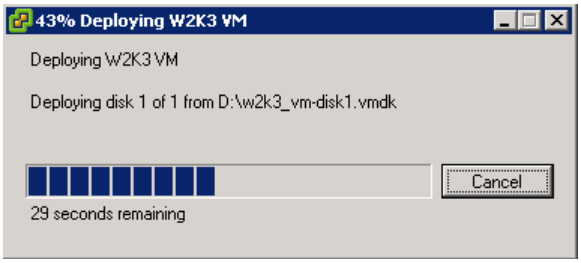
Step 43 Select the “Thick provisioned lazy zeroed” format and click “Next>”



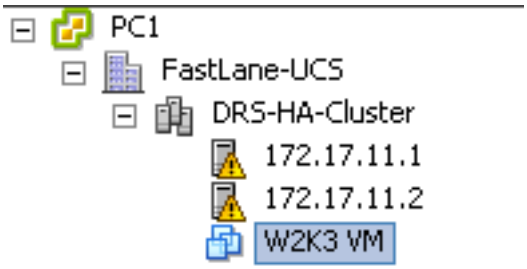
Step 44 Review and click finish



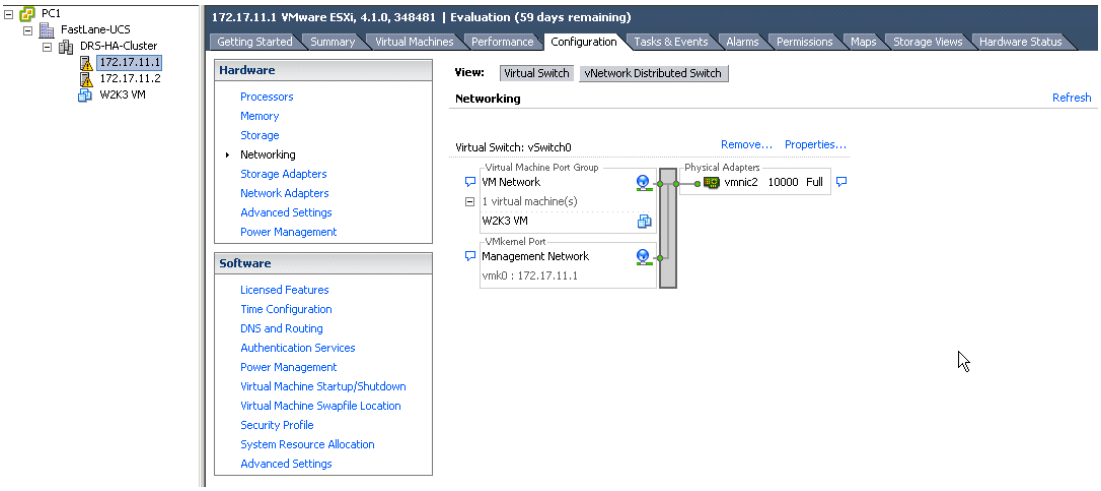
Step 45 Watch the progress bar while the OVF is being deployed as a virtual machine in the cluster.



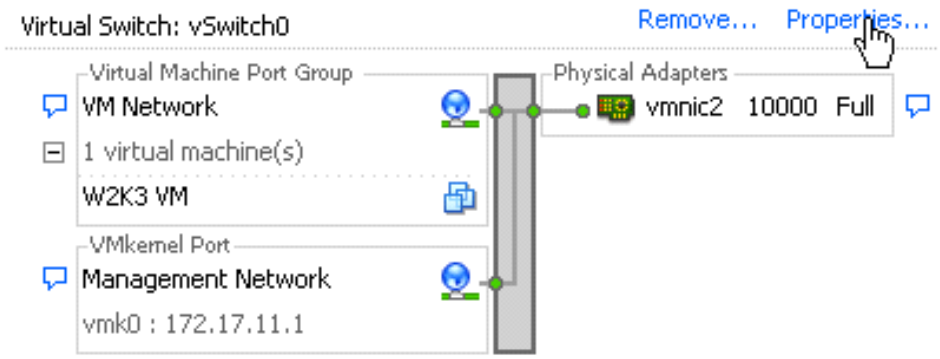
Step 46 Note the (powered-off) virtual machine has been placed in the cluster.



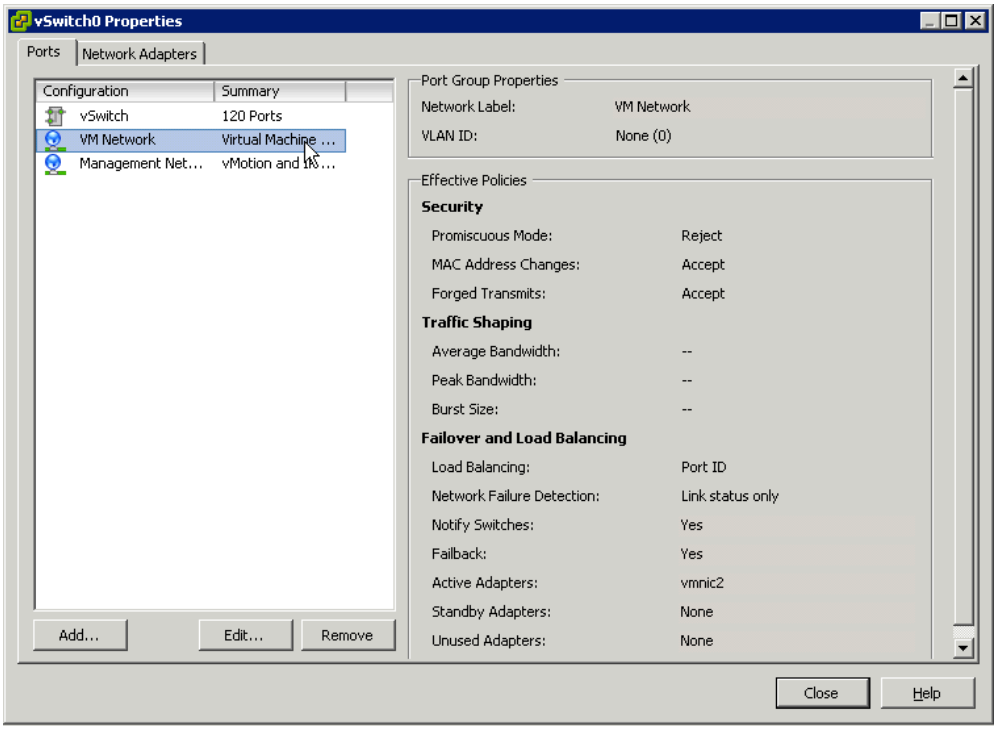
Step 47 The virtual machine needs to be connected to the correct network. Click ESXi1 in the navigation pane, select the “Configuration” tab and select “Networking” in the hardware box



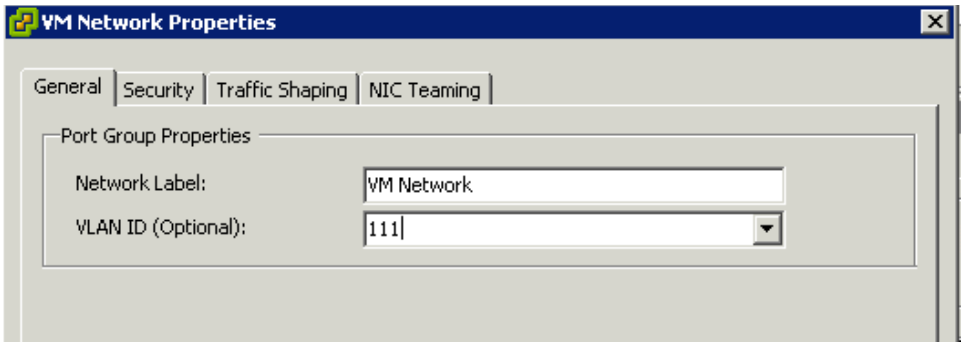
Step 48 Select “Properties” on vSwitch0



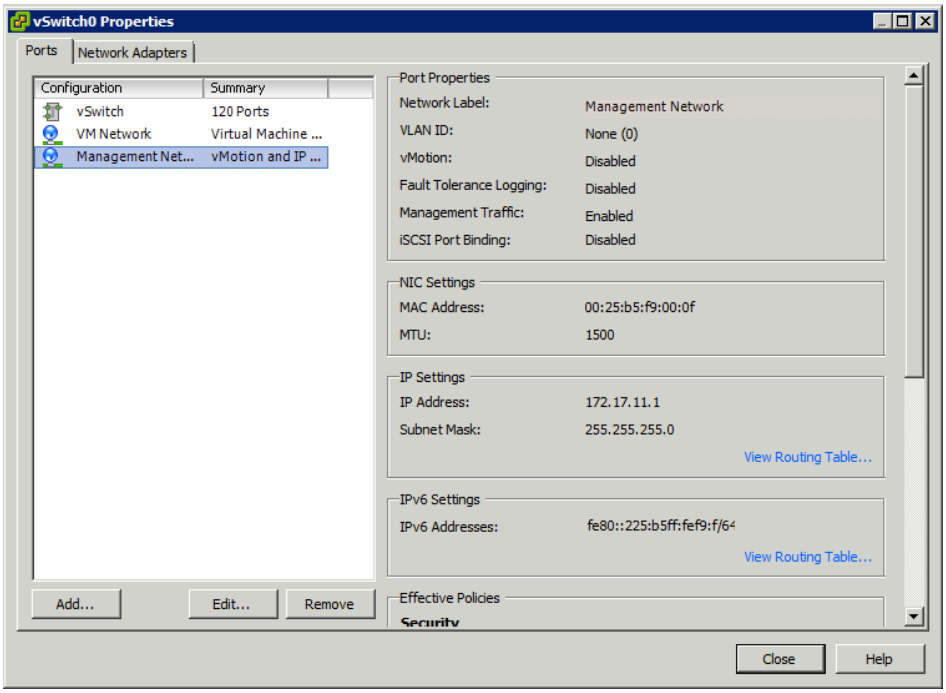
Step 49 Select “VM Network” and click edit.



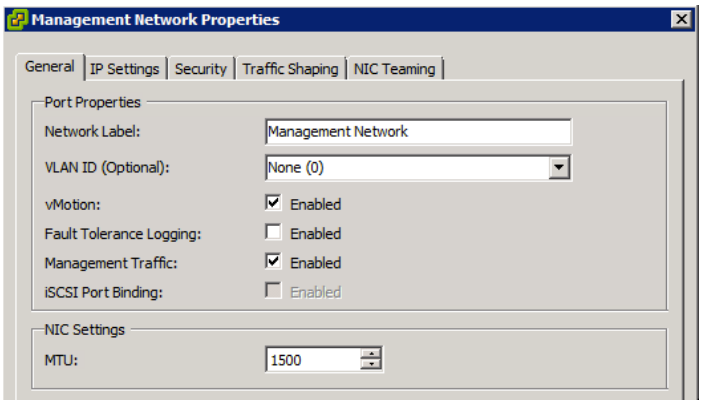
Step 50 Change the VLAN identifier to vlan LP1 (L is the lab#, P is our pod#) (hopefully you remember we've placed two vlans into the vNIC template we created a lot earlier in this class), click OK



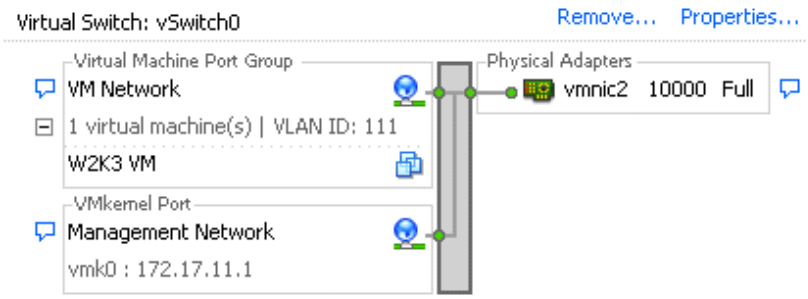
Step 51 Now select "Management Network", note in the right information pane vMotion is disabled.



Step 52 We could create an extra vMotion network/adapter, but we will just enable vMotion on the Management Network (it is a cut-though 10GE link…). Select "Edit" and enable vMotion. (DO NOT configure a VLAN! None/0 means native/untagged)

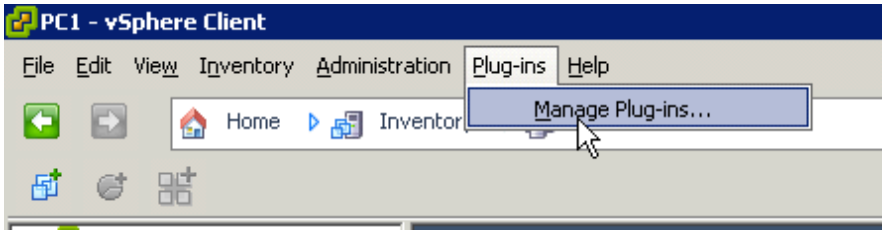


Step 53 Close the vSwitch properties dialog and validate, VM Network should now show YOUR Data VLAN.

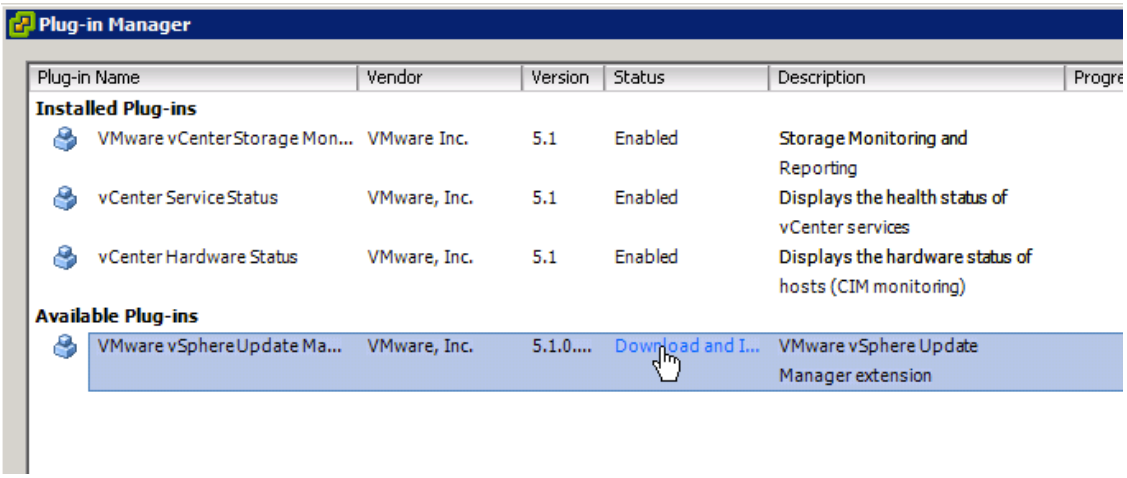


Step 54 **<u>Also adjust "VM Network" AND "Management Network" configuration on ESXi2 in the same manner.</u>**

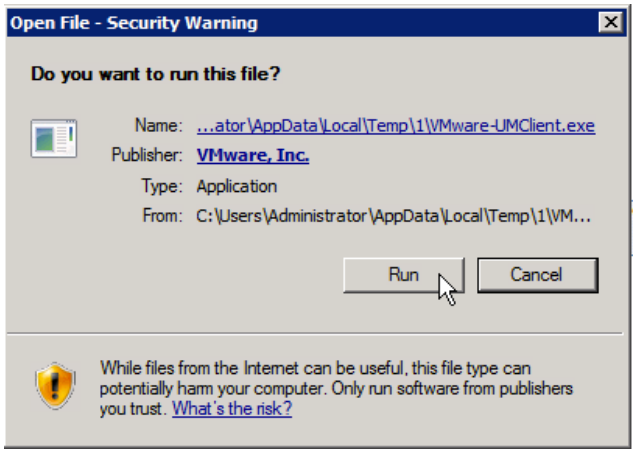
Step 55 Finally we need to install Update Manager into our vSphere client.
Click the "Plugins" menu in vSphere and select "Manage Plugins…"



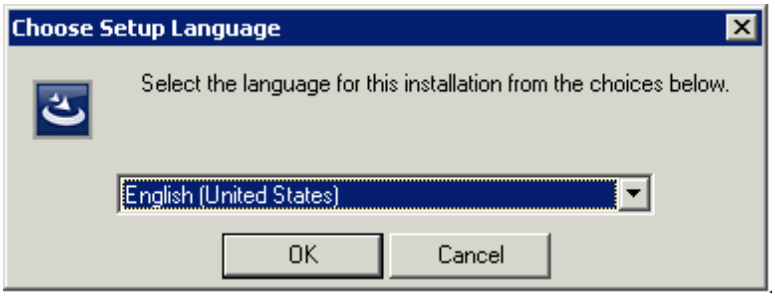
Step 56 Note Update Manager is "available" but not installed. Click "Download and Install".



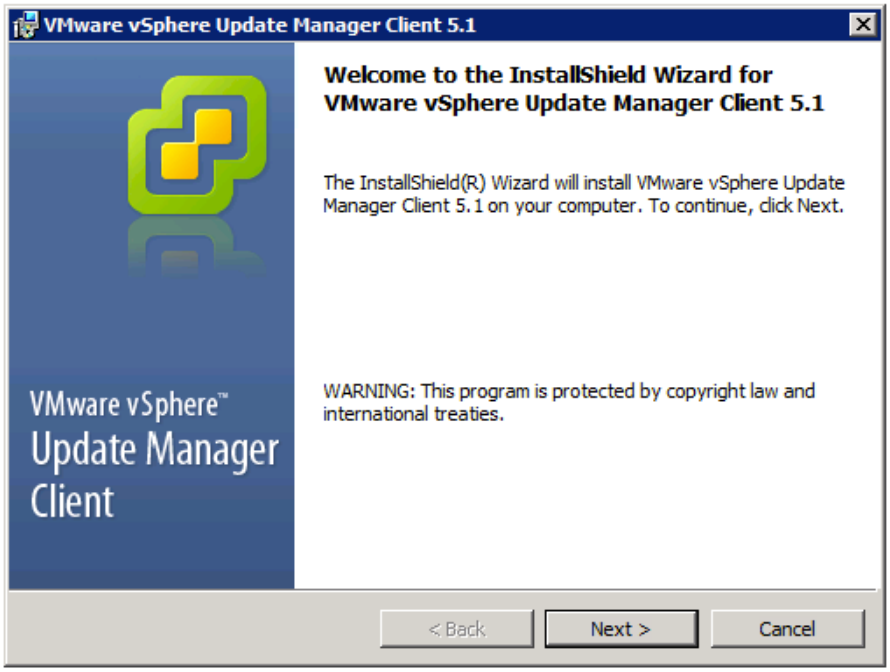
Step 57 Confirm the Windows Security Warning



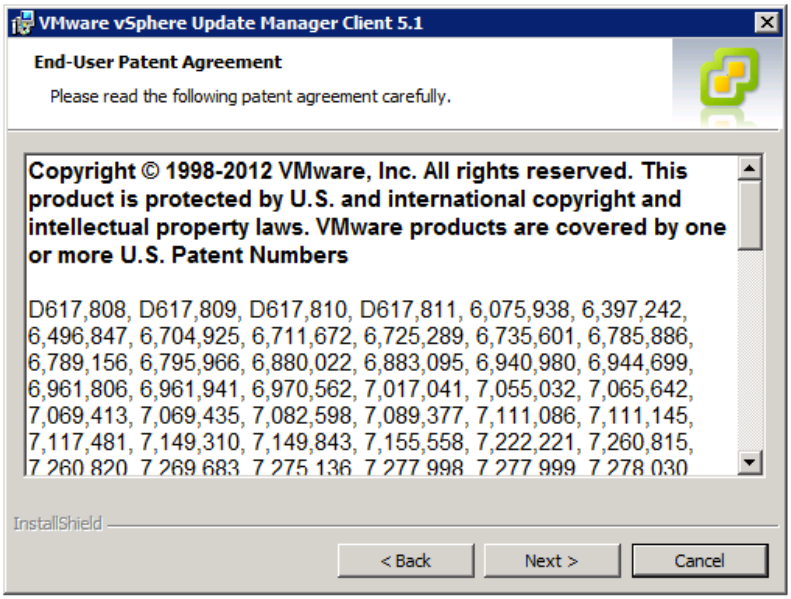
Step 58 Click OK to accept English (or change the language, but keep in mind this lab guide is based on the English installation)



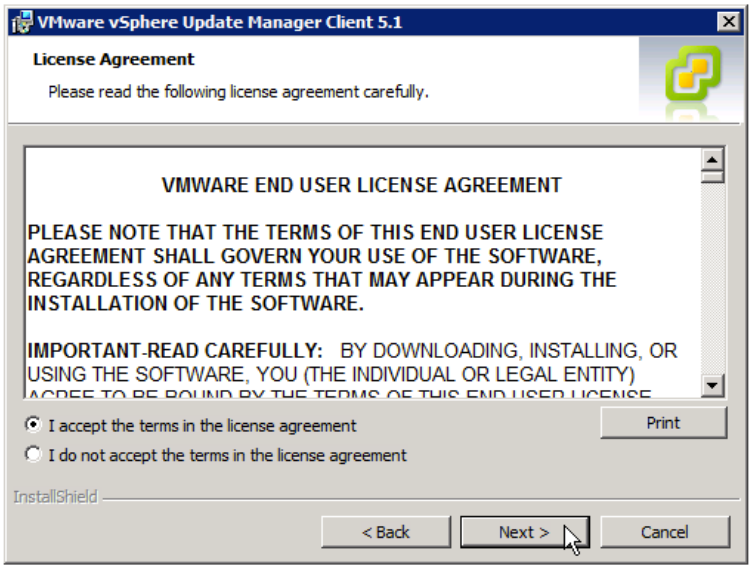
Step 59 Click "Next>" to start installation



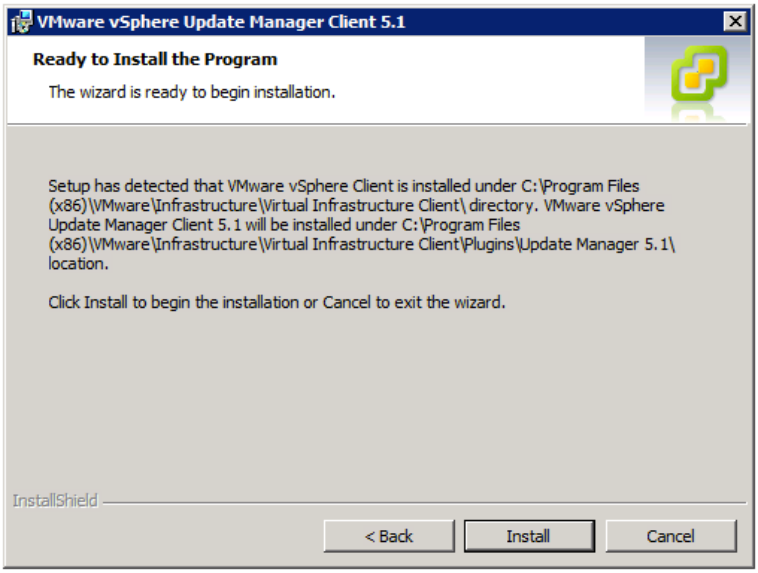
Step 60 Click "I agree…" and "Next>" to accept the Patent Agreement.



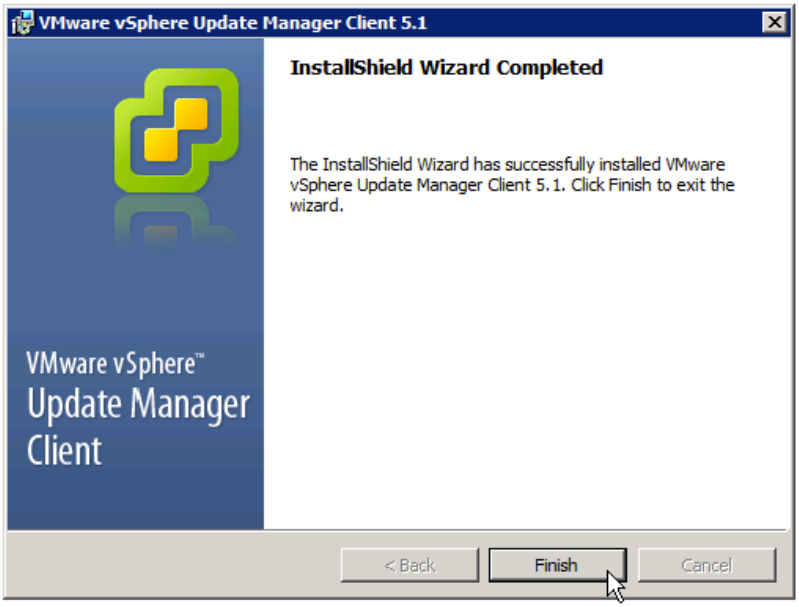
Step 61 Click "I agree…" and "Next>" to accept the EULA.



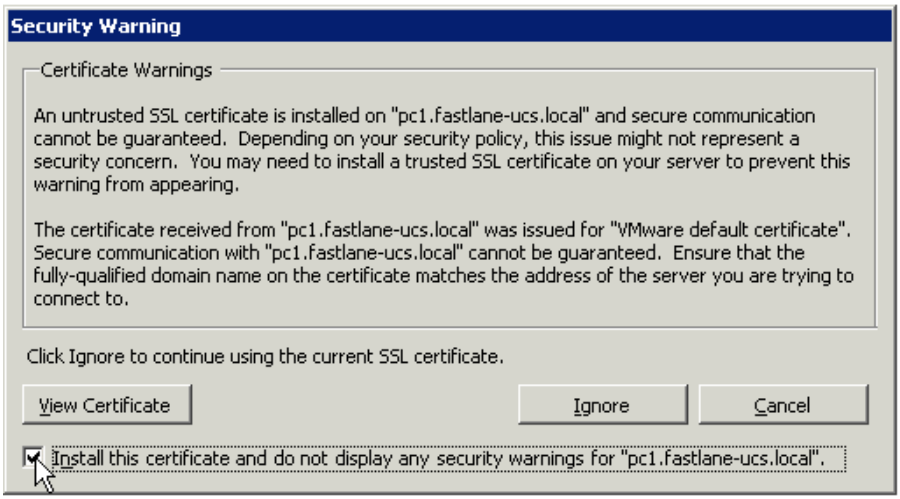
Step 62 VUM Client Setup confirms your vSphere Client installation. Click "Install" to install. **This takes about 1 Minute**.



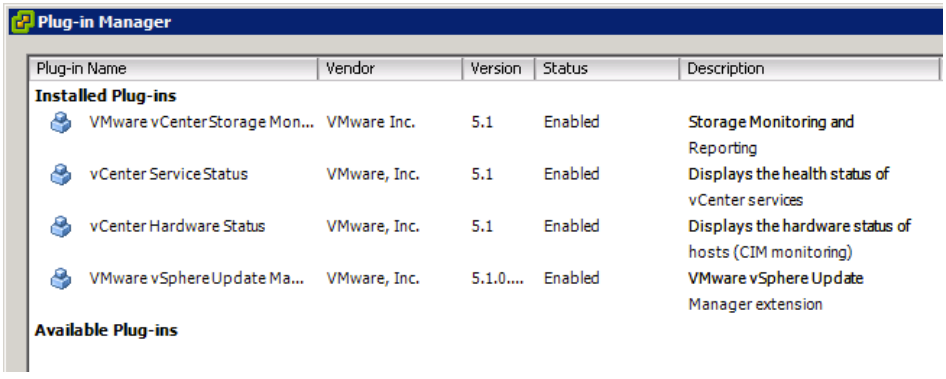
Step 63 Click Finish to close the Installer.



Step 64 When the Security Warning pops up, click "install certificate…" and "Ignore" to accept VUMs certificate.



Step 65 Note the Plugin Window now shows VMWare Update Manager as "installed"



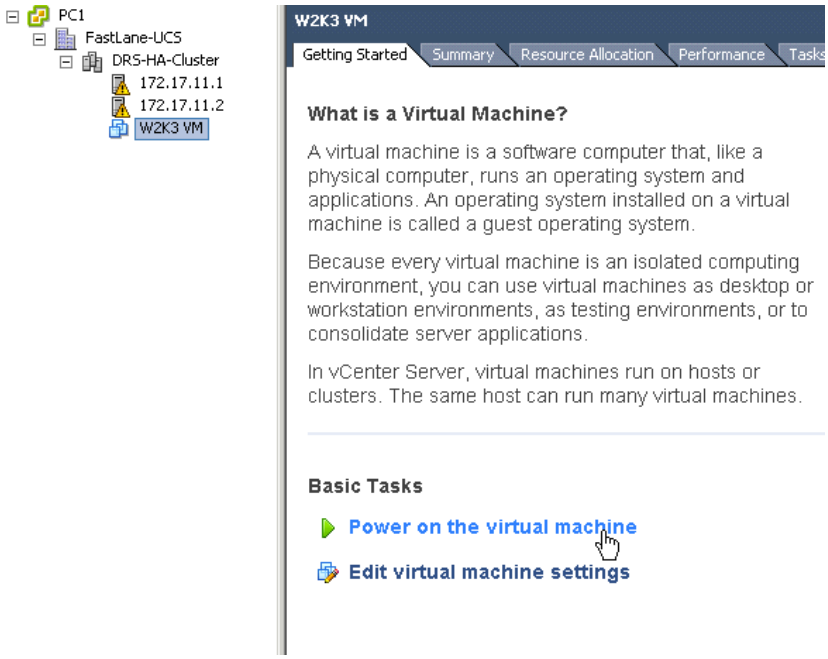
Task 6: Power on, test and vMotion a virtual machine.

In this task, you will power on the VM, test connectivity and vMotion.

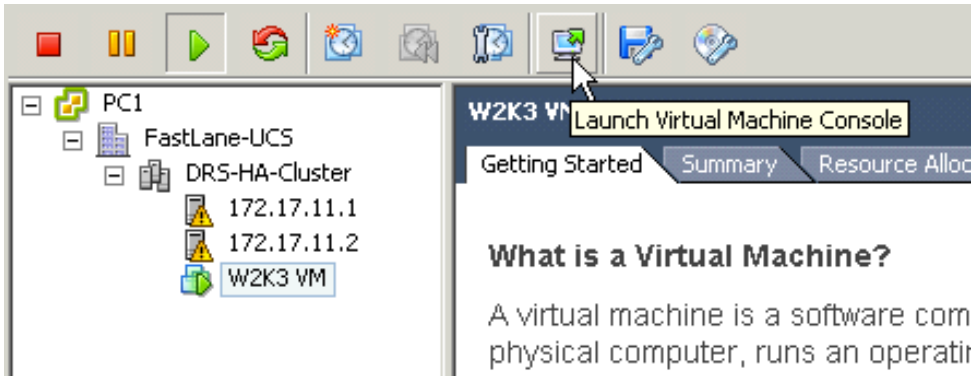
Activity Procedure

Complete these steps:

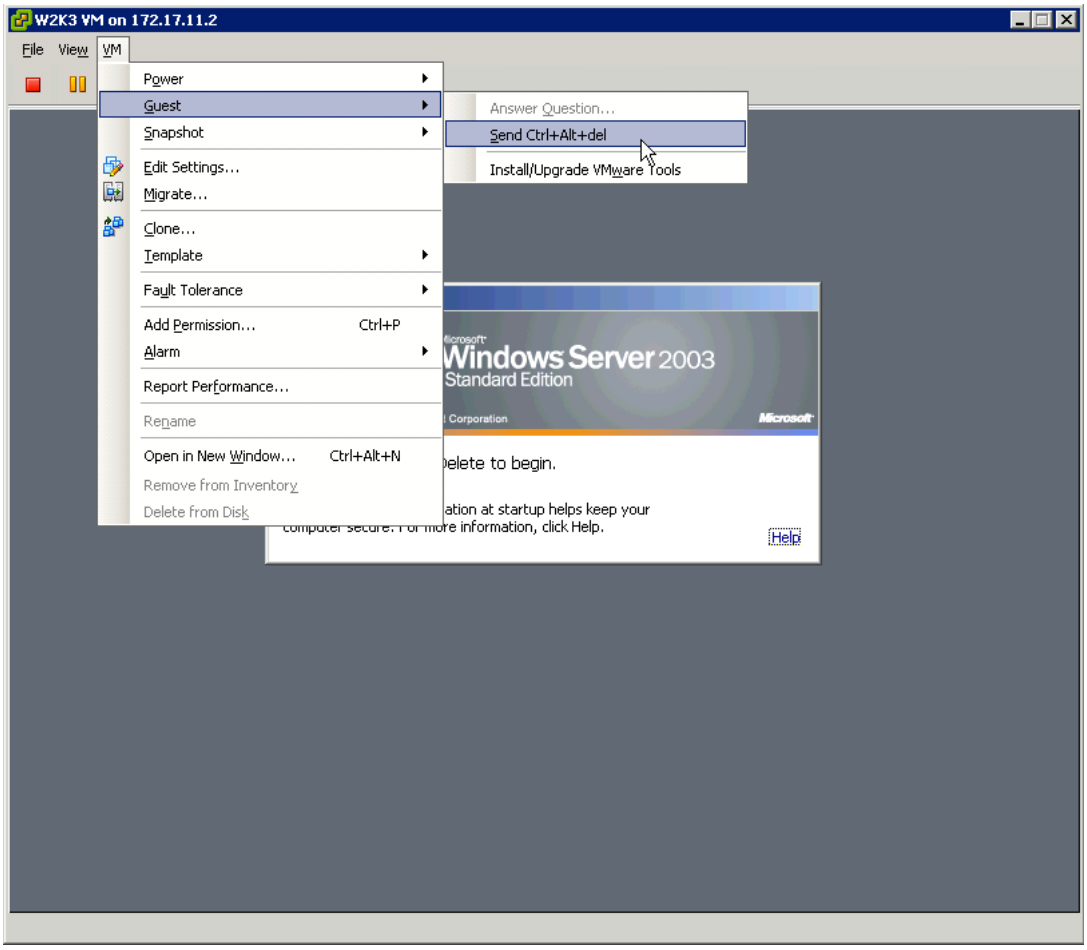
Step 1 Select the Win2K3 VM in the navigation pane and click “Power On virtual machine” (or use the “play” button in the toolbar)



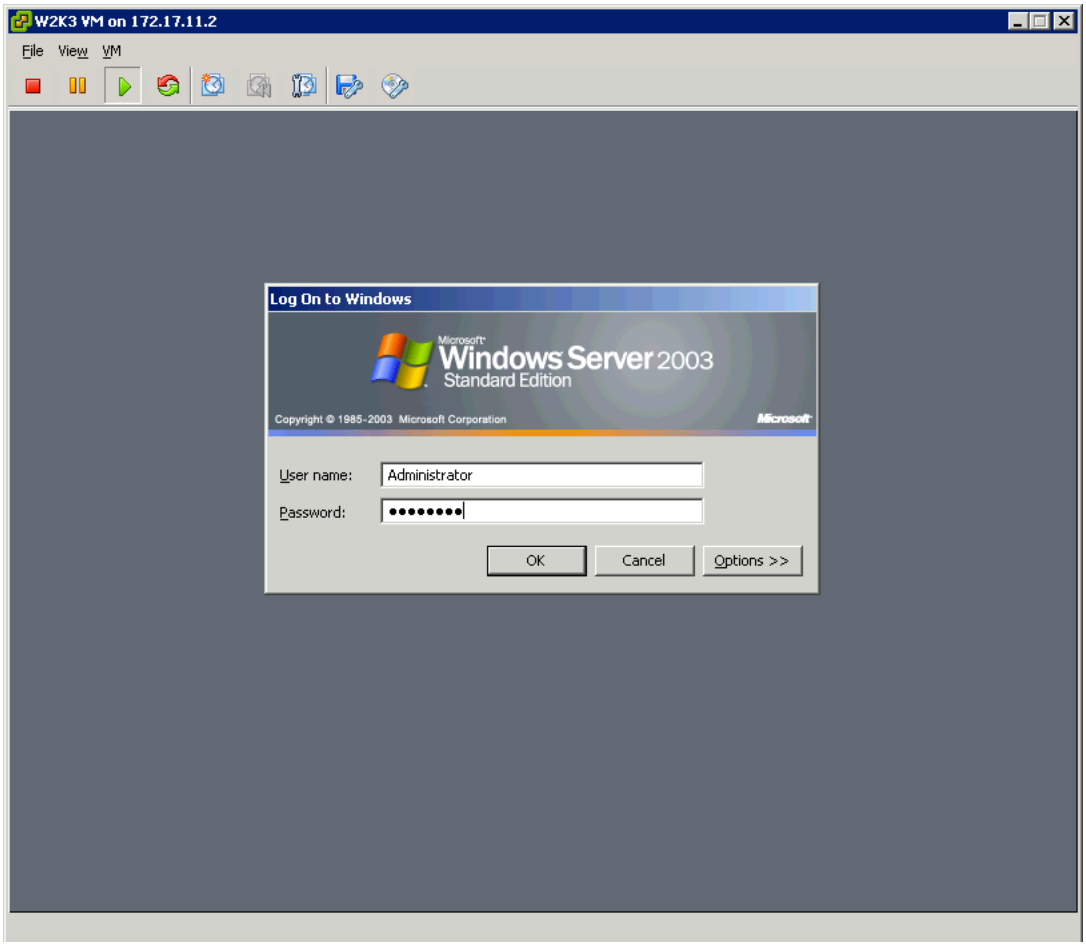
Step 2 Click “Lauch Virtual Machine Console” in the tool bar.



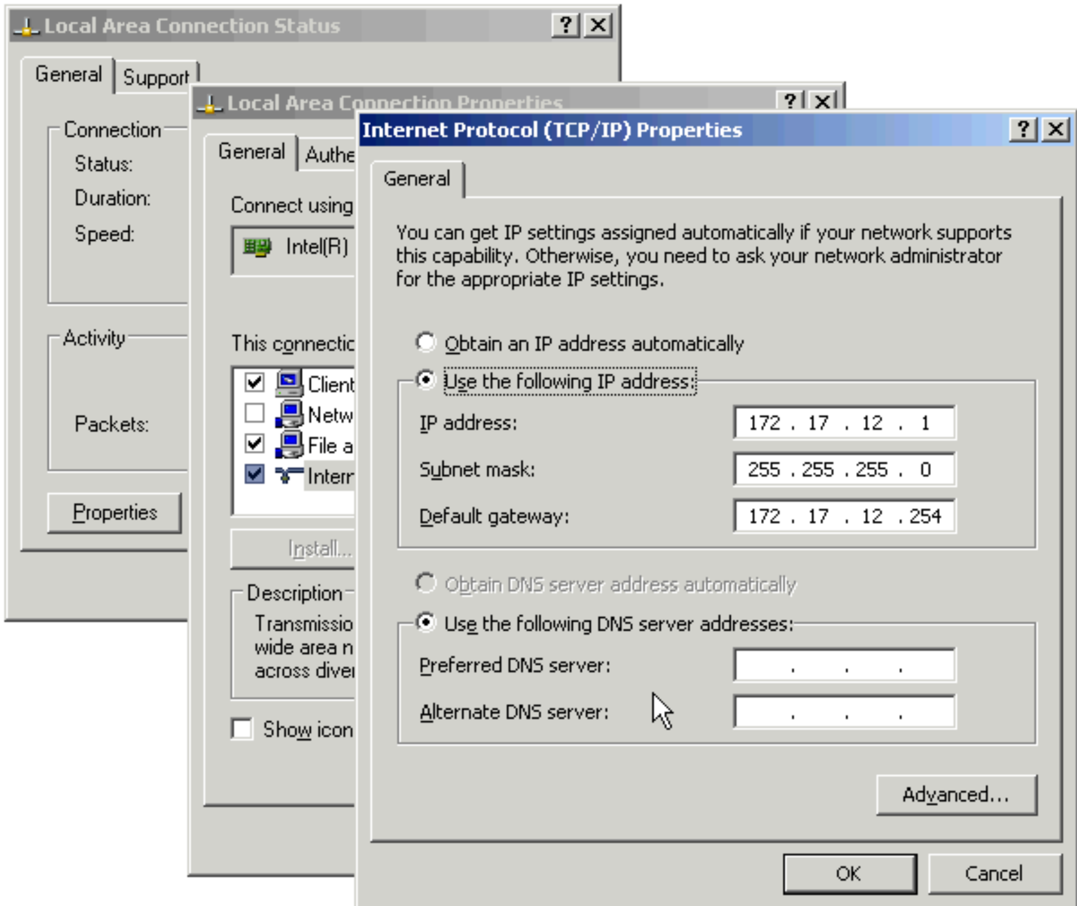
Step 3 Click VM->Guest->Send CRTL/ALT/DEL to log into the server



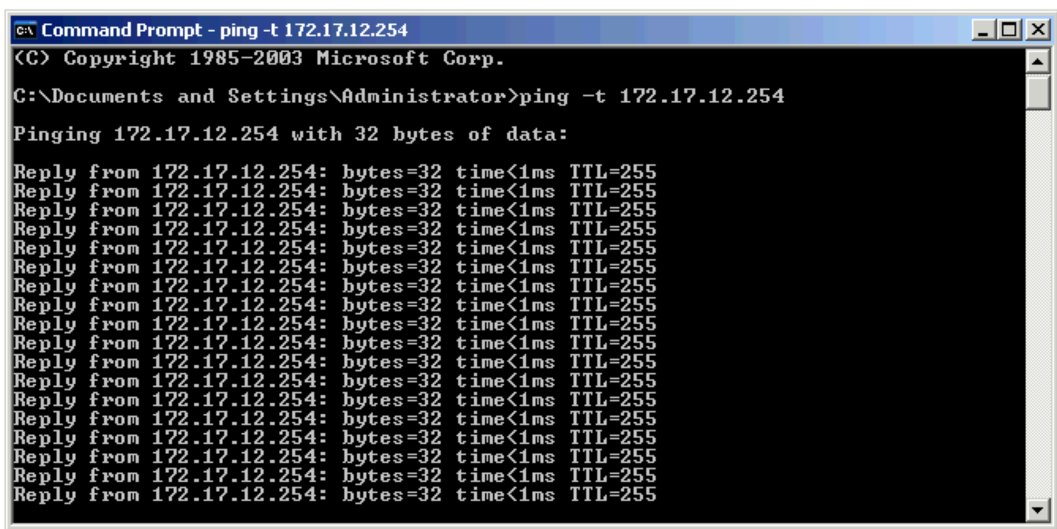
Step 4 Log in with user “administrator” and password “1234QWer”



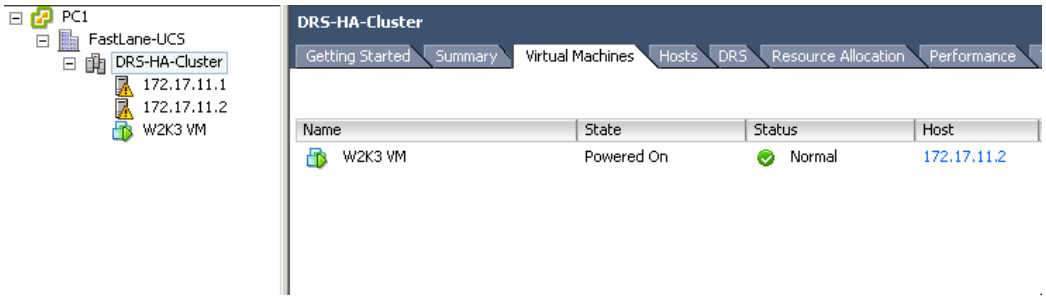
Step 5 Assign IP address 172.17.P2.1/24 with default gateway 172.17.P2.254 to the NIC.



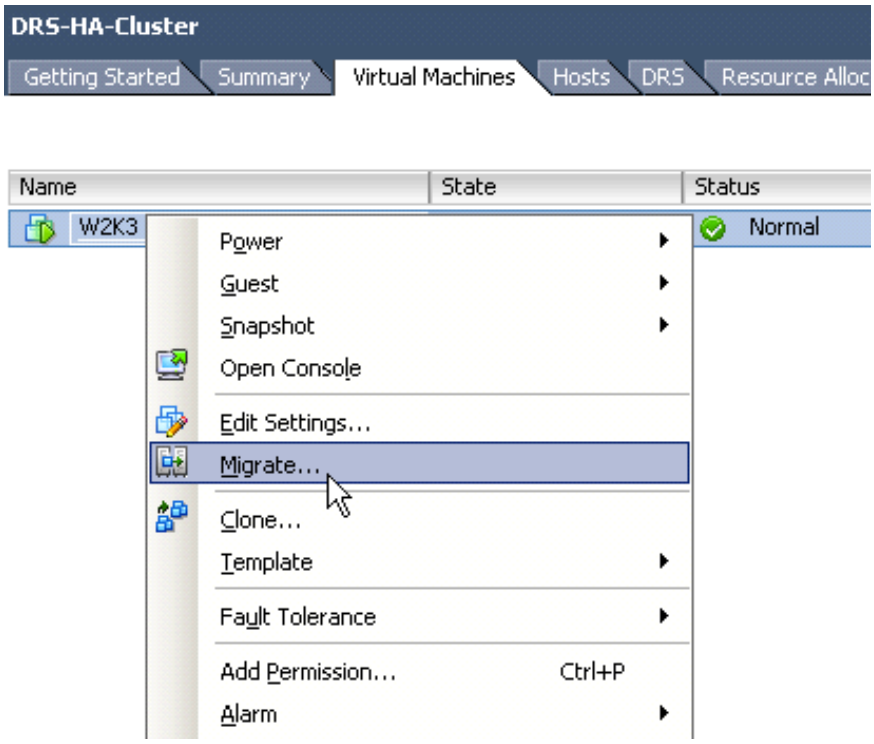
Step 6 Open a command prompt and ping –t the default gateway 172.17.P2.254



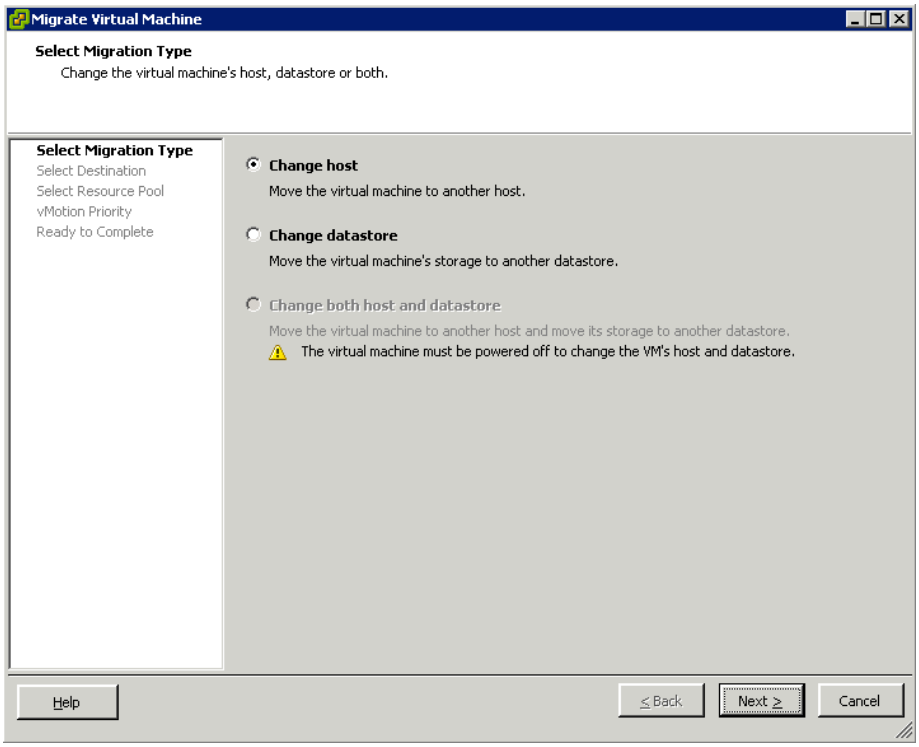
Step 7 Leave the ping running and return to vCenter. Select the cluster and the "Virtual Machines" Tab. Note DRS has placed the VM on one of your ESXi hosts.



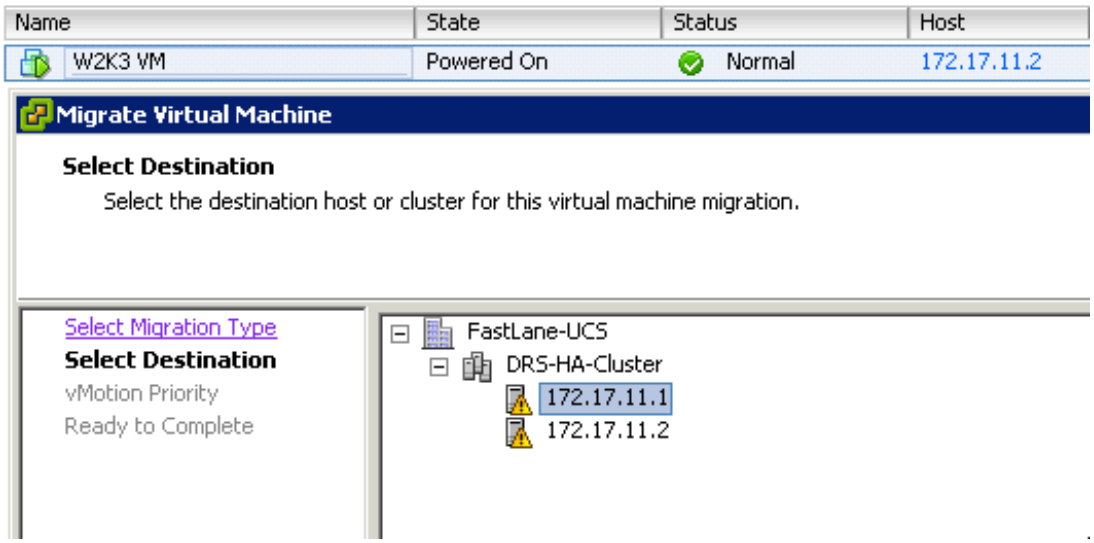
Step 8 Right-click the VM and select “Migrate”



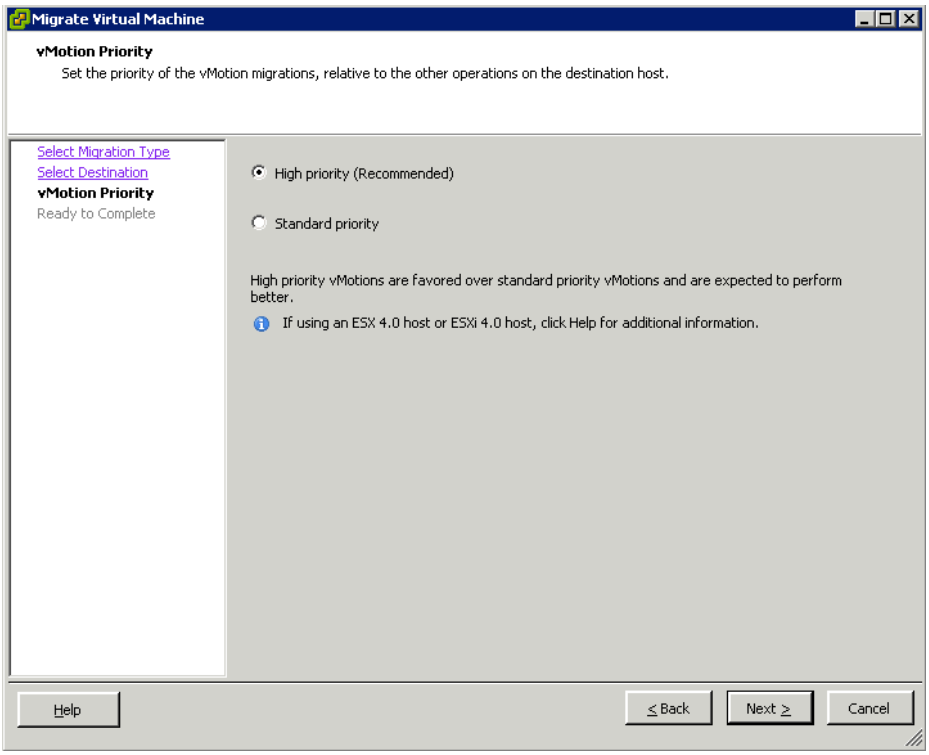
Step 9 Select “Change Host” and click “Next>”



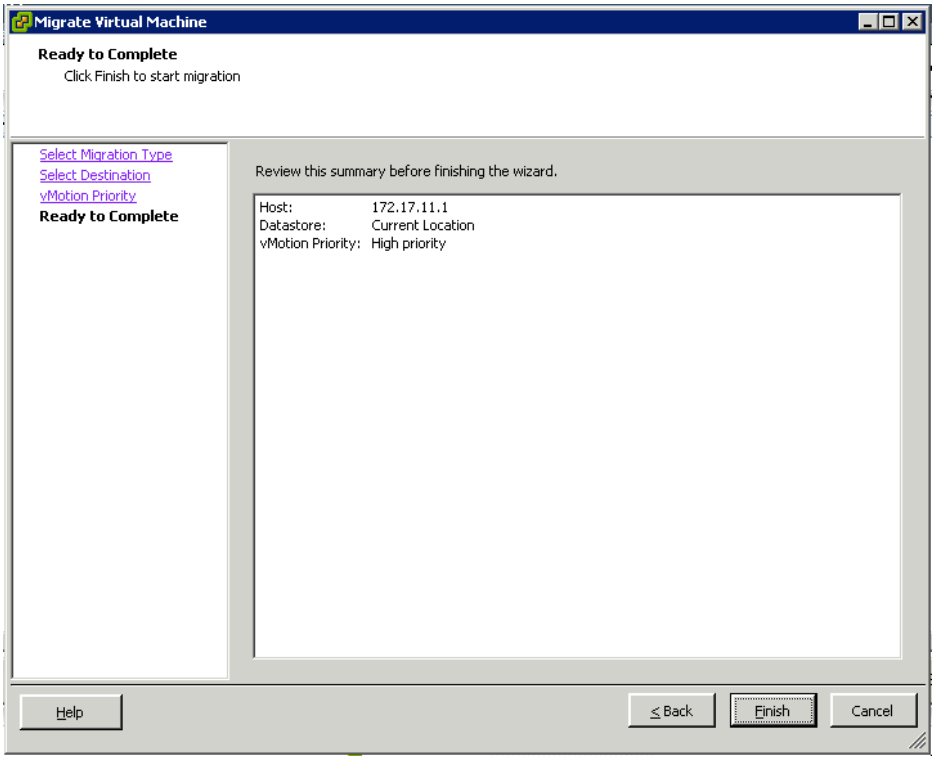
Step 10 Select the OTHER ESXi Host and click “Next>”



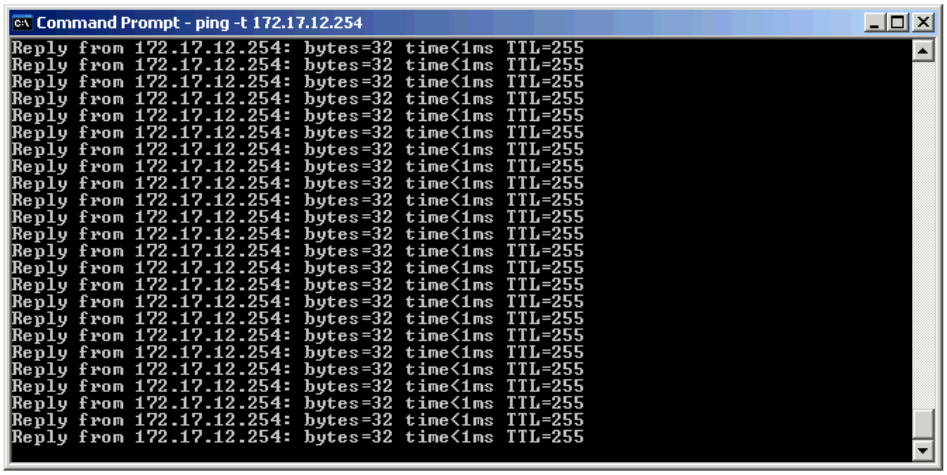
Step 11 Keep “high Priority” and click “Next>” (it does not make ANY difference in this lab)



Step 12 Review and click “Finish” to start.



Step 13 Switch to the Virtual machine console. Notice the console itself pauses briefly but we did not loose a single packet, you can’t even tell from the delay where vMotion actually happened.



Step 14 Note the timestamps for start and end of vMotion the vCenter log at the bottom of the window.

Lab 5-2: Configure Cisco VM-FEX

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

Activity Objective

In this activity, you will add a VM on your ESXi host and provision the VM networking with the DVS.

- Connect UCS Manager to vCenter
- Validate VM configuration
- Add ESXi host to the DVS
- Provision the Windows 2008 virtual machine to use the DVS port group
- Validate the VM port state and connectivity with the ping command
- Demonstrate VMotion of hosts and M81-KR port profile mobility

Required Resources

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

- Student PC
- Lab implementation information

Task 1: Provision VMware Integration with Cisco UCS Manager

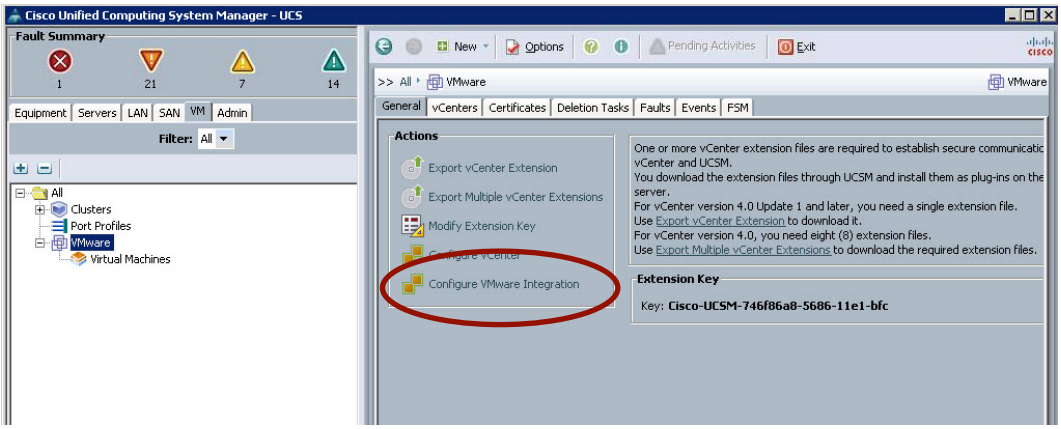
In this task, you will provision VMware integration in Cisco UCS Manager.

Activity Procedure

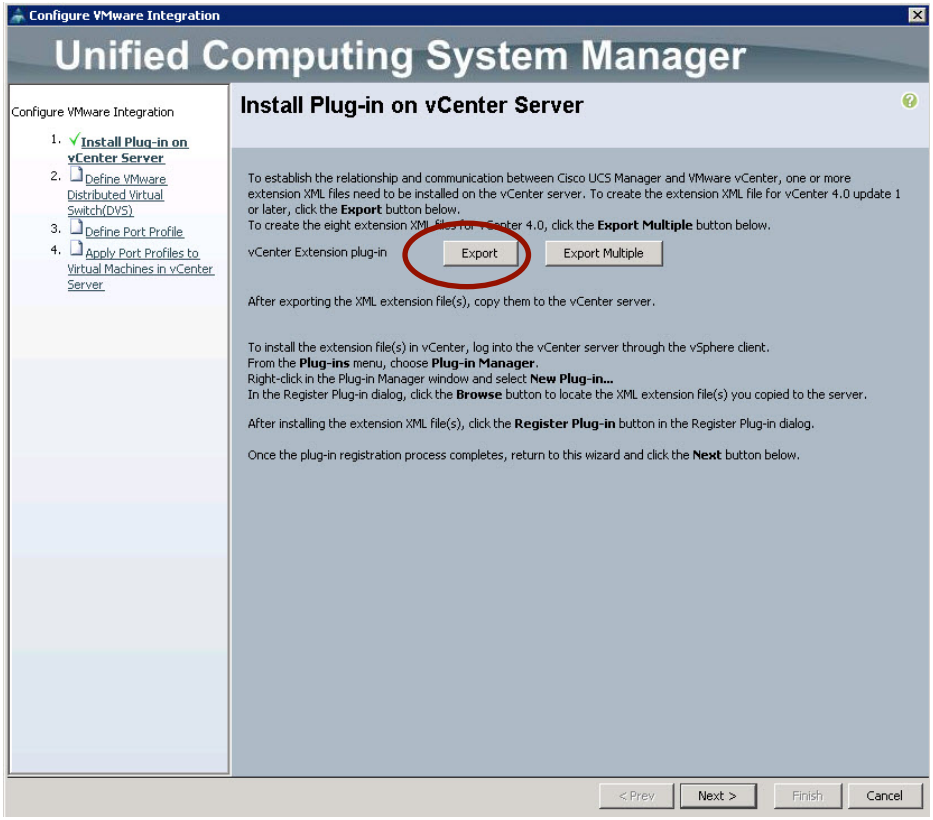
Complete these steps:

Step 1 Open Cisco UCS Manager and go to the **VM** tab.

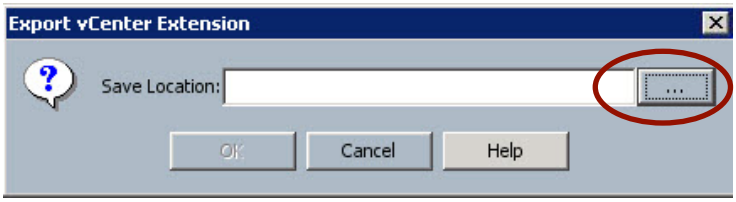
Step 2 Select **VMware** and click **Configure VMware Integration**.



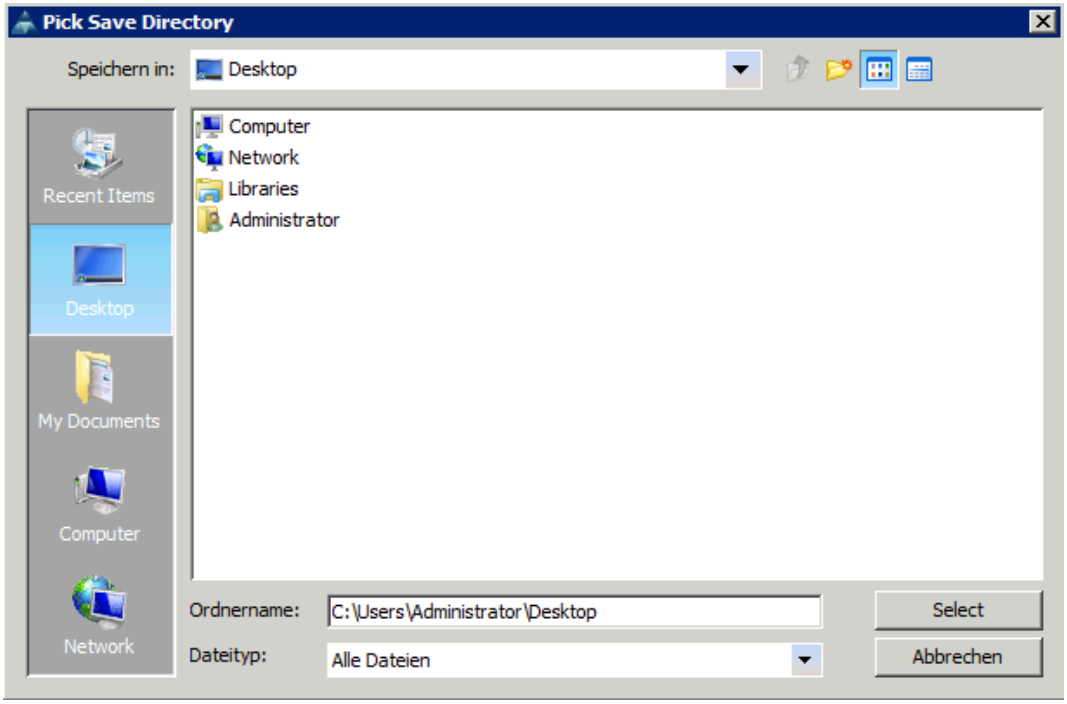
Step 3 Click **Export** to download the Cisco UCS Manager extension file.



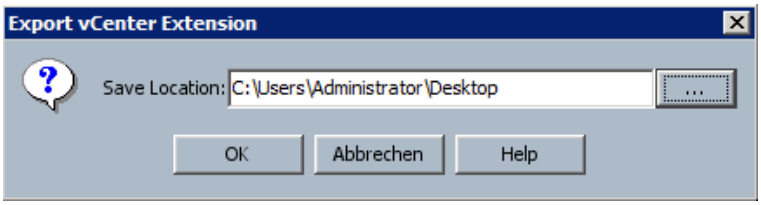
Step 4 Click the ellipsis (**…**) to select a location.



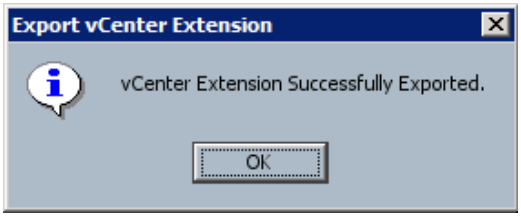
Step 5 Click **Desktop** and then **Select**.



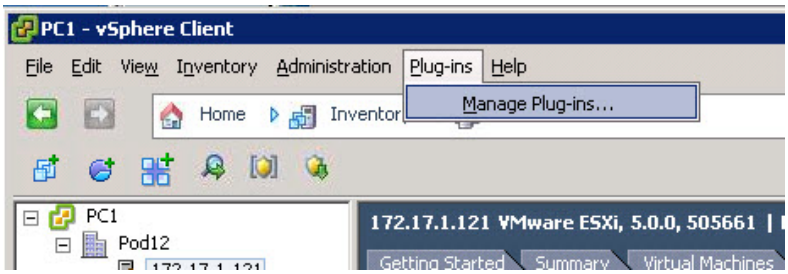
Step 6 Click **OK** to export the extension.



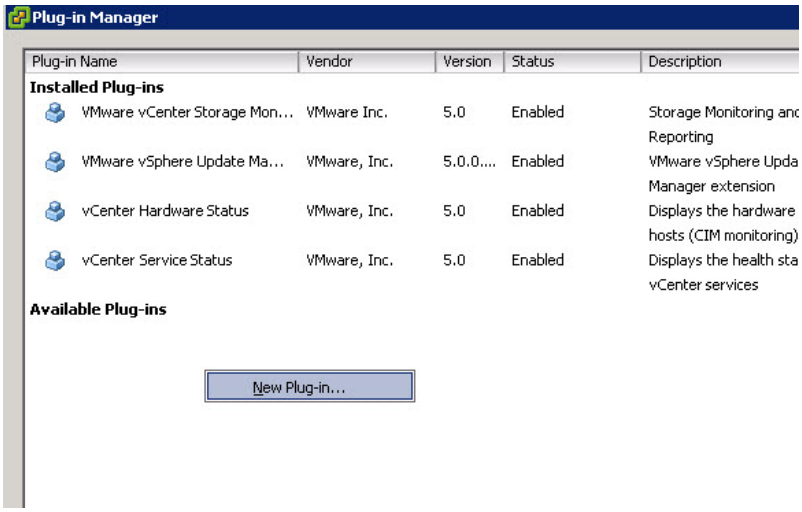
Step 7 Click **OK** to close the message for the successful export.



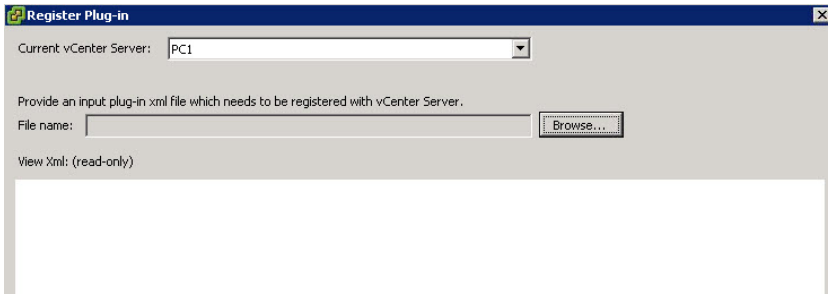
Step 8 Leave the wizard open and open vSphere Client, click **Plug-ins** and choose **Manage Plug-ins**.



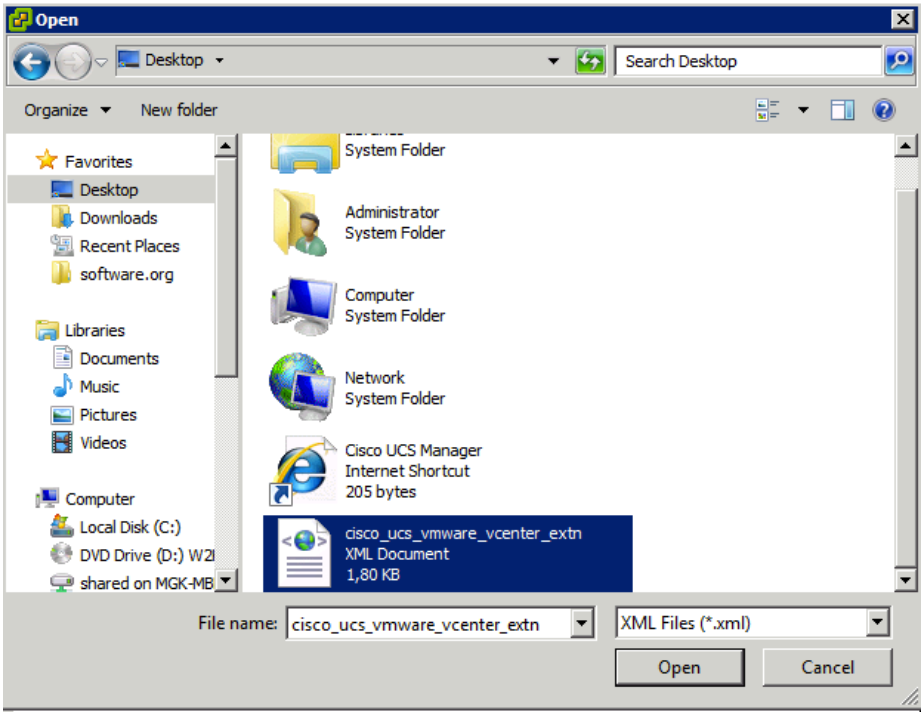
Step 9 In the white space, right-click and choose **New Plug-in…**



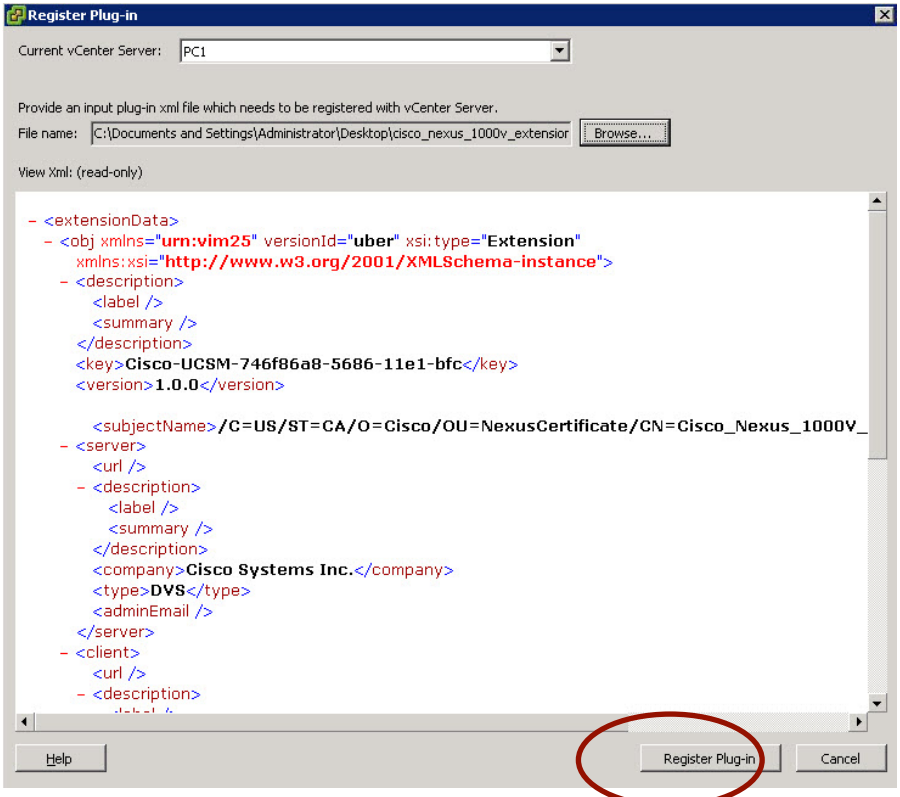
Step 10 Click **Browse** to select the Cisco UCS Manager extension.



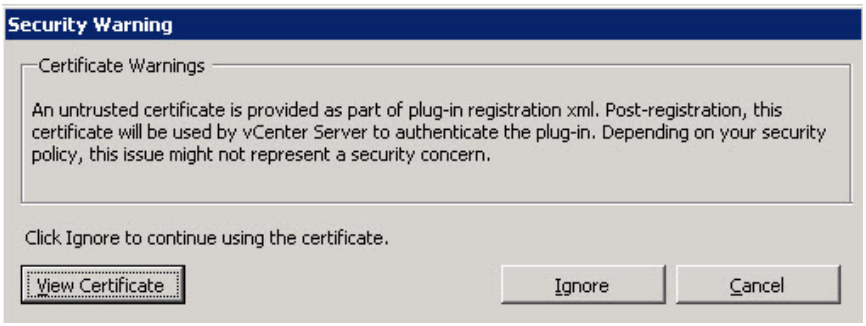
Step 11 Browse to the desktop and select the extension file. Click **Open** to continue.



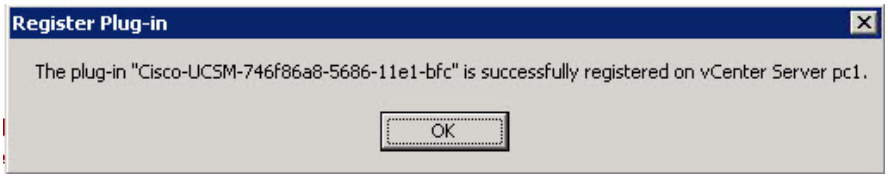
Step 12 Click **Register Plug-in**.



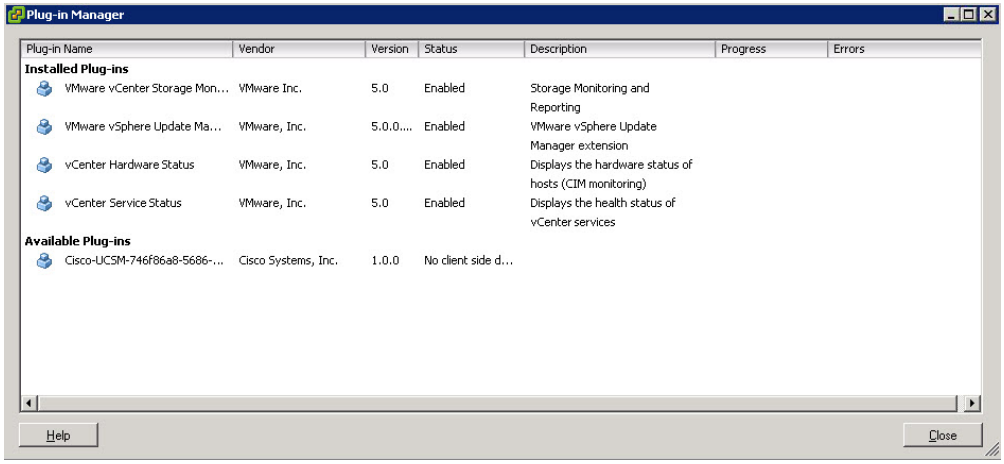
Step 13 Click **Ignore** at the Security Warning window.



Step 14 Click **OK** on the message for the successful plug-in registration.

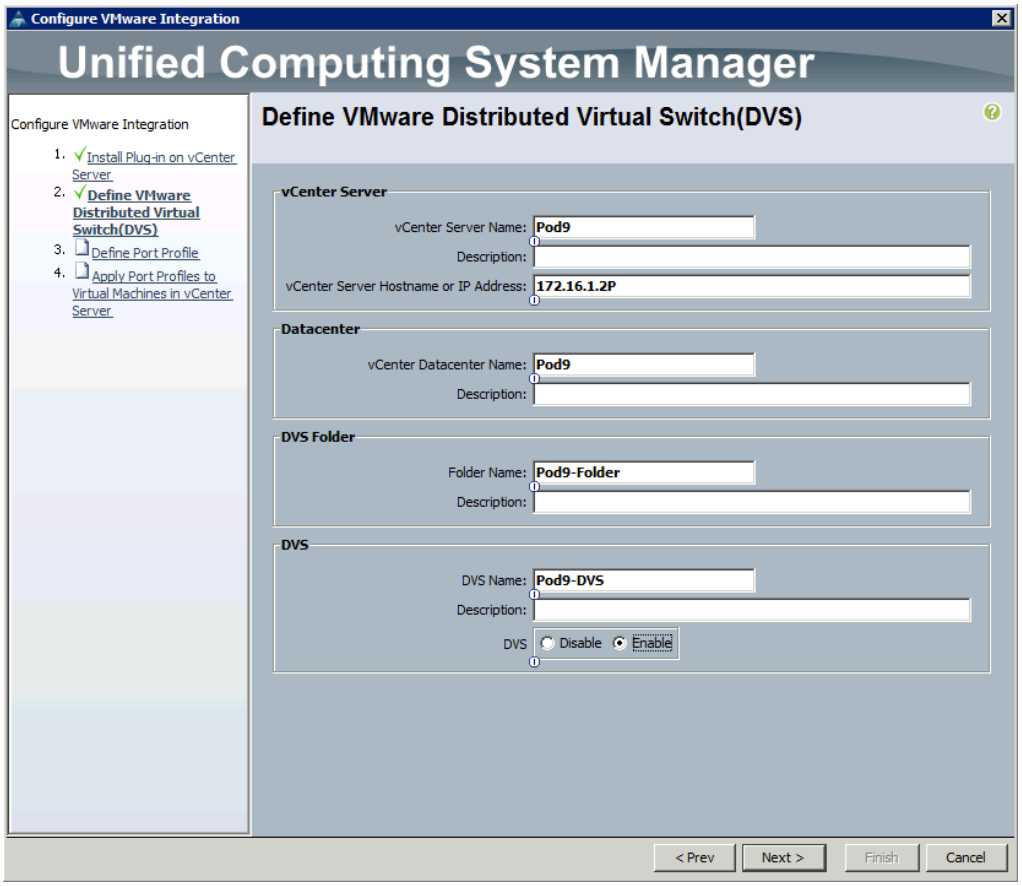


Step 15 You will observe the Cisco UCS Manager plug-in in the Plug-ins Manager. Click **Close** to exit.

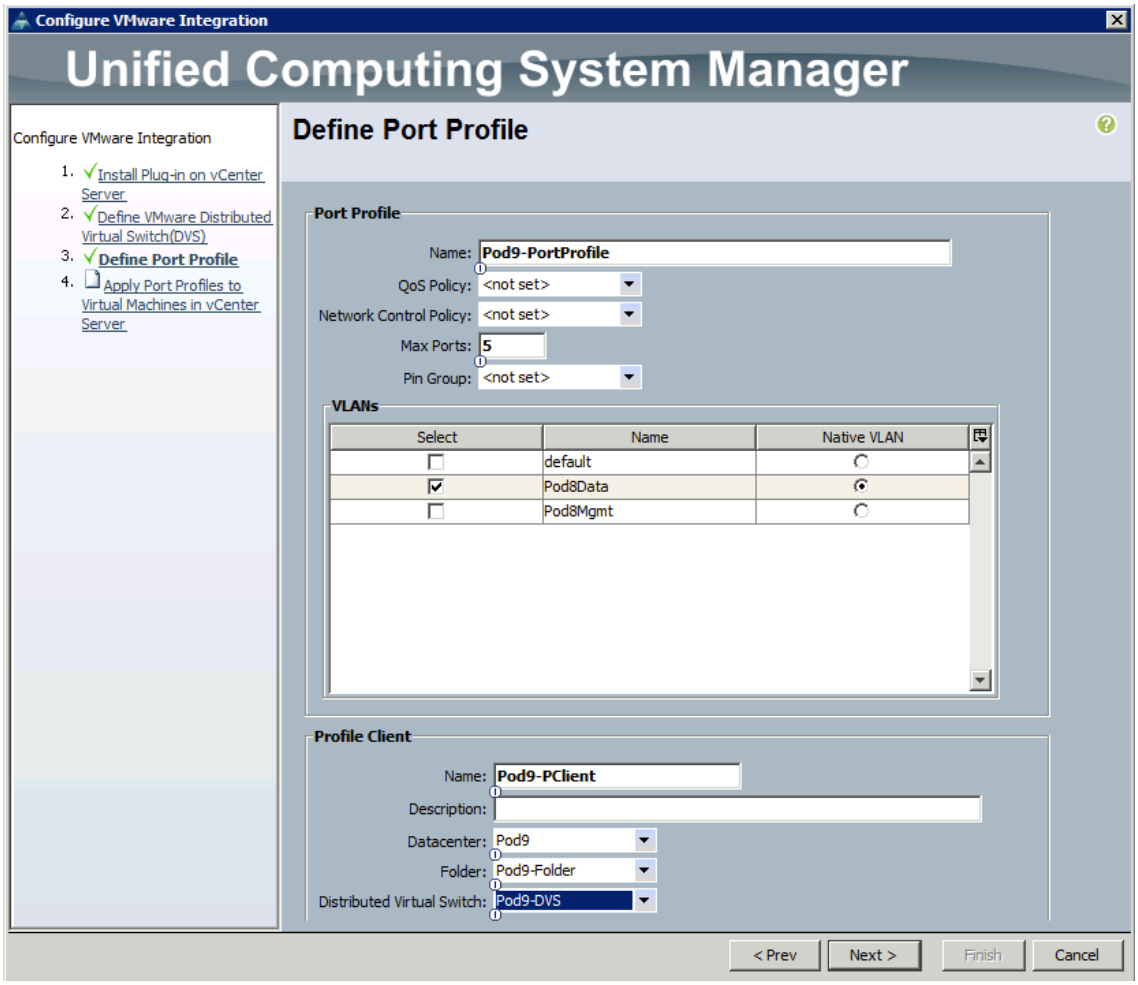


Step 16 Return to the Cisco UCS Manager VMware integration wizard and click **Next**.

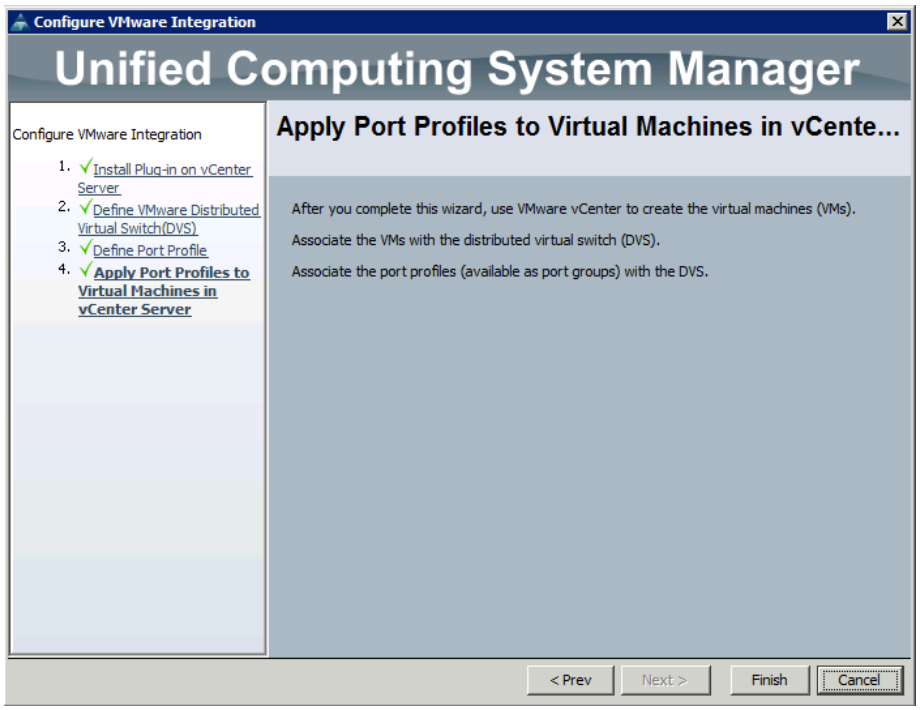
Step 17 Set the vCenter server name as **Pod#**, where **#** is the podnumber. Set the **IP address** of the vCenter server as **172.16.1.2#**, where # is your pod number. Set the **vCenter Datacenter Name** to your datacenter **Pod#**, where **#** is the pod number. Set the **DVS Folder** name to **Pod#-Folder**, again where **#** is the pod number. Set the **DVS Name** to **Pod#-DVS**, where **#** is your pod number. Set the **DVS** state to **Enable**. Click **Next** to continue.



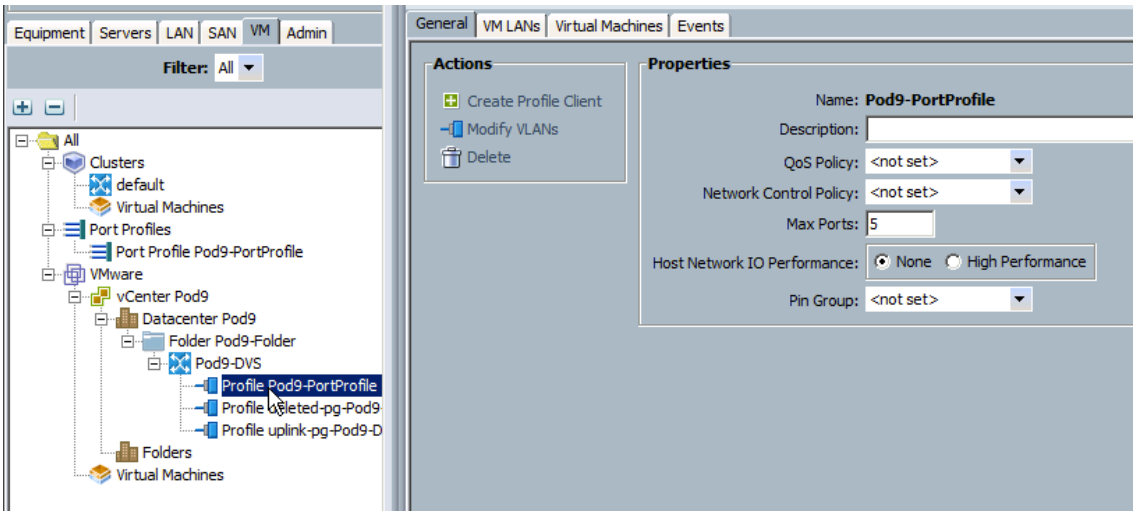
Step 18 Set the **Port Profile Name** to **Pod#-PortProfile**, where **#** is your pod number. Set **Max Ports** to **5**. Select your pod Pod#Data VLAN and make it native. Set the **Profile Client Name** to **Pod#-PClient**, where **#** is your pod number. From the drop-down menus, select your **Datacenter**, **Folder**, and **DVS**. Click **Next** to continue.



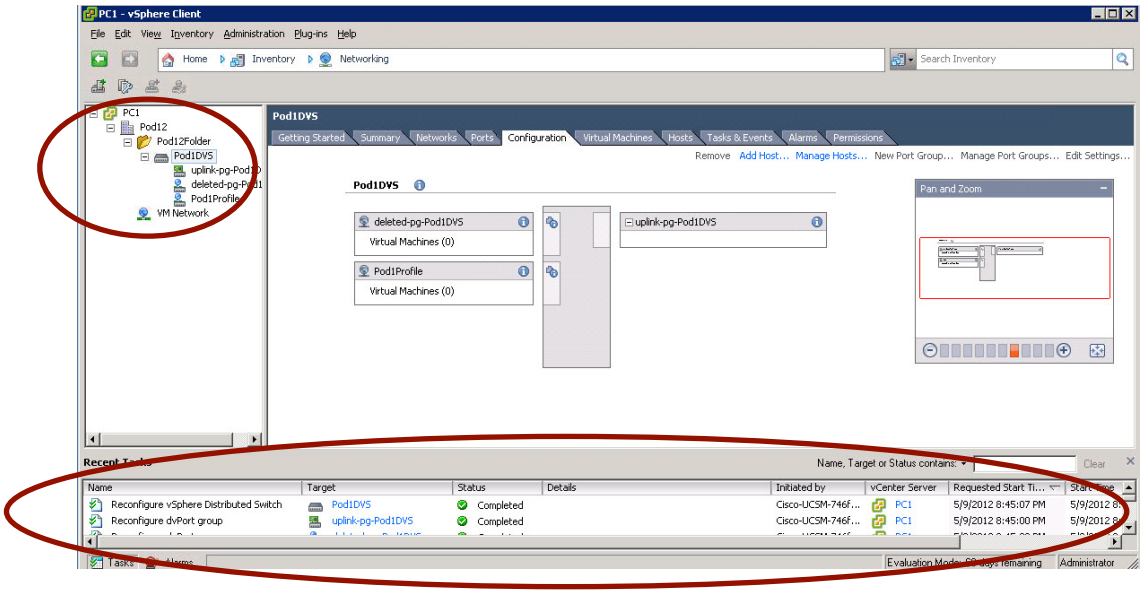
Step 19 Click **Next>** and **Finish** to complete the confgiuration.



Step 20 Expand all of the subsections of **VMware** in the **VM** tab. Select your port profile. The new DVS is created.



Step 21 In vSphere Client, navigate to **Home > Inventory > Networking**. Validate that a new DVS is created. Observe in Recent Tasks the messages for the creation of the DVS.



Activity Verification

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

- You have successfully integrated the Cisco UCS Manager with vCenter Server.
- You can see the new DVS in vCenter Server.

Task 2: Create a Dynamic vNIC Connection and Associate It

In this task, you will create a dynamic vNIC connection policy and associate it with the service profile.

Activity Procedure

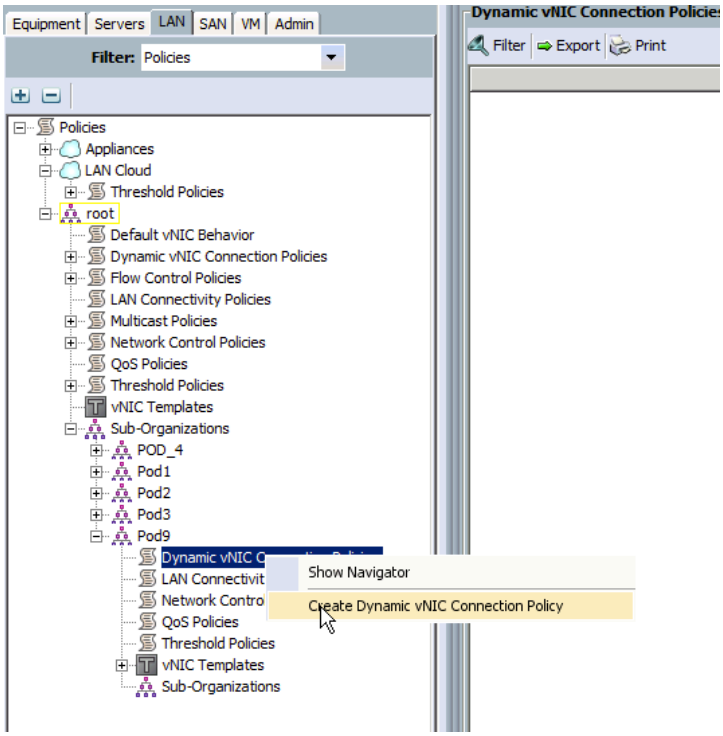
Complete these steps:

Step 1 In Cisco UCS Manager, select the **LAN** tab.

Step 2 From the **Filter** field, choose **Policies**.

Step 3 Select and expand your organization under **Policies**.

Step 4 Right-click **Dynamic vNIC Connection Policies** and select **Create Dynamic vNIC Connection Policy**.

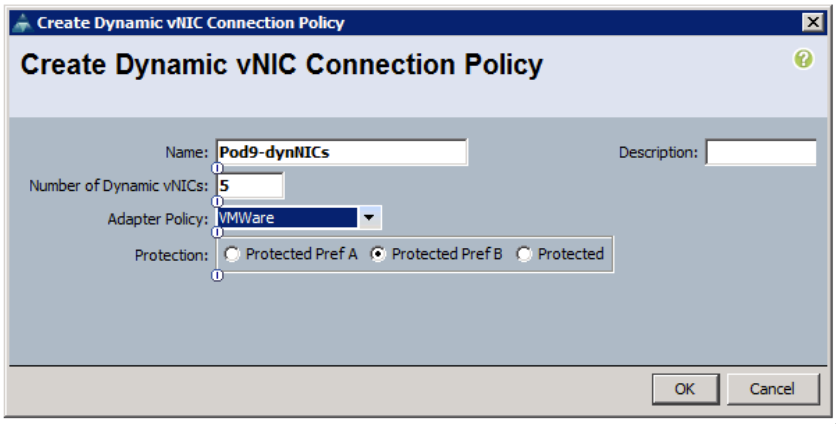


Step 5 In the new window, set the **Name** of the policy according to Pod#-dynNICs.

Step 6 Set the **Number of Dynamic vNICs** to **5**.

Step 7 Choose the VMWare adapter policy from the drop-down list.

Step 8 Choose "Protected, Pref B" as the Protection.

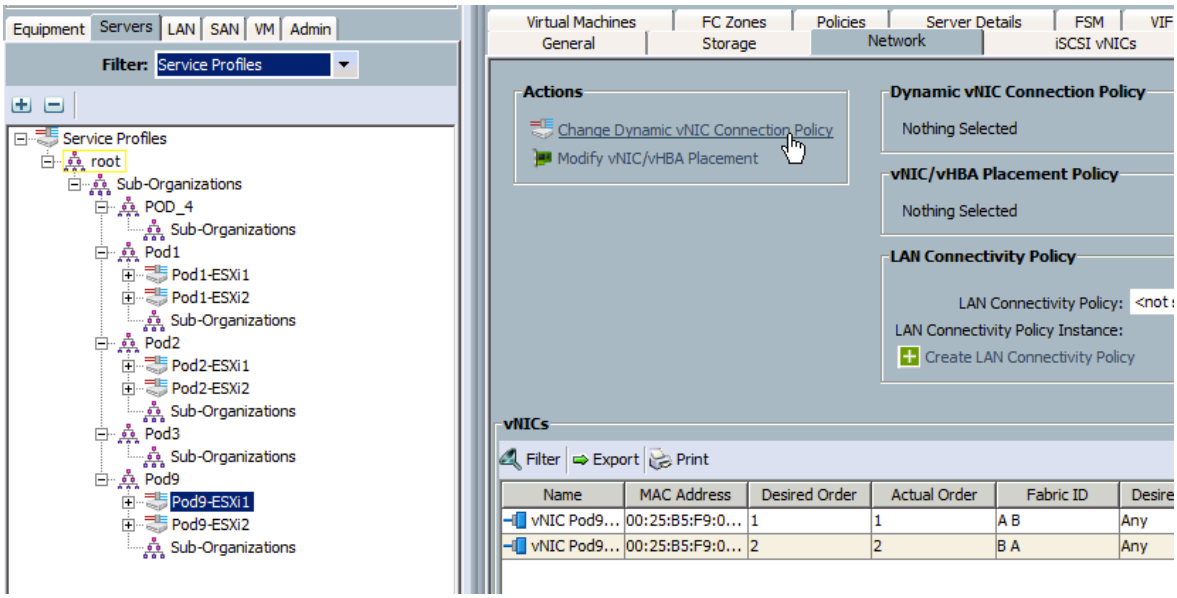


Step 9 Click **OK** to finish.

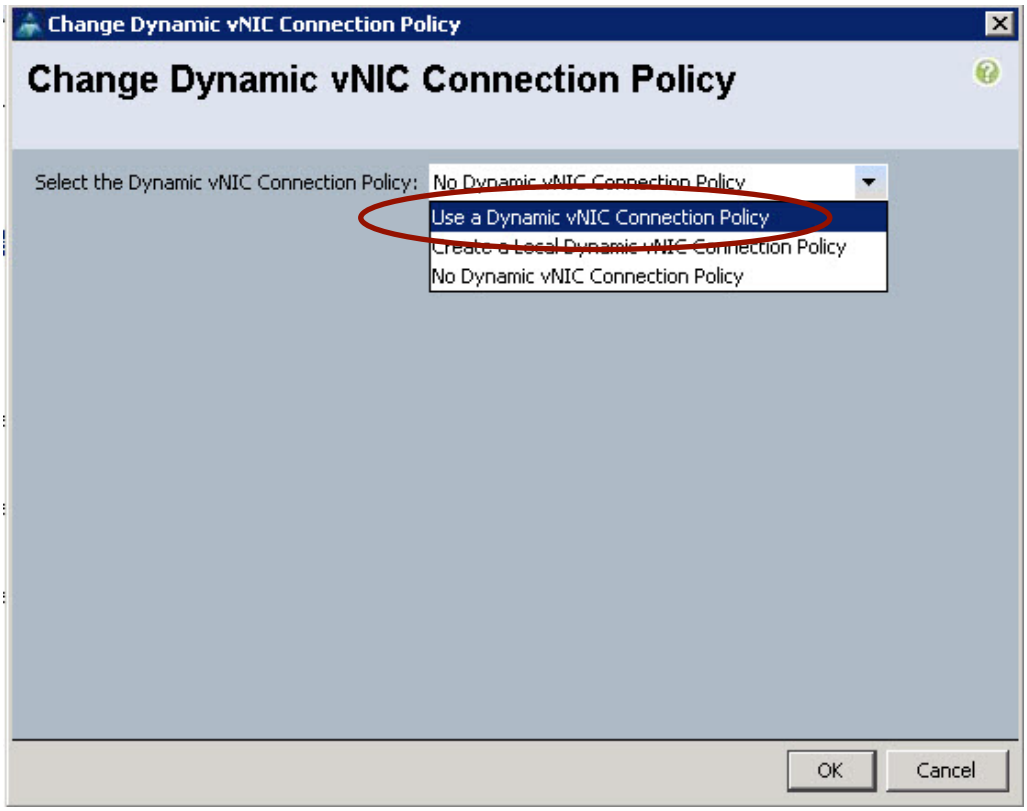
Step 10 Navigate to **Service Profile** in the **Server** tab.

Step 11 Go to your organization and select your firstservice profile template.

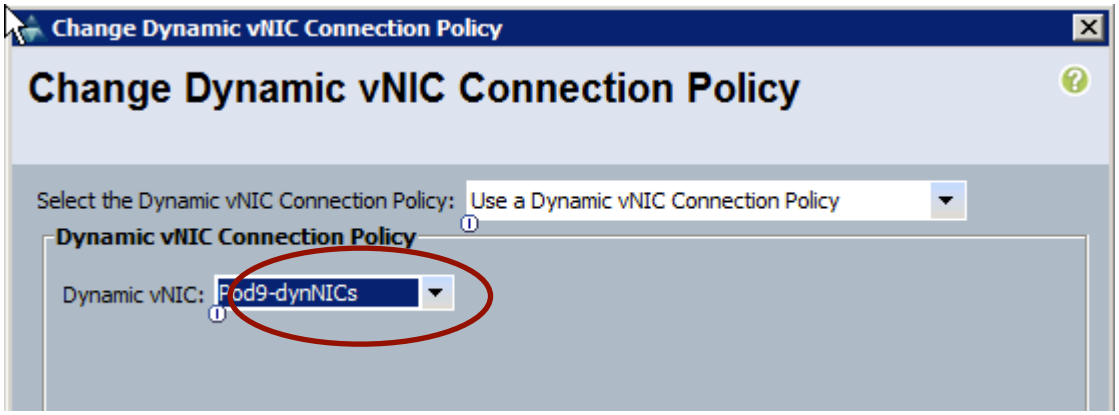
Step 12 From the **Network** tab, click **Change Dynamic vNIC Connection Policy**.



Step 13 In the new window, choose **Use a Dynamic vNIC Connection Policy** from the drop-down menu.

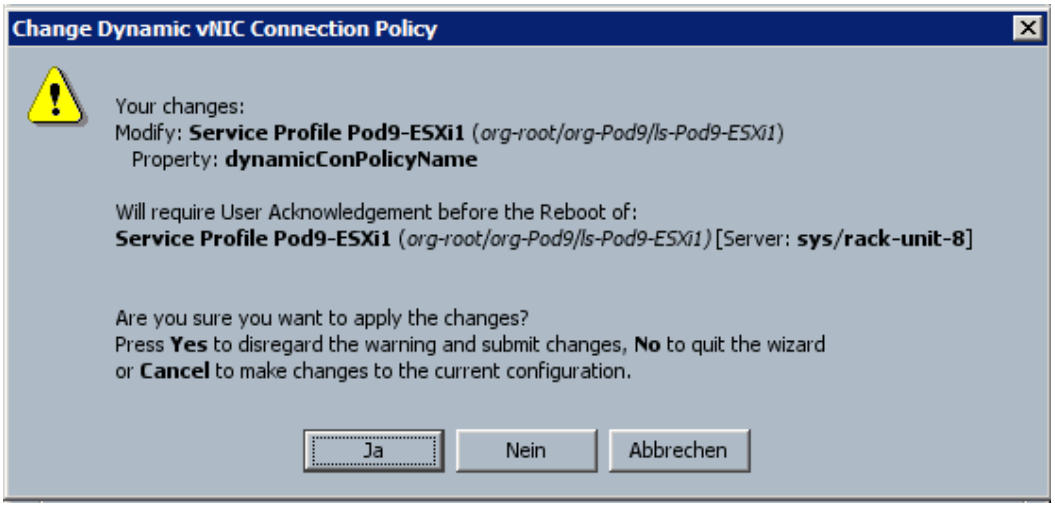


Step 14 From the new drop-down menu, choose the dynamic vNIC connection policy you created in the previous steps.

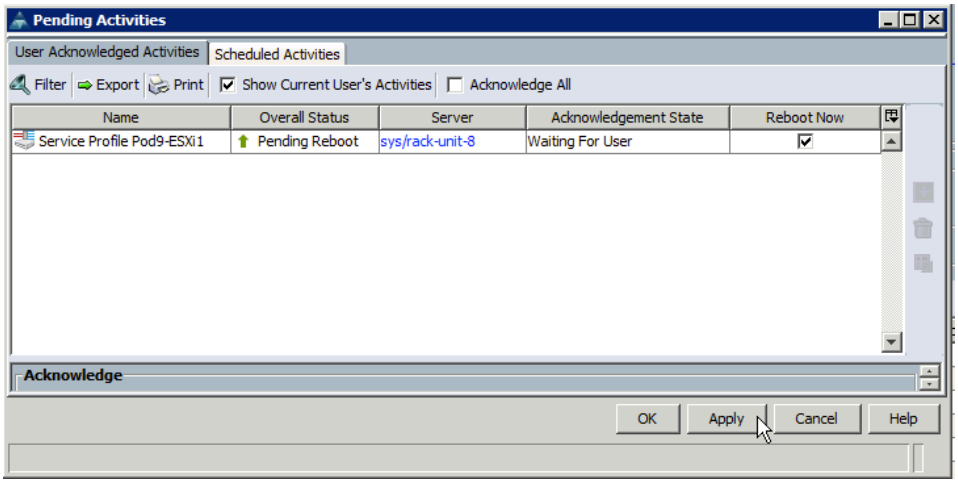


Step 15 Click **OK** to finish.

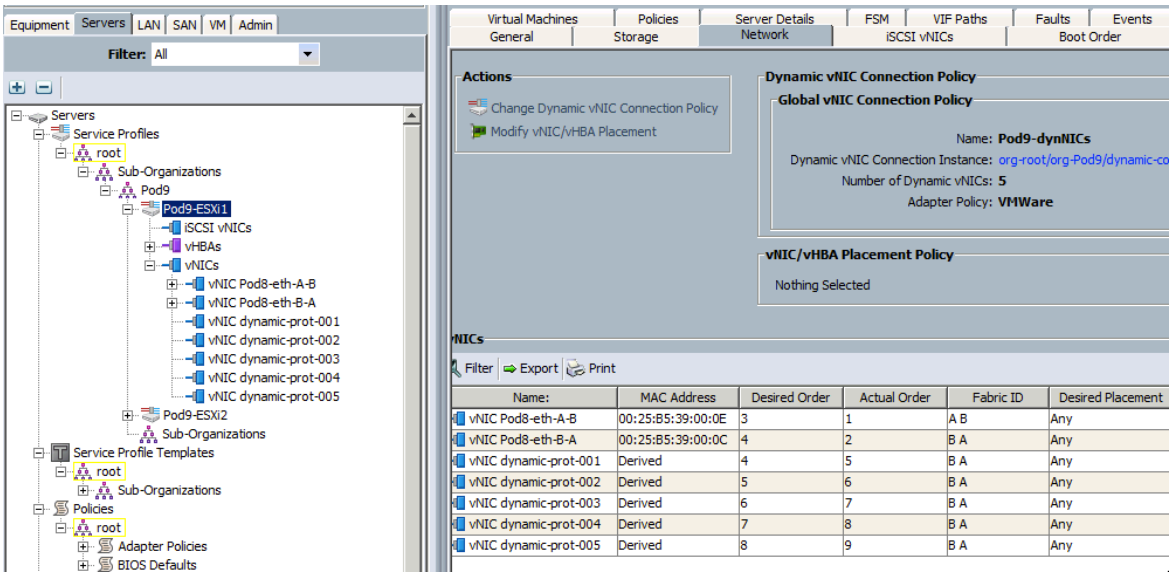
Step 16 Confirm that this change requires a reboot of the server



Step 17 Confirm reboot in "Pending Activities". ALWAYS make sure to ONLY reboot YOUR OWN servers.



Step 18 Wait for the reconfiguration to complete (UUOS is not needed and used), then confirm the dynamic vNICS have been added to your first service profile.

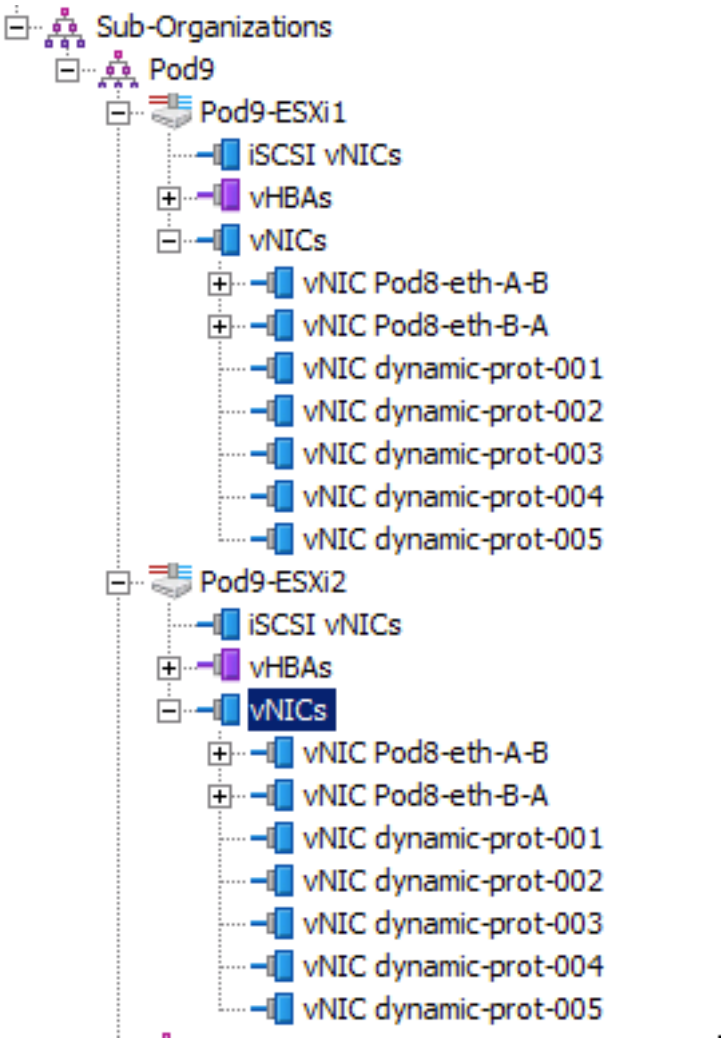


Step 19 Navigate to **Service Profiles** and select your organization.

Step 20 Choose your second service profile in the **Network** tab.

Step 21 Reconfigure your second service profile to use the same dynamic vNIC connection policy.

Step 22 Confirm BOTH ESXI Servers now support 5 dynamic vNICs each.



Activity Verification

You have completed this activity when you have achieved this goal:

- You can see the new dynamic vNIC connection policy and the dynamic vNICs in the Network tab of your service profile.

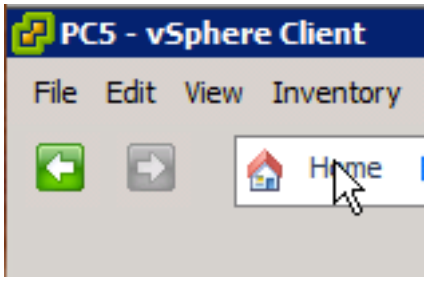
Task 4: Installing the VM-FEX VEM using VUM

In this task, you will add the necessary patch files to ESXi servers using VUM.

Activity Procedure

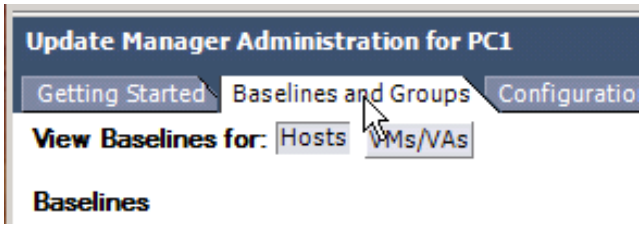
Complete these steps:

Step 1 Click “Home” in vSphere Client

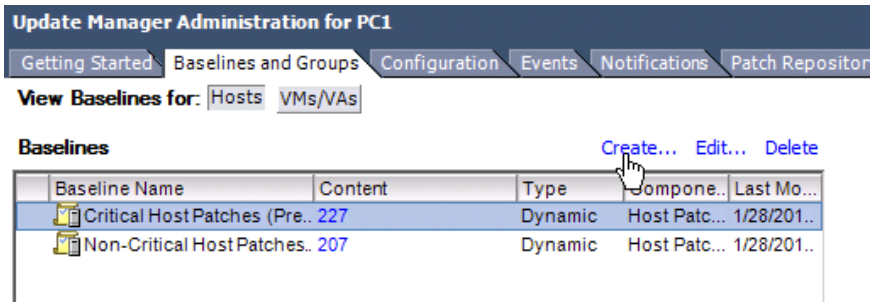


Step 2 Navigate to **Solutions and Applications -> Update Manager**

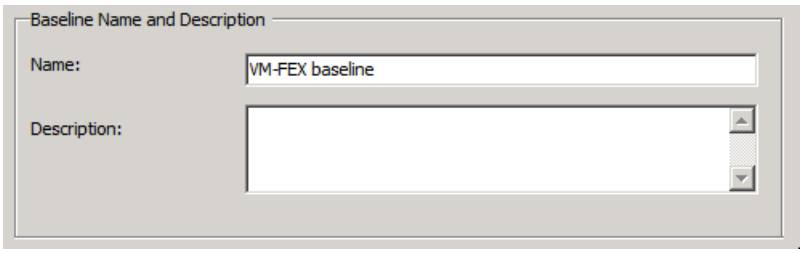
Step 3 Select the **Baseline and Groups** Tab



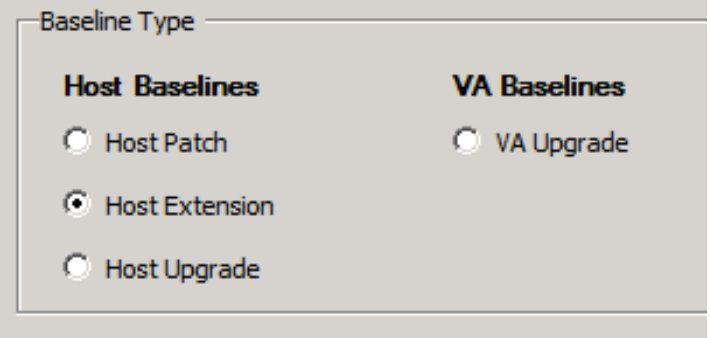
Step 4 Click **Create…** at Baselines.



Step 5 Name the Baseline “VM-FEX baseline”

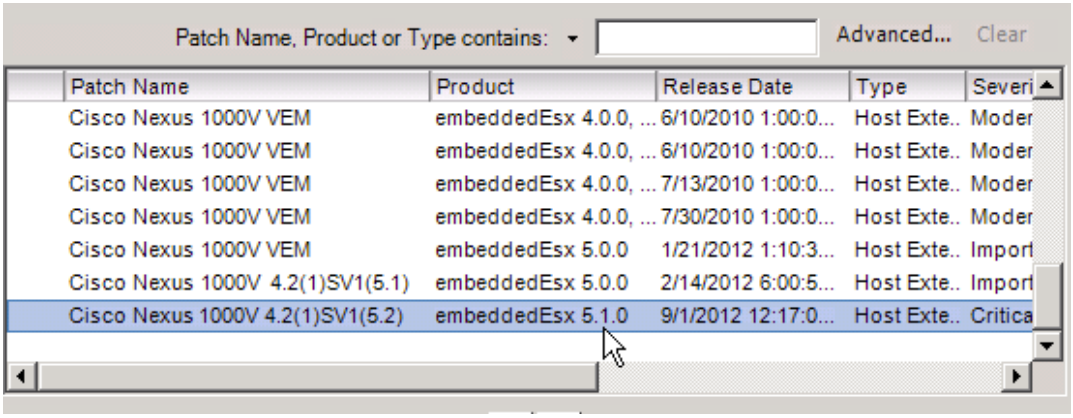


Step 6 Make sure “Host Extension” is selected as the Baseline Type



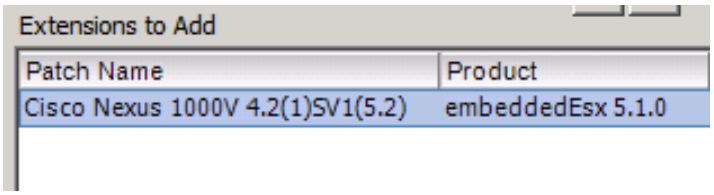
Step 7 Click “Next>”

Step 8 Scroll down and select the “Cisco Nexus 1000v 4.2(1)SV1(5.2)” for ESX 5.1 (enlarge the “Product” column), DO NOT use any other version.



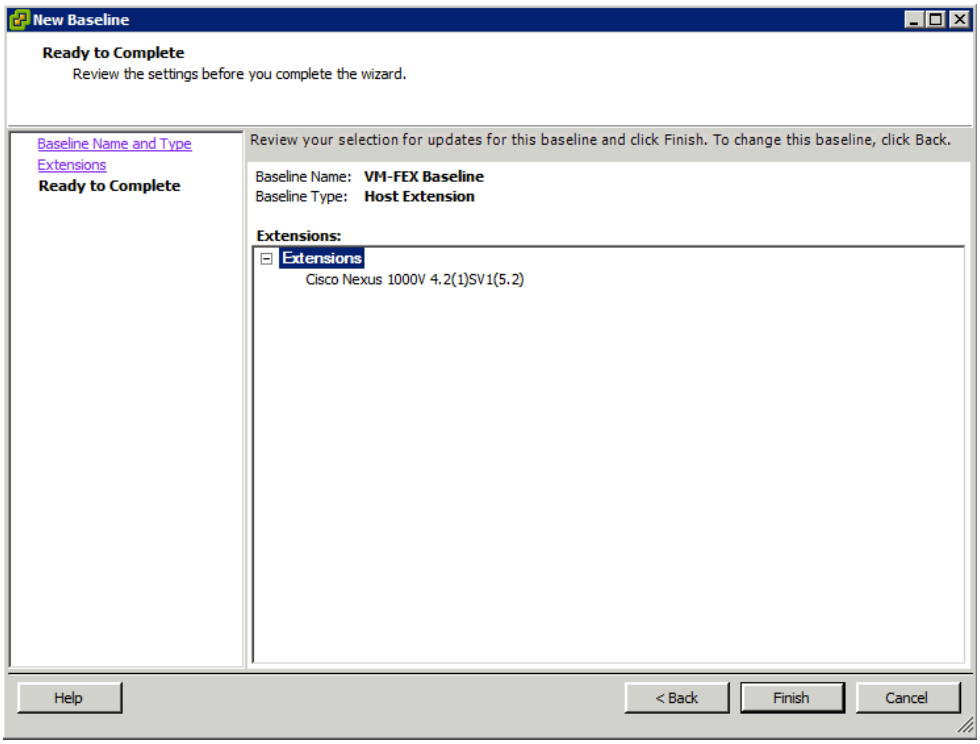
Step 9 Use the V button to move the host extension into the baseline.

Step 10 Double-check the Extension to add.

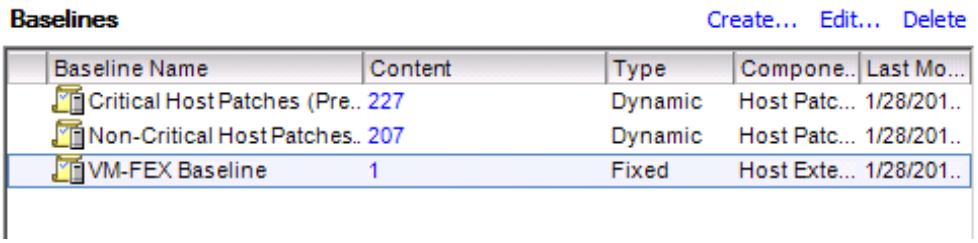


Step 11 Click “Next>”

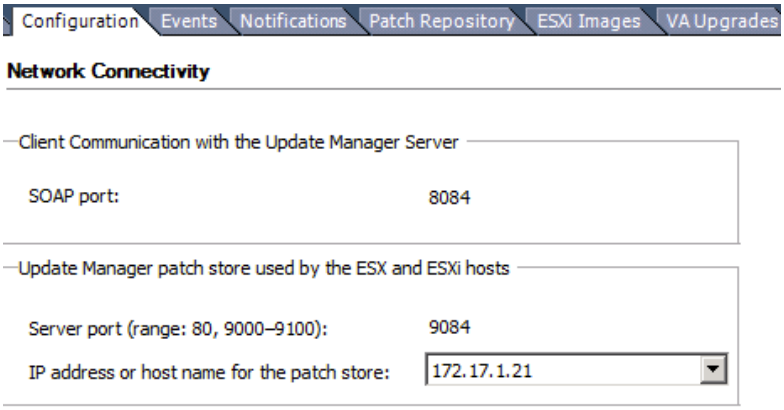
Step 12 Review and click “Finish”



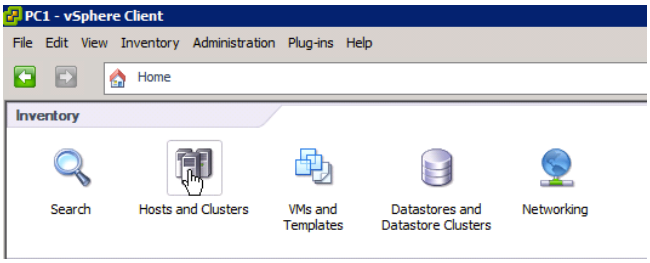
Step 13 Confirm the baseline is now available.



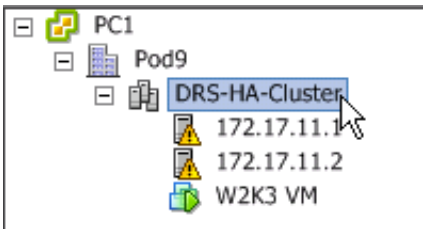
Step 14 Choose the "Configuration" tab and make sure IP 172.17.1.2P is selected as the patch store address.



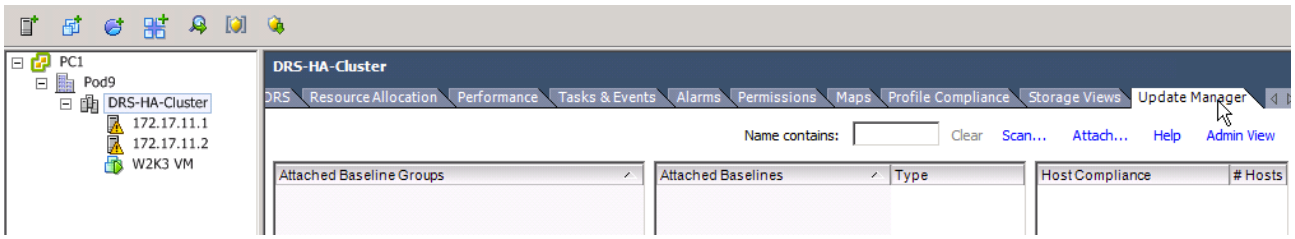
Step 15 In vSphere Client go to Inventory->Hosts and Clusters



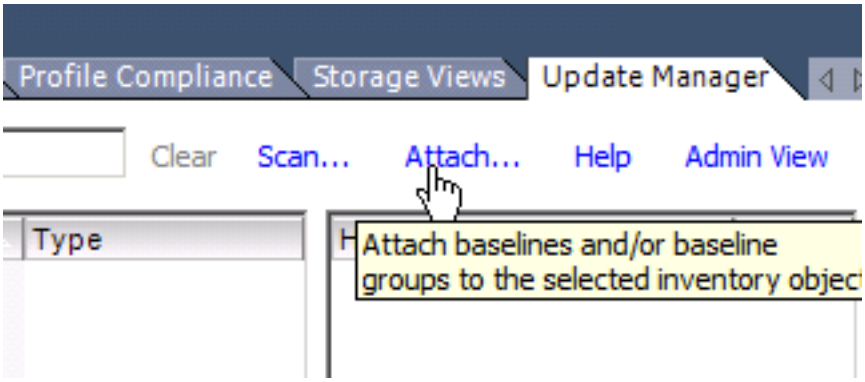
Step 16 Select your "DRS-HA-Cluster"



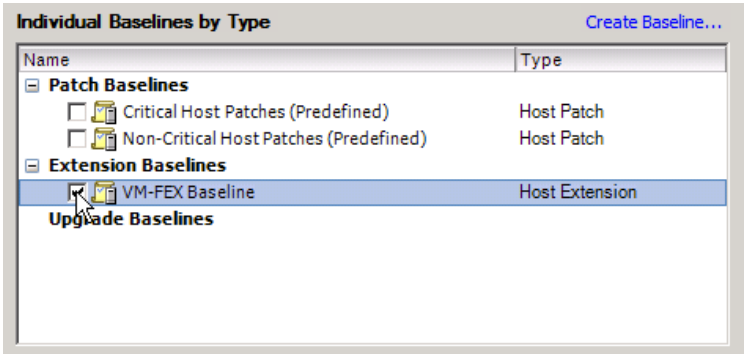
Step 17 Select the tab Update Manager (you may have to scroll to see it)



Step 18 Select **Attach…**

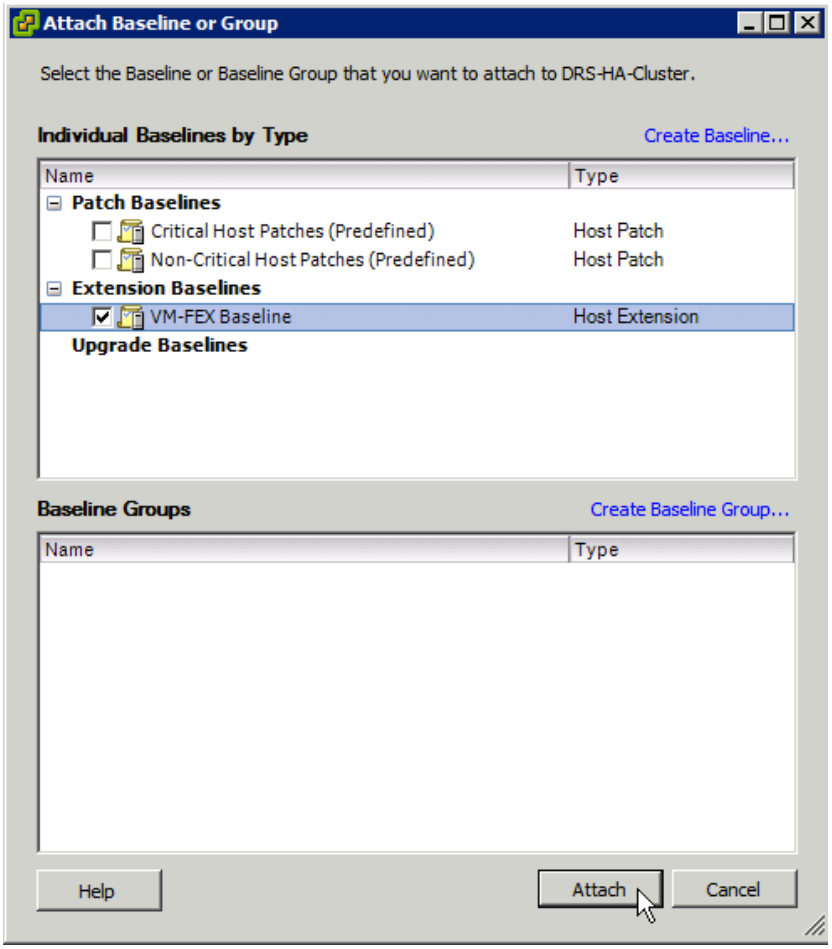


Step 19 Select the "VM-FEX baseline" we just created.

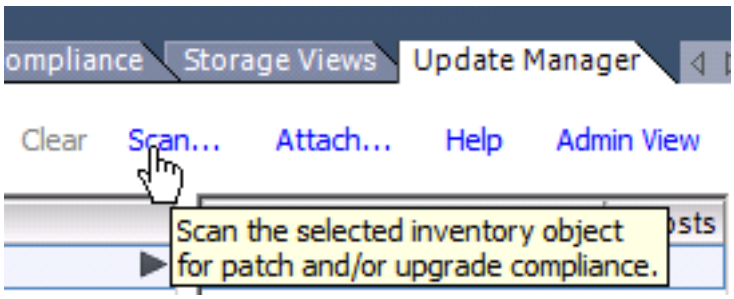


Caution Do NOT select the patches in this lab since patching will take a long time!

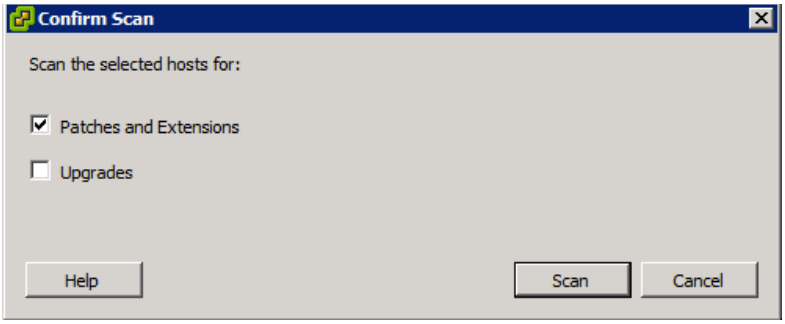
Step 20 Click "Attach"



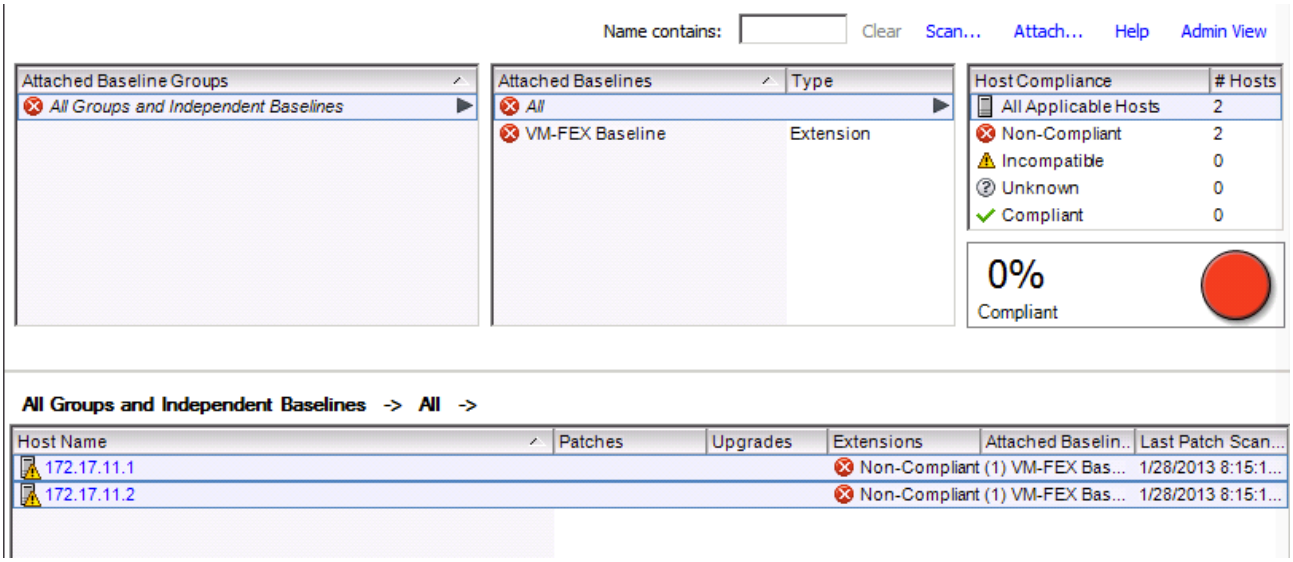
Step 21 Click **Scan…**



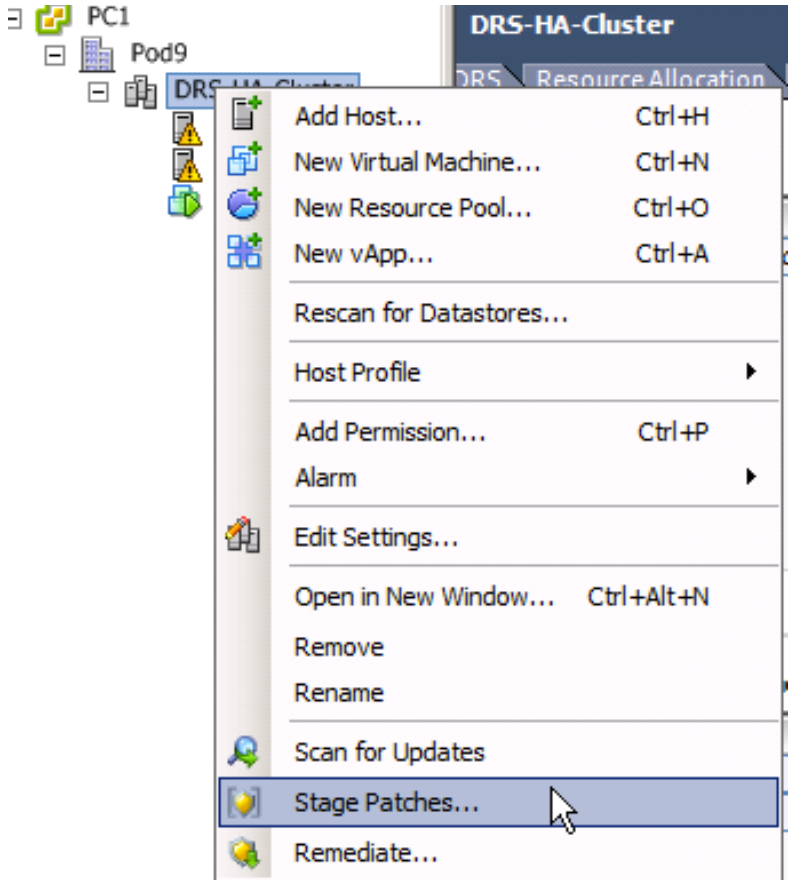
Step 22 Confirm scanning for Patches and Extensions



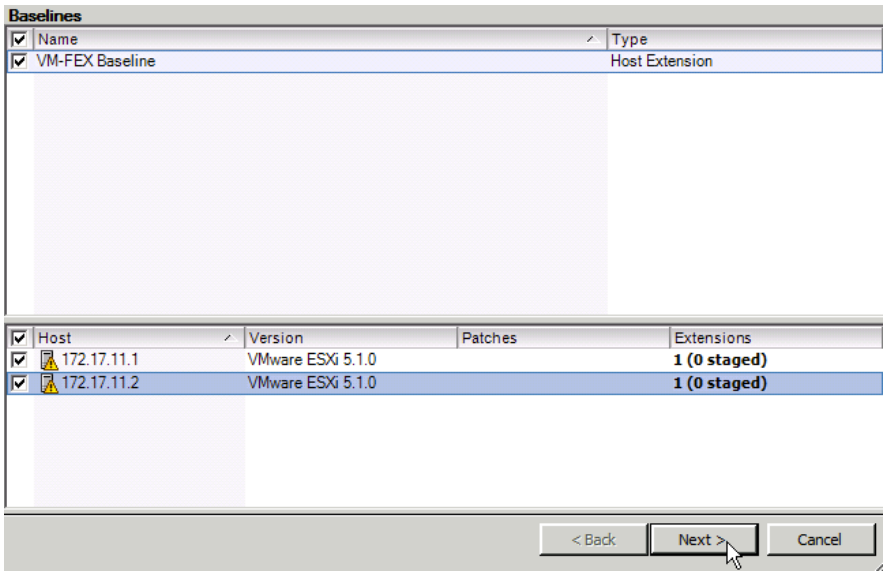
Step 23 Wait for the scan to complete. Note all hosts are non-compliant (no software installed)



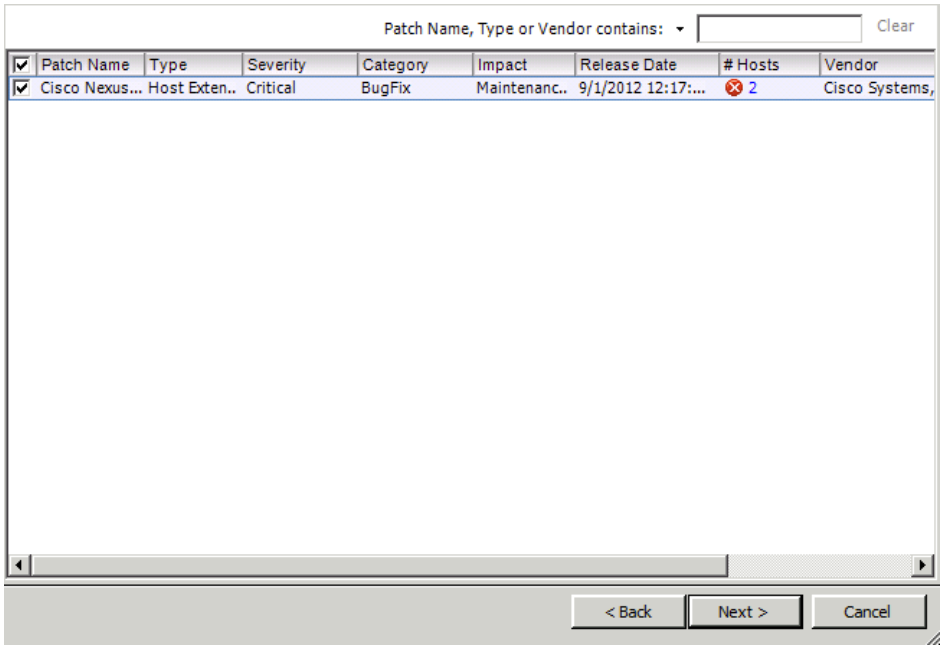
Step 24 Right-click the Cluster and select "Stage Patches…" (or use the "Stage…" Button in the Update Manager tab)



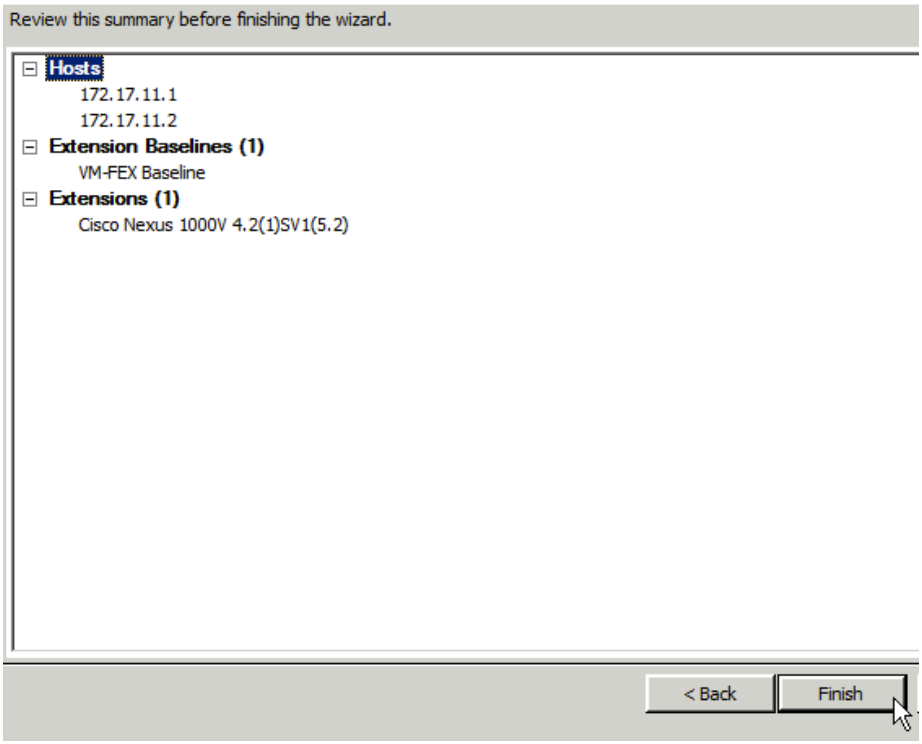
Step 25 Select the VM-FEX baseline and both hosts and click "Next>"



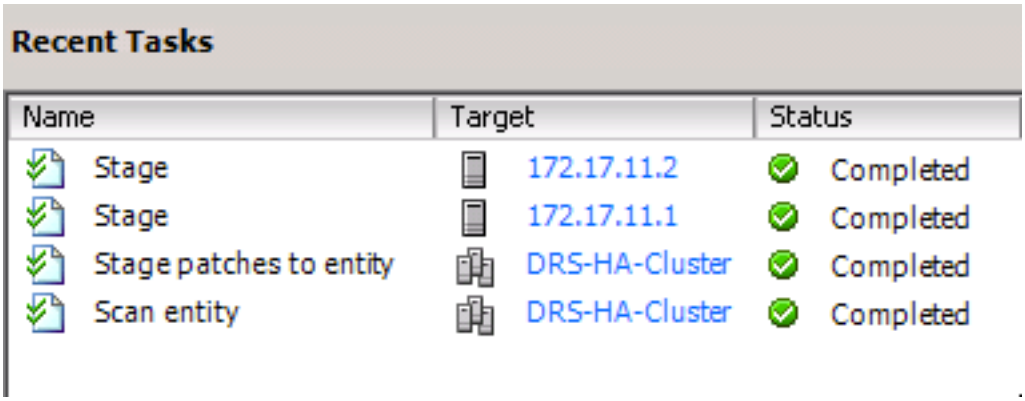
Step 26 Confirm staging of the Nexus 1000v VEM to both hosts with "Next>"



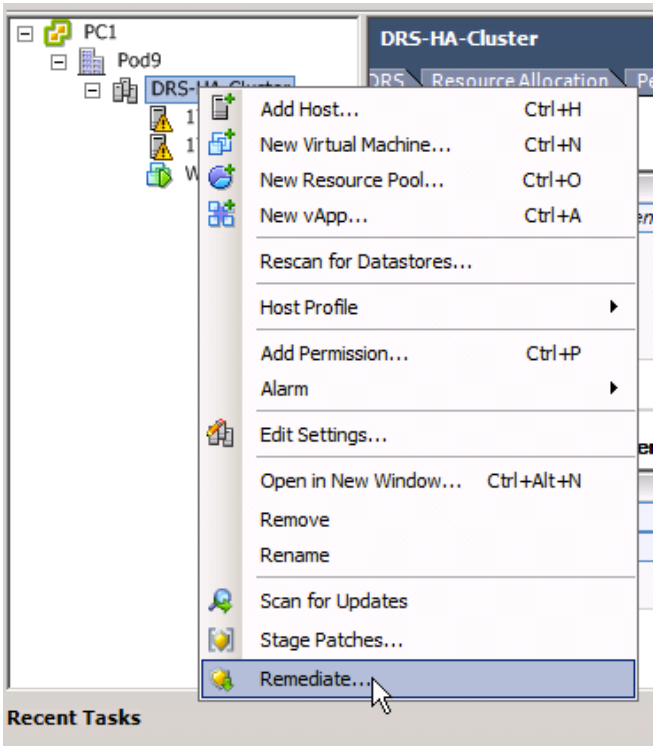
Step 27 Review and click "Finish"



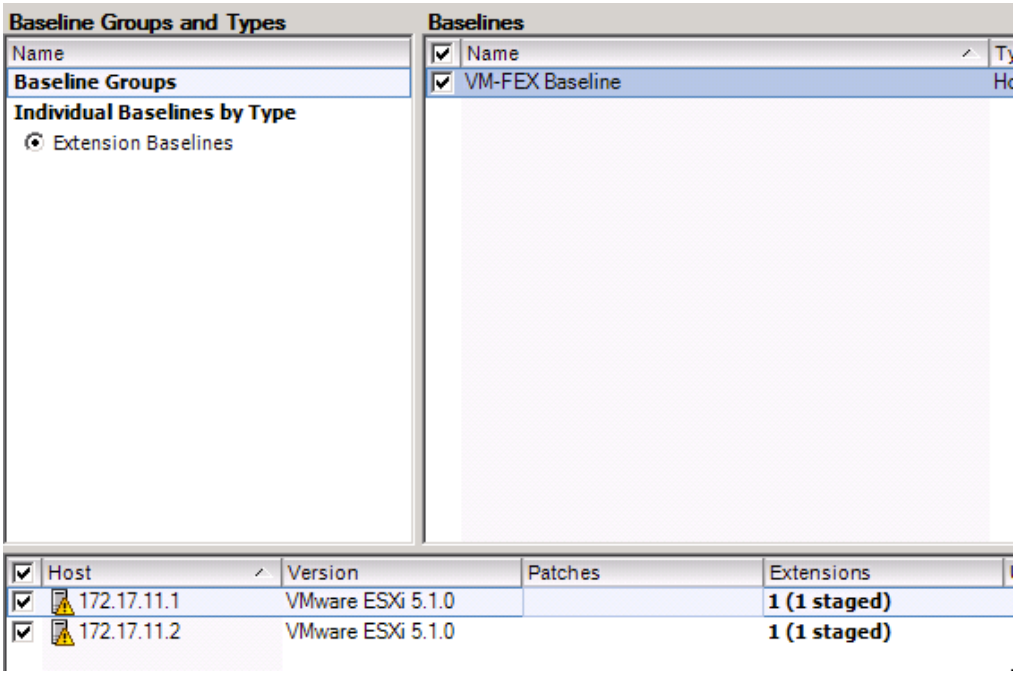
Step 28 View the taskbar and wait for the staging to complete



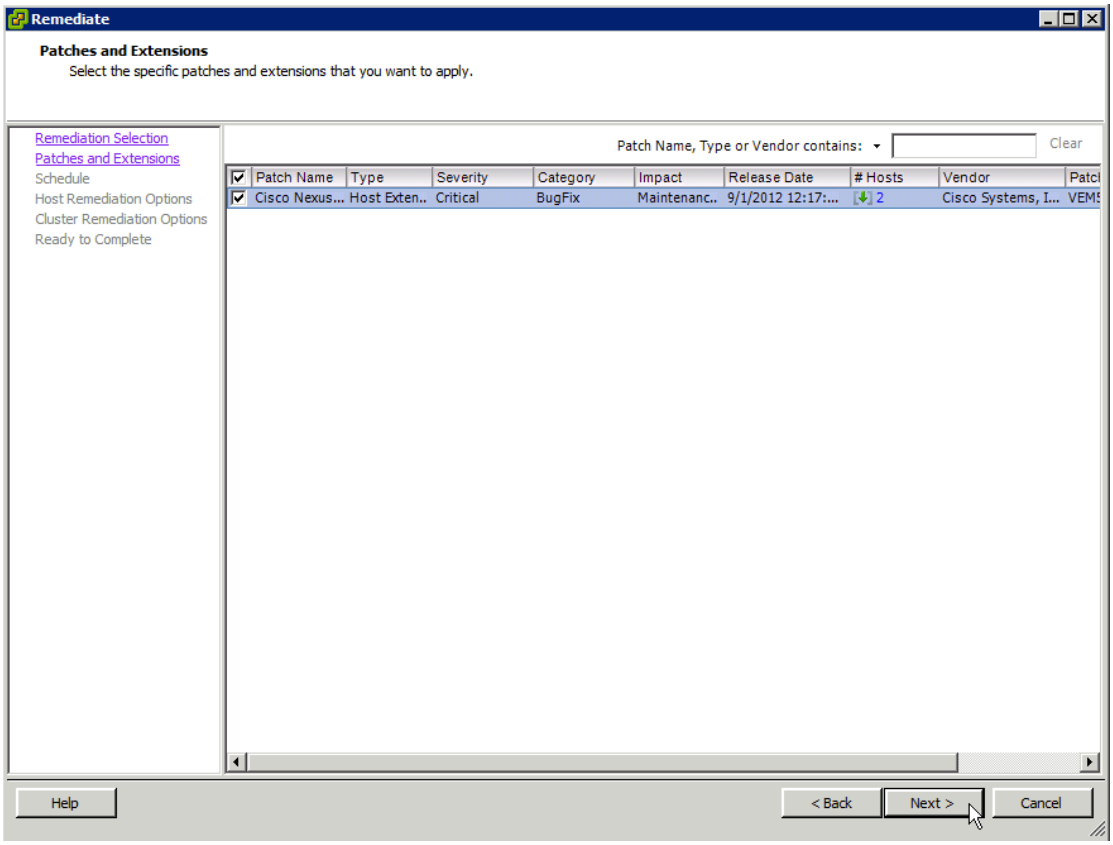
Step 29 Right-click the Cluster and select “Remediate” (or click the “Remediate” Button in the Update Manager tab)



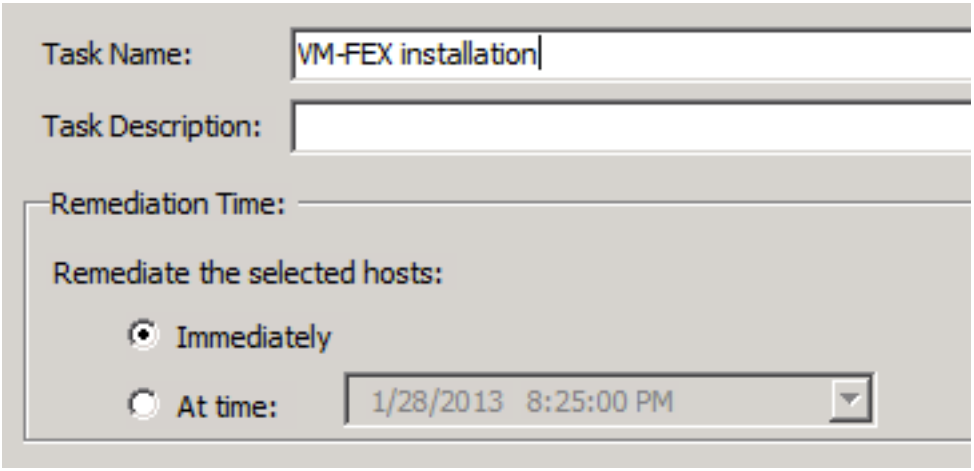
Step 30 Select the VM-FEX baseline and both hosts and click “Next>”



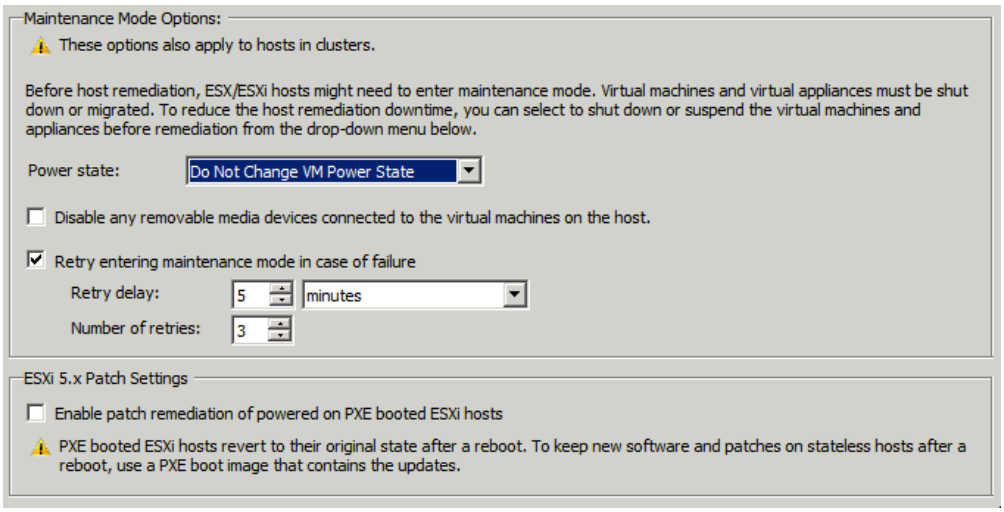
Step 31 Confirm installation of the Nexus 1000v VEM on two hosts with “Next>”



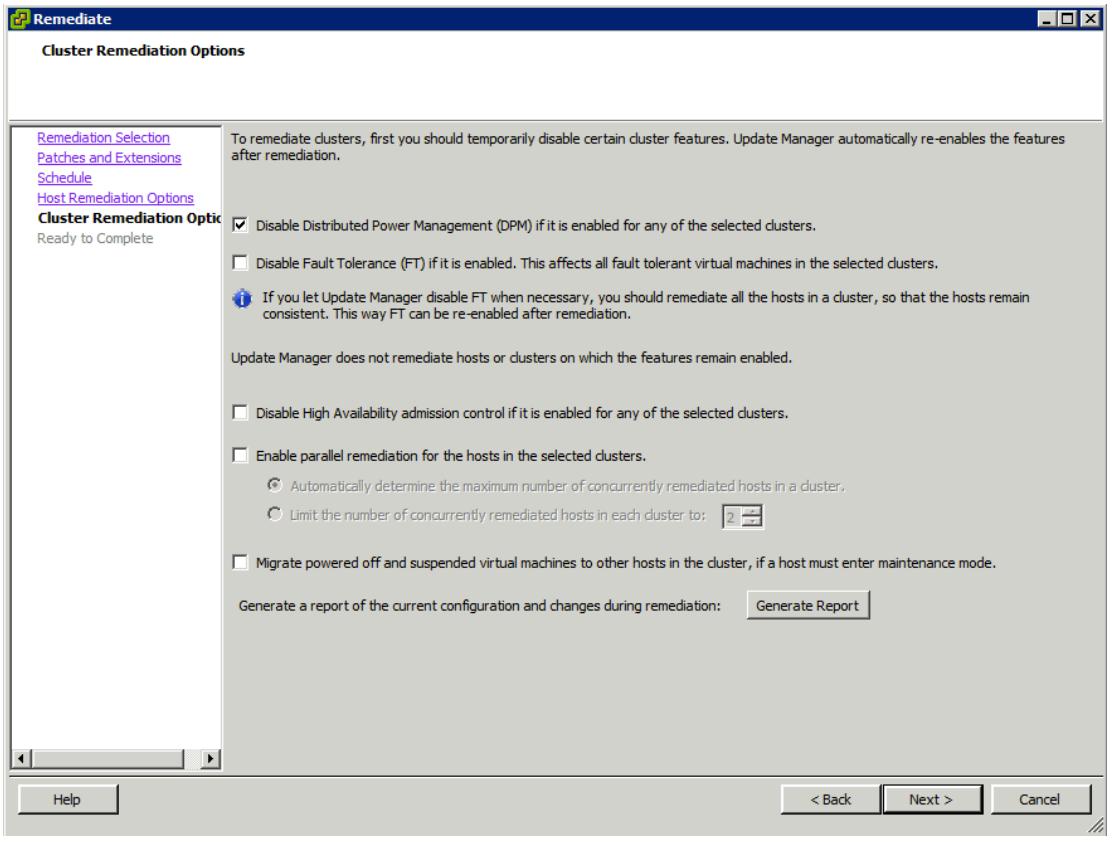
Step 32 Confirm "Immediately" as the Remediation Time with "Next>"



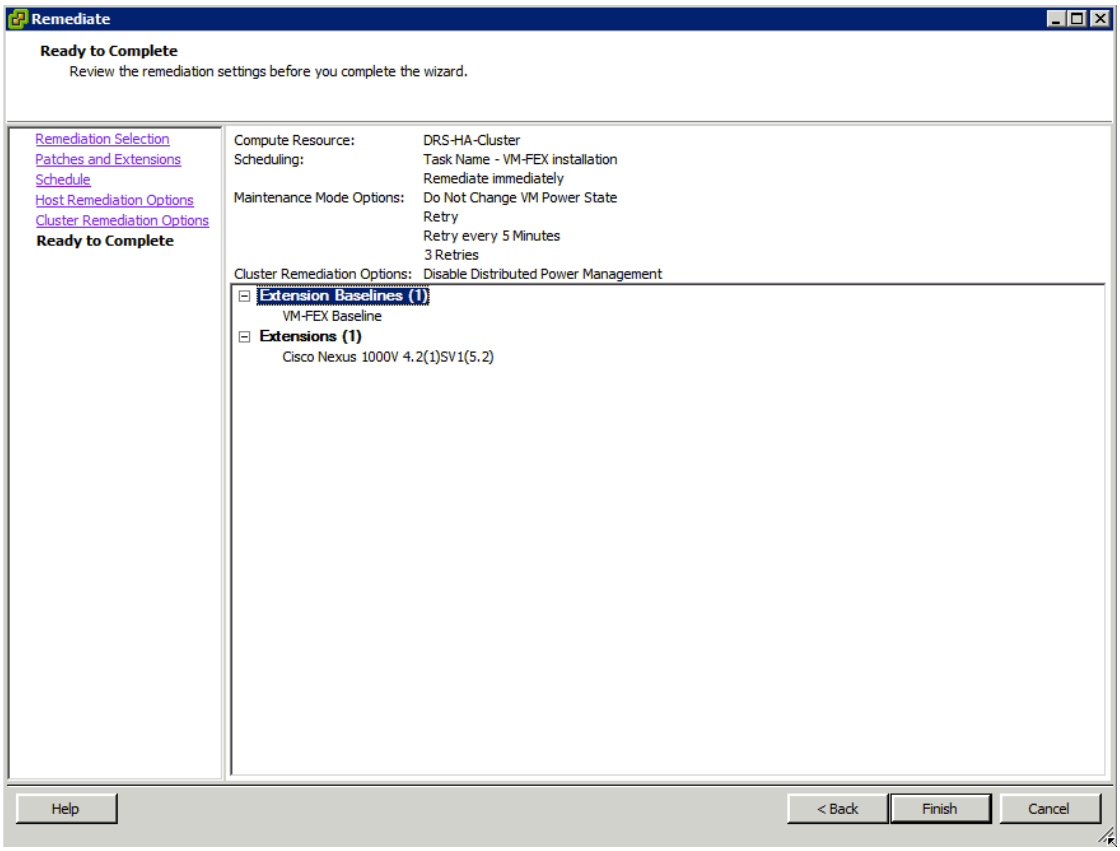
Step 33 Confirm Maintenance Mode Options with "Next>"



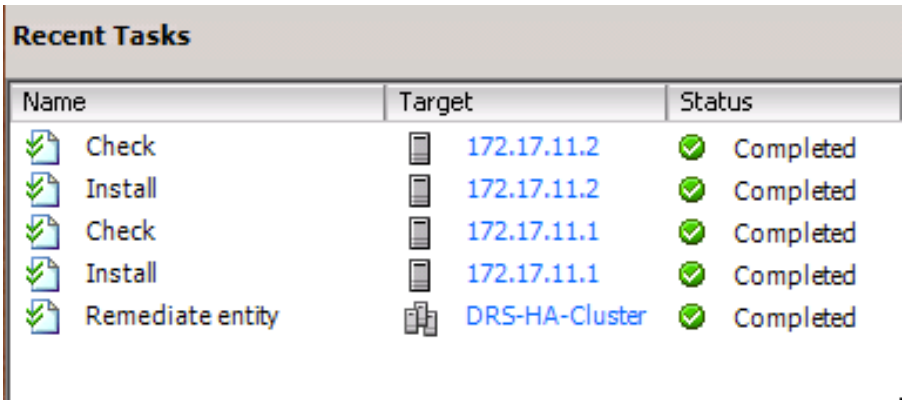
Step 34 Confirm Cluster Remediation Options with "Next>"



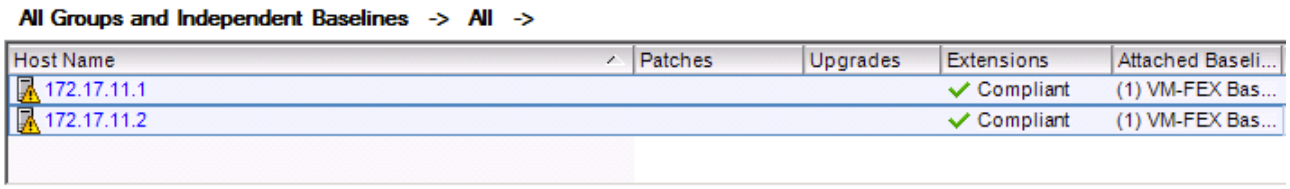
Step 35 Review and start remediation with "Finish"



Step 36 View the Taskbar and wait for Remediation/Installation to complete.



Step 37 Note all hosts are now compliant with the VM-FEX baseline



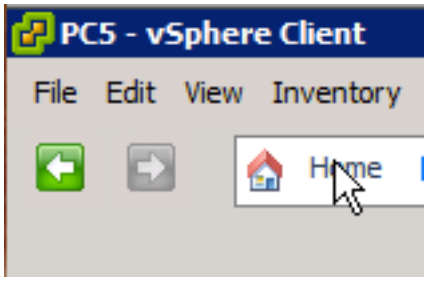
Task 4: Add ESXi Hosts to the DVS

In this task, you will add the ESXi host to the DVS.

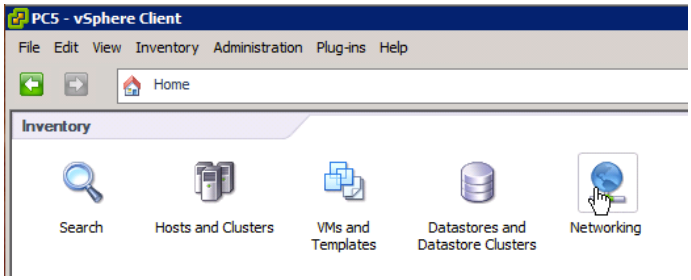
Activity Procedure

Complete these steps:

Step 38 Click “Home” in vSphere Client

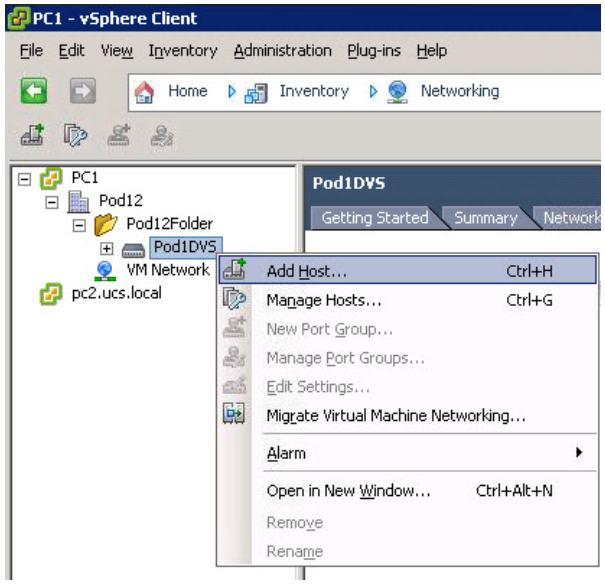


Step 39 Navigate to **Inventory > Networking**

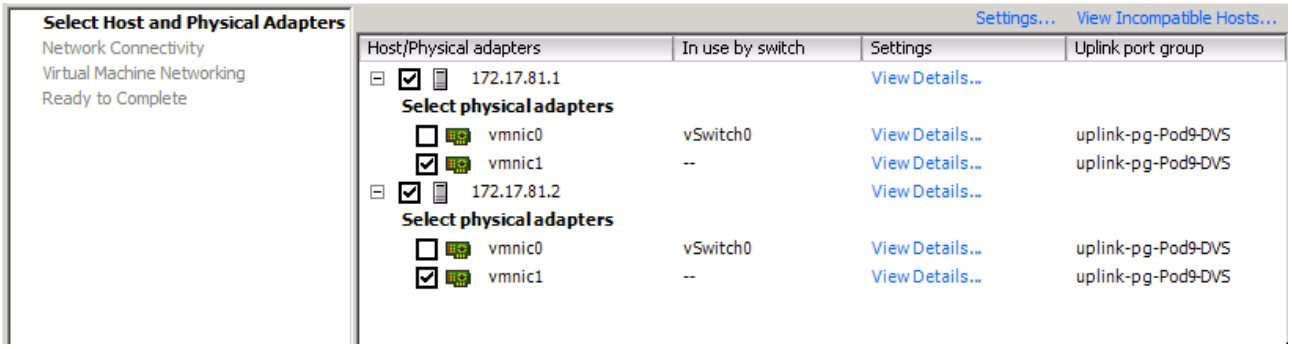


Step 40 Select your DVS.

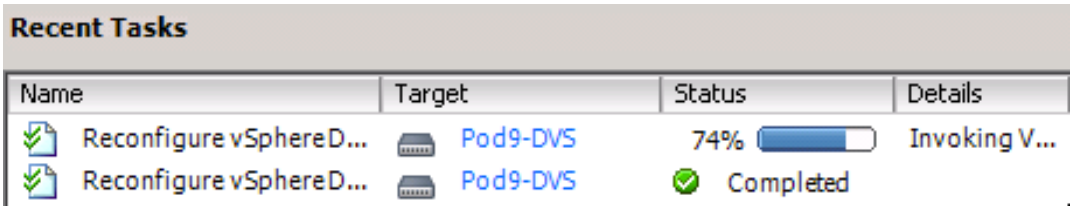
Step 41 Right-click and choose **Add Host**.



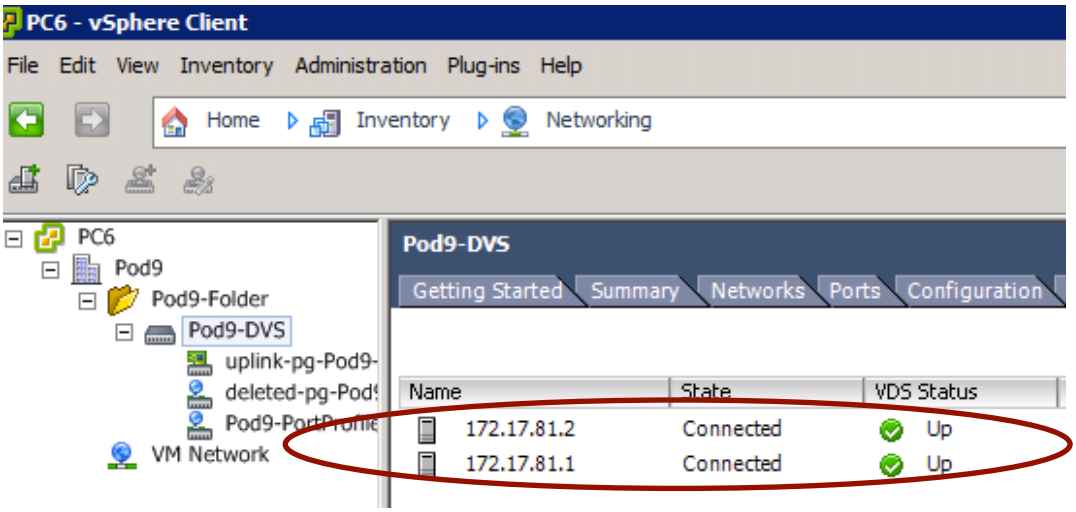
Step 42 In the new window, select your ESXi hosts and the vmnic, which is NOT connected to the vSwitch0 and NOT using the iSCSI Mac address (remember the "FF" inside the MAC address!). Click **Next** to continue.



Step 43 Click **Next** for the remaining steps without selecting anything and finally click **Finish**.



Step 44 When the process has finished, the ESXi hosts will be available in the **Hosts** tab of the DVS switch.



Activity Verification

You have completed this activity when you have achieved this goal:

- You have successfully added the ESXi host to the DVS.

Task 4: Provision the Windows Virtual Machine to use VM-FEX

In this task, you will link the VM vNIC to the DVS port group.

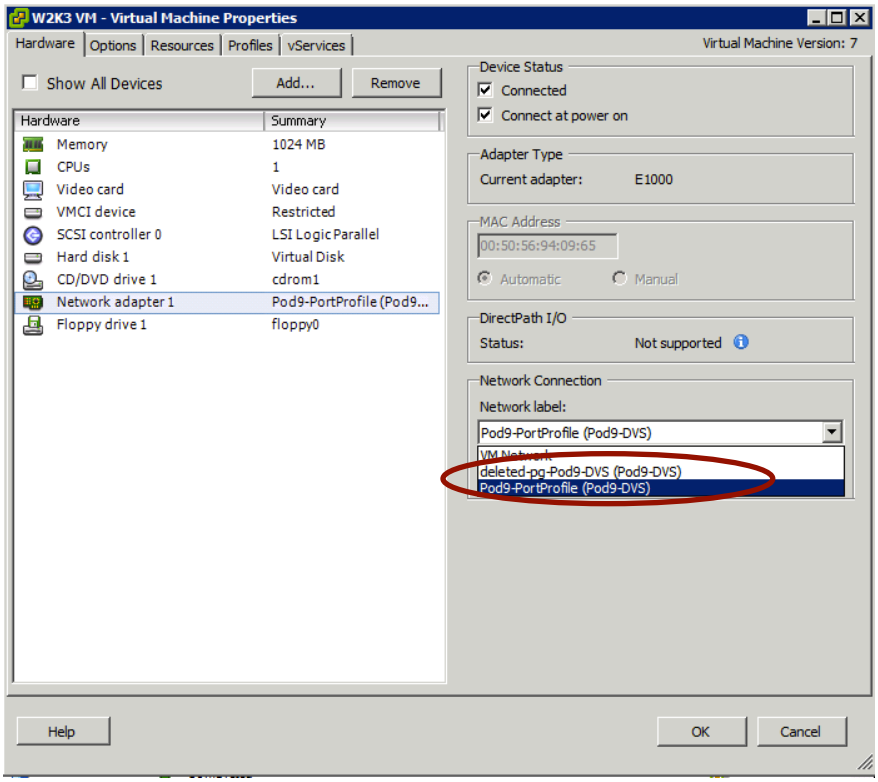
Activity Procedure

Complete these steps:

Step 1 Navigate to **Home > Inventory > Hosts and Clusters** and select your VM.

Step 2 In the **Summary** tab, click **Edit Settings**.

Step 3 Select the **Network adapter**. From the **Network Label** drop-down menu, choose your port profile.



Step 4 Check the **Connected** check box and click **OK** to finish.

Activity Verification

You have completed this activity when you have achieved this goal:

- You have successfully changed the network label for the VM network adapter.

Task 5: Validate the VM Port State and Connectivity with the ping Command

In this task, you will validate the VM connectivity through the DVS.

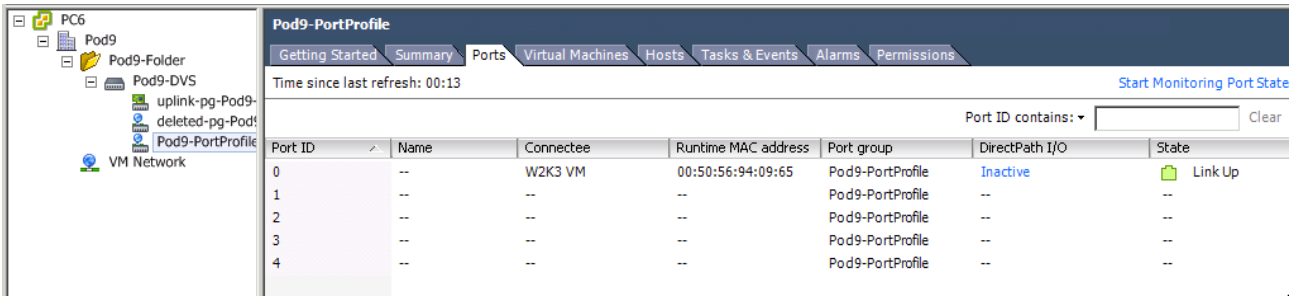
Activity Procedure

Complete these steps:

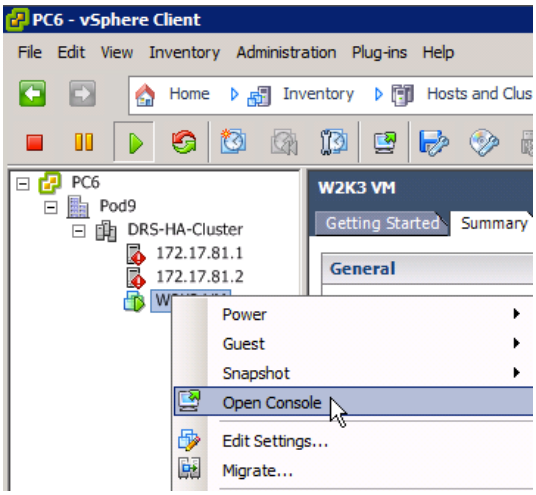
Step 1 Navigate to **Home > Inventory > Networking**.

Step 2 Expand the DVS and select the port profile.

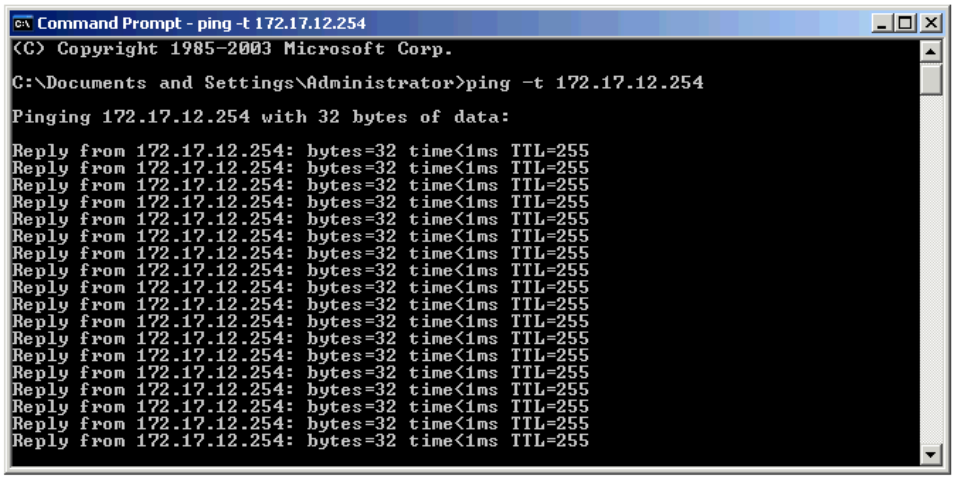
Step 3 Select the **Ports** tab and validate the status of the VM port on the DVS.



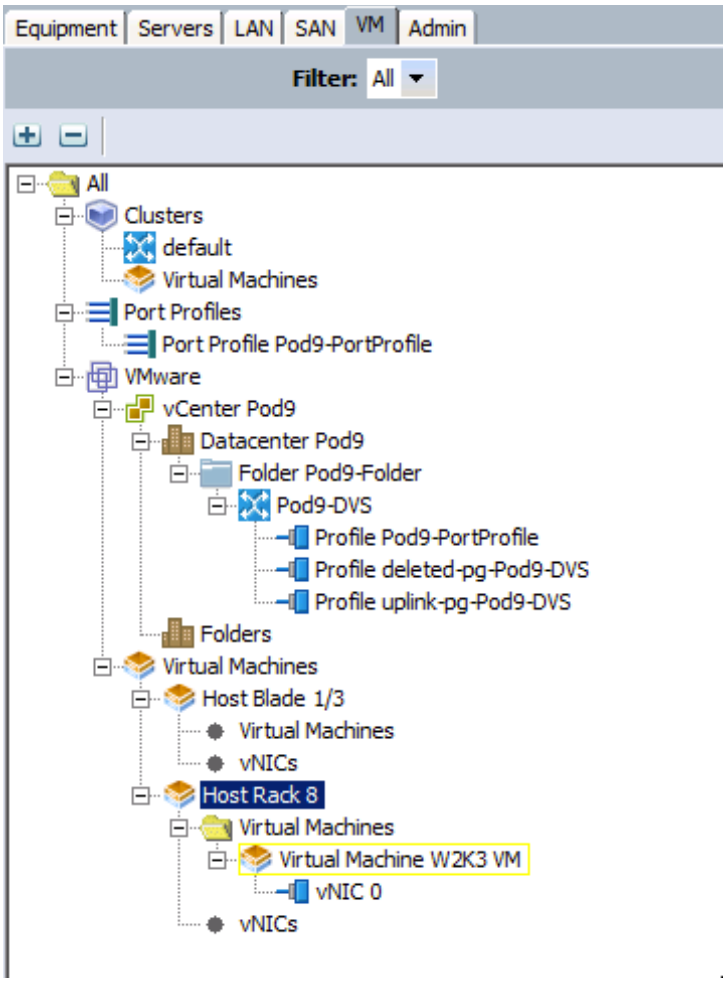
Step 4 Open to the VM console.



Step 5 Open a command prompt and ping –t the default gateway 172.17.P2.254



Step 6 Open the VM tab in UCS Manager, expand the VMWare and Virtual Machines tab, note you can see the VM in UCS Manager now because it is connected to the UCS VM-FEX DVS



Activity Verification

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

- You have successfully executed a ping command using a VM-FEX supported VM.

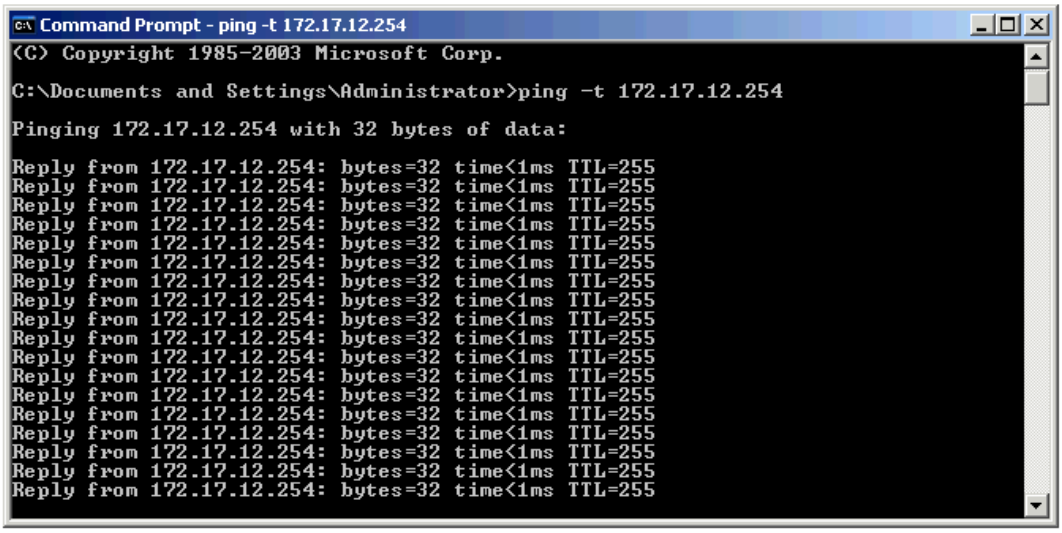
Task 6: Demonstrate VMotion of Hosts with Cisco VM-FEX in Standard Mode

In this task, you will perform a VMotion with Cisco VM-FEX.

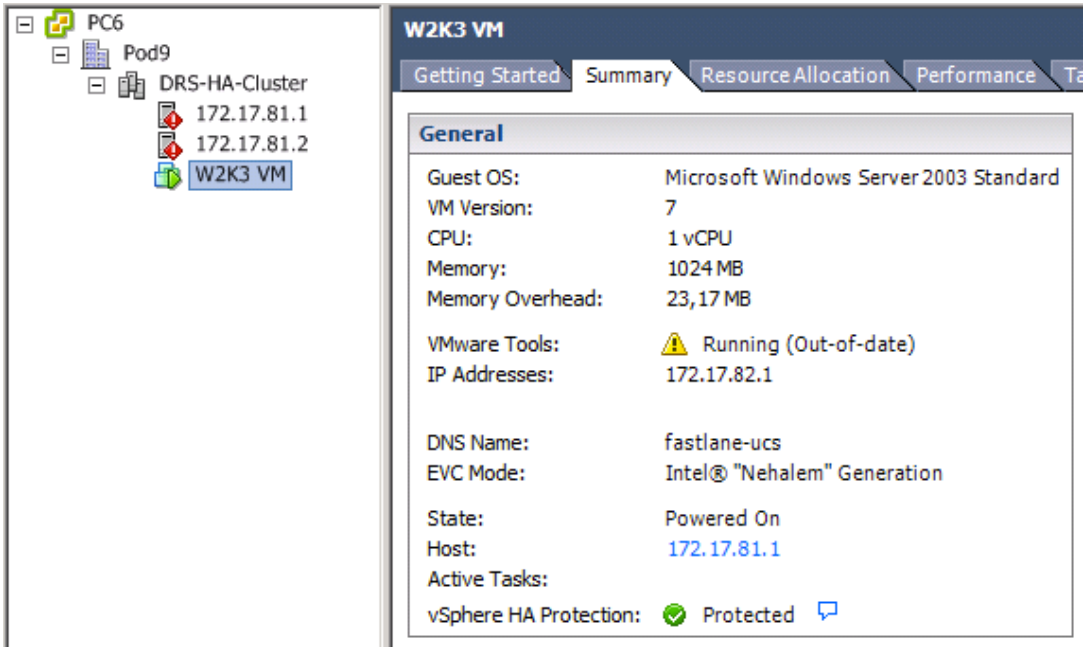
Activity Procedure

Complete these steps:

Step 1 On the VM, start a continuous ping to the default gateway 172.17.P2.254

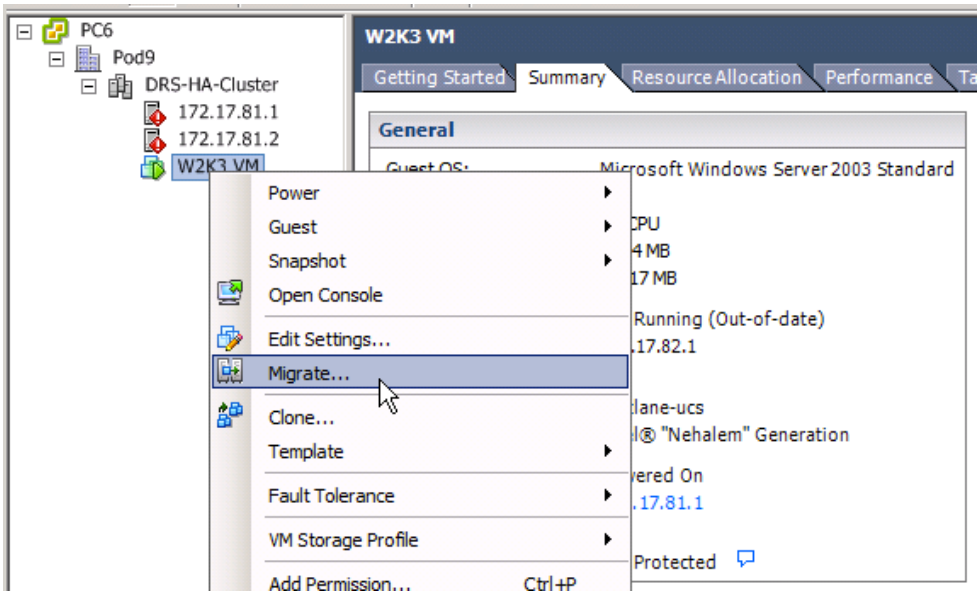


Step 2 Navigate to **Home > Inventory > Hosts and Clusters** and select your VM.

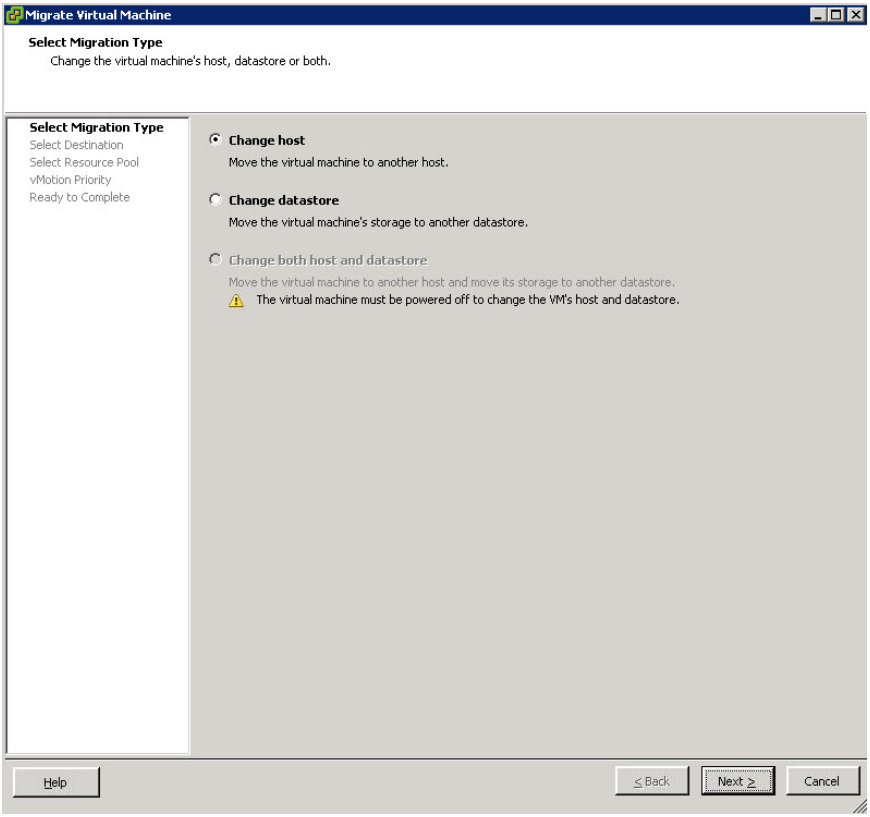


Q1) Which ESX server does the VM run on?

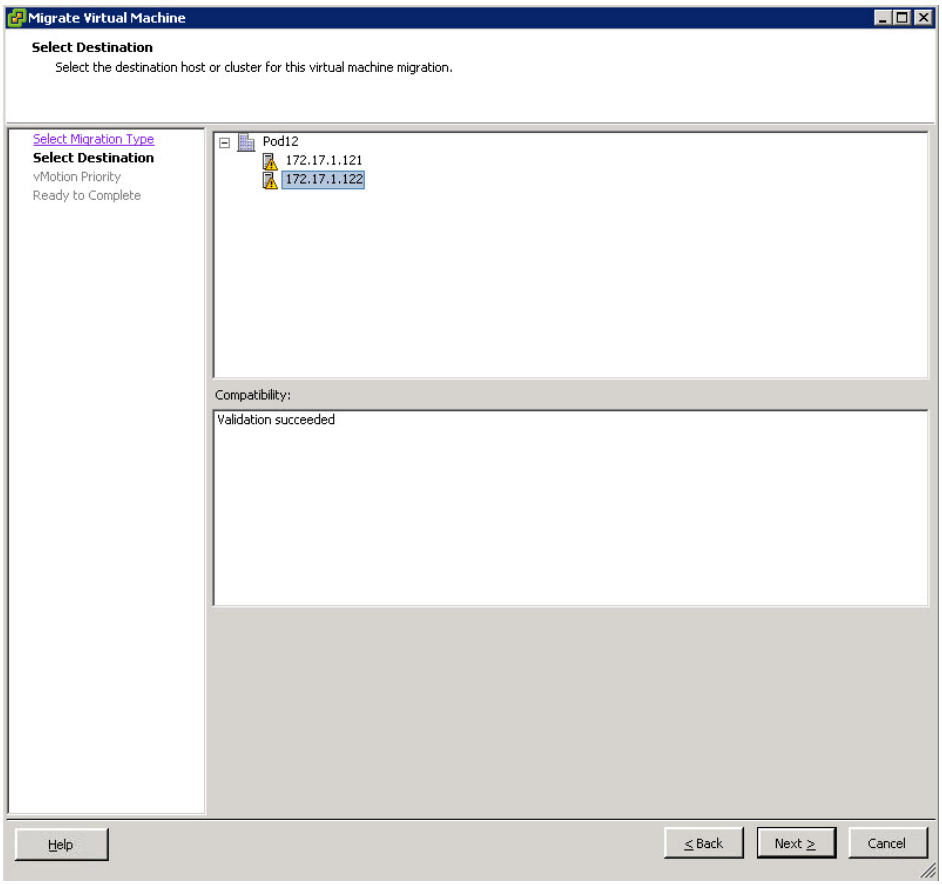
Step 3 Right-click your VM. Choose **Migrate**.



Step 4 Select **Change Host** and click **Next** to continue.



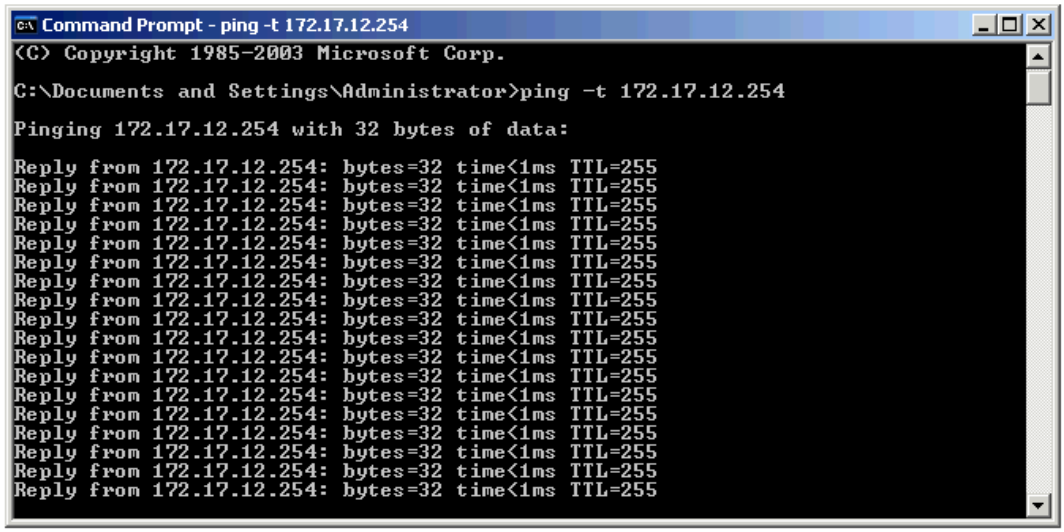
Step 5 Select your OTHER ESXi host as destination and click **Next**.



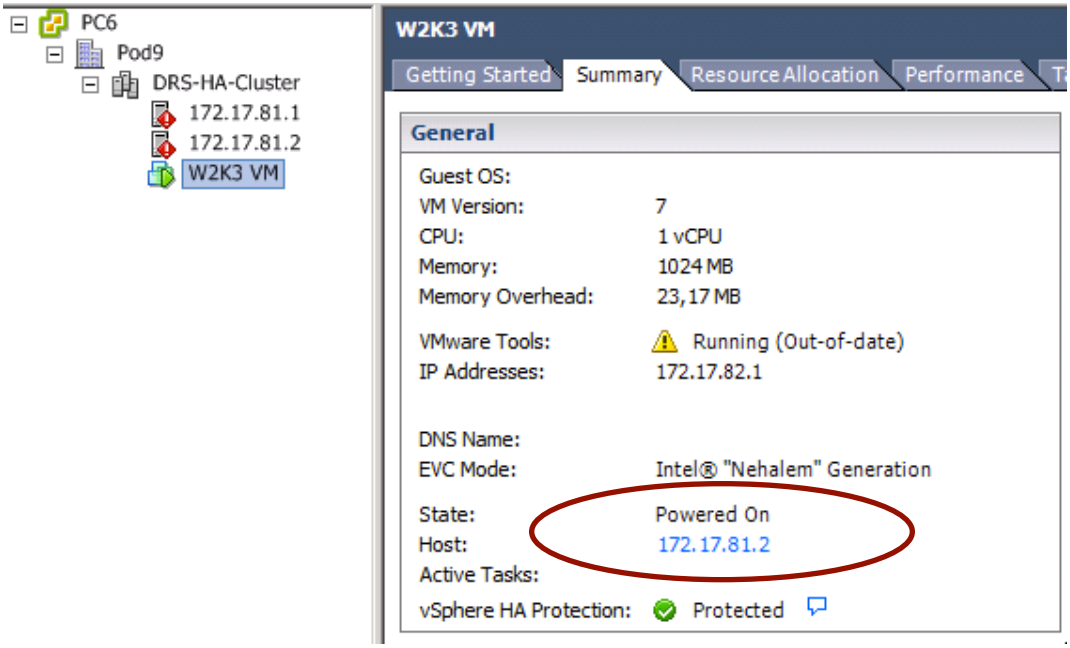
Step 6 At the next step, leave the default setting and click **Next**.

Step 7 Click **Finish** to start the migration.

Step 8 Open the VM console to monitor the continuous ping during VMotion.



Step 9 Navigate to **Home > Inventory > Hosts and Clusters** to validate that the VM is on the other ESXi host.



Activity Verification

You have completed this activity when you have achieved this goal:

- You have successfully moved the VM on the other host using VMotion and Cisco VM-FEX.