Cisco Nexus 1000V Series Switch Deployment Guide with Cisco Unified Computing System

Deployment Guide

April, 2012

For further information, questions and comments please contact ccbu-pricing@cisco.com

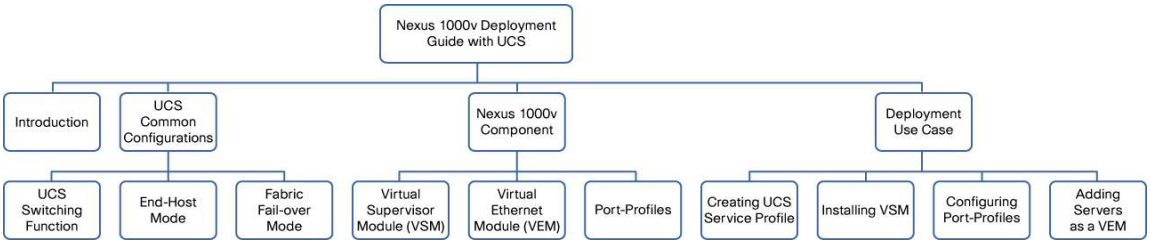
Contents

Overview

This document provides design and configuration guidance for deploying the Cisco Nexus® 1000V Series Switches with VMware vSphere. For detailed configuration documentation, refer to the Cisco® and VMware product configuration guides.

What Will Be Discussed

Figure 1. Content and Structure of This Guide



Audience

This document is intended for network architects, network engineers, virtualization administrators, and server administrators interested in understanding and deploying VMware vSphere hosts in a Cisco data center environment.

Introduction

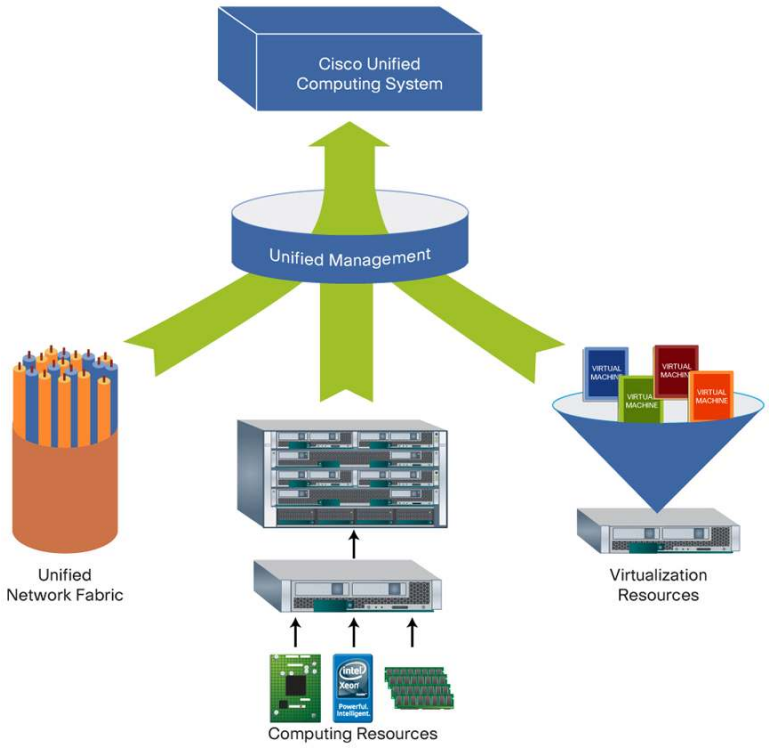
The Cisco Unified Computing System™ (Cisco UCS™) is increasingly deployed in data centers because of its advantages in the server virtualization environment. At the same time, in server virtualization environments in general, it is becoming increasingly complex to manage and the network and be sure that network functionality requirements are met. The Cisco Nexus 1000V distributed virtual switch provides these network requirements and allows the networking team the visibility to manage the growing virtual data center.

Some functions in the Cisco UCS are similar to those offered by the Cisco Nexus 1000V Series Switches, but with a different set of applications and design scenarios. The Cisco UCS offers the capability to present adapters to physical and virtual machines directly. This solution is a hardware-based Cisco VM-FEX solution, while the Cisco Nexus 1000V Series is a software-based VN-Link solution. This document will not go into the differences between the two solutions.

This document will focus on how to deploy the Cisco Nexus 1000V Series within a UCS blade server environment. We will detail best practices for configuring the 1000V that best fit within the UCS environment. We will explain how some of the advanced features of both UCS and Cisco Nexus 1000V facilitate the recommended deployment of the solution.

Figure 2 shows a high-level view of the Cisco UCS.

Figure 2. Unified Computing System Components



Cisco Unified Computing System Common Configurations

The following sections discuss some of the areas of special interest in the Cisco UCS that pertain to the configuration and use of the Cisco Nexus 1000V Series. The configurations discussed here apply regardless of the adapter type used in the UCS blade server.

Cisco Unified Computing System Switching Functions

The Cisco UCS offers eight adapter types, which can be grouped into three classes of functionality:

Dual 10 Gigabit Ethernet Port Adapters:

- Cisco UCS 82598KR-CI Intel 82598 Based 10 Gigabit Ethernet Adapter
- Cisco UCS M61KR-I Intel 82599 Based 10 Gigabit Ethernet Adapter
- Cisco UCS M51KR-I Broadcom 57711 Based 10 Gigabit Ethernet Adapter

Dual 10 Gigabit Ethernet Port and Dual 10 Gigabit Fibre Channel over Ethernet (FCoE) Converged Network Adapters (CNA):

- Cisco UCS M71KR-Q QLogic 2642 Based 4G FCoE CNA
- Cisco UCS M71KR-E Emulex LP21000 Based 4G FCoE CNA
- Cisco UCS M72KR-Q QLogic 8152 Based 10 Gigabit FCoE CNA
- Cisco UCS M72KR-E Emulex OCe10102-F Based 10 Gigabit FCoE UCNA

Virtual Interface Card (VIC) with User Configurable Ethernet and FCoE ports

- Cisco UCS M81KR VIC

Each of these cards has a pair of 10 Gigabit Ethernet connections to the Cisco UCS backplane that support the IEEE 802.1 Data Center Bridging (DCB) function to facilitate I/O unification within these adapters. On each adapter type, one of these backplane ports is connected through 10GBASE-KR to the A-side I/O module; then that connection goes to the A-side Fabric Interconnect. The other connection is 10GBASE-KR to the B-side I/O module; that connection then goes to the B-side Fabric Interconnect.

Within the Cisco UCS M71KR-E, M71KR-Q, and M81KR adapter types, the Cisco UCS can enable a fabric failover capability in which loss of connectivity on a path in use will cause remapping of traffic through a redundant path within the Cisco UCS.

The Cisco UCS 6100 Series Fabric Interconnects operate in two discrete modes with respect to flows in the Cisco UCS. The first is assumed to be more common and is called end-host mode; the other is the switched mode, in which the fabric interconnect acts as a normal Ethernet bridge device. Discussion of the differences between these modes is beyond the scope of this document; however, the Cisco Nexus 1000V Series Switches on the server blades will operate regardless of the mode of the fabric interconnects. With respect to a VMware environment running the Cisco Nexus 1000V Series, the preferred solution is end-host mode to help ensure predictable traffic flows.

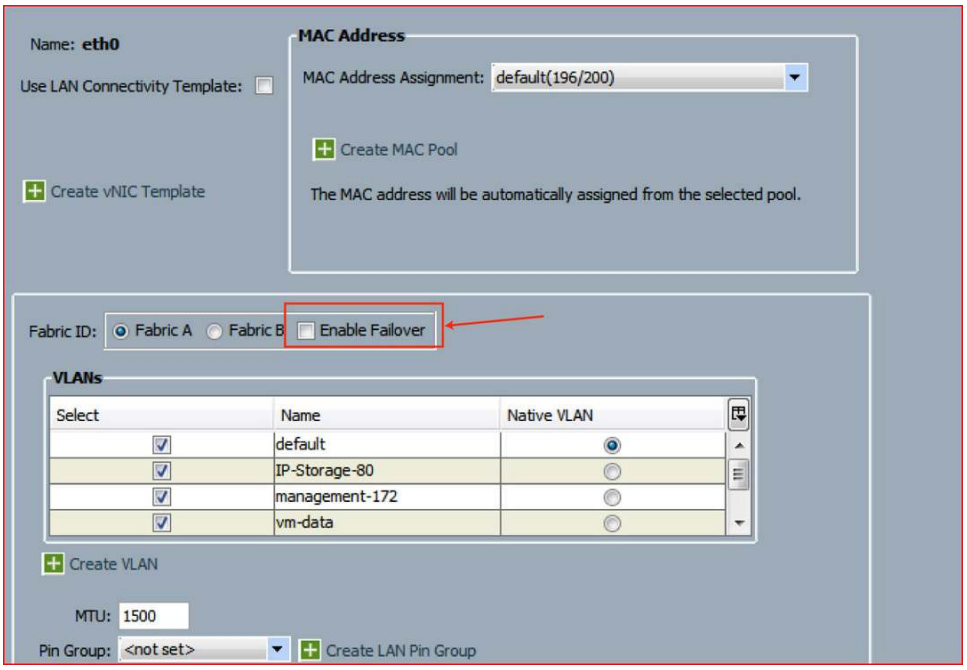
End-Host Mode

With the end-host mode configuration, when Layer 2 communication flows within the Cisco Nexus 1000V Series, these flows may be either local to a given Cisco UCS 6100 Series Fabric Interconnect or through the upstream data center switch with more hops. Applying a quality-of-service (QoS) policy here to help ensure a minimum bandwidth is recommended. The recommended action in the Cisco Nexus 1000V Series is to assign a class of service (CoS) to the VMware service console and VMkernel flows.

Fabric Fail-Over Mode

Within the Cisco UCS M71KR-E, M71KR-Q and M81KR adapter types, the Cisco Unified Computing System can enable a fabric failover capability in which loss of connectivity on a path in use will cause remapping of traffic through a redundant path within the Cisco Unified Computing System. It is recommended to allow the Cisco Nexus 1000V redundancy mechanism to provide the redundancy and not to enable fabric fail-over when creating the network interfaces within the UCS Service Profiles. Figure 3 shows the dialog box. Make sure the Enable Failover checkbox is not checked.

Figure 3. UCS Server Profile Network Configuration



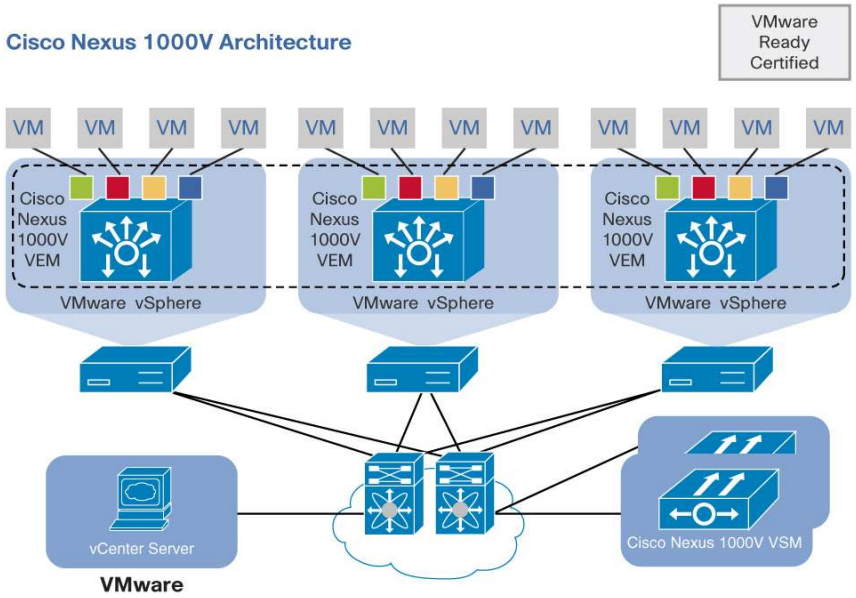
Cisco Nexus 1000V Series Components

The Cisco Nexus 1000V Series Switch consists of the following components:

- Virtual Supervisor Module (VSM): The control plane of the virtual switch that runs Cisco NX-OS.
- Virtual Ethernet Module (VEM): A virtual line card embedded into each VMware vSphere (ESX/ESXi) host.

Figure 4 shows how these components work together.

Figure 4. Cisco Nexus 1000V Solution Components



Virtual Supervisor Module

The VSM acts as the control plane for the virtual switch and communicates with the VEMs (line cards) through an external network fabric. The VSM is a “guest operating system” or virtual machine (VM) that resides on a physical ESX/ESXi server. The VSM has three possible roles:

- **Standalone:** This VSM role will be the only VSM and will not have a secondary VSM to act as a backup.
- **Primary:** This VSM role is the primary “supervisor” that will always have the module slot number 1. In this role, the VSM can have a secondary VSM to act as a backup supervisor module.
- **Secondary:** This VSM will become the secondary supervisor that will always have module slot number 2.

Note: The standalone role is not recommended for production networks and is typically used for lab environments. The primary and secondary roles allow the VSMs to create a dual-supervisor environment, similar to a director class modular chassis for high availability. Whatever VSM is active is not determined by the role of the VSM. Both the primary or secondary VSM can be active and the other will become the standby supervisor.

With the Cisco Nexus 1000V, a single instance can manage up to 64 VEMs. These VEMs will start with the module number 3 (slot 1 and 2 are reserved for the VSMs) and continue to module number 66. A single Cisco Nexus 1000V instance, including dual- redundant VSMs and managed VEMs, forms a switch domain. Each Cisco Nexus 1000V domain within a VMware vCenter Server needs to be distinguished by a unique integer called the Domain Identifier.

VSM Network Interfaces

The VSM utilizes three network interfaces that provide separate functions. They are the following:

- **Network Adapter 1** - control interface: This interface is used to communicate to and from the VSM to VEM. The communication between the VSM and VEM is done through Layer 2 as the default, which requires the VSM Control Interface and also that all of the VEMs are on the same Layer 2 domain (same VLAN). Layer 3 support is available as well.
- **Network Adapter 2** - management interface: This interface is used for administrative connectivity to the VSM, which is the management 0 interface. Layer 3 support is available on this interface for VSM to VEM communication and is the recommended interface to be used.
- **Network Adapter 3** - packet interface: This interface is used for the Cisco Nexus 1000V protocols, such as Cisco Discovery Protocol (CDP) and multicast traffic. Communication on this interface occurs only between VSM and VEM.

VLAN Mapping

When creating these VSM network interfaces as a VM, these three network interfaces will initially be using VMware’s vSwitch port-group configuration. This will require a creation of a port-group name for these interfaces and an appropriate VLAN.

The simplest configuration is to create a single port-group (for example, VSM-Interfaces) with all of the interfaces using this port-group and the same VLAN number. In many environments, the management interface is reserved for a specific VLAN in the data center network and may not allow other types of traffic to reside on that same VLAN.

In environments such as this, you can create and configure two port-groups (2 VLANs). You can create a port-group called VSM-Management (for example, VLAN 10) for the management interface and another port-group called VSM-Control-Packet (for example, VLAN 11) for the control and packet interfaces.

Separate VLANs for each of the interfaces can be configured as well, but this is typically not recommended because it does not really provide any real added benefit.

VSM to vCenter Communication

Given the tight integration of the Cisco Nexus 1000V with VMware vCenter, there is a communication link that is established between the VSM and the vCenter server. This connection requires a registered plug-in of the extension key of the Cisco Nexus 1000V VSM. Once that plug-in is registered, the configuration of the SVS (software virtual switch) connection on the VSM completes the communication link. This allows the VSM to have a secured communication between the VSM and the vCenter server for network configurations.

This communication is going through the management interface of the VSM to the vCenter Server IP address, using port 80 by default. There are two methods to establish this communication:

- **Manual registration:** The extension key is an XML file that is downloaded through an Internet browser that resides on the Cisco Nexus 1000V VSM. Once this file is downloaded, registration of this plug-in is done through the vCenter Server by importing this file into the “plug-in” management of vCenter server. When you configure the SVS connection, you configure the IP address of the vCenter server and the data center name, which establishes the connection to the vCenter server.
- **Installation wizard:** The automation of registering the plug-in to the vCenter server and establishing the connection from the VSM to the vCenter server is done through the installation application, which can be executed by opening an Internet browser and connecting to the VSM management IP Address. Click the Installer Application link, which will start the installation wizard.

Virtual Ethernet Module (VEM)

The VEMs are physical ESX/ESXi servers that will become like an Ethernet modular line card. The VEM is capable of locally switching between VM virtual network interface cards (vNICs) within the VEM. The VSM runs the control plane protocols and configures the state of each VEM, but it never takes part in the actual forwarding of packets. For the ESX/ESXi server to become a VEM and be managed by the Cisco Nexus 1000V VSM, it is critical that the VEM is able to communicate with the VSM. There are Layer 2 or Layer 3 methods for this setting up this communication.

- **Over Layer 2:** The control interface from the VSM communicates to the VEM through a VLAN designated as the control VLAN. This control VLAN needs to exist through all the network switches along the path between the VSM and the VEM.
- **Over Layer 3 (recommended):** Communication between the VSM and the VEM is done through Layer 3, using the management interface of the VSM and a VMkernel interface of the VEM. Layer 3 connectivity mode is the recommended mode.

The Layer 3 mode encapsulates the control and packet frames through User Datagram Protocol (UDP). This process requires configuration of a VMware vmkernel interface on each VMware ESX host, ideally the service console of the VMware ESX server. Using the ESX/ESXi management interface alleviates the need to consume another vmkernel interface for Layer 3 communication and another IP address. Configure the VMware VMkernel interface and attach it to a port profile with the l3control option.

```
Nexus1000V(config)# port-profile type vethernet L3vmkernel
Nexus1000V(config-port-profile)# switchport mode access
Nexus1000V(config-port-profile)# switchport access vlan <X>
Nexus1000V(config-port-profile)# vmware port-group
Nexus1000V(config-port-profile)# no shutdown
Nexus1000V(config-port-profile)# capability l3control
Nexus1000V(config-port-profile)# system vlan <X>
Nexus1000V(config-port-profile)# state enable
```

Note: <X> is the VLAN number that will be used by the VMkernel interface.

The l3control configuration sets up the VEM to use this interface to send Layer 3 packets, so even if the Cisco Nexus 1000V Series is a Layer 2 switch, it can send IP packets.

Layer 3 (L3) mode is the recommended option, in part for simplicity in troubleshooting communication problems between the VSM and VEM. Communication between the VSM and VEM is crucial, and use of Layer 3 is simpler for troubleshooting purposes. If the VMware ESXi (VEM) vmkernel interface cannot ping the management interface of the VSM, then it is easier to troubleshoot Layer 3 routing problems. With Layer 2 (L2) mode, all switches between the VEM and VSM must have the control VLAN in place. Troubleshooting Layer 2 mode can become cumbersome because after the physical network switches are configured, the server administrator needs to troubleshoot the VEM to verify that the appropriate VLANs and MAC addresses of the VSM are seen. This additional process can make troubleshooting VSM-to-VEM communication difficult. Therefore, the recommended approach is to enable Layer 3 mode.

Figure 5 illustrates the use of the same fabric interconnect for Layer 3 VSM to VEM communication. In this configuration, both Server 1 and Server 3 are using vmnic0 as the primary interface that allows the management interface of the VSM and the VMkernel management interface of the VEM. The VSM to VEM communication will need to flow only to the fabric interconnect.

Figure 5. Layer 3 VSM to VEM Communication: Using Same Fabric Interconnect

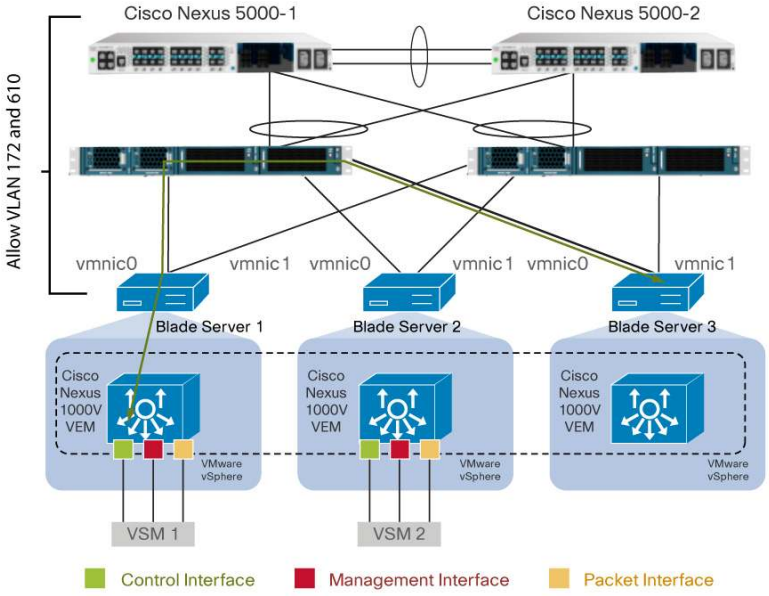
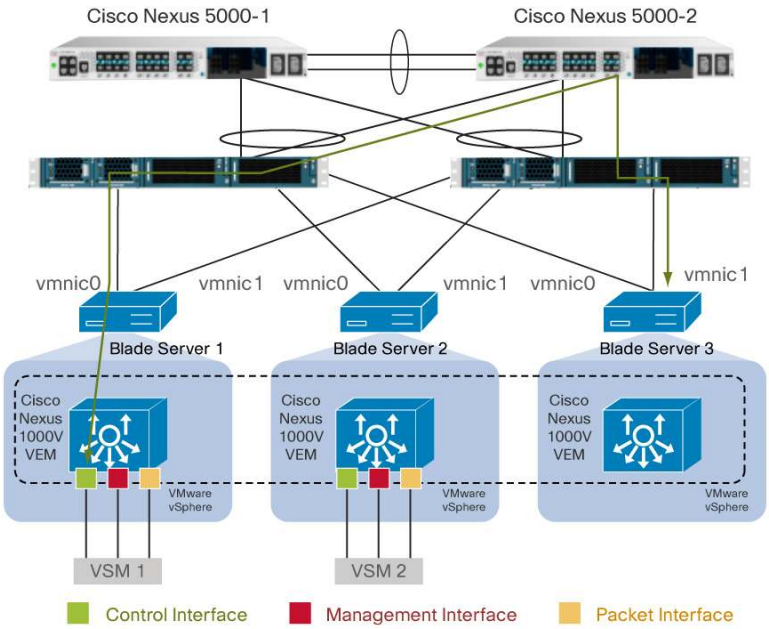


Figure 6 illustrates using a different fabric interconnects for the VSM to VEM communication. Server 1 (vmnic0) has the primary interface that allows the VSM management interface and Server 3 (vmnic1) has the primary interface that allows the VMkernel interface of the VEM on a different fabric interconnects. The VSM to VEM communication will need to flow to the Cisco Nexus 5000 Series Switch.

Figure 6. Layer 3 VSM to VEM Communication: Using Different Fabric Interconnects



Port-Profiles

Port-profiles are network configuration containers that allow the networking team to build network attributes for particular types of VM traffic. Used in this way, port-profiles are a networking concept within the Cisco Nexus 1000V that are mapped to the vCenter port-group. So when a server administrator attaches a port-group to a particular VM, the Cisco Nexus 1000V port-profiles will be part of the drop-down list.

The Cisco Nexus 1000V VSM uses two types of port-profiles:

- **Type Ethernet:** This type of port-profile is used to define network configurations that will be bound to the physical Ethernet interfaces (NICs) on the ESX/ESXi servers. This allows the type of traffic for the VEM to flow through a particular set of interfaces. This type of port-profile, also known as uplink port-profiles, will be configured as a switchport mode trunk, which will allow multiple VLANs to traverse these physical NICs.
- **Type vEthernet:** This type of port-profile, which is the default port-profile type, will define network attributes that will be associated to the vNICs of the VMs and the VMkernels of the ESX/ESXi servers. This port-profile will typically be set as an access port, which will allow only a single VLAN.

The following is a sample configuration of port-profile of type Ethernet:

```
J05-UCSB-N1KV# show running-config port-profile system-uplink

!Command: show running-config port-profile system-uplink
!Time: Mon Feb 13 23:30:51 2012

version 4.2(1)SV1(5.1)
port-profile type ethernet system-uplink
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 1, 51-53, 80, 172
  channel-group auto mode on mac-pinning
  no shutdown
  system vlan 80,172
 description “Uplink Profile for standard UCS Blade Servers”
  state enabled
```

Note: Within the type Ethernet port-profile, it is recommended to set the channel-group mode to mac-pinning within a Cisco UCS and Nexus 1000V deployment. This will allow the automatic creation of a virtual port-channel that will load-balance between the multiple links based upon MAC address of the virtual machine.

The following is a sample configuration of port-profile of type vEthernet:

```
J05-UCSB-N1KV# show running-config port-profile web-52

!Command: show running-config port-profile web-52
!Time: Mon Feb 13 23:32:31 2012

version 4.2(1)SV1(5.1)
```

```
port-profile type vethernet web-52
  vmware port-group
  switchport mode access
  switchport access vlan 52
  no shutdown
  state enabled
```

The port-profile of Ethernet type is critical in that it has to allow the management interface VLAN for the communication between VSM and VEM to be a part of this configuration. Another critical configuration for this Ethernet port-profile is to define the management interface VLAN as a “system VLAN.”

System VLANs

System VLANs are VLANs that are used for critical communication between the VSM and VEMs and the bring up of the Cisco Nexus 1000V system. These critical VLANs are control VLAN (if using Layer 2 mode), packet VLAN, management VLAN (if using Layer 3 mode), and VLANs that are used by VMware’s VMkernel (that is, NAS and iSCSI storage VMkernel and management interface). The VMkernel for vMotion is not critical in the process since it is not critical to bring up the Cisco Nexus 1000V system. Once the Cisco Nexus 1000V system is online, the rest of the communication of the other port-profiles and VLANs are then brought up. We recommend that you use these system VLANs for the particular interfaces, as described earlier.

The following is a sample configuration of a port-profile of type vEthernet with a system VLAN:

```
J05-UCSB-N1KV(config-port-prof)# show running-config port-profile ESXi-Management

!Command: show running-config port-profile ESXi-Management
!Time: Mon Feb 13 23:48:06 2012

version 4.2(1)SV1(5.1)
port-profile type vethernet ESXi-Management
  capability l3control
  vmware port-group
  switchport mode access
  switchport access vlan 172
  no shutdown
  system vlan 172
  state enabled
```

When the Ethernet port-profiles are configured correctly with the appropriate VLAN communications, adding of the ESX/ESXi server as a VEM becomes a simple task for the server administrator.

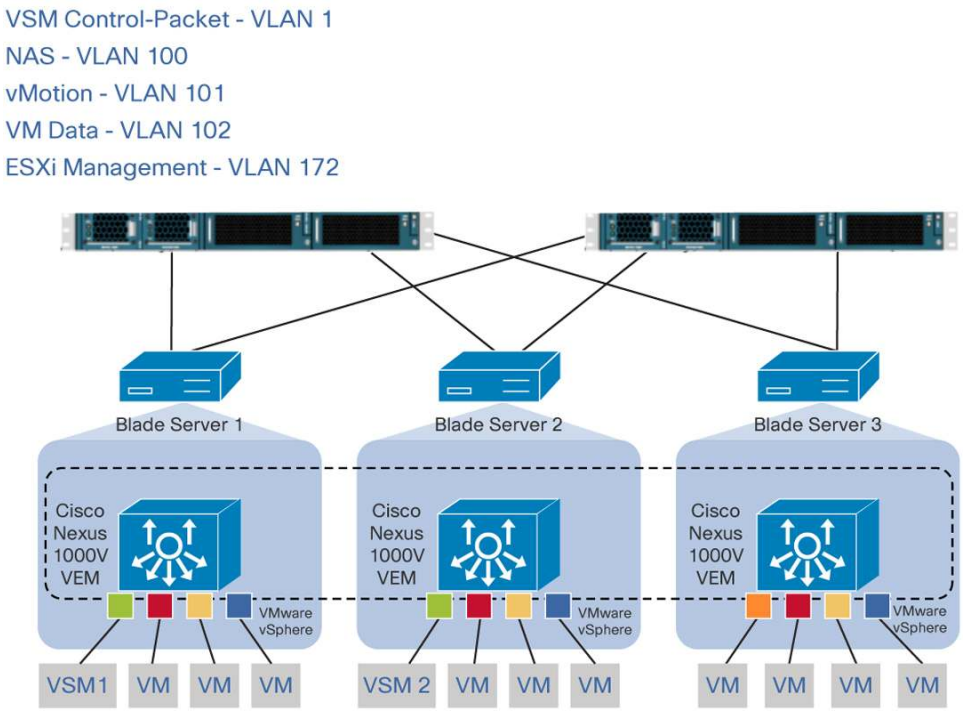
Deployment Topology Use Case

The following will be the most common deployment of the Cisco UCS with the Nexus 1000V Series. With the Cisco UCS and Nexus 1000V being strictly a Layer 2 switch, connectivity from the UCS fabric interconnects to an upstream Layer 3 device is required to allow communication across Layer 2 domain. In the sample environment, the upstream connectivity from the fabric interconnect is to a pair of Cisco Nexus 5000 Series Switches. The following components were used:

- Cisco Nexus 5000 Series - firmware 5.1(3)N1(1)
- Cisco Nexus 1000V Series - firmware 4.2(1)SV1(5.1)
- Cisco UCS
  - UCS Manager version 2.0(1t)
  - Fabric Interconnect - firmware 5.0(3)N2(2.1t)
  - I/O Module - firmware 2.0(1t)
  - Blade Server
    - Cisco Integrated Management Controller - firmware 2.0(1s)
    - BIOS - firmware 2.0.1c.0.100520111716
    - M81KR Adapter - firmware 2.0(1s)
- ESXi 5.0 build 469512

Figure 7 shows the topology of the Cisco Nexus 1000V Series with Cisco Unified Computing System

Figure 7. Cisco Nexus 1000V with Unified Computing System Topology



Note: The shared storage within the environment will be utilizing NFS storage, which will be in VLAN 80.

UCS Service Profile

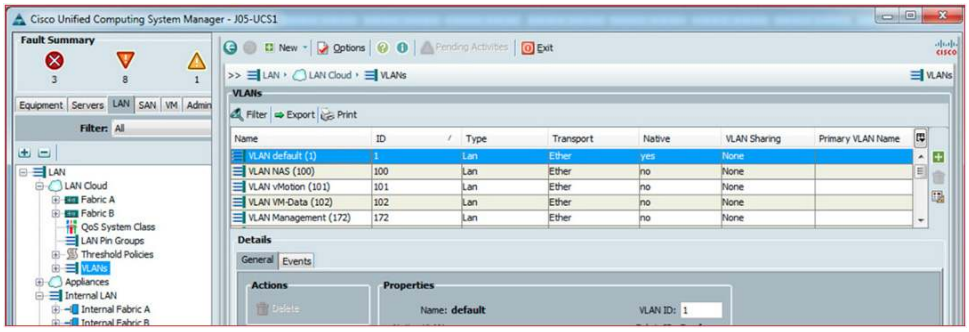
Using the sample topology for this use case, we need to create the UCS Service Profile to prepare the physical blade servers to be used as VMware ESX/ESXi under the control of the Cisco Nexus 1000V. Here are the overall high-level tasks needed to complete the creation of the Service Profile:

- Create Necessary VLANs
  - ESXi management VLAN 172
  - Control and packet VLAN 1 for VSM
  - NAS storage VLAN 100
  - vMotion VLAN 101
  - VM data VLAN 102
- Create Service Profile
  - Create network interfaces
  - Provide appropriate VLAN traffic to traverse those network interfaces

Creating VLANs within UCS

Prior to creating the service profiles, we will need to create the necessary network VLANs so that the service profile can use the appropriate VLANs for deploying Cisco Nexus 1000V. Figure 8 shows an example of configuring the UCS network VLANs. It is always recommended to make the VLANs accessible across both Cisco UCS Fabric Interconnects, as shown in Figure 8.

Figure 8. UCS Network VLAN Configurations



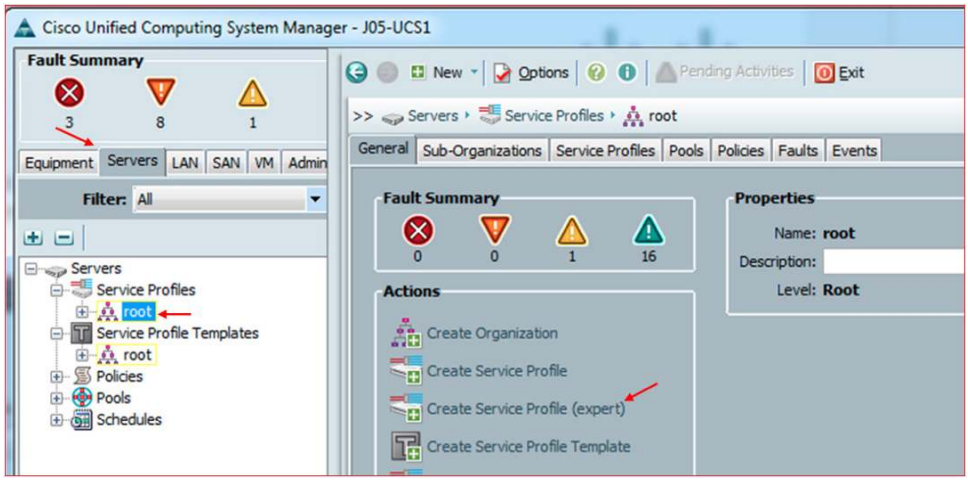
Note: In this example use case, all of the necessary VLANs are created within the UCS LAN tab.

Creating UCS Service Profile

There are various methods of creating the service profile within UCS. The following screen shots will walk through on how to build a sample service profile. Once completed, it is possible to clone this service profile or make a template, to bind it to other blade servers that will be used for the Cisco Nexus 1000V. Detailed understanding of boot policies, BIOS settings, maintenance policies, and so on will not be described in this document. What will be shown is a sample configuration for the Cisco Nexus 1000V.

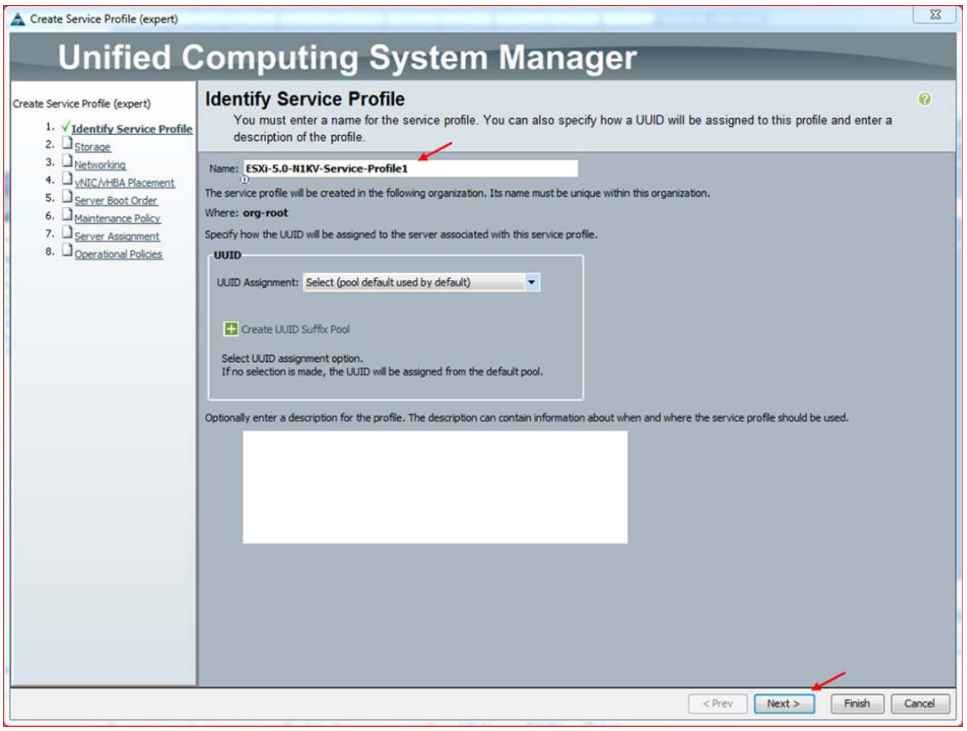
To start, open the Cisco UCS Manager and click the Servers tab, as shown in Figure 9. Then click root under the Service Profiles. In the right-hand pane, click Create Service Profile (expert) to start the wizard.

Figure 9. Creating Service Profile



In the wizard box, fill in the name for the service profile and click Next (Figure 10). The default for the UUID assignment is fine.

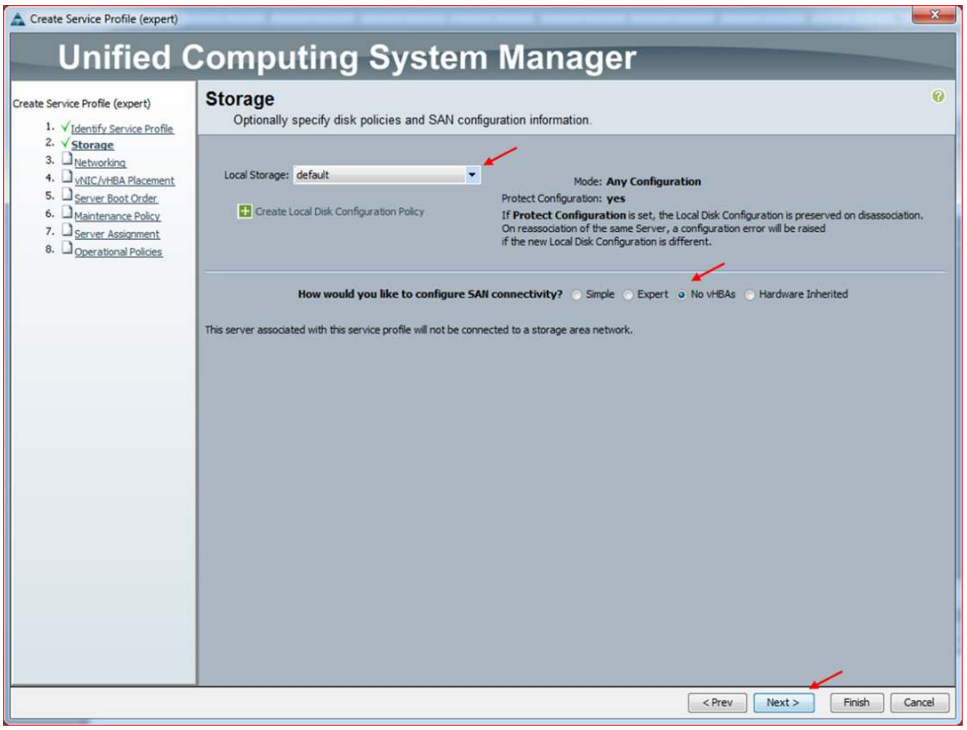
Figure 10. Naming the Service Profile



In this environment, there is local storage on the blade servers so that VMware ESXi will be installed. The shared storage used for the virtual machines will be utilizing NFS storage and does not require Fibre Channel or FCoE storage. So in the next window, there is no need to create vHBAs. Select the No vHBAs button and click Next (Figure 11).

Cisco UCS allows for creation of local storage policies, which will not be discuss in this guide. Please refer to UCS documentation for instructions on how to configure local storage policies and how to configure virtual HBAs.

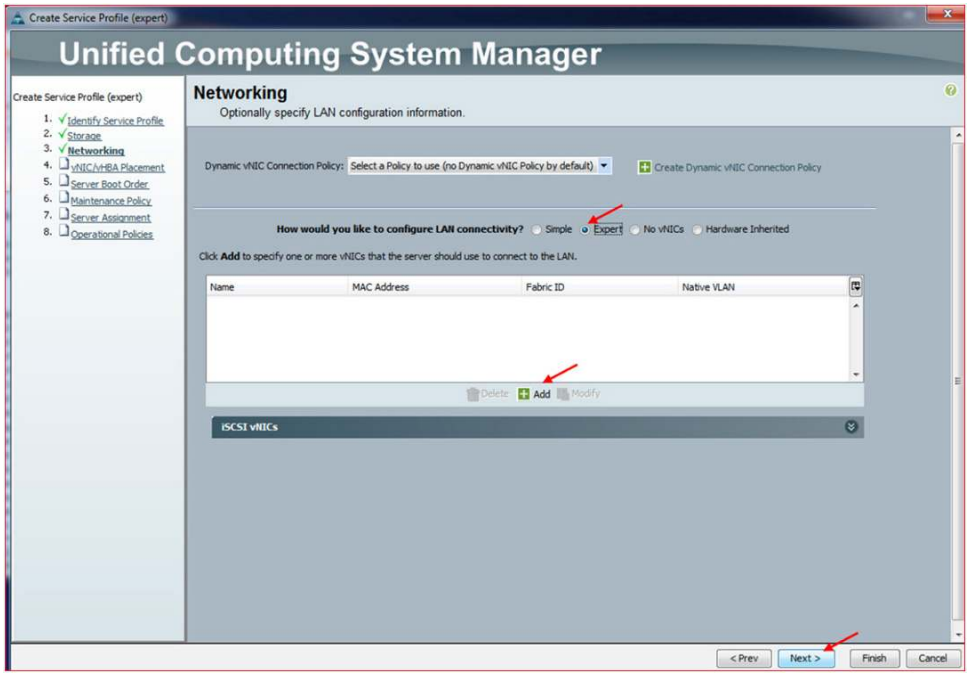
Figure 11. Selecting No vHBAs



UCS provides enhanced capabilities for creating virtual Ethernet interfaces that allow the ESX/ESXi server to see separate VMNICs with varying bandwidth. To simplify deployment and allow the Cisco Nexus 1000V to provide the necessary security and quality of service, creating just two 10 Gigabit Ethernet interfaces is recommended. When you create the NICs for the service profile, it is critical to allow the proper VLANs to traverse these interfaces. The following figures walk you through how to do this.

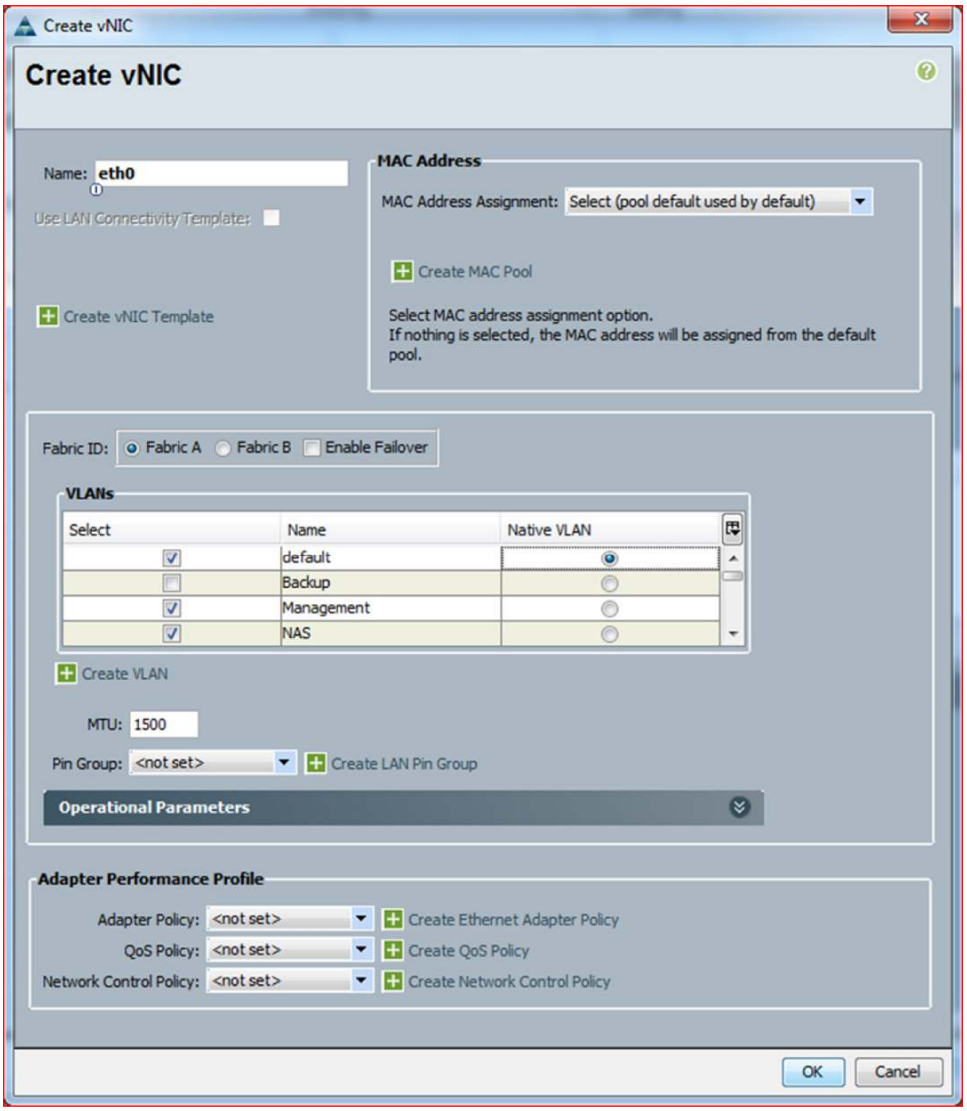
In the Dynamic vNIC Connection Policy, the drop-down box, verify that Select a Policy to use (no Dynamic vNIC Policy by default) is selected. Then select the Expert option. Finally, click the Add button to add a network interface (Figure 12).

Figure 12. Selecting the Dynamic vNIC Connection Policy and Adding the Interface



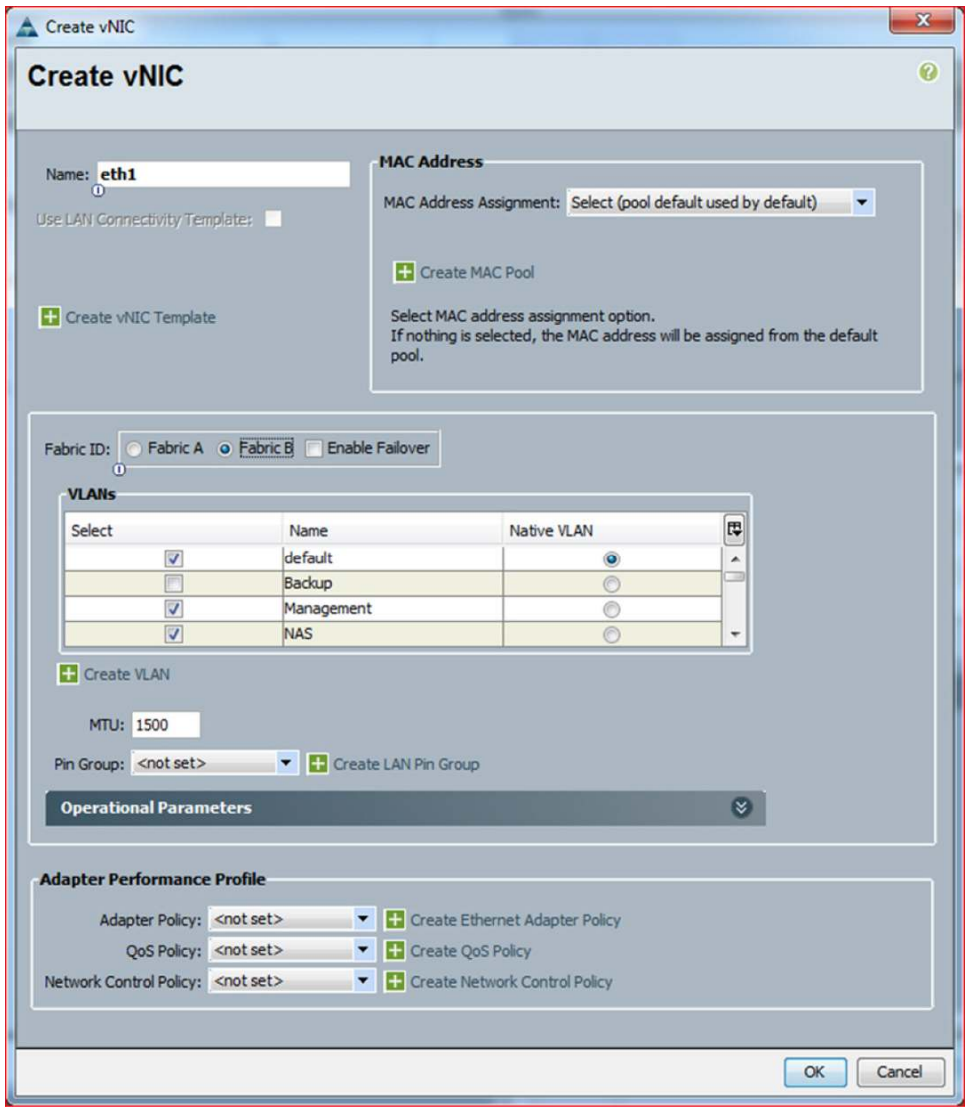
In the next window (Figure 13), you enter in the name of the interface. For the MAC Address section, you can leave the default: Select (pool default used by default). Since this is the first NIC (eth0), we will map this to Fabric A. Under this section, a list of available VLANs is shown. Please select all of the appropriate VLANs. Also it is important to select a Native VLAN, which in this example is the default (VLAN 1). Please note that it is not recommended to select Enable Failover for network interfaces that will be used by the Cisco Nexus 1000V. All other settings can be left as default. Click OK to complete the task.

Figure 13. Creating the First Network Interface



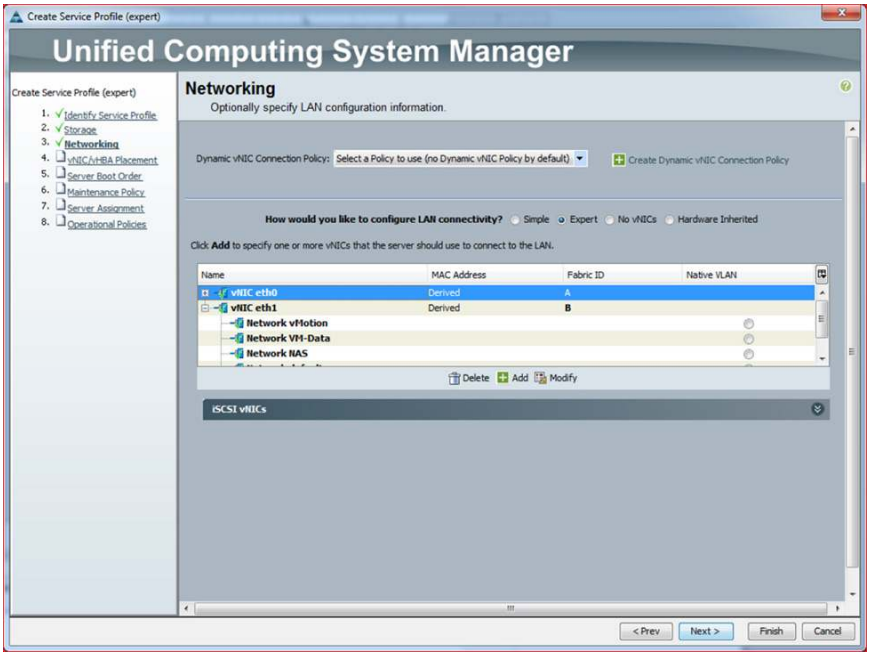
Repeat the same steps to create the second network interface (eth1) for Fabric B, as shown in Figure 14.

Figure 14. Creating a Second Network Interface



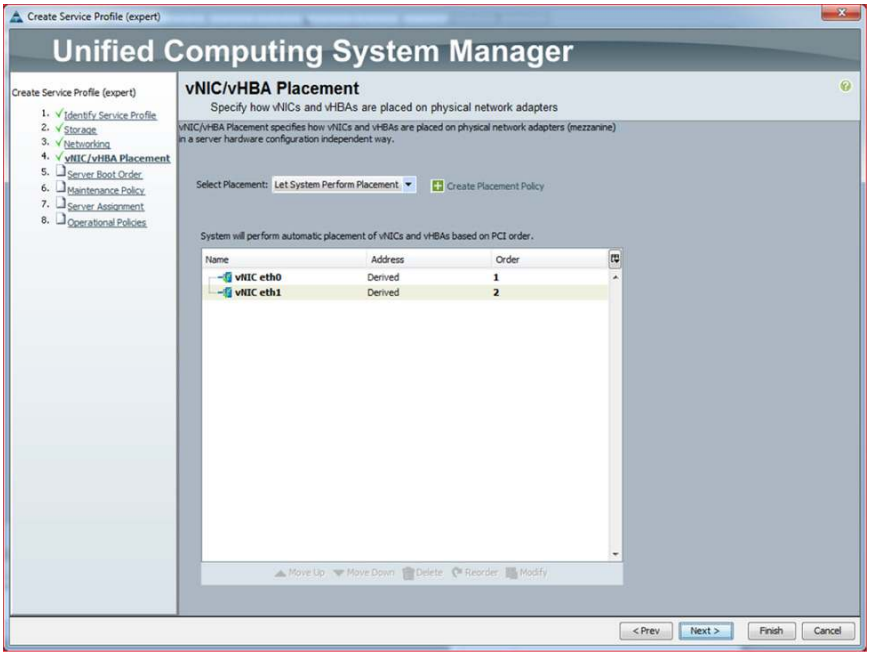
For the network configuration, there should now be two Ethernet interfaces called eth0 and eth1 with the same VLAN mappings, as shown in Figure 15. Click Next.

Figure 15. Network Interface Configurations



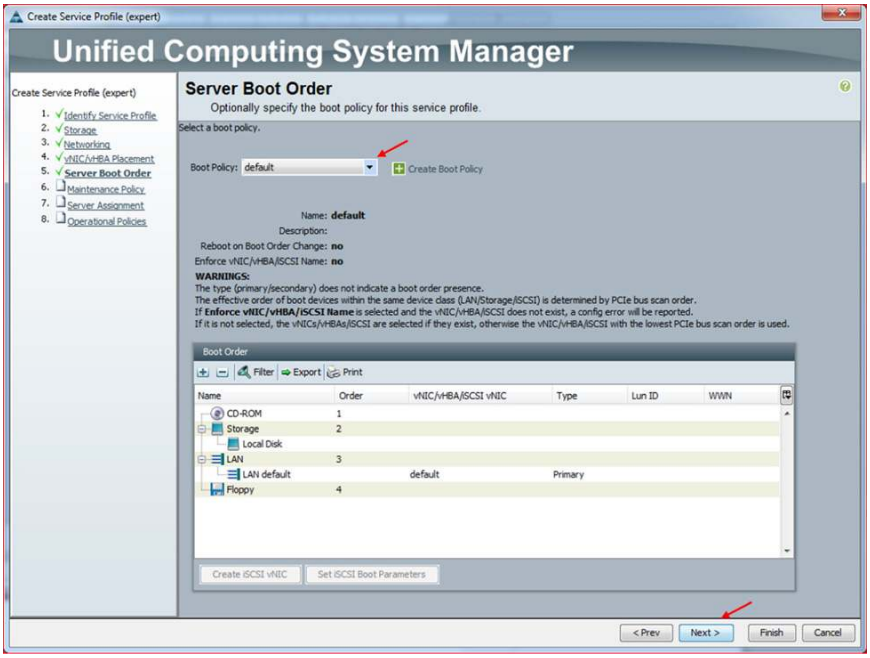
In the next window, shown in Figure 16, select the order of the network interfaces that you've created. In the Select Placement pull-down, leave the default, Let System Perform Placement, and click Next.

Figure 16. Selecting the Order of the Network Interfaces



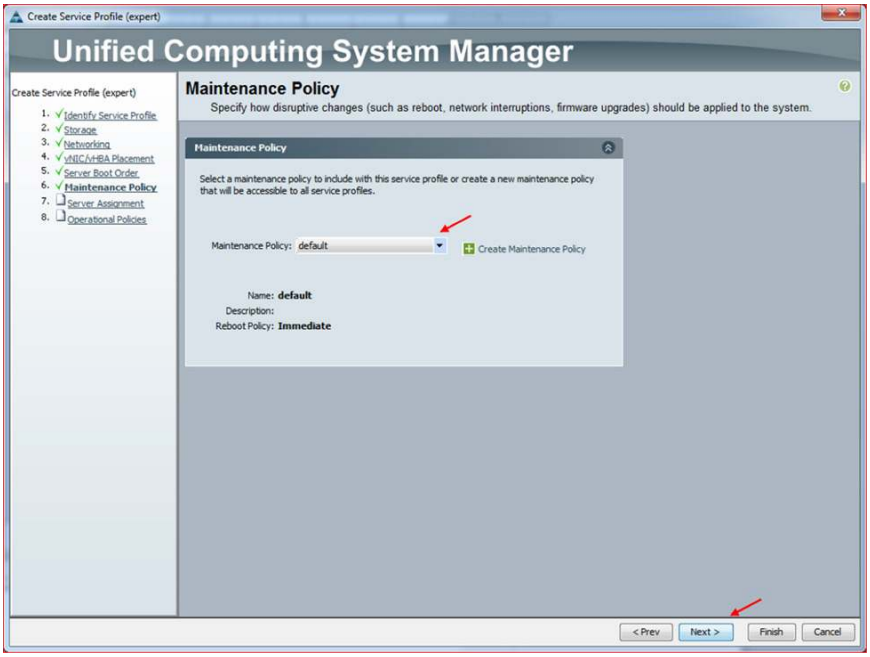
In the next window (Figure 17), select the default in the Boot Policy pull-down. Click Next to continue.

Figure 17. Selecting the Boot Policy



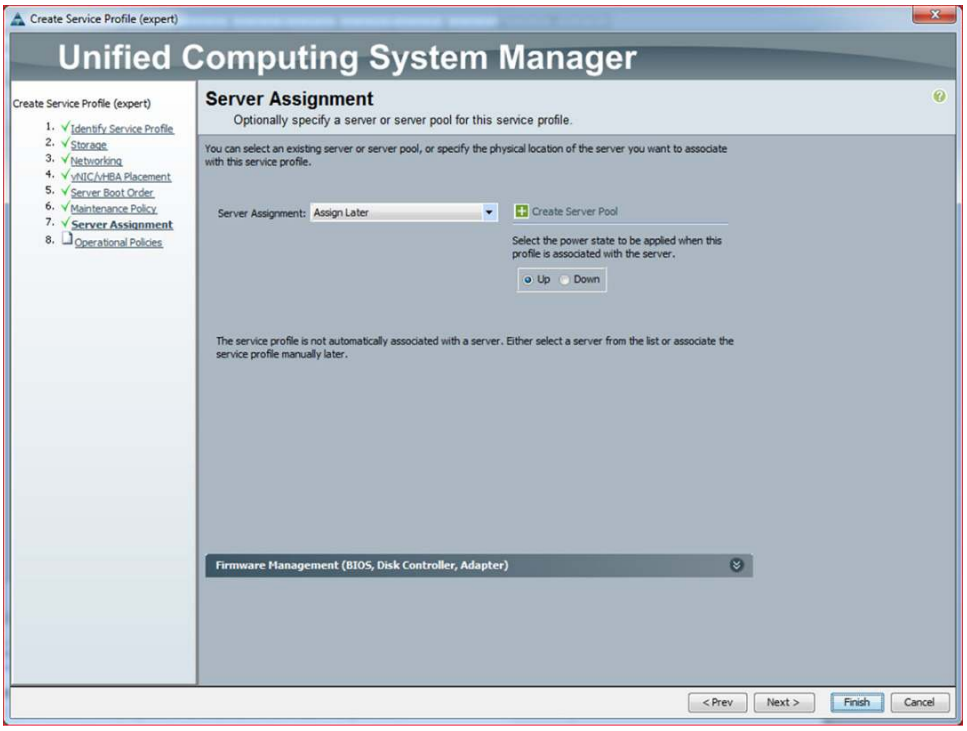
In the next window, you set the maintenance policy; in this example, we will select the default (Figure 18). When you create the UCS service profile for your system, please select the maintenance policy that meets the standards in your environment. Click Next to continue.

Figure 18. Setting the Maintenance Policy



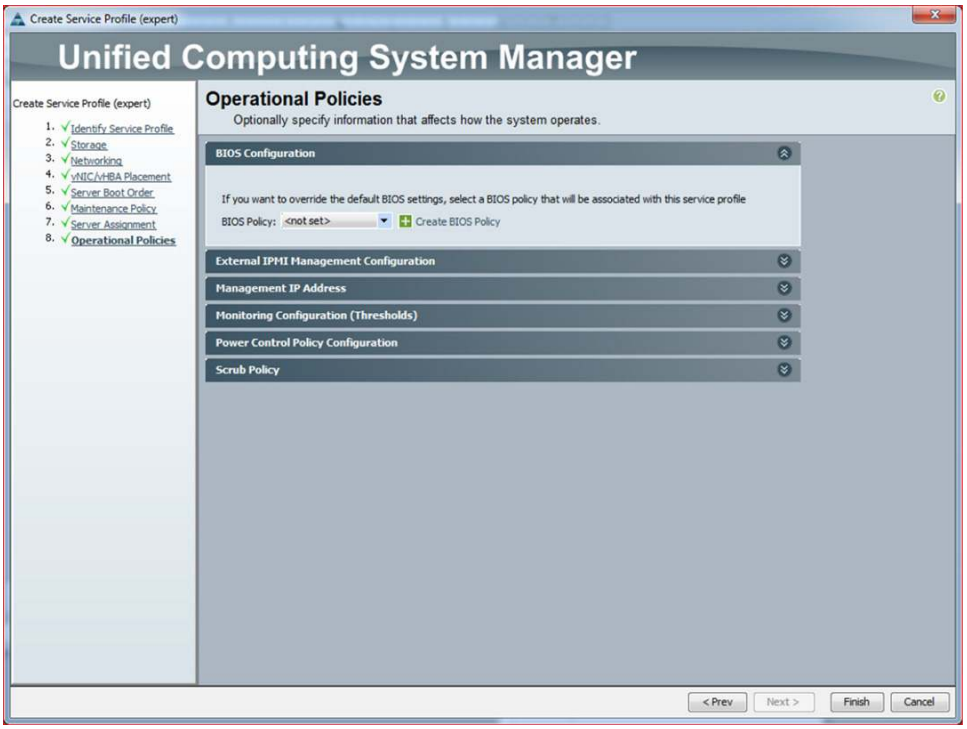
Once the service policy is configured, it is possible to assign it to a particular UCS blade server in the chassis (Figure 19). In this example, there are three blade servers but we will assign them to the service profile at a later time. Click Next to continue.

Figure 19. Server Assignment Window (Setting Deferred at This Point)



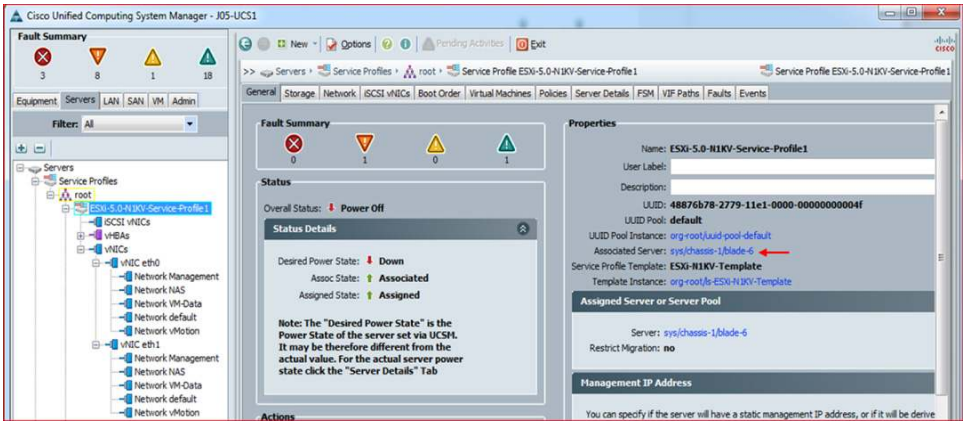
The BIOS setting is the last item to configure in this service profile. In our example, we will use the default BIOS policy (Figure 21). Click Finish to complete the creation of the service profile.

Figure 20. Setting the BIOS Policy



Now that the service profile is complete, we can assign it to a particular blade server and also clone the service profile to be assigned to other blade servers. A detail description on how to assign a physical blade server to the service profile is not shown and can be found on the UCS Configuration guide at http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html. Within this topology, there are three blade servers in a UCS chassis. The Figure 21 shows the service profiles in the left pane. Note that the first service profile (ESXi-5.0-N1KV-Service-Profile1) is assigned to `sys/chassis-1/blade-6`

Figure 21. Assigning the Service Profiles

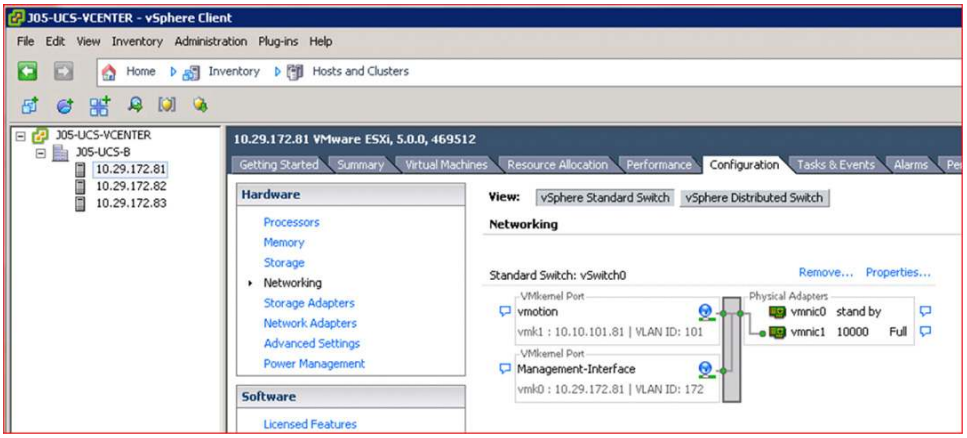


Installation of VSM

With the blade servers configured to use the service profile created in the previous section, you can now install VMware ESX/ESXi onto those blade servers. This document will not go through how to install ESX/ESXi or any configuration related to specific functions solely of VMware features (that is, VMkernels, Fault Tolerance, and so on). This section will describe the tasks needed to install the VSM as a virtual machine (VM) on the ESX/ESXi servers.

ESXi 5.0 was installed for this topology. Figure 22 shows the sample Network configuration for the ESXi blade servers.

Figure 22. ESXi vSwitch Network Configurations



Note: Each of the blade servers has configured the vSwitch0 to have port-groups for vMotion and the management interface, which is used for ESXi management traffic. Both interfaces (vmnic0/vmnic1) are at 10 Gigabit Ethernet speeds.

Cisco Nexus 1000V Installer Application

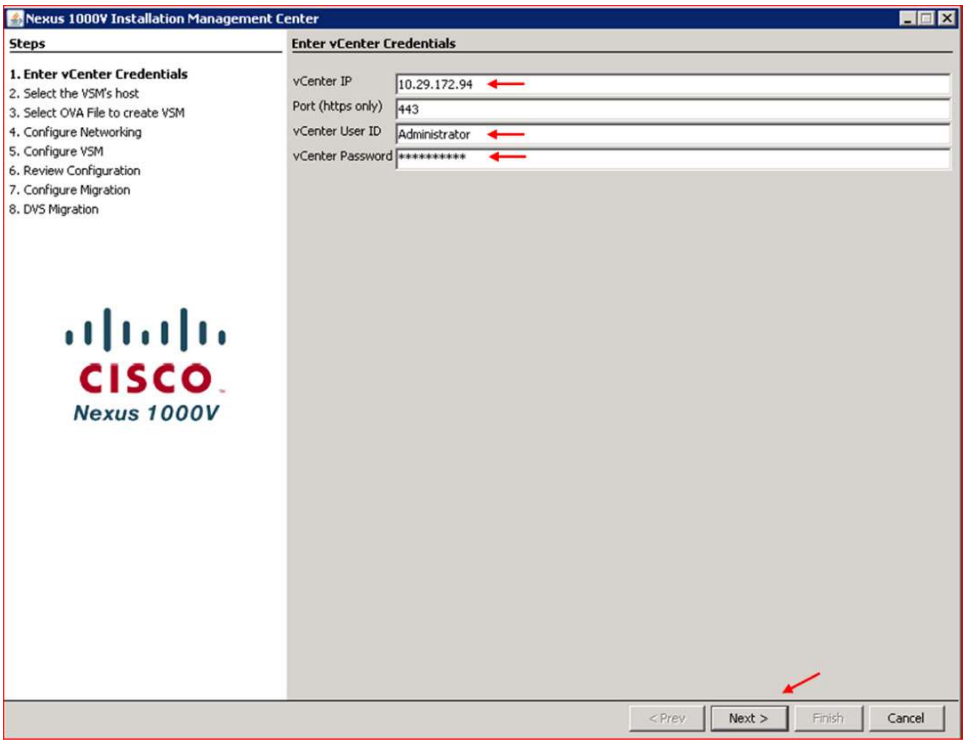
With Cisco Nexus 1000V version 1.5.1, the installer application is a part of the Cisco Nexus 1000V 1.5 zip file, with the path located at Nexus1000v.4.2.1SV1.5.1\VSM\Installer_App\ Nexus1000V-install.jar. Execute the "Nexus1000V-install.jar" command to start the installer application.

The installer application will do the following tasks.

- Install Primary and Secondary VSM
- Register VSM Plug-in onto the vCenter Server
- Create the svs connection on the VSM

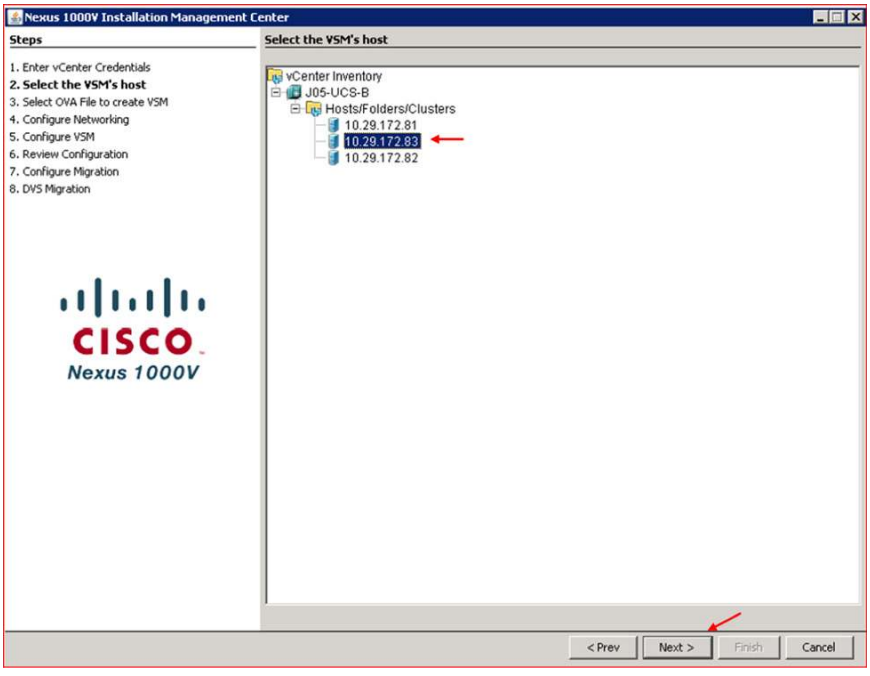
When the installer application starts, you'll first need to enter in the vCenter credentials (Figure 23). Then click Next.

Figure 23. Installer Application vCenter Credentials



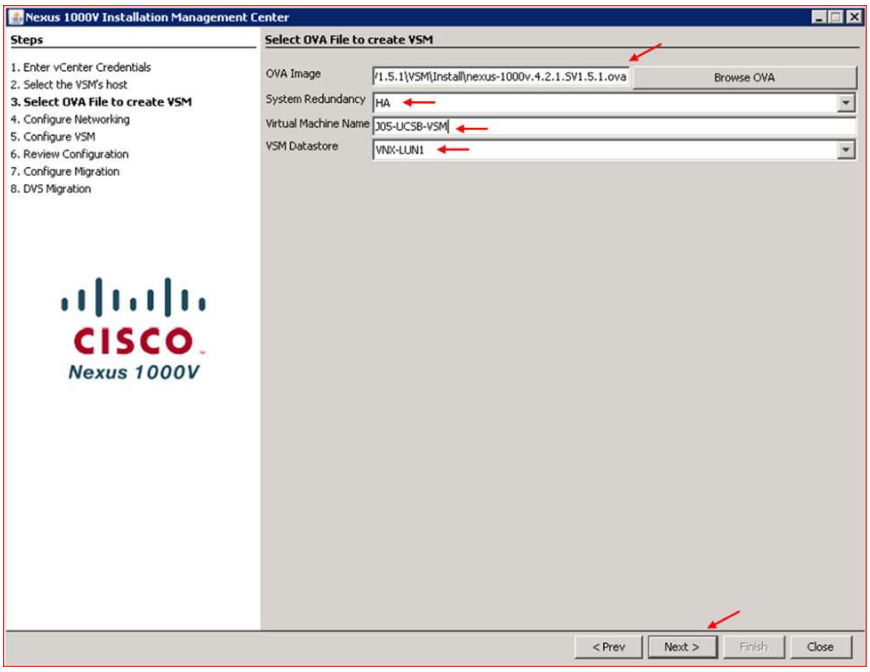
Select the vSphere server to host the primary and secondary VSMs (Figure 24).

Figure 24. Host Selection for VSMs



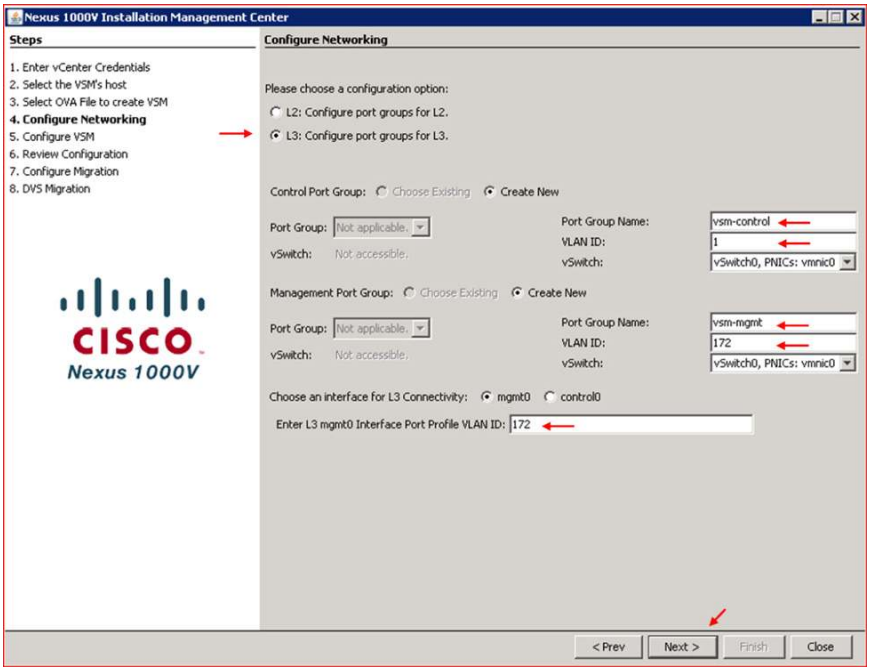
Browse to select the OVA file for the VSM installation and provide necessary information (Figure 25).

Figure 25. OVA File Selection for VSM



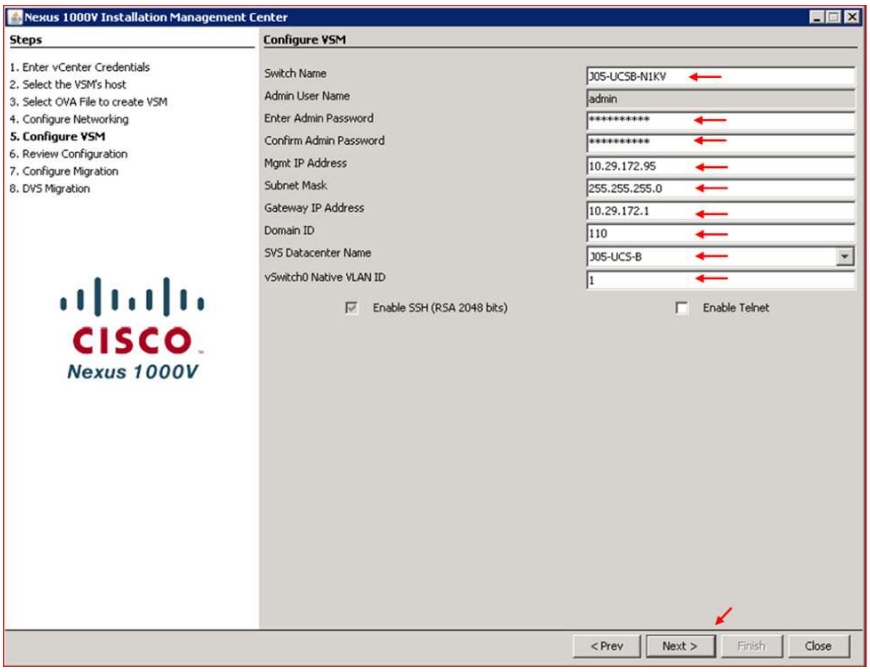
The next screen asks for network configuration of the VSM, such as layer 2 versus layer 3. Other network configuration will be needed as shown below (Figure 26).

Figure 26. VSM Network Configurations



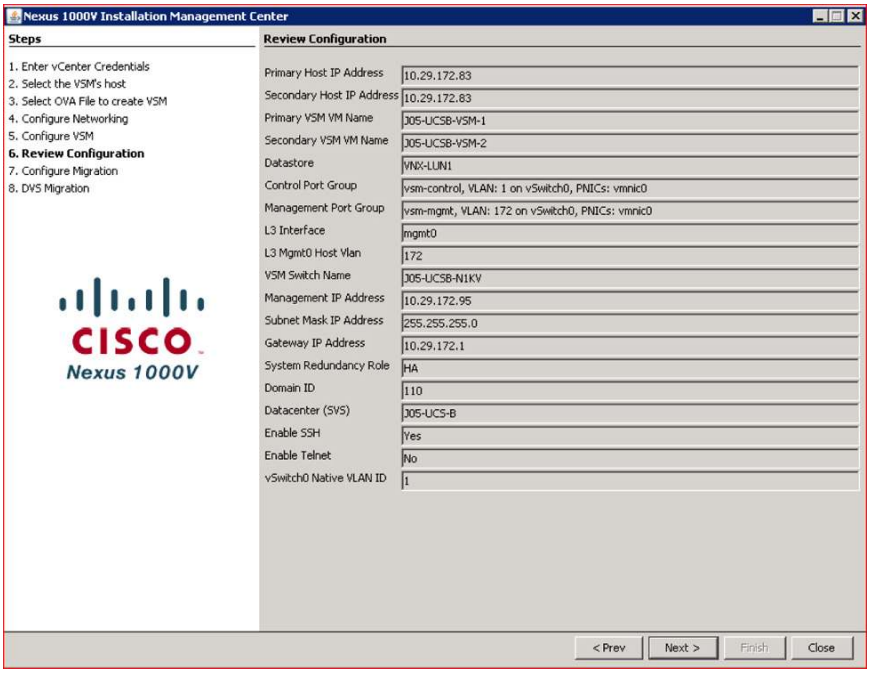
With the vSwitch network configuration defined for the VSM, the following screen defines the VSM (Figure 27).

Figure 27. VSM Configuration



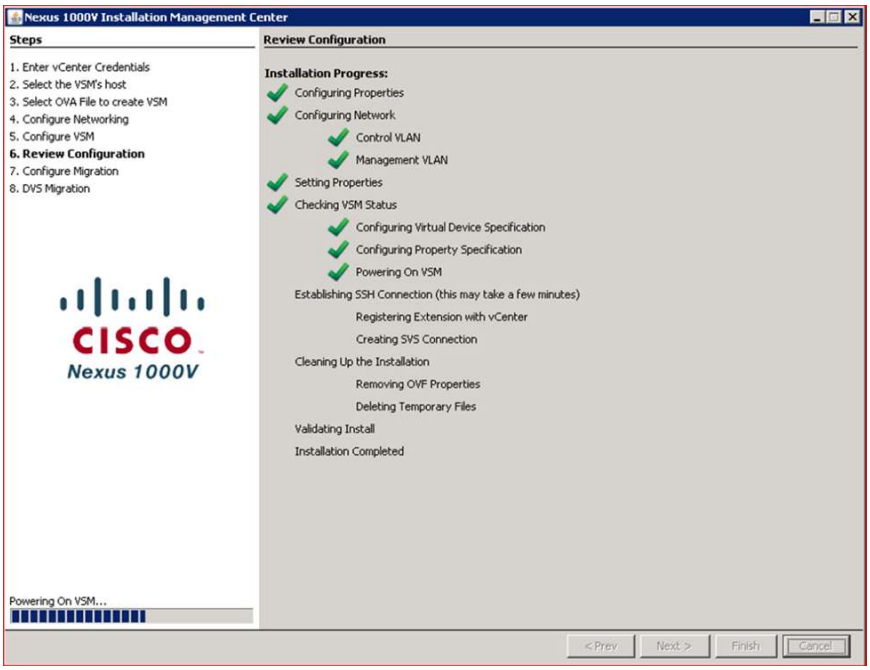
Review the configuration and click on Next (Figure 28).

Figure 28. Configuration Review



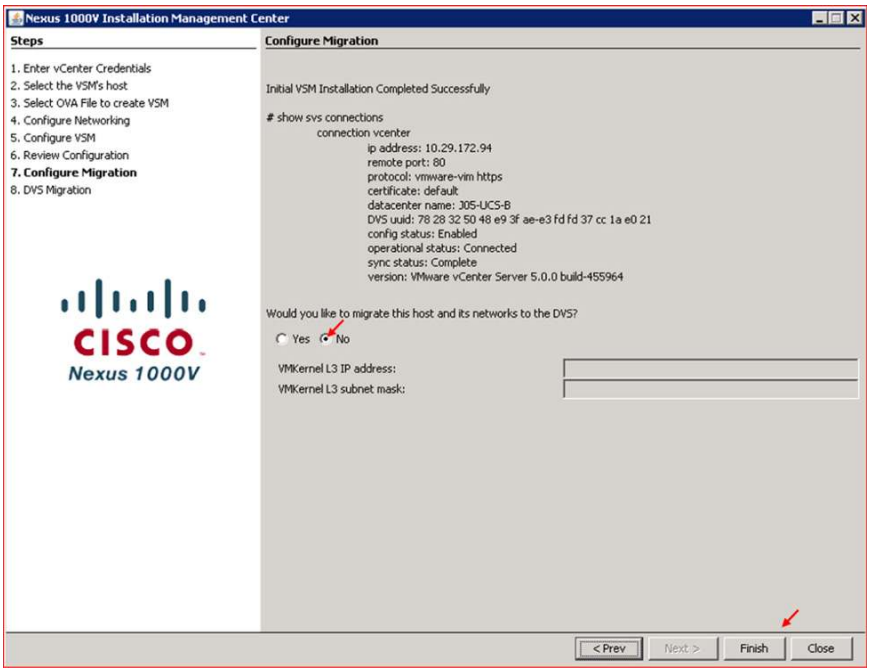
Once the review is done, the installer application begins the installation of the VSMs virtual machines (Figure 29).

Figure 29. Installation of VSMs



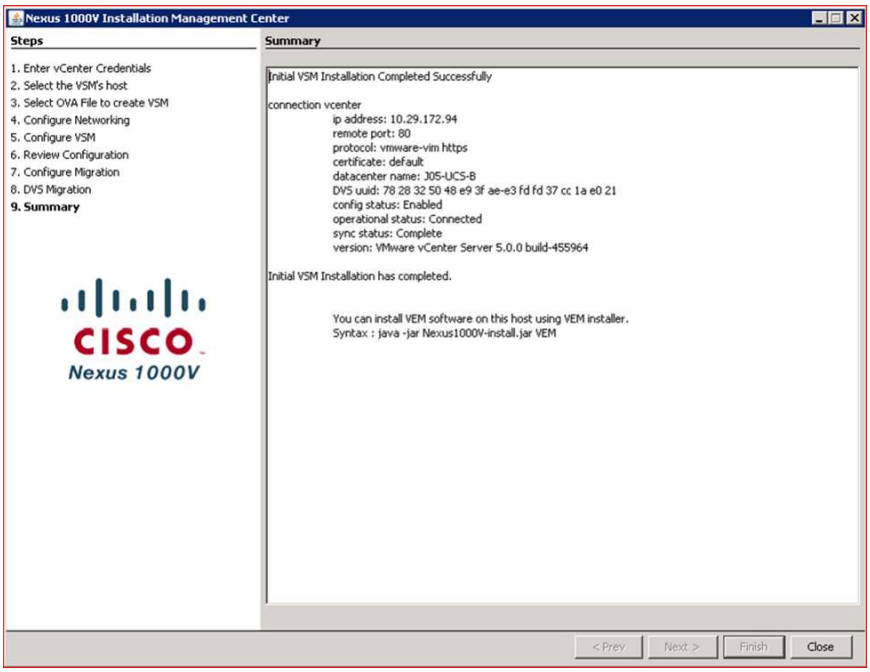
In the next screen, select No when asked about migrating the host and its networks to the Nexus 1000V DVS (Figure 30). Then click on Finish.

Figure 30. Configuration Migration



Click on Close to complete the installer application (Figure 31).

Figure 31. Completion of Installer Application



Note: The installer application places both primary and secondary VSM on the same host. As a best practice, the primary and secondary VSM should reside on different host.

Verify that both primary and secondary VSMs are installed and the svs connection is configured. Execute the following commands:

```
J05-UCSB-N1KV# show module
Mod       Ports     Module-Type                    Model        Status
-----     -----     ---------------------          ---------    ------------
1         0         Virtual Supervisor Module      Nexus1000V   active *
2         0         Virtual Supervisor Module      Nexus1000V   ha-standby

Mod       Sw                          Hw
-----     ------------------          ------------------------------------
1         4.2(1)SV1(5.1)              0.0
2         4.2(1)SV1(5.1)              0.0

Mod       MAC-Address(es)                                        Serial-Num
-----     --------------------------------------------------     ----------
1         00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8                 NA
2         00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8                 NA

Mod       Server-IP           Server-UUID                 Server-Name
-----     ---------------     -------------------------   --------------------
1         10.29.172.95        NA                               NA
```

```
2         10.29.172.95        NA                                  NA

* this terminal session
J05-UCSB-N1KV# show svs connection

connection vcenter:
    ip address: 10.29.172.94
    remote port: 80
    protocol: vmware-vim https
    certificate: default
    datacenter name: J05-UCS-B
    admin:
    max-ports: 8192
    DVS uuid: 78 28 32 50 48 e9 3f ae-e3 fd fd 37 cc 1a e0 21
    config status: Enabled
    operational status: Connected
    sync status: Complete
    version: VMware vCenter Server 5.0.0 build-455964
    vc-uuid: 05A8CD2F-2890-44D2-8757-238B970D8047
```

Configuring Port-Profiles

Once the VSM has been installed, the next task is to configure the port-profiles. Before you add the ESX/ESXi servers as VEMs, you must create the port-profiles. As explained earlier, there are two types of port-profiles. Use the following sections as a guide in creating them.

Type Ethernet Port-Profiles

The uplink port-profile will need to allow all of the VLANs for the environment. The other requirements are to configure the appropriate system VLANs and to configure the channel-group for the virtual port-channel for the VEMs.

Before you configure the uplink port-profile, you must create the VLANs for the VSM. VLAN 1 is created by default. The following shows the configuration for creating the additional VLANs:

```
J05-UCSB-N1KV# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
J05-UCSB-N1KV(config)# vlan 100
J05-UCSB-N1KV(config-vlan)# name iSCSI-Storage
J05-UCSB-N1KV(config-vlan)# vlan 172
J05-UCSB-N1KV(config-vlan)# name Management
J05-UCSB-N1KV(config-vlan)# vlan 101
J05-UCSB-N1KV(config-vlan)# name vMotion
J05-UCSB-N1KV(config-vlan)# vlan 102
J05-UCSB-N1KV(config-vlan)# name VM-Data
J05-UCSB-N1KV(config-vlan)# show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
```

```
1    default                          active
100  iSCSI-Storage                    active
101  vMotion                          active
102  VM-Data                          active
172  Management                       active

VLAN Type
---- -----
1    enet
100  enet
101  enet
102  enet
172  enet

Remote SPAN VLANs
------------------------------------------------------------------------------
Primary  Secondary  Type             Ports
-------  ---------  ---------------  --------------------------------
```

With the VLANs created, here's how to create the uplink port-profile:

```
J05-UCSB-N1KV# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
J05-UCSB-N1KV(config)# port-profile type ethernet system-uplink
J05-UCSB-N1KV(config-port-prof)# vmware port-group
J05-UCSB-N1KV(config-port-prof)# switchport mode trunk
J05-UCSB-N1KV(config-port-prof)# switchport trunk allowed vlan 100-102, 172
J05-UCSB-N1KV(config-port-prof)# no shutdown
J05-UCSB-N1KV(config-port-prof)# system vlan 100, 172
J05-UCSB-N1KV(config-port-prof)# channel-group auto mode on mac-pinning
J05-UCSB-N1KV(config-port-prof)# state enabled
J05-UCSB-N1KV(config-port-prof)# show running-config port-profile system-uplink
!Command: show running-config port-profile system-uplink
!Time: Fri Mar 18 00:27:49 2011

version 4.2(1)SV1(5.1)
port-profile type ethernet system-uplink
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 100-102,172
  channel-group auto mode on mac-pinning
  no shutdown
  system vlan 100,172
     state enabled
```

Note: For layer 3 mode, you are required to set the management VLAN to be a system VLAN within the uplink port-profile. It is also recommended to set the VMkernel VLANs to be system VLANs. In our example, that is VLAN

100 (iSCSI storage) and VLAN 172 (ESXi management). Within the Cisco UCS blade server environment, it is also recommended to set the channel-group mode to mac-pinning.

Type vEthernet Port-Profiles

Once you've created the uplink port-profile, it's time to create the port-profiles used by virtual machines and VMkernels. These profiles are of type vEthernet, which is the default type. With layer 3 communication between the VSM and VEM, a port-profile of type vEthernet is needed that is capable to do this layer 3 communication. During the installer application procedure, this port-profile was already created. The name of this port-profile is n1kv-L3. The configuration output is shown below.

```
J05-UCSB-N1KV# show running-config port-profile n1kv-L3

!Command: show running-config port-profile n1kv-L3
!Time: Fri Mar 18 00:36:16 2011

version 4.2(1)SV1(5.1)
port-profile type vethernet n1kv-L3
  capability l3control
  vmware port-group
  switchport mode access
  switchport access vlan 172
  no shutdown
  system vlan 172
  state enabled
```

Note: This port-profile has the entry capability l3control and is configured as a system vlan.

When you create port-profiles for VMkernels, it is recommended that you make them system VLANs. We recommend that you create all the necessary port-profiles before adding the first host to become a VEM. This allows for the migration of all of the interfaces for VMs and VMkernels at the time of adding the VEM. Table 1 lists examples of the port-profiles you create.

Table 1. Example Port-Profiles with System VLANs

Port-Profiles with System VLANs	Regular Port-Profiles
ESXi Management	vMotion
IP storage	Management (other than service console)
	VM data

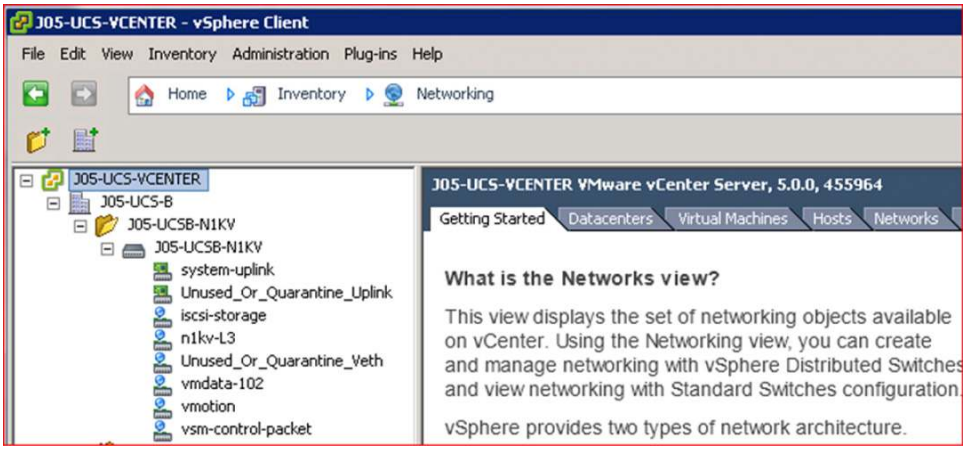
The following shows the port-profiles of type vEthernet for the rest of the environment.

```
J05-UCSB-N1KV# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
J05-UCSB-N1KV(config)# port-profile iscsi-storage
J05-UCSB-N1KV(config-port-prof)# vmware port-group
J05-UCSB-N1KV(config-port-prof)# switchport mode access
J05-UCSB-N1KV(config-port-prof)# switchport access vlan 100
```

```
J05-UCSB-N1KV(config-port-prof)# no shutdown
J05-UCSB-N1KV(config-port-prof)# system vlan 100
J05-UCSB-N1KV(config-port-prof)# state enabled
J05-UCSB-N1KV(config-port-prof)# exit
J05-UCSB-N1KV(config)# port-profile vmotion
J05-UCSB-N1KV(config-port-prof)# vmware port-group
J05-UCSB-N1KV(config-port-prof)# switchport mode access
J05-UCSB-N1KV(config-port-prof)# switchport access vlan 101
J05-UCSB-N1KV(config-port-prof)# no shutdown
J05-UCSB-N1KV(config-port-prof)# state enabled
J05-UCSB-N1KV(config-port-prof)# exit
J05-UCSB-N1KV(config)# port-profile vmdata-102
J05-UCSB-N1KV(config-port-prof)# vmware port-group
J05-UCSB-N1KV(config-port-prof)# switchport mode access
J05-UCSB-N1KV(config-port-prof)# switchport access vlan 102
J05-UCSB-N1KV(config-port-prof)# no shutdown
J05-UCSB-N1KV(config-port-prof)# state enabled
J05-UCSB-N1KV(config-port-prof)# exit
J05-UCSB-N1KV(config)# port-profile vsm-control-packet
J05-UCSB-N1KV(config-port-prof)# vmware port-group
J05-UCSB-N1KV(config-port-prof)# switchport mode access
J05-UCSB-N1KV(config-port-prof)# switchport access vlan 1
J05-UCSB-N1KV(config-port-prof)# no shutdown
J05-UCSB-N1KV(config-port-prof)# state enabled
J05-UCSB-N1KV(config-port-prof)# exit
```

Once all the port-profiles created, verify in vSphere that you can see them through vCenter. The window in Figure 32 verifies that the port-profiles have been synched to vCenter.

Figure 32. Verifying the Port-Profiles



Adding a Server as a VEM

When you add a VEM, there are two methods of installing the VEM binaries onto the ESX/ESXi servers: manually or through the VMware Update Manager (VUM). In our example, the VUM is installed and will be used. In this

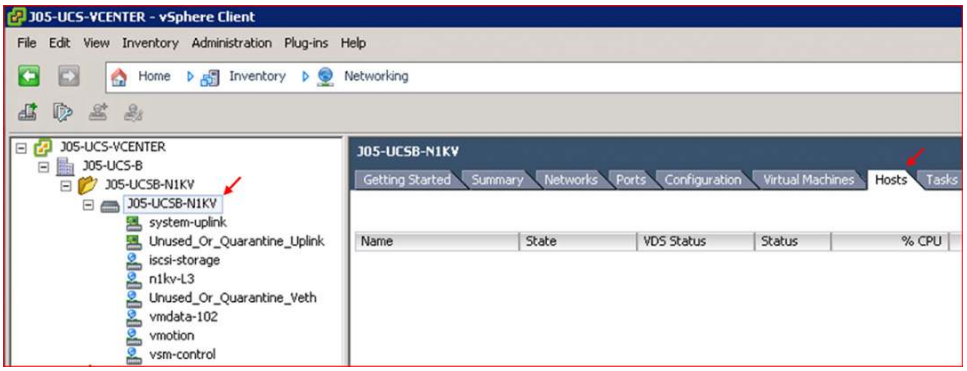
process, both the primary and secondary VSM will be migrated behind the VEM. In the procedure for adding the VEM, all the VMkernels will be migrated as well to the Cisco Nexus 1000V Series.

Adding a VEM, Migrating VMkernels and VSM behind the VEM

The server 10.29.172.82 is hosting the primary VSM and will be the first server to be added to the Cisco Nexus 1000V.

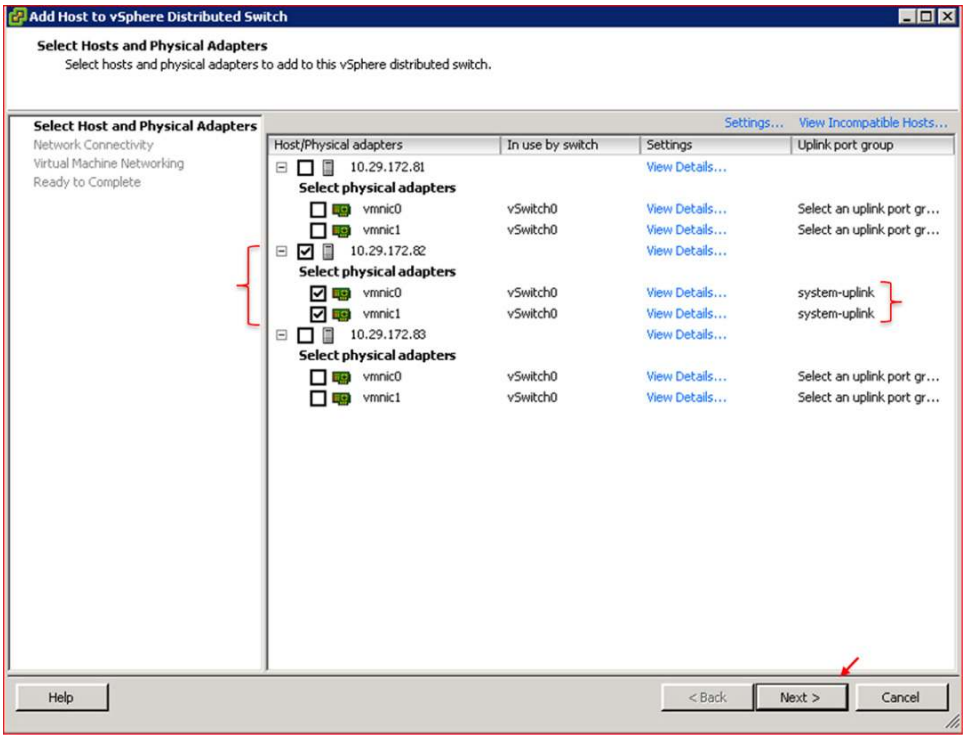
From the Networking view (Figure 33), select the Nexus 1000V virtual switch (J05-UCSB-N1KV) and click the Hosts tab. To add a host to this distributed virtual switch, right-click and select Add Host… or press Ctrl+H.

Figure 33. Adding a Server as a VEM: Screen 1



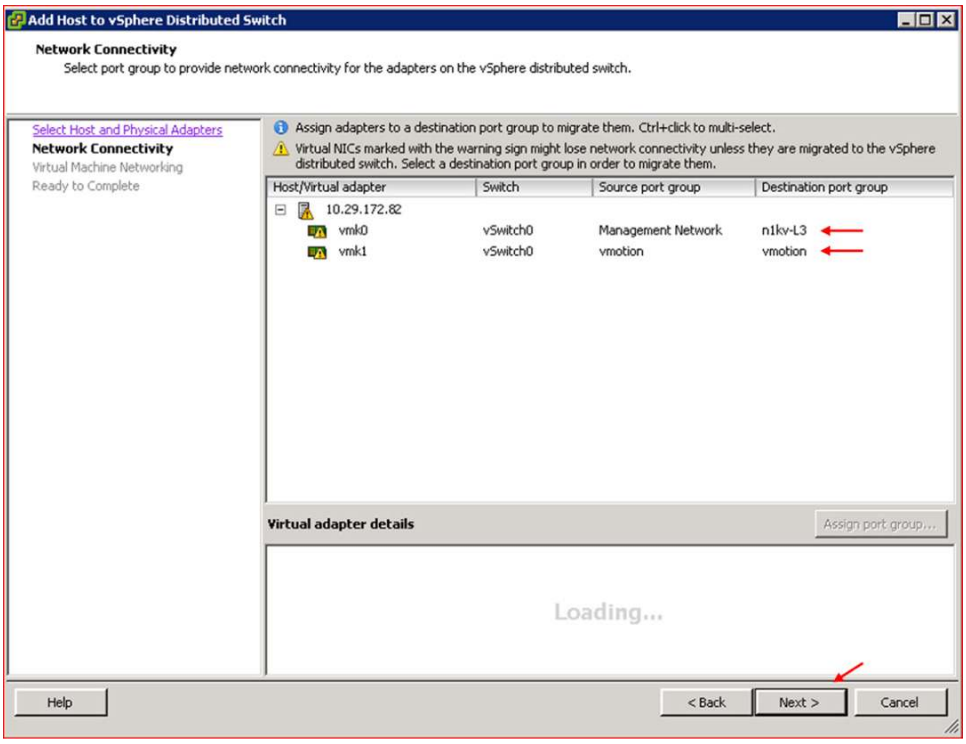
The window shown in Figure 34 provides a list all the servers. We will select the VMNICs for server 10.29.172.82 to be used by the Cisco Nexus 1000V. Once the checkbox is selected, you must select the dvUplink port-group for those interfaces, which correlates to the uplink port-profile that was created in the previous section. Click that the drop-down box, select system-uplink for both interfaces, as shown in Figure 34, and click Next.

Figure 34. Adding a Server as a VEM: Screen 2



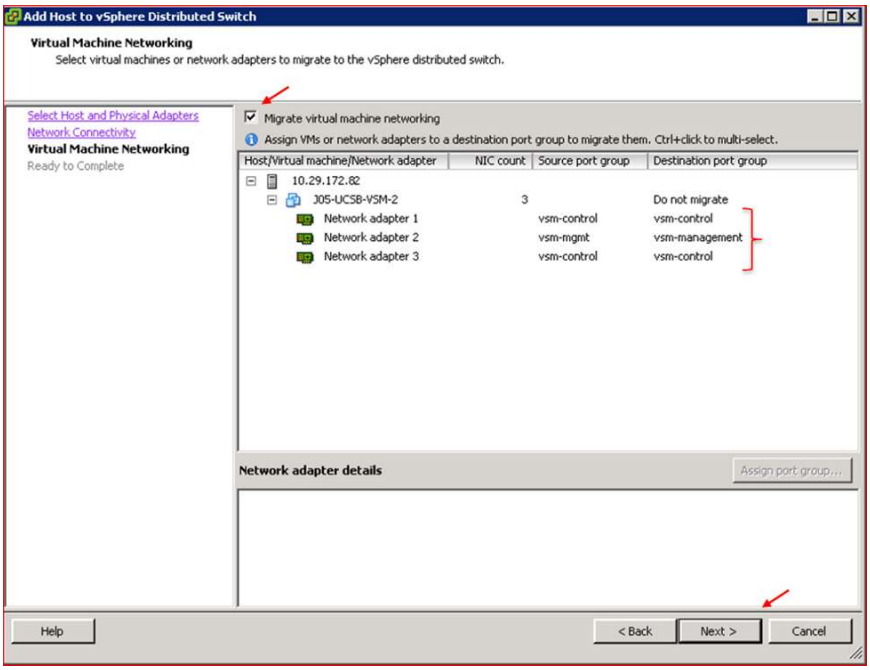
The next window lists the VMkernels on this server and provides the option to migrate the VMkernels over to the Cisco Nexus 1000V. Since the port-profiles have already been created, select the appropriate port-profiles for the listed VMkernels as shown in Figure 35. Then click Next.

Figure 35. Adding a Server as a VEM: Screen 3



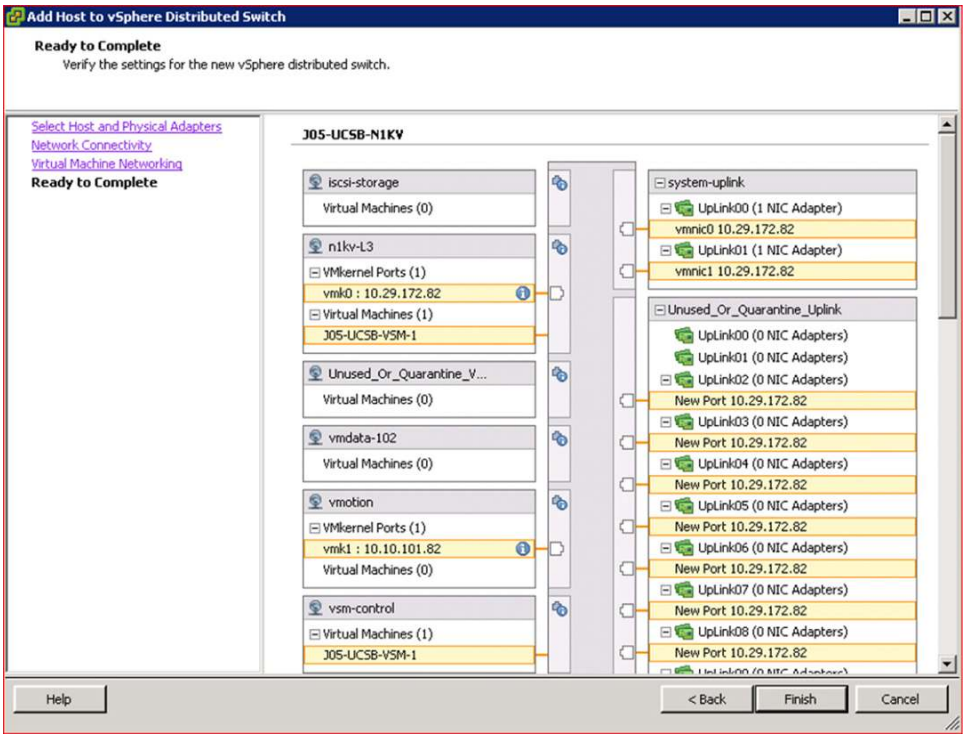
The next window (Figure 36) lists the virtual machines that reside on this server. Since this server has only the primary VSM, click the checkbox called Migrate virtual machine networking and expand the server list to see the virtual machines. With the primary VSM network adapters, go to the Destination port group and select the appropriate port-profiles, as shown in Figure 36. Then click Next.

Figure 36. Adding a Server as a VEM: Screen 4



Click Finished to complete the adding of the server. The VEM binaries will now be installed onto the server by VUM, and the server will be shown as another module in the VSM. The vCenter server will also see that the server has been added. The VMkernels and virtual Ethernet interfaces for the primary VSM will be added as well. Use the show commands to see the result shown in Figure 37.

Figure 37. Adding a Server as a VEM: Screen 5



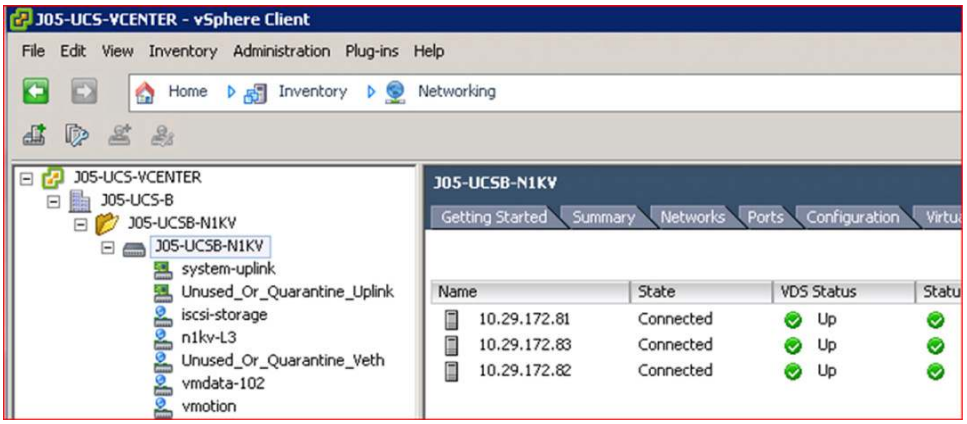

```
J05-UCSB-N1KV# show module
Mod  Ports  Module-Type                    Model              Status
---  -----  ----------------------------  ------------     ----
1    0      Virtual Supervisor Module   Nexus1000V          active *
2    0      Virtual Supervisor Module   Nexus1000V          ha-standby

Mod  Sw                 Hw
---  -----------------  ------------------------------------------------
1    4.2(1)SV1(5.1)     0.0
2    4.2(1)SV1(5.1)     0.0

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
2    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA

Mod  Server-IP        Server-UUID                           Server-Name
---  ---------------  ------------------------------------  -----------
1    10.29.172.95     NA                                    NA
2    10.29.172.95     NA                                    NA

* this terminal session
```

```
J05-UCSB-N1KV# show interface brief

--------------------------------------------------------------------------------
Port     VRF          Status IP Address           Speed    MTU
--------------------------------------------------------------------------------
mgmt0    --           up     10.29.172.181        1000     1500

--------------------------------------------------------------------------------
Ethernet      VLAN   Type Mode   Status  Reason         Speed     Port
Interface                                                       Ch #
--------------------------------------------------------------------------------
Eth3/1        1      eth  trunk  up      none           10G       1
Eth3/2        1      eth  trunk  up      none           10G       1

--------------------------------------------------------------------------------
Port-channel VLAN  Type Mode   Status  Reason          Speed  Protocol
Interface
--------------------------------------------------------------------------------
Po1          1     eth  trunk  up      none            a-10G(D)  none

--------------------------------------------------------------------------------
Vethernet     VLAN   Type Mode   Status  Reason        Speed
--------------------------------------------------------------------------------
Veth1         101    virt access up      none          1000
Veth2         172    virt access up      none          1000

--------------------------------------------------------------------------------
Port     VRF          Status IP Address               Speed    MTU
--------------------------------------------------------------------------------
control0 --           up     --                       1000     1500
```

Note: Notice that the physical interfaces Eth3/1 and Eth3/2 are automatically part of the port-channel 1. All the VMkernels and VM interfaces (primary VSM VM) are, in turn, now part of the Cisco Nexus 1000V Series.

Repeat these steps for the other servers. When completed, the vCenter networking section will show the added hosts and the VSM will show these hosts as VEMs (Figure 37).

Figure 38. List of VEMs



The following is the output of the VSM commands of the Cisco Nexus 1000V environment.

```
J05-UCSB-N1KV# show module
Mod  Ports  Module-Type                    Model           Status
---  -----  ----------------------------  --------------  -----
1    0      Virtual Supervisor Module     Nexus1000V      active*
2    0      Virtual Supervisor Module     Nexus1000V      ha-standby
3    248    Virtual Ethernet Module       NA              ok
4    248    Virtual Ethernet Module       NA              ok
5    248    Virtual Ethernet Module       NA              ok

Mod  Sw                  Hw
---  ------------------  ------------------------------------------------
2    4.2(1)SV1(5.1)      0.0
3    4.2(1)SV1(5.1)      VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
4    4.2(1)SV1(5.1)      VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
5    4.2(1)SV1(5.1)      VMware ESXi 5.0.0 Releasebuild-469512 (3.0)

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
2    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
3    02-00-0c-00-03-00 to 02-00-0c-00-03-80  NA
4    02-00-0c-00-04-00 to 02-00-0c-00-04-80  NA
5    02-00-0c-00-05-00 to 02-00-0c-00-05-80  NA

Mod  Server-IP      Server-UUID                           Server-Name
---  -------------  ------------------------------------  -----------
2    10.29.172.98   NA                                    NA
3    10.29.172.82   48876b78-2779-11e1-0000-00000000003f  10.29.172.82
4    10.29.172.81   48876b78-2779-11e1-0000-00000000004f  10.29.172.81
5    10.29.172.83   48876b78-2779-11e1-0000-00000000002f  10.29.172.83
```

```
    * this terminal session
```

Cisco Nexus 1000V Quality of Service

With all of the different types of traffic flowing through the two 10 Gigabit Ethernet interfaces, the Cisco Nexus 1000V in Version 4.2(1)SV1(5.1) provides enhanced quality of service with class-based weighted-fair queuing (CBWFQ). The Cisco Nexus 1000V can efficiently classify traffic and provide granular queuing policies for various service levels of VMs and types of traffic, such as management, vMotion, and so on. For more detailed explanations and sample CBWFQ configurations, see the Cisco Nexus 1000V Series Quality of Service white paper.

Summary

Among the many advanced management capabilities provided by Cisco UCS in hardware and software, an important one is its ability to rapidly deploy data center applications. Cisco UCS complements the virtualized data center provided by Cisco Nexus 1000V series in a VMware environment, enhancing the operational tasks and visibility to the virtualized machines. Understanding how the various components in Cisco UCS and the Cisco Nexus 1000V integrates together makes it easy for network administration teams to deploy this solution.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

Printed in USA C07-704280-00 04/12