Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to http://www.cisco.com/go/sba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

SBA

DATA CENTER

DEPLOYMENT GUIDE

Virtualization with Cisco UCS, Nexus 1000V, and VMware Deployment Guide

SMART BUSINESS ARCHITECTURE

August 2012 Series

Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in August 2012 are the "August 2012 Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100 
100 100 100
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

If you would like to comment on a guide or ask questions, please use the SBA feedback form.

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

Table of Contents

What's In This SBA Guide

Cisco SBA Data Center

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Data Center is a comprehensive design that scales from a server room to a data center for networks with up to 10,000 connected users. This design incorporates compute resources, security, application resiliency, and virtualization.

Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

About This Guide

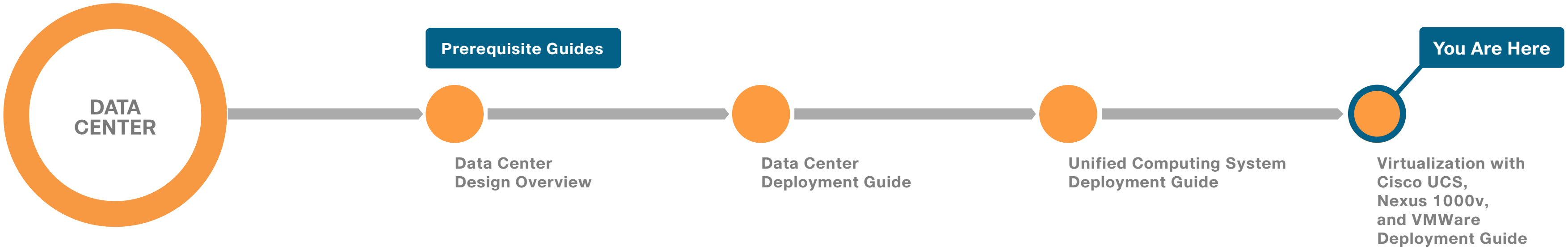
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- Business Overview—Describes the business use case for the design. Business decision makers may find this section especially useful.
- Technology Overview—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- Deployment Details—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel


DATA CENTER
Prerequisite Guides
Data Center Design Overview
Data Center Deployment Guide
Unified Computing System Deployment Guide
You Are Here
Virtualization with Cisco UCS, Nexus 1000v, and VMWare Deployment Guide

Introduction

The *Cisco SBA—Data Center Virtualization with Cisco UCS , Nexus 1000V, and VMware Deployment Guide* is designed to build upon the Cisco Unified Computing System (UCS) B-Series and C-Series server foundation deployment detailed in the *Cisco SBA—Data Center Unified Computing System Deployment Guide*. This guide describes how to use VMware virtualization, the Cisco Unified Computing System, and Cisco Nexus 1000V Series virtual switch to accelerate delivery of new services.

This guide includes the following modules:

- The first module explains how to deploy VMware on the Cisco Unified Computing System, which includes both Cisco B-Series Blade Servers and Cisco C-Series Rack-Mount Servers. This module includes the installation of VMware ESXi, configuration for Ethernet and storage area network (SAN) storage connectivity, and how to set up the environment with VMware tools to deploy and manage the virtualized servers.
- The second module explains how to install and deploy Cisco Nexus 1000V Series Switches to provide a full-featured virtual switch for the VMware servers. Port profiles are built and deployed to provide a faster way to configure virtual switch port interfaces to the VMware virtual machines. Nexus 1000V virtual switches and port profiles are integrated into the VMware network configuration flow to avoid having to jump between multiple consoles to deploy your virtual machines and network settings.

Related Reading

The *Cisco SBA—Data Center Design Overview* provides an overview of the data center architecture. This guide discusses how the SBA data center architecture is built in layers—the foundation of Ethernet and storage networks and computing resources; the data center services of security, application resilience, and virtual switching; and the user services layer that contains applications and user services.

The *Cisco SBA—Data Center Deployment Guide* focuses on the processes and procedures necessary to deploy your data center foundation Ethernet and storage transport. The data center foundation is designed to support the flexibility and scalability of the Cisco Unified Computing System and provides details for the integration of functionality between the server and the network for Cisco and non-Cisco servers. The foundation design includes data center services like security with firewall and intrusion prevention, and application resiliency with advanced server load-balancing techniques. This guide also discusses the considerations and options for data center power and cooling. The supplemental *Data Center Configuration Files Guide* provides snapshots of the actual platform configurations used in the design.

The *Cisco SBA—Data Center Unified Computing System Deployment Guide* provides the processes and procedures necessary to deploy a Cisco Unified Computing System using both the Cisco B-Series Blade Server system and Cisco C-Series Rack-Mount Servers to a point where they are ready to deploy an operating system or hypervisor software.

The supplemental *NetApp Storage Deployment Guide* provides a concise yet detailed process of deploying a NetApp storage array in your data center in order to complete the design.

Business Overview

Smaller organizations face many of the same IT challenges as larger organizations when trying to accommodate increasing demand for new IT capabilities and services. They often place even greater emphasis on cost savings and on protecting business-critical systems and data because they have smaller IT staffs and budgets, and they need to leverage IT assets to their fullest extent. Organizations require cost-effective solutions that can better leverage their existing server, storage, and network resources.

To improve availability and ensure business continuity, organizations need efficient ways to back up and restore production systems while minimizing downtime. Virtualization technology simplifies IT so that organizations can more effectively use their storage, network, and computing resources to control costs and respond faster. The virtual approach to IT management creates virtual services out of the physical IT infrastructure, enabling administrators to allocate these resources quickly to the highest-priority applications and the business needs that require them the most.

With virtualization, hardware management is completely separated from software management, and hardware equipment can be treated as a single pool of processing, storage, and networking resources to be reallocated on the fly to various software services. In a virtual infrastructure, users see resources as if they were dedicated to them—while administrators gain the ability to efficiently manage and optimize resources to serve the needs of the organization.

VMware equips organizations with technology solutions that allow them to optimize the use of their existing IT assets and resources as well as protect the systems, data, and applications that run the business. With analysts predicting that more and more organizations will adopt virtualization, these benefits are making this compelling technology a mainstream mandate.

One aspect of the virtual machines (VMs) created in this new paradigm is that the VMs may easily be migrated from one hardware platform to another, and in conjunction with centralized storage, VMs improve availability and reduce downtime for the organization. However, server virtualization does introduce its own level of complexity to the data center architecture. What was previously a clearly defined demarcation between server configuration and network configuration is now blended, as elements of the network environment reside in software on the physical server platform. In a basic VMware configuration, port settings must be defined on a per-VM basis, which can become repetitive and potentially error-prone for new server initialization.

Managing the virtual machines on the physical servers and the connected networks requires a design that integrates all of these systems so that they work together without creating an operational burden on the IT staff who must maintain them. Using proven and tested designs lowers the time needed to deploy these new solutions and reduces the time required to deploy new applications.

Technology Overview

Virtualization allows you to run multiple workloads in one or more virtual machines (VMs) on a single physical server, with each VM consisting of an operating system and one or more applications. With virtualization, you can quickly move workloads from one physical server to another without any application downtime, enabling flexible and dynamic alignment of business needs with computing resources.

VMs are highly portable and can run unchanged on different physical servers because they consist only of a small number of files encapsulating applications, patches, data, and so forth. This structure allows separation of services from the underlying hardware.

This document explores the ways customers can use VMware virtualization to maximize their business in a Cisco SBA network with Cisco Unified Computing System (UCS) B-Series and C-Series servers.

VMware ESXi is the next-generation, operating system–independent hypervisor that makes virtualization easy to deploy. Also known as the vSphere hypervisor, it enables organizations to partition a physical server into multiple VMs to quickly start experiencing the benefits of virtualization. Requiring minimal configuration, users can be up and running in minutes with a production-ready hypervisor that scales to run the most resource-intensive applications.

VMware Scalable Solutions

VMware vSphere Editions

VMware vSphere is available for organizations in three main offerings targeted for various deployment scenarios. Each edition is licensed based on the number of processors on the physical server hosts that you want to virtualize. Each of the three editions scales easily when you add more licenses to your environment:

- VMware vSphere Standard provides an entry solution for basic consolidation of applications in order to slash hardware costs while accelerating application deployment.
- VMware vSphere Enterprise provides a strategic platform for minimizing downtime, protecting applications and data, and automating resource management.
- VMware vSphere Enterprise Plus includes the full range of components and features for transforming data centers into dramatically simplified cloud-computing environments that can provide the next generation of flexible, reliable IT services to their businesses.

For more information regarding entitlements included per VMware vSphere edition, refer to the following:
http://www.vmware.com/products/vsphere/buy/editions_comparison.html

Starter kits are available that contain essential tools to manage your environment and can be grown to larger deployments. For more information about starter kits, see the following:
http://www.vmware.com/products/vsphere/small-business/overview.html

Management Servers

VMware vCenter Server is the simplest, most efficient way to manage VMware vSphere with scalability from a few to tens of thousands of VMs. From a single console, vCenter provides unified management of all the hosts and VMs in your data center. vCenter is available in several offerings targeted for various deployment scenarios. Each option includes vCenter, the central management tool for configuring, provisioning and managing distributed virtual IT environments:

- VMware vCenter Server Standard provides large-scale management of VMware vSphere deployments for rapid provisioning, monitoring, orchestration, and control of virtual machines.
- VMware vCenter Foundation is the central management tool for up to three physical servers and is suitable for smaller environments looking to rapidly provision, monitor, and control virtual machines.
- VMware vSphere Essentials provides the same features as vCenter Foundation and is integrated with the Essentials and Essentials Plus starter kits.

VMware Enhanced Data Center Availability

VMware offers a wide range of products and solutions offering virtualization and resilience. VMware High Availability (HA) provides rapid and automated restart and failover of VMs without the cost or complexity of solutions used with physical infrastructure. For server failures, VMware HA automatically and intelligently restarts affected VMs on other production servers.

VMware Fault Tolerance provides true continuous availability for infrastructure and applications to further enhance service continuity. It enables critical applications to run with zero downtime and prevents data loss in spite of hardware failures.

VMware vMotion reduces planned downtime from server maintenance activities by enabling the live migration of running VMs from one server to another with no disruption or downtime.

For more information on application mobility, please refer to the following series:
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns749/landing_site_selection.html

VMware also offers storage virtualization and migration between datastores.

For more information on the latest acceleration kits, contact your local reseller or visit the following:
www.vmware.com

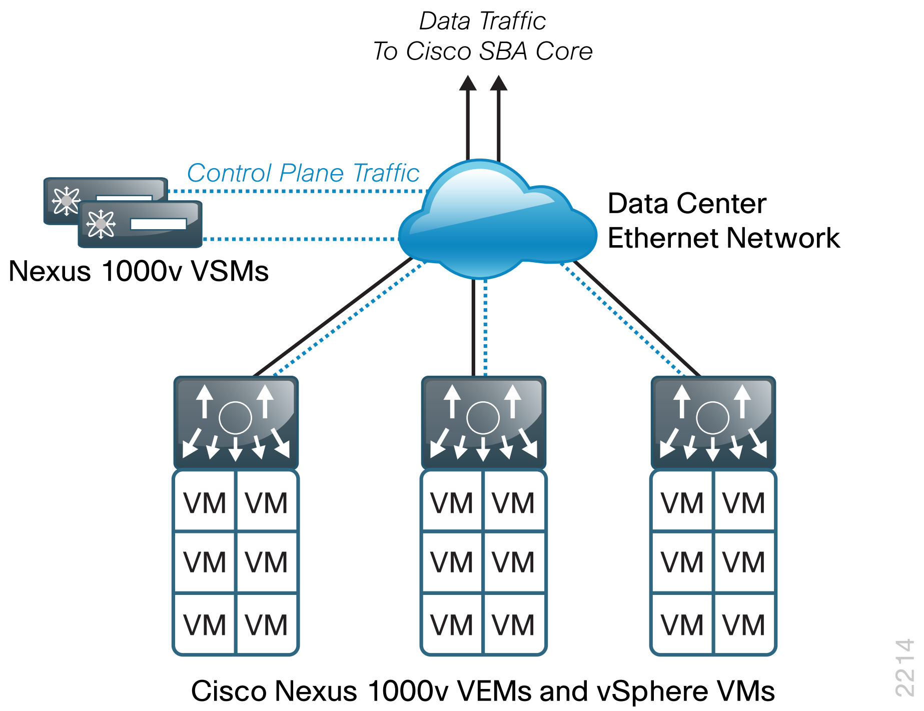
Virtual Switching with Nexus 1000V

The Cisco Nexus 1000V Series switch is a software-based switch designed for hypervisor environments that implements the same Cisco NX-OS operating system as the Cisco Nexus 5500 Series switching platforms that comprise the primary Ethernet switch fabric for the SBA Data Center Architecture. This allows a consistent method of operation and support for both the physical and virtual switching environments. The Cisco Nexus 1000V allows for policy-based VM connectivity using centrally defined port profiles that may be applied to multiple virtualized servers, simplifying the deployment of new hosts and virtual machines. As virtual machines are moved between hardware platforms for either balancing of workloads or implementation of new hardware, port configuration migrates right along with them, increasing the ease of use of the overall solution. The Cisco Nexus 1000V is currently supported with hypervisor software from VMware as an integrated part of the vSphere server virtualization environment.

Cisco Nexus 1000V integrates with VMware vSphere version 4.1 or later and requires Enterprise Plus licensing. This design guide was tested with Nexus 1000V version 4.2(1)SV1(5.1a) and VMware ESXi version 4.1U1.

The Cisco Nexus 1000V virtual switch provides Layer-2 data center access switching to VMware ESX and ESXi hosts and their associated VMs. The two primary components of the solution are the Virtual Supervisor Module (VSM), which provides the central intelligence and management of the switching control plane, and the Virtual Ethernet Module (VEM), which resides within the hypervisor of each host. Together, the VSM and multiple VEMs comprise a distributed logical switch, similar to a physical chassis–based switch with resilient supervisors and multiple physical line cards. This model provides a common distributed architectural approach with Cisco Nexus 5500/2000 Series switches, as well as the Cisco UCS fabric interconnects and I/O modules. A logical view of the Nexus 1000V architecture is shown in the following figure.

Figure 1 - Cisco Nexus 1000V logical view of control and VM traffic flow



Nexus 1000V VEM

The Cisco Nexus 1000V Virtual Ethernet Module (VEM) executes as part of the VMware ESX or ESXi kernel and provides a richer alternative feature set to the basic VMware Virtual Switch functionality. The VEM leverages the VMware vNetwork Distributed Switch (vDS) API, which was developed jointly by Cisco and VMware, to provide advanced networking capability to virtual machines. This level of integration ensures that the Cisco Nexus 1000V switch is fully aware of all server virtualization events, such as VMware vMotion and Distributed Resource Scheduler (DRS). The VEM takes configuration information from the VSM and performs Layer 2 switching and advanced networking functions:

- Port channels
- Quality of service (QoS)
- Security—private VLAN, access control lists, port security, Dynamic Host Configuration Protocol (DHCP) snooping
- Monitoring—NetFlow, Switch Port Analyzer (SPAN), Encapsulated Remote SPAN (ERSPAN)

In the event of loss of communication with the VSM, the VEM has nonstop forwarding capability to continue to switch traffic based on the last known configuration. In short, the Nexus1000V brings data center switching and its operational model into the hypervisor to provide a consistent network management model from the core to the virtual machine network interface card (NIC).

Cisco Nexus 1000V provides centralized configuration of switching capabilities for VEMs supporting multiple hosts and VMs, allowing you to enable features or profiles in one place instead of reconfiguring multiple switches.

Nexus 1000V VSM

The Cisco Nexus 1000V Series Virtual Supervisor Module (VSM) controls multiple VEMs as one logical modular switch. Instead of physical line-card modules, the VSM supports multiple VEMs running in software inside of the physical servers. Configuration is performed through the VSM and is automatically propagated to the VEMs. Instead of configuring soft switches inside the hypervisor on a host-by-host basis, administrators can define configurations for immediate use on all VEMs being managed by the VSM from a single interface. The VSM may be run as a VM on an ESX/ESXi host or on the dedicated Cisco Nexus 1010 hardware platform.

By using the capabilities of Cisco NX-OS, Cisco Nexus 1000V Series provides these benefits:

- Flexibility and Scalability—Port profiles, a new Cisco NX-OS feature, provides configuration of ports by category, enabling the solution to scale to a large number of ports. Common software can run all areas of the data center network, including the LAN and SAN.
- High Availability—Synchronized, highly available VSMs enable rapid, stateful failover and help ensure an always-available virtual machine network.
- Manageability—The Cisco Nexus 1000V Series can be accessed through the Cisco CLI, Simple Network Management Protocol (SNMP), XML API, Cisco Data Center Network Manager, and Cisco Prime LAN Management Solution (Prime LMS).

The VSM is also tightly integrated with VMware vCenter Server so that the virtualization administrator can take advantage of the network configuration in Cisco Nexus 1000V.

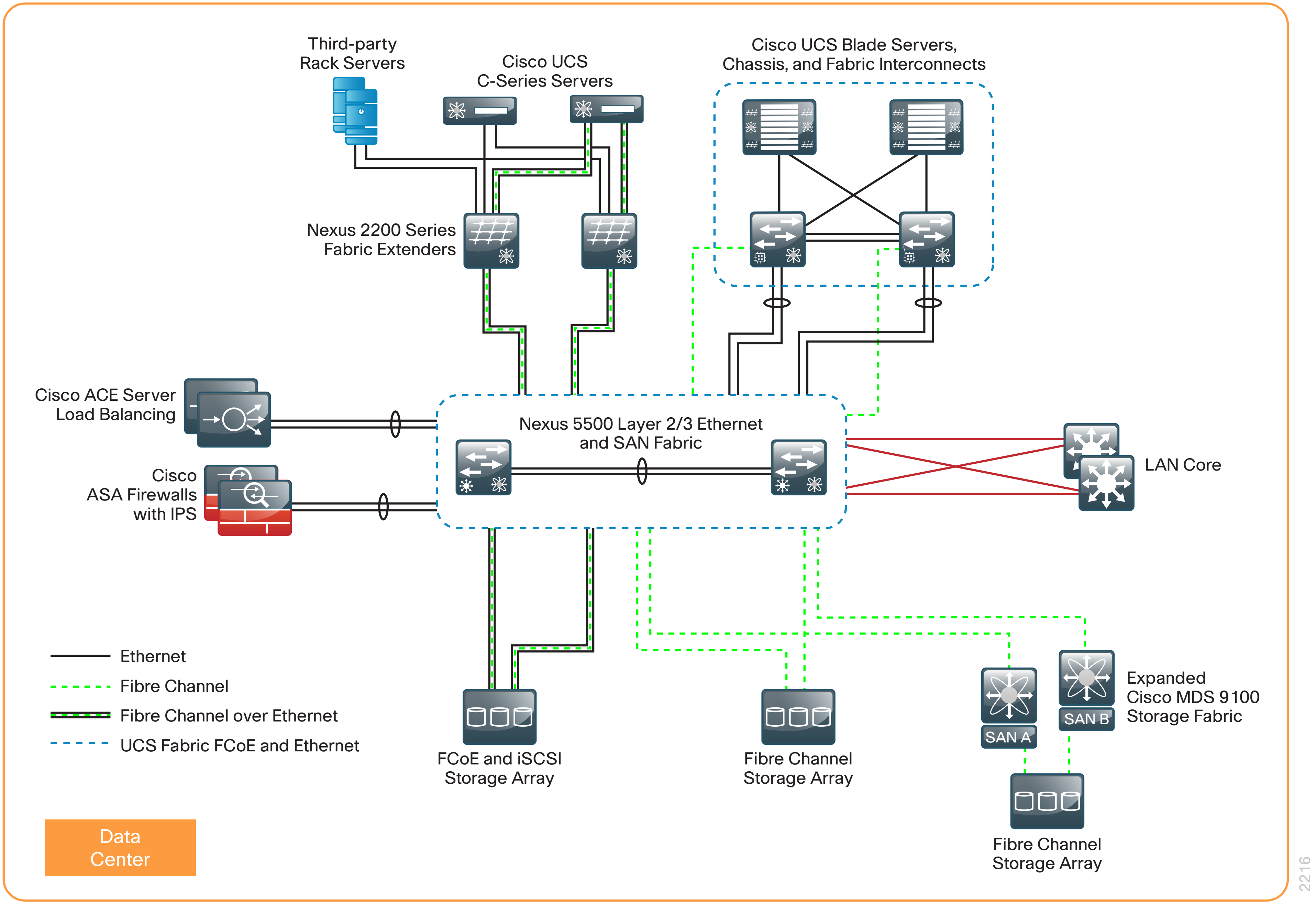
Nexus 1000V Port Profiles

To complement the ease of creating and provisioning VMs, Cisco Nexus 1000V includes the port profile feature in order to address configuration consistency challenges, which provides lower operational costs and reduces risk. Port profiles enable you to define reusable network policies for different types or classes of VMs from the Cisco Nexus 1000V VSM and then apply the profiles to individual VM virtual NICs through VMware's vCenter.

VMware in Cisco SBA

The Cisco SBA Data Center Foundation has been designed to support a virtual machine computing environment. The foundation Ethernet and storage designs support the movement of VMs to balance loads, accommodate system maintenance, and react to physical server failures. The Cisco Unified Computing System provides enhanced flexibility and integration for VMware environments.

Figure 2 - Cisco SBA data center architecture



Unified Computing System Server Hardware

The primary computing platforms deployed in the Cisco SBA reference architecture are Cisco UCS B-Series Blade Servers and Cisco UCS C-Series Rack-Mount Servers. The Cisco UCS Manager graphical interface provides ease of use that is consistent with the goals of Cisco SBA. When deployed in conjunction with the SBA Data Center network foundation, the environment provides the flexibility to support the concurrent use of the Cisco UCS B-Series Blade Servers, Cisco UCS C-Series Rack-Mount Servers, and third-party servers connected to 1- and 10-Gigabit Ethernet connections and the storage network.

Cisco UCS Blade Chassis System Components

The Cisco UCS Blade Chassis system has a unique architecture that integrates compute resources, data network access, and storage network access into a common set of components under a single-pane-of-glass management interface. This architectural approach provides a modular way to grow computing resources, lowers the time to provision new resources, and complements server virtualization by virtualizing the physical server to a profile that can be loaded on demand. The primary components included within this architecture are as follows:

- Cisco UCS fabric interconnects—The Cisco UCS 6100 and 6200 Series fabric interconnects provide both network connectivity and management capabilities to the other components in the system. It is recommended that the fabric interconnects are clustered together as a pair, providing resilient management access—as well as 10-Gb Ethernet, Fibre Channel, and Fibre Channel over Ethernet (FCoE) capabilities—to the system. The newer Cisco UCS 6200 fabric interconnect provides higher capacity, higher port density, lower power consumption, and the flexibility of unified ports, which enables a port to run Ethernet or Fibre Channel. For modular growth, the fabric interconnects support up to twenty UCS Blade Server Chassis.
- Cisco UCS fabric extenders—The Cisco UCS 2100 and 2200 Series fabric extenders, also referred to as *I/O modules*, are installed directly within the Cisco UCS 5100 Series Blade Server Chassis enclosure. Similar to the Cisco Nexus 2000 FEX, which can connect to the data center foundation Nexus 5500 Series, this logically extends the fabric from the UCS fabric interconnects into each of the enclosures for Ethernet, Fibre Channel over Ethernet (FCoE), and management purposes. The newer UCS 2200 Series fabric extender provides higher capacity and scalability for the UCS 5100 Series Blade Server Chassis.
- Cisco UCS 5100 Series Blade Server Chassis—Provides an enclosure to house up to eight half-width or four full-width blade servers, their associated fabric extenders, and four power supplies for system resiliency. The recommended design dual-homes every blade server chassis to the two fabric interconnects for increased reliability.
- Cisco UCS B-Series Blade Servers—Allows customers to easily customize their compute resources to the specific needs of their most critical applications. Available in half-width or full-width form factors, with a variety of high-performance processors and memory architectures.
- Cisco UCS B-Series Network Adapters—Allows the switch fabric to provide multiple interfaces to a server, via a variety of mezzanine adapter cards.
    - Ethernet adapters—The baseline 10-Gigabit Ethernet adapters can present up to two Ethernet interfaces to a server.
    - Converged network adapters—Cisco converged network adapters are available in multiple models, with chip sets from multiple manufacturers, to meet specific needs. These adapters combine Ethernet and FCoE traffic on a single wire and provide two 10-Gigabit Ethernet interfaces and two Fibre Channel interfaces to a server.
    - Virtual interface cards—The Cisco virtual interface cards (VICs) feature new technology from Cisco, allowing additional network interfaces to be dynamically presented to the server complementing the hypervisor technologies. The Cisco VIC is capable of supporting up to 256 total virtual interfaces split between virtual NICs and Fibre Channel virtual host bus adapters (vHBAs). The number of virtual interfaces currently supported depends on the Cisco UCS infrastructure, including the fabric interconnect, fabric extender, VIC model, and version of Cisco UCS Manager.

Cisco UCS Manager

Cisco UCS Manager is embedded software that resides on the fabric interconnects, providing complete configuration and management capabilities for all of the components in the Cisco UCS system. This configuration information is replicated between the two fabric interconnects, providing a highly available solution for this critical function. The most common way to access UCS Manager for simple tasks is to use a Web browser to open the Java-based GUI. For command-line or programmatic operations against the system, a command-line interface (CLI) and an XML API are also included with the system.

Cisco UCS C-Series Rack-Mount Servers

Cisco UCS C-Series servers extend Unified Computing System innovations and benefits to rack-mount servers. Designed to operate in a standalone environment or as part of the Cisco Unified Computing System, Cisco UCS C-Series servers can be used to satisfy smaller regional or remote-site requirements, or they can be used as an approach to deploy rack-mounted servers on an incremental basis. Like the UCS B-Series, the UCS C-Series servers offer a wide array of processor, memory, network adapter, and disk options.

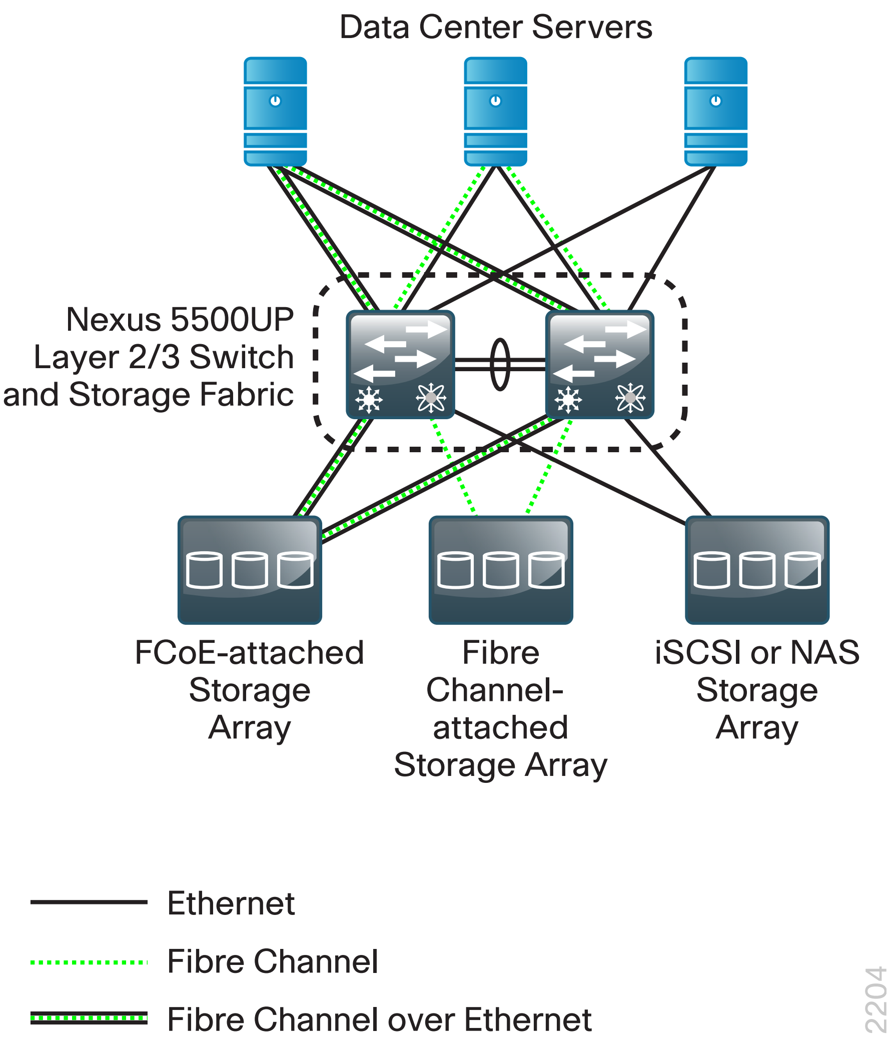
The Cisco Integrated Management Controller (Cisco IMC) is the management service for Cisco UCS C-Series servers. Cisco IMC runs within the server. Cisco IMC allows you to use a web-based GUI or Secure Shell (SSH) Protocol–based CLI to remotely access, configure, administer, and monitor the server. Almost all tasks can be performed in either interface, and the results of tasks performed in one interface are displayed in the other. You can use Cisco IMC to control power, view and configure server properties and sensors, upgrade firmware, and monitor server status.

The Cisco UCS Manager can manage the UCS C-Series servers if the servers are deployed connected to the fabric interconnects via Cisco Nexus 2232PP fabric extenders, as detailed in the *Cisco SBA—Data Center Unified Computing System Deployment Guide*. This type of deployment enables the flexibility of both rack-mounted and blade servers with a single-pane-of-glass management of all Cisco UCS servers in the data center.

Network and Storage Connectivity

The *Cisco SBA—Data Center Virtualization with Cisco UCS, Nexus 1000V, and VMware Deployment Guide* is designed as an extension of the *Data Center Deployment Guide*. The basis of this architecture is an Ethernet switch fabric consisting of two Cisco Nexus 5500UP switches, as shown in the following figure.

Figure 3 - Cisco SBA data center architecture switch fabric


Data Center Servers
Nexus 5500UP
Layer 2/3 Switch
and Storage Fabric
FCoE-attached Storage Array
Fibre Channel-attached Storage Array
iSCSI or NAS Storage Array
Ethernet
Fibre Channel
Fibre Channel over Ethernet
2204

The data center core switch fabric provides Layer 2 and Layer 3 Ethernet switching services to servers and other attached devices. The two Cisco Nexus 5500UP switches form the Ethernet switch fabric using Virtual Port Channel (vPC) technology. This feature provides loop-prevention services and allows the two switches to appear as one logical Layer-2 switching instance to attached devices. In this way, the foundation Ethernet provides the flexibility to extend VLANs across the data center without creating spanning-tree loops and avoiding spanning-tree–blocked links, providing more bandwidth for traffic. The Cisco Nexus 2000 Series Fabric Extenders provide extension of the core switch ports to provide scalable fan-out of Gigabit Ethernet and 10-Gigabit Ethernet ports for server connectivity.

Storage networking is provided for the VMware environment by the data center core Cisco Nexus 5500UP Series switches. The Universal Port (UP) capability allows the switch to provide Ethernet and FCoE or Fibre Channel on any port. This provides your organization with the flexibility to run one or multiple SAN protocols, such as Internet Small Computer System Interface (iSCSI), Fibre Channel, FCoE, or network attached storage (NAS), over a single network core.

Notes

Deployment Details

The following processes guide you through:

- The preparation of the data center shared storage environment for VMware installation.
- The installation and setup of VMware vSphere virtualization on Cisco UCS B-Series blade servers and Cisco UCS C-Series rack-mount servers.
- The installation and deployment of Cisco Nexus 1000V Series switch in a VMware environment.

Preparing the Environment for VMware

If you will be using shared storage for your VMware installation, this section will guide you through the steps necessary to access shared storage via Fibre Channel. If you are using iSCSI to access shared storage, you will still need to provision storage logical unit numbers (LUNs) on your storage array for your VMware virtual machines.

Process

Preparing the Environment for Server Access to SAN

1. Configure a storage array
2. Configure SAN zones
3. Configure service profiles on UCS Manager

If you are installing VMware on a Cisco UCS B-Series server, the target server for installing VMware must have a configured service profile associated with that server. The service profile contains all of the information and settings that are applied to the server. Detailed instructions for configuring and installing the Cisco UCS B-Series Blade Server system are contained in the *Cisco SBA—Data Center Unified Computing System Deployment Guide*.

Procedure 1 and Procedure 2 of this process are also necessary if your server will be using Fibre Channel SAN–based shared storage for virtual machines on the Cisco UCS B-Series or C-Series servers.

The ability to boot your VMware server from storage area network (SAN) enables a stateless computing environment where the server can be provisioned on demand without requiring the operating system to be preloaded on disks that physically reside on the server you are using. With boot-from–Fibre Channel SAN, the operating system software image resides on the storage array connected to the Fibre Channel SAN, and the server communicates with the SAN through a virtual host bus adapter (vHBA). The vHBA's BIOS contain the instructions that enable the server to find the boot disk. The Cisco UCS M81KR and M82-8P VIC in the Cisco UCS B-Series server is capable of booting from SAN.

There are three distinct phases of the process for preparing the environment for Cisco UCS B-Series to boot-from-SAN:

1. Storage array configuration
2. SAN zone configuration
3. Cisco UCS B-Series service profile configuration

Procedure 1 Configure a storage array

This installation procedure provides a summary for configuring storage when you are using a NetApp FAS3200 storage array, which was used in the Cisco SBA data center validation. For detailed steps for creating logical unit numbers (LUNs), initiator groups, and mapping, please refer to the *Cisco SBA—Data Center NetApp Storage Deployment Guide*. If you are using another manufacturer's storage array, the requirements are similar, but the exact steps may differ.

First, the storage array administrator has to provision LUNs of the required size for installing the operating system and to enable boot-from-SAN. The boot-from-SAN LUN should be LUN 0. The SAN administrator also needs to know the Fibre Channel World Wide Port Name (WWPN) of the adapter to perform the necessary LUN masking. LUN masking is a critical step in the SAN LUN configuration.

The LUN masking procedure is storage array–specific and is usually done using the array's device manager or CLI.

If you are installing to a bootable SAN device, configure a LUN on the SAN, connect to the SAN, and verify that only one path exists from the SAN vHBA to the LUN. In this design, you use Fibre Channel to connect the NetApp storage array to the data center core Cisco Nexus 5500UP switches that are running Fibre Channel switching. The following is a summary of the steps to prepare the NetApp storage array for Cisco UCS B-Series SAN boot, or for UCS B-Series or C-Series access to Fibre Channel SAN–based shared storage for virtual machines. Configuration of the NetApp storage array uses NetApp System Manager.

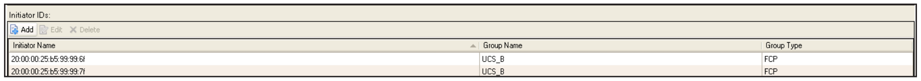
Step 1: Log in to the NetApp System Manager using the username root and the password you configured on the NetApp.

Step 2: Under **Storage**, click **LUNs**.

Step 3: On the right pane, in the LUN Management tab, click **Create**, and then follow the Create LUN Wizard to create a new LUN.

Step 4: In the Initiator groups tab, create an FC or FCoE initiator group.

Step 5: In the initiator group that you just created, for initiator IDs, enter the WWPNs of the newly added vHBAs in the Cisco UCS B-Series server.


Initiator IDs:

Initiator Name	Group Name	Group Type
20:00:00:25:b5:99:99:6f	UCS_B	FCP
20:00:00:25:b5:99:99:7f	UCS_B	FCP

Step 6: After the LUN and initiator groups are created, map the LUN to the initiator group. LUN 0 is used for boot volumes.

Procedure 2 Configure SAN zones

SAN zoning maps the vHBA from the Cisco UCS B-Series blade server to the target boot LUN on the Fibre Channel SAN fabric. The vHBA has to have complete visibility to the array LUN in order for boot-from-SAN to succeed. To create a zone and zoneset, configure the following on the data center core Cisco Nexus 5500UP switches. For detailed Fibre Channel SAN setup see the *Cisco SBA—Data Center Deployment Guide*. The example Fibre Channel SAN numbering is continued from the *Data Center Deployment Guide*.

Table 1 - Fibre Channel SAN zones

Data center core switch	Fibre Channel VSAN number	FCoE VSAN number	SAN fabric
Nexus 5548UP-1	4	304	SAN-A
Nexus 5548UP-2	5	305	SAN-B

This procedure configures the zoning for the initiating server vHBA1 WWPN and the target boot LUN WWPN provided by the storage array administrator.

Step 1: Log in to the console of the first Nexus 5500UP switch and create a zone.

Example

```
zone name p11-ucs-b-hbafc0-a-NETAPP1 vsan 4
  member pwwn 20:00:00:25:b5:99:99:7f
  member pwwn 50:0a:09:82:89:ea:df:b1
```

Step 2: Add the zone created in Step 1 to an existing zoneset, or create a new zoneset if none exists.

```
zoneset name FCOE_4 vsan 4
  member p11-ucs-b-hbafc0-a-NETAPP1
```

Step 3: Activate the zoneset.

```
zoneset activate  name FCOE_4 vsan 4
```

Reader Tip

Always execute the **zoneset activate** command when you make changes to zones. If you don't, the zone never becomes activated and remains in the inactive state. If you need to create a new virtual SAN (VSAN), follow the steps from the *Cisco SBA—Data Center Deployment Guide*.

Step 4: When the operation is completed, check to see if the above zone becomes active.

```
dc5548#  show zone active vsan 4
zone name p11-ucs-b-hbafc0-a-NETAPP1 vsan 4
* fcid 0xdf0006 [pwwn 20:00:00:25:b5:99:99:7f]
* fcid 0xdf0004 [pwwn 50:0a:09:82:89:ea:df:b1] [NetApp-1-e2a-
FCOE]
```

Step 5: For the second vHBA connected to the second Cisco Nexus 5500 Series switch, repeat the preceding Step 1 through Step 4.

Procedure 3 Configure service profiles on UCS Manager

For detailed steps for creating service profiles, please see the *Cisco SBA—Data Center Unified Computing System Deployment Guide*.

The VMware setup includes four virtual Ethernet NICs (vNICs) and two virtual Fibre Channel host bus adapters (vHBAs) defined in a Cisco UCS service profile. These are presented to the vSphere ESXi operating system as VMNICs and VMHBAs. Two of the VMNICs are provisioned to manage the ESXi host. The remaining VMNICs will carry traffic corresponding to virtual machines, vMotion, and IP storage.

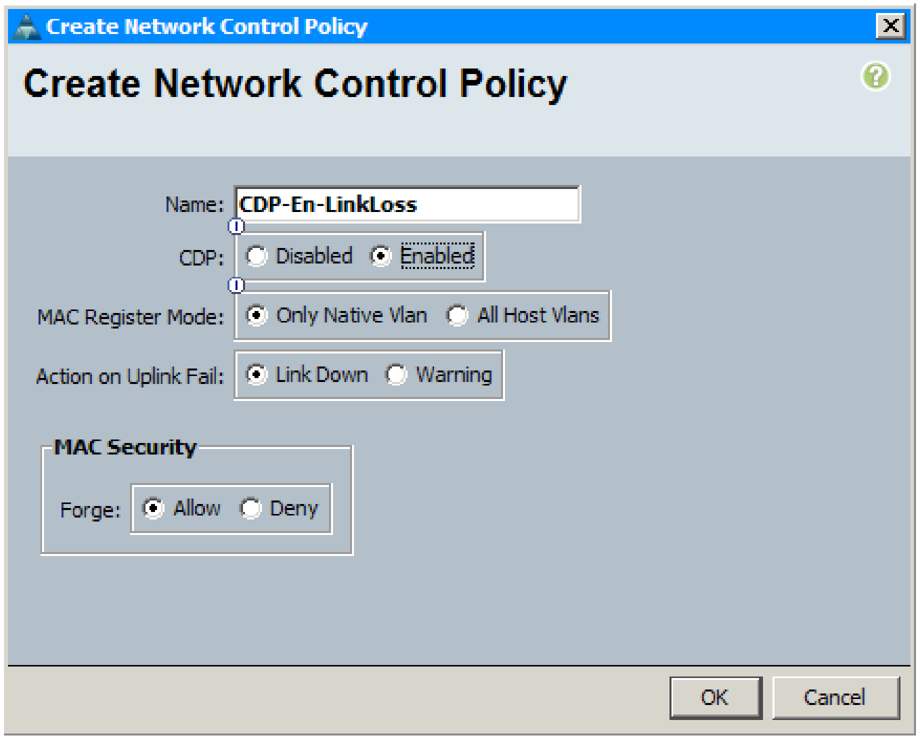
The Cisco UCS M81KR Virtual Interface Card used in the Cisco UCS B-Series blade servers supports fabric failover. Internally, each of the two blade server's converged network adapters is connected to each of the two Cisco UCS 2208XP or 2204XP Fabric Extenders through the chassis mid-plane. Loss of connectivity on a path in use causes traffic to be remapped through a redundant path within Cisco UCS. When fabric failover is enabled on a vNIC, the MAC address of the adapter (*implicit* MAC address) and the MAC address of a virtual machine (*learned* MAC address) are synced to the peer fabric interconnects automatically. When a failover occurs, the second fabric interconnect sends gratuitous Address Resolution Protocol (ARP) packets upstream for both implicit and learned MAC addresses so that the external network knows that the new path goes through the second fabric interconnect.

It is recommended that you not enable fabric failover for the ESX server running vSwitch, Distributed Virtual Switch, or Cisco Nexus 1000V. You will define a link-down network control policy to push a notification to Nexus 1000V switch in the event that one of the fabric interconnects completely fails. The link-down notification will cause the Nexus 1000V switch to route network traffic onto the backup link to the second fabric interconnect.

In this design, the soft switch sees a failed path, and the vNIC goes to state down and issue gratuitous ARP packets on behalf of the connected VMs. This requires the use of VMware's NIC teaming or Cisco Nexus 1000V vPC Host-mode, which is discussed in the later sections of this guide.

Step 1: In Cisco UCS Manager, select **LAN > root > Network Control Policies**, right-click **Network Control Policies**, and then click **Create Network Control Policy**.

Step 2: Name the policy, select CDP **Enabled** and **Link Down**, and then click **OK**.



Name: CDP-En-LinkLoss

CDP: ○ Disabled ● Enabled

MAC Register Mode: ● Only Native Vlan ○ All Host Vlans

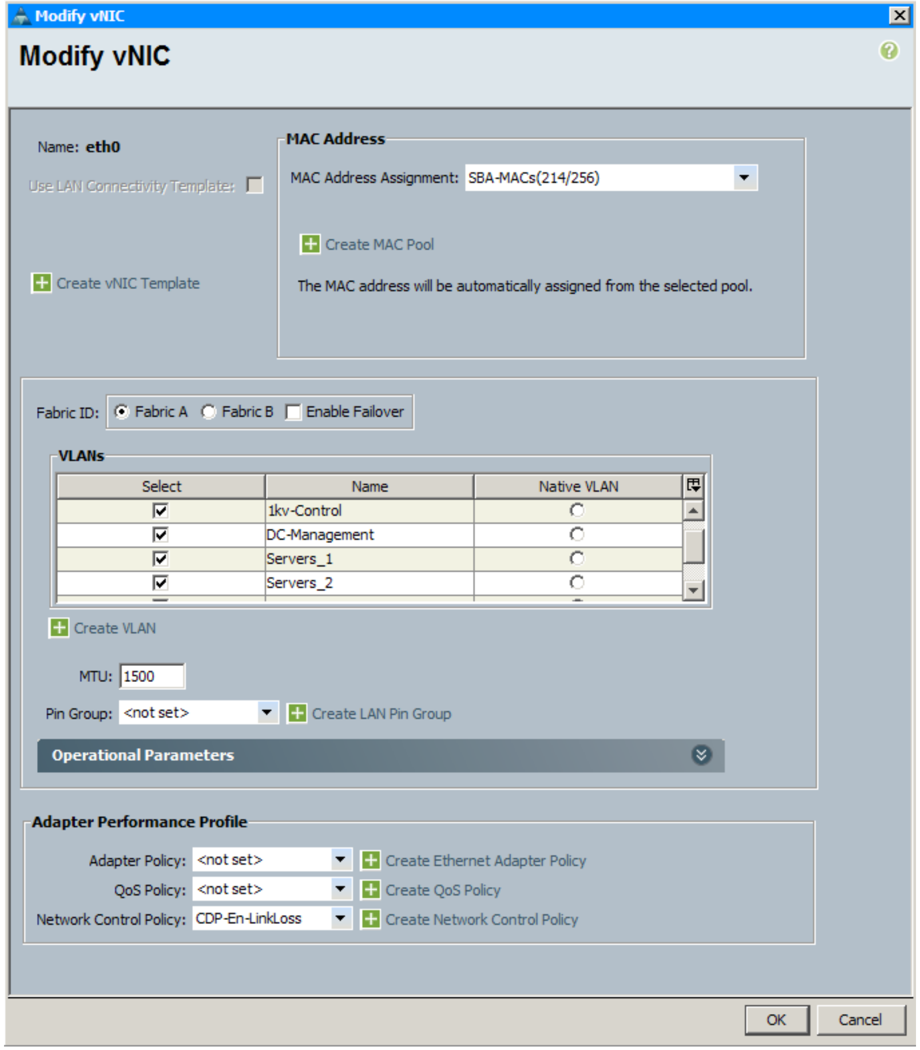
Action on Uplink Fail: ● Link Down ○ Warning

Forge: ● Allow ○ Deny

Step 3: In the navigation pane, click the Servers tab, select the service profile that you plan to assign to the server, and then in the work pane, click the Network tab.

Step 4: Select the vNIC that you previously created in the *Data Center Unified Computing System Deployment Guide*, and then at the bottom of the screen, click **Modify**.

Step 5: Clear **Enable Failover**, and then in the Adapter Performance Profile section, in the **Network Control Policy** drop down, choose the control policy created in Step 2, and then click **OK**. It is recommended that you do not enable fabric failover for the virtual switch uplinks.



Modify vNIC

Name: eth0

Use LAN Connectivity Template: □

MAC Address

MAC Address Assignment: SBA-MACs(214/256)

The MAC address will be automatically assigned from the selected pool.

Fabric ID: ● Fabric A ○ Fabric B □ Enable Failover

VLANs

Select	Name	Native VLAN
☑	1kv-Control	○
☑	DC-Management	○
☑	Servers_1	○
☑	Servers_2	○

MTU: 1500

Pin Group: <not set>

Adapter Performance Profile

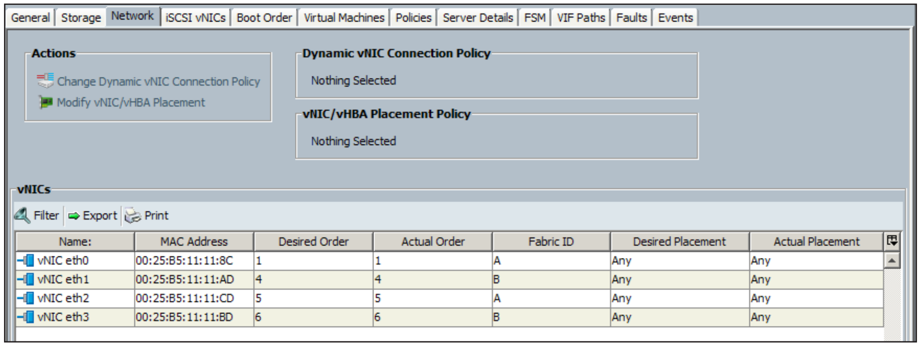
Adapter Policy: <not set>

QoS Policy: <not set>

Network Control Policy: CDP-En-LinkLoss

Step 6: If you need to add additional vNICs to the profile, at the bottom of the Network tab, click the plus sign (**+**).

Step 7: Connect vNIC ETH0 and vNIC ETH2 to Fabric A, and then connect vNIC ETH1 and vNIC ETH3 to Fabric B. ETH0 and ETH1 will carry management traffic, and ETH2 and ETH 3 will carry the rest of the traffic, such as virtual machine and storage traffic. You have created total of four vNICS, with failover disabled.



Dynamic vNIC Connection Policy

Nothing Selected

vNIC/vHBA Placement Policy

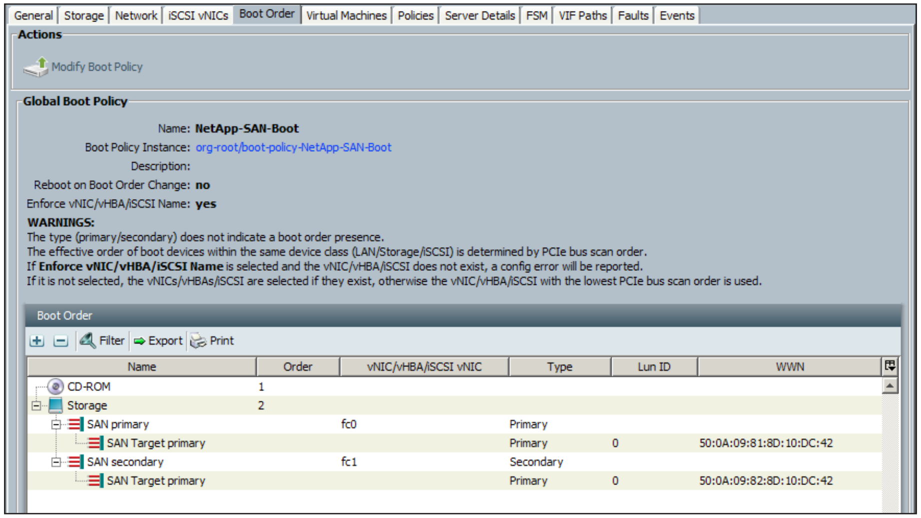
Nothing Selected

vNICs

Name:	MAC Address	Desired Order	Actual Order	Fabric ID	Desired Placement	Actual Placement
vNIC eth0	00:25:B5:11:11:8C	1	1	A	Any	Any
vNIC eth1	00:25:B5:11:11:AD	4	4	B	Any	Any
vNIC eth2	00:25:B5:11:11:CD	5	5	A	Any	Any
vNIC eth3	00:25:B5:11:11:BD	6	6	B	Any	Any

Step 8: Select a service profile.

Step 9: On the Boot Order tab, ensure that you have configured the correct boot policy (either SAN Boot policy or Local Disk boot policy). If you are using SAN boot policy, ensure that the SAN boot target configurations are correct.



Global Boot Policy

Name: **NetApp-SAN-Boot**

Boot Policy Instance: org-root/boot-policy-NetApp-SAN-Boot

Description:

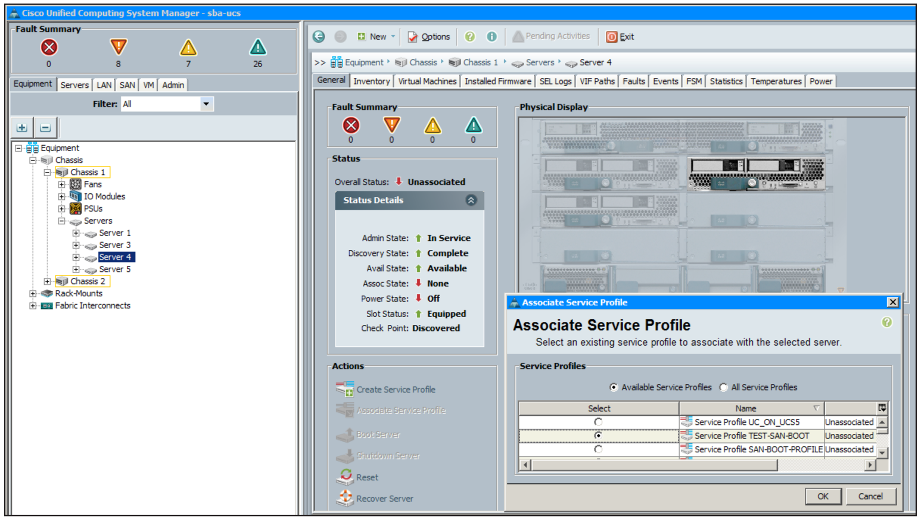
Reboot on Boot Order Change: **no**

Enforce vNIC/vHBA/iSCSI Name: **yes**

WARNINGS:
The type (primary/secondary) does not indicate a boot order presence.
The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.
If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.
If it is not selected, the vNICs/vHBAs/iSCSI are selected if they exist, otherwise the vNIC/vHBA/iSCSI with the lowest PCIe bus scan order is used.

Name	Order	vNIC/vHBA/iSCSI vNIC	Type	Lun ID	WWN
CD-ROM	1				
Storage	2				
SAN primary		fc0	Primary		
SAN Target primary			Primary	0	50:0A:09:81:8D:10:DC:42
SAN secondary		fc1	Secondary		
SAN Target primary			Primary	0	50:0A:09:82:8D:10:DC:42

Step 10: After the service profile is created and boot policy is assigned, associate the service profile to an open server on the chassis. The server automatically boots with the new service policy.



Status

Overall Status: Unassociated

Status Details

Admin State: In Service
Discovery State: Complete
Avail State: Available
Assoc State: None
Power State: Off
Slot Status: Equipped
Check Point: Discovered

Associate Service Profile

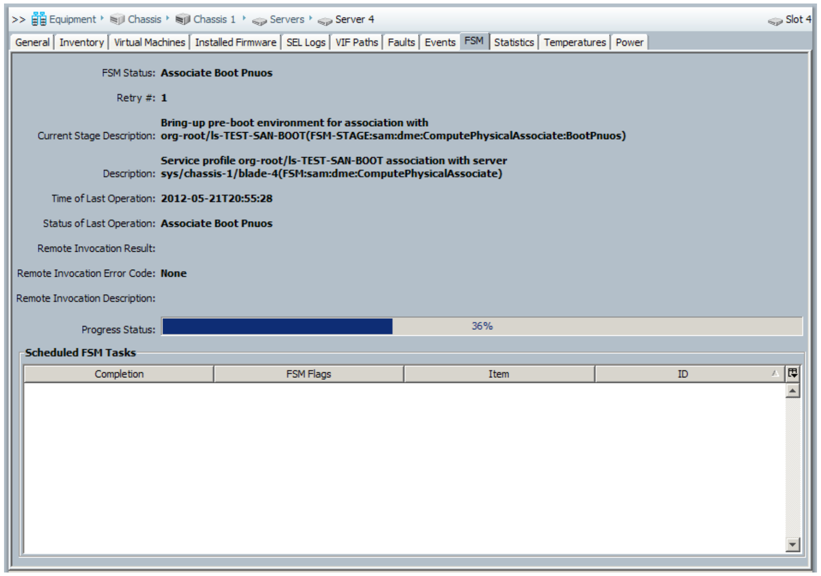
Select an existing service profile to associate with the selected server.

Service Profiles

● Available Service Profiles ○ All Service Profiles

Select	Name	
○	Service Profile UC_ON_UCS5	Unassociated
●	Service Profile TEST-SAN-BOOT	Unassociated
○	Service Profile SAN-BOOT-PROFILE	Unassociated

Step 11: In the work pane, on the FSM tab, check the progress of the service profile that is being applied on the server.



FSM Status: Associate Boot Pnuos

Retry #: 1

Current Stage Description: Bring-up pre-boot environment for association with org-root/ls-TEST-SAN-BOOT(FSM-STAGE:sam:dme:ComputePhysicalAssociate:BootPnuos)

Description: Service profile org-root/ls-TEST-SAN-BOOT association with server sys/chassis-1/blade-4(FSM:sam:dme:ComputePhysicalAssociate)

Time of Last Operation: 2012-05-21T20:55:28

Status of Last Operation: Associate Boot Pnuos

Remote Invocation Result:

Remote Invocation Error Code: None

Remote Invocation Description:

Progress Status: 36%

Scheduled FSM Tasks

Completion	FSM Flags	Item	ID

This completes the association of a service profile to the Cisco UCS B-Series server.

VMware vSphere Installation and Setup

Process

Installing VMware ESXi on Cisco UCS Servers

1. Mapping the ESXi ISO file using virtual KVM
2. Install vSphere hypervisor (ESXi)

Before you install VMware vSphere, ensure that you have the following information:

- IP address, subnet mask, and default gateway for ESXi hosts
- Host names for ESXi hosts
- Primary domain name for the ESXi hosts
- Primary and secondary Domain Name System (DNS) IP addresses
- Password for the ESXi management console

You can install VMware ESXi by using an ISO burned with the proper utility to a CD or mounted as remote media on the Cisco Integrated Management Controller (Cisco IMC). This example shows you how to use the virtual keyboard, video and mouse (KVM) console Virtual Media to install ESXi from a local ISO on your desktop, running the Cisco UCS Manager in your browser.

Some processes and steps in this section are specific to the Cisco UCS B-Series server and some specific to the UCS C-Series server. Where appropriate, the differences are noted.

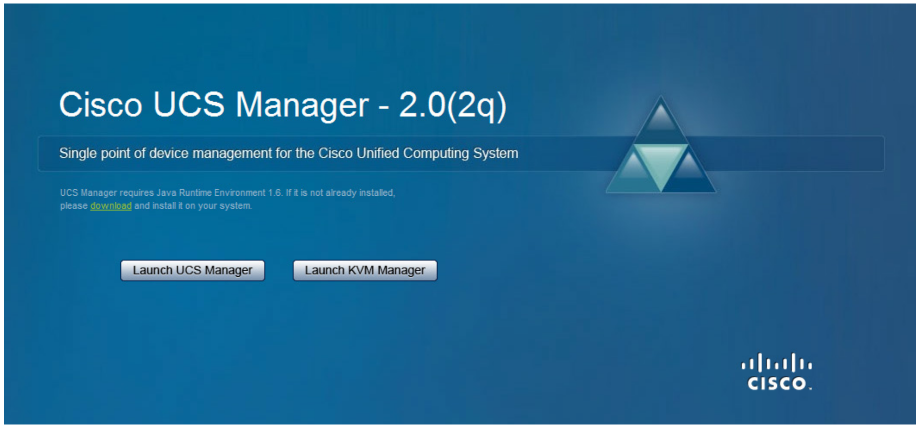
Procedure 1 Mapping the ESXi ISO file using virtual KVM

If you are using a Cisco UCS B-Series server, complete Option 1. If you are using a Cisco UCS C-Series server, complete Option 2.

Option 1. For a Cisco UCS B-Series server

Step 1: Use a browser to connect to Cisco UCS Manager using your UCS Virtual Management IP address.

Step 2: Click **Launch UCS Manager**, and then log in to Cisco UCS Manager, using your administrator username and password.



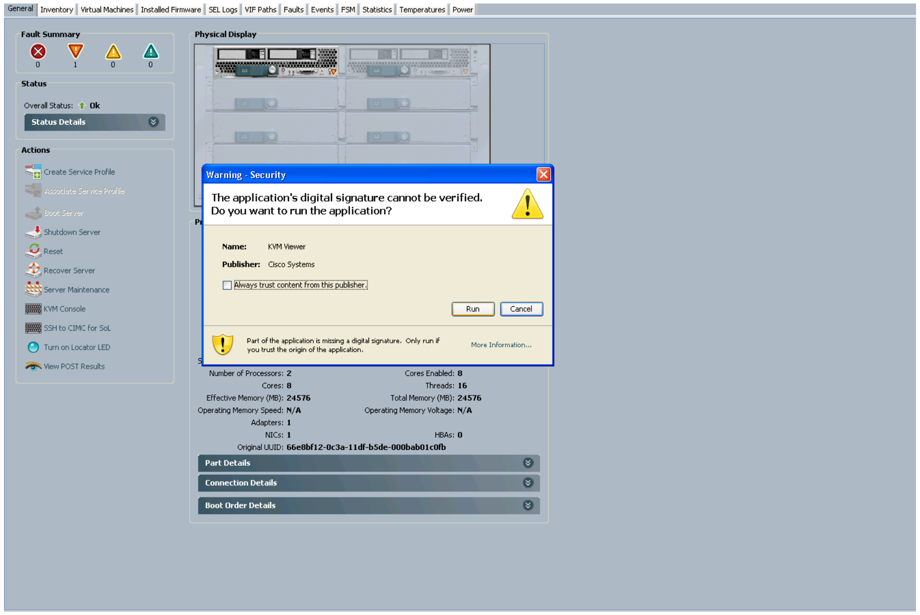
Cisco UCS Manager - 2.0(2q)

Single point of device management for the Cisco Unified Computing System

UCS Manager requires Java Runtime Environment 1.6. If it is not already installed, please download and install it on your system.

In the navigation pane, on the Equipment tab, expand **Equipment > Chassis > Chassis_Number > Servers**, and then choose the server that you want to access through the KVM console.

Step 3: In the work pane, on the General tab, in the Actions area, click **KVM Console**. The KVM console opens in a separate window.



Warning - Security

The application's digital signature cannot be verified.
Do you want to run the application?

Name: KVM Viewer

Publisher: Cisco Systems

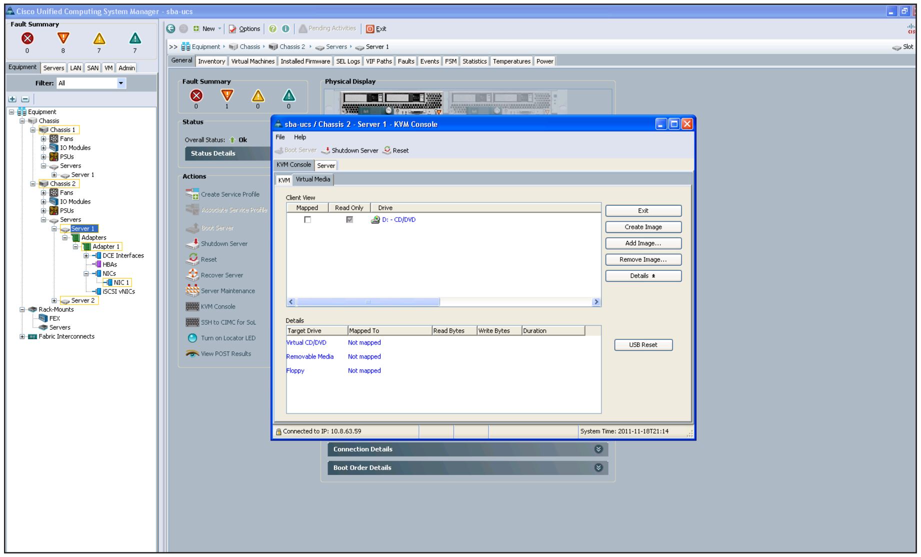
□ Always trust content from this publisher.

Part of the application is missing a digital signature. Only run if you trust the origin of the application.

Number of Processors: 2 Cores Enabled: 8
Cores: 8 Threads: 16
Effective Memory (MB): 24576 Total Memory (MB): 24576
Operating Memory Speed: N/A Operating Memory Voltage: N/A
Adapters: 1
NICs: 1 HBAs: 0
Original UUID: 66e8bf12-0c3a-11df-b5de-000bab01c0fb

Overall Status: Ok

Step 4: In the KVM console window, on the KVM Console tab, click the secondary **Virtual Media** tab.



sba-ucs / Chassis 2 - Server 1 - KVM Console

Client View

Mapped	Read Only	Drive
□	☑	D: - CD/DVD

Details

Target Drive	Mapped To	Read Bytes	Write Bytes	Duration
Virtual CD/DVD	Not mapped			
Removable Media	Not mapped			
Floppy	Not mapped			

Connected to IP: 10.8.63.59

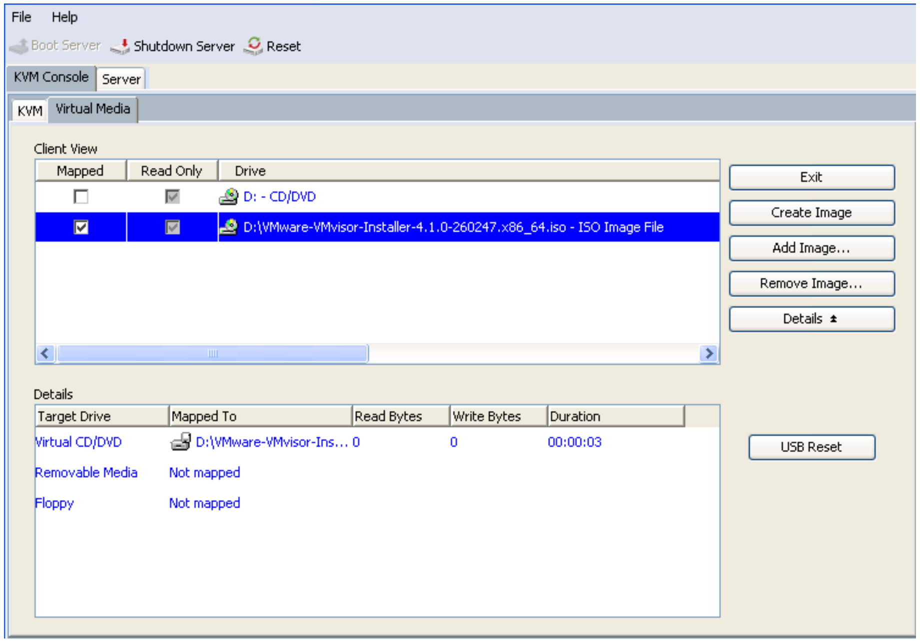
System Time: 2011-11-18T21:14

Step 5: Click **Add Image**, navigate to the VMware-VMvisor ISO file, and then select it. The ISO image is displayed as a device in the Client View pane.

Step 6: For the ISO image you added in the preceding step, select the **Mapped** check box, and then wait for mapping to be completed. Observe the progress in the Details pane. Do not press exit here, and leave the window open while the file downloads.

Tech Tip

Leave the KVM Virtual Media window open, and do not press exit until you are told to in Step 5 of the next procedure, "Install vSphere hypervisor (ESXi)".



Client View

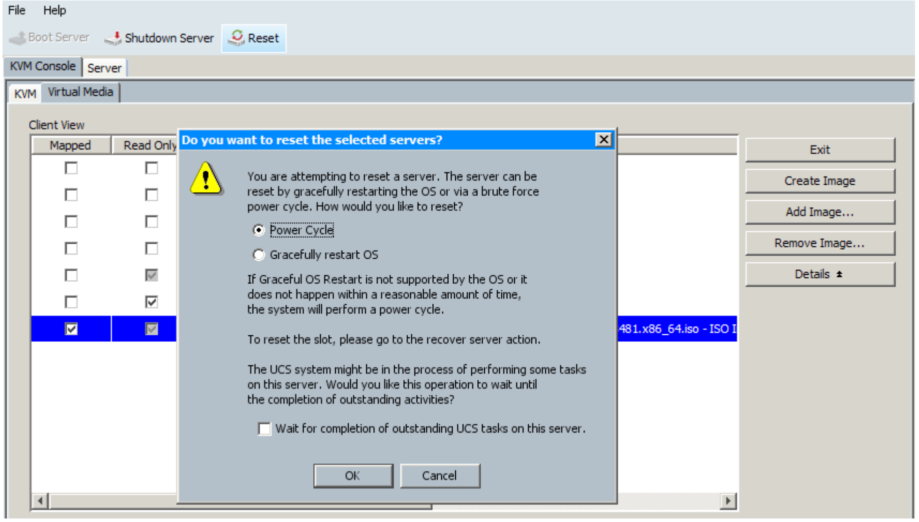
Mapped	Read Only	Drive
☐	☑	D: - CD/DVD
☑	☑	D:\VMware-VMvisor-Installer-4.1.0-260247.x86_64.iso - ISO Image File

Details

Target Drive	Mapped To	Read Bytes	Write Bytes	Duration
Virtual CD/DVD	D:\VMware-VMvisor-Ins...	0	0	00:00:03
Removable Media	Not mapped			
Floppy	Not mapped			

Step 7: When mapping is complete, at the top of the screen, click **Reset**.

Step 8: Select **Power Cycle**, and then click **OK**. This cycles power on the server so that the server reboots from the virtual CD/DVD that is mapped to the ISO installation image, and the BIOS recognizes the media that was just added. The server uses the boot order that is defined in its Cisco UCS Manager service profile.



Do you want to reset the selected servers?

You are attempting to reset a server. The server can be reset by gracefully restarting the OS or via a brute force power cycle. How would you like to reset?

● Power Cycle

○ Gracefully restart OS

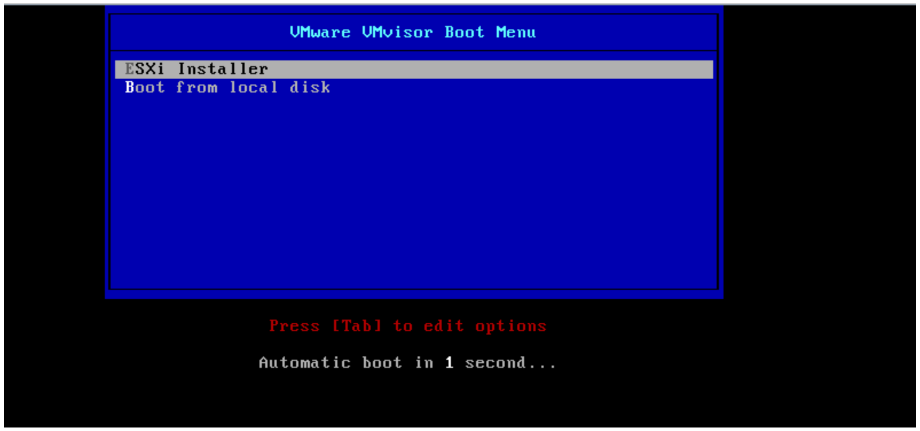
If Graceful OS Restart is not supported by the OS or it does not happen within a reasonable amount of time, the system will perform a power cycle.

To reset the slot, please go to the recover server action.

The UCS system might be in the process of performing some tasks on this server. Would you like this operation to wait until the completion of outstanding activities?

☐ Wait for completion of outstanding UCS tasks on this server.

Step 9: When the VMware VMvisor Boot Menu appears, select **ESXi Installer**. In the next procedure, you continue configuration in the ESXi Installer.



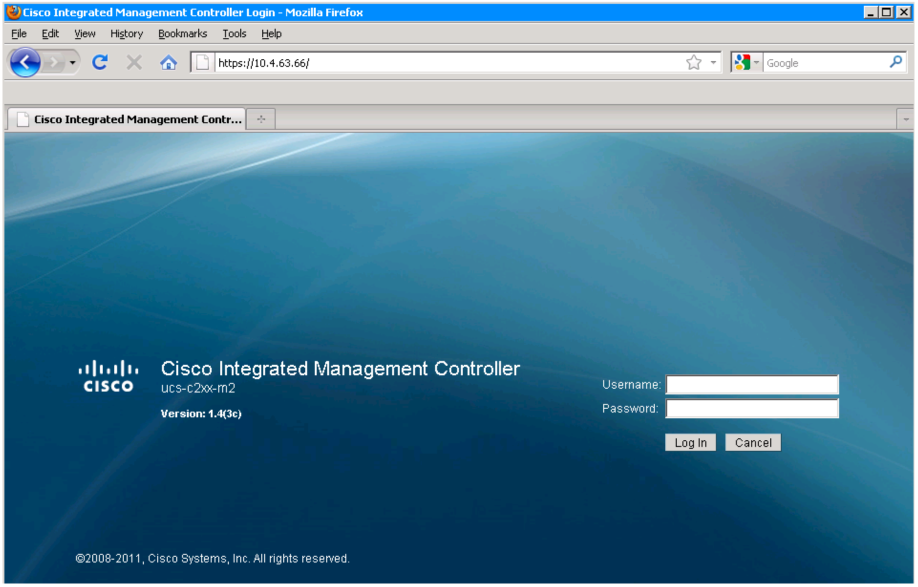
```
VMware VMvisor Boot Menu

ESXi Installer
Boot from local disk

Press [Tab] to edit options

Automatic boot in 1 second...
```

Option 2. For a Cisco UCS C-Series server

Detailed deployment for programming the Cisco UCS C-Series server management interface, the Cisco Integrated Management Controller (Cisco IMC), is provided in the *Cisco SBA—Data Center Unified Computing System Deployment Guide*. It is assumed that you have completed the UCS C-Series preparation before beginning this procedure.

Step 1: In a browser, enter the Cisco IMC IP address.

Step 2: Log in by using the administrator username and password you set when you configured Cisco IMC.



Cisco Integrated Management Controller Login - Mozilla Firefox

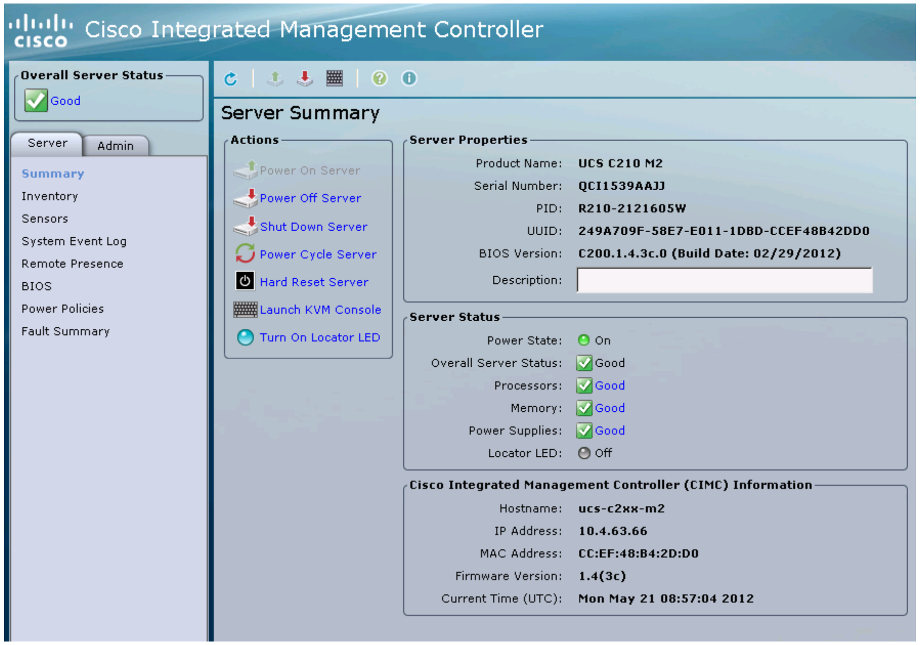
https://10.4.63.66/

Cisco Integrated Management Controller
ucs-c2xx-m2
Version: 1.4(3c)

Username:
Password:

©2008-2011, Cisco Systems, Inc. All rights reserved.

Step 3: On the Server tab, click **Summary**, and then in the work pane, click **Launch KVM Console**.



Cisco Integrated Management Controller

Overall Server Status: Good

Server Summary

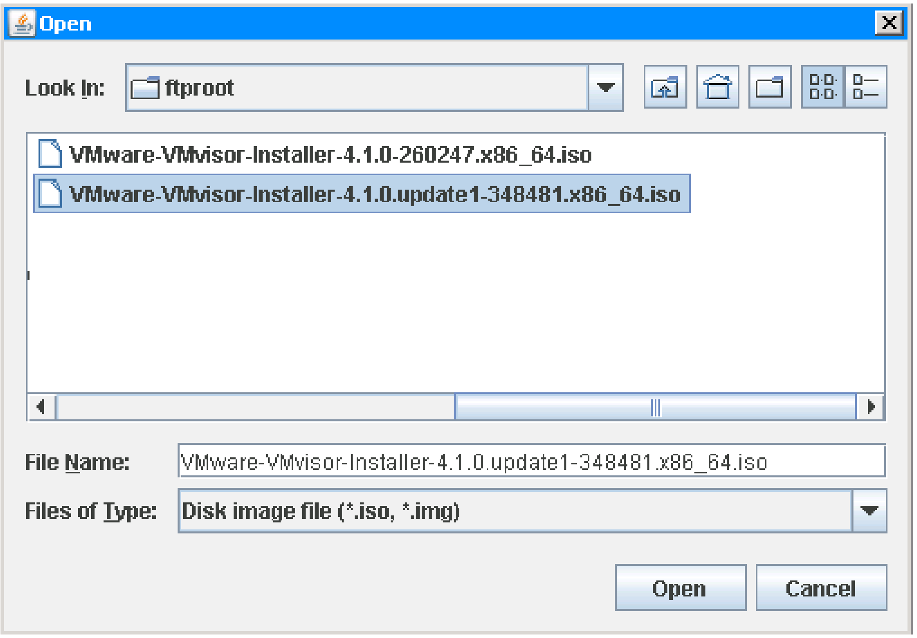
Server Properties
Product Name: UCS C210 M2
Serial Number: QCI1539AAJJ
PID: R210-2121605W
UUID: 249A709F-58E7-E011-1DBD-CCEF48B42DD0
BIOS Version: C200.1.4.3c.0 (Build Date: 02/29/2012)
Description:

Server Status
Power State: On
Overall Server Status: Good
Processors: Good
Memory: Good
Power Supplies: Good
Locator LED: Off

Cisco Integrated Management Controller (CIMC) Information
Hostname: ucs-c2xx-m2
IP Address: 10.4.63.66
MAC Address: CC:EF:48:B4:2D:D0
Firmware Version: 1.4(3c)
Current Time (UTC): Mon May 21 08:57:04 2012

Step 4: In the KVM console, click the **VM** tab.

Step 5: In the Open dialog box, click **Add Image**, select your ISO file, and then click **Open**.



Open

Look In: ftproot

VMware-VMvisor-Installer-4.1.0-260247.x86_64.iso

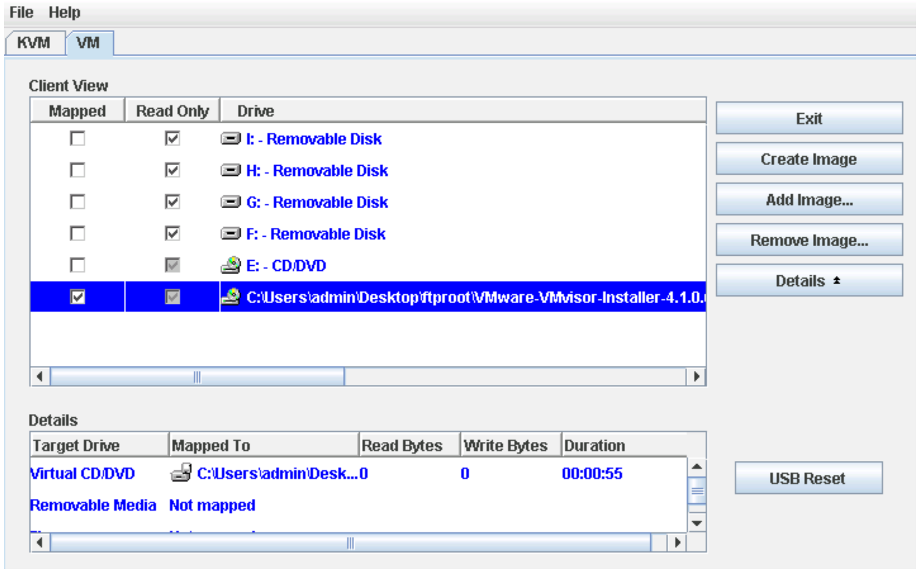
VMware-VMvisor-Installer-4.1.0.update1-348481.x86_64.iso

File Name: VMware-VMvisor-Installer-4.1.0.update1-348481.x86_64.iso

Files of Type: Disk image file (*.iso, *.img)

Open | Cancel

Step 6: For the image you selected in the preceding step, select the **Mapped** check box. Do not click **Exit**.



File Help

KVM | VM

Client View

Mapped	Read Only	Drive
□	☑	I: - Removable Disk
□	☑	H: - Removable Disk
□	☑	G: - Removable Disk
□	☑	F: - Removable Disk
□	☑	E: - CD/DVD
☑	☑	C:\Users\admin\Desktop\ftproot\VMware-VMvisor-Installer-4.1.0.

Exit | Create Image | Add Image... | Remove Image... | Details

Details

Target Drive	Mapped To	Read Bytes	Write Bytes	Duration
Virtual CD/DVD	C:\Users\admin\Desk...0		0	00:00:55
Removable Media	Not mapped			

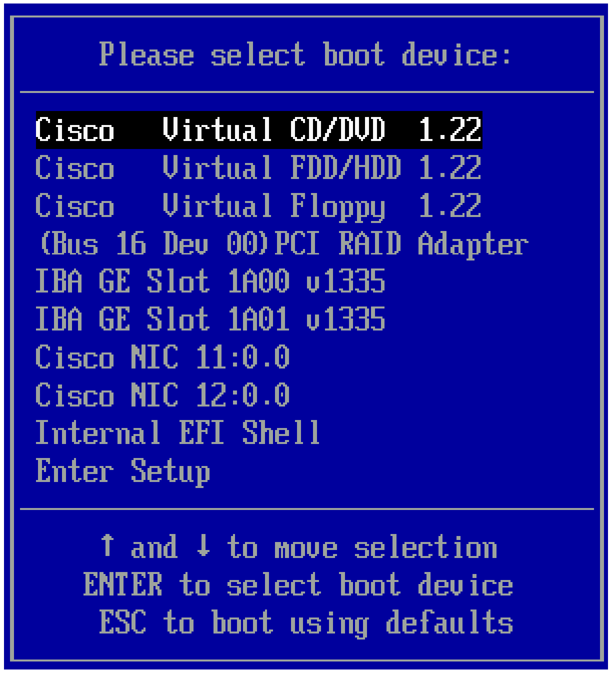
USB Reset

Tech Tip

Leave the KVM Virtual Media window open, and do not press exit until you are told to in Step 5 of the next procedure, “Install vSphere hypervisor (ESXi)”.

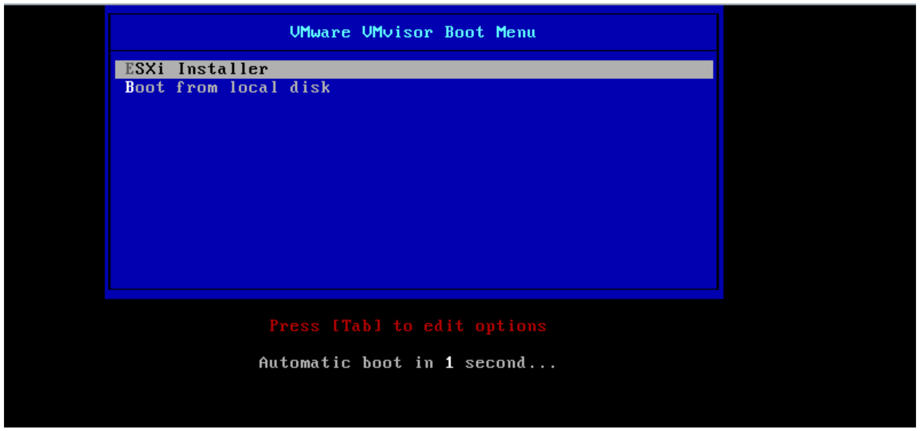
Step 7: On the KVM tab, in the menu bar, choose **Macros**, and then press **Ctrl-Alt-Del**. This reboots the server.

Step 8: When the server reboots, press **F6** to enter the boot menu, and then select **Cisco Virtual CD/DVD**. Selecting the correct boot device enables files from the ISO file to be read and the ESXi installation to begin.



```
Please select boot device:

Cisco    Virtual CD/DVD   1.22
Cisco    Virtual FDD/HDD  1.22
Cisco    Virtual Floppy   1.22
(Bus 16 Dev 00)PCI RAID Adapter
IBA GE Slot 1A00 v1335
IBA GE Slot 1A01 v1335
Cisco NIC 11:0.0
Cisco NIC 12:0.0
Internal EFI Shell
Enter Setup

↑ and ↓ to move selection
ENTER to select boot device
ESC to boot using defaults
```

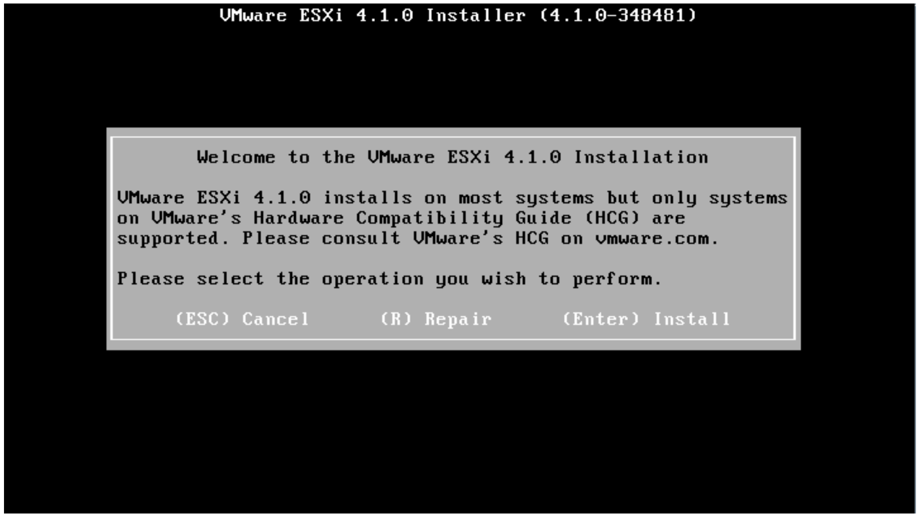
Step 9: When the VMware VMvisor Boot Menu appears, select **ESXi Installer**.



```
VMware VMvisor Boot Menu

ESXi Installer
Boot from local disk

Press [Tab] to edit options

Automatic boot in 1 second...
```

Procedure 2 Install vSphere hypervisor (ESXi)

Step 1: Wait until the following screen is displayed, and then press **Enter**.

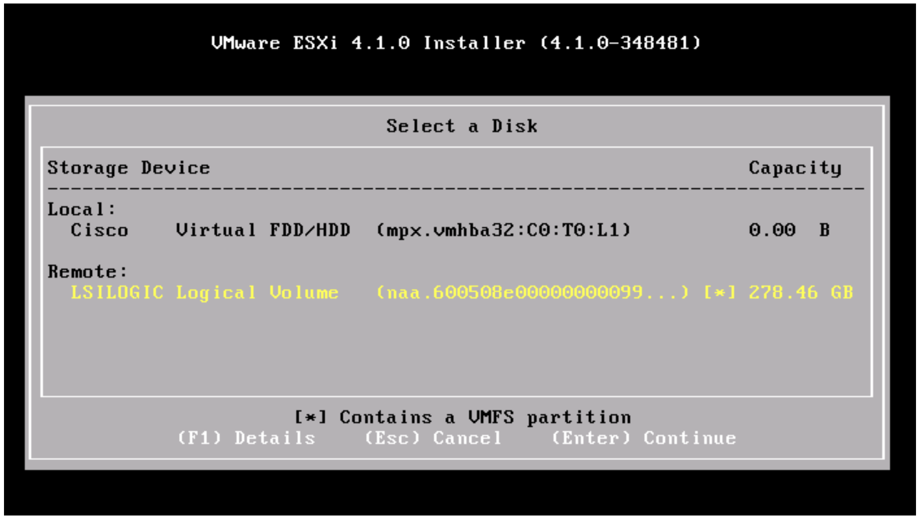


```
VMware ESXi 4.1.0 Installer (4.1.0-348481)

Welcome to the VMware ESXi 4.1.0 Installation

VMware ESXi 4.1.0 installs on most systems but only systems
on VMware's Hardware Compatibility Guide (HCG) are
supported. Please consult VMware's HCG on vmware.com.

Please select the operation you wish to perform.

(ESC) Cancel        (R) Repair        (Enter) Install
```

Step 2: On the End User License Agreement screen, press **F11.**

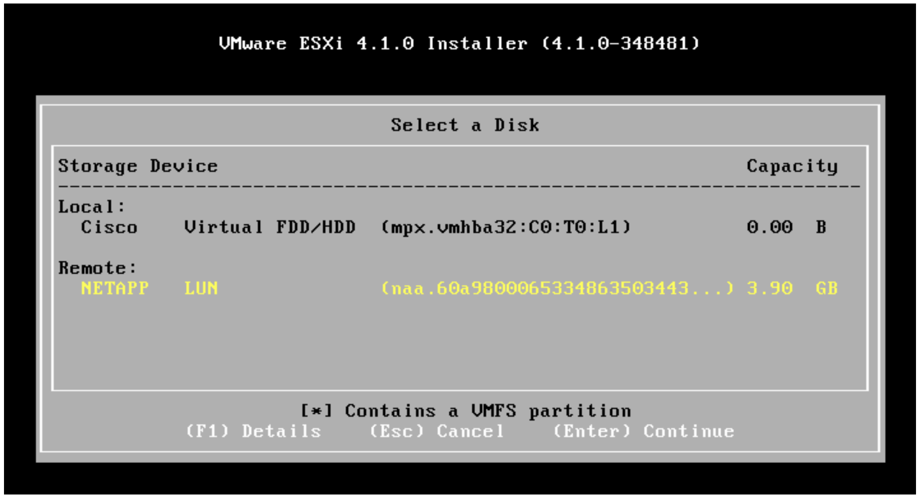
Step 3: If you are installing on a Cisco UCS B-Series server, select the installation target LUN on a storage array or a local disk, and then press **Enter**.

Figure 4 - Cisco UCS B-Series local disk



```
                   VMware ESXi 4.1.0 Installer (4.1.0-348481)

                              Select a Disk

 Storage Device                                                   Capacity
 ---------------------------------------------------------------------------
 Local:
   Cisco    Virtual FDD/HDD  (mpx.vmhba32:C0:T0:L1)               0.00  B

 Remote:
   LSILOGIC Logical Volume   (naa.600508e00000000099...) [*] 278.46 GB

                        [*] Contains a VMFS partition
              (F1) Details    (Esc) Cancel    (Enter) Continue
```

Figure 5 - Cisco UCS B-Series storage array–based LUN



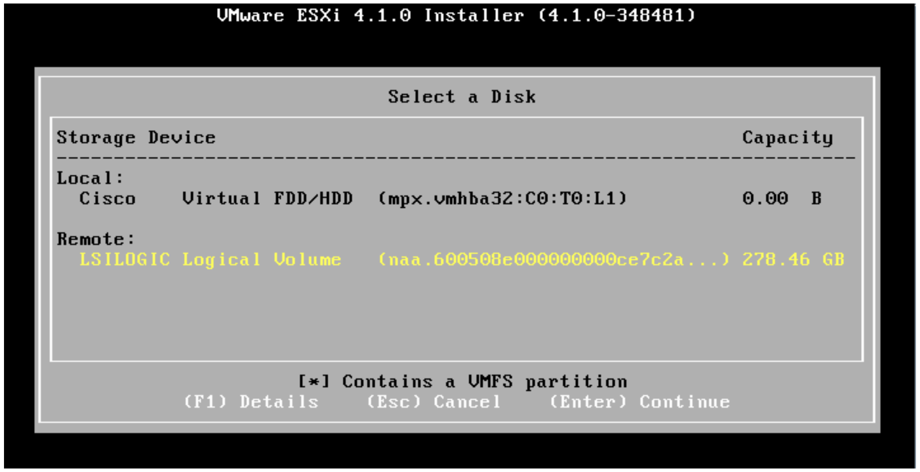
```
                   VMware ESXi 4.1.0 Installer (4.1.0-348481)

                              Select a Disk

 Storage Device                                                   Capacity
 ---------------------------------------------------------------------------
 Local:
   Cisco    Virtual FDD/HDD  (mpx.vmhba32:C0:T0:L1)               0.00  B

 Remote:
   NETAPP   LUN              (naa.60a98000653348635034443...) 3.90  GB

                        [*] Contains a VMFS partition
              (F1) Details    (Esc) Cancel    (Enter) Continue
```

If you are installing on a Cisco UCS C-Series server, you can install the ESXi on either a local disk or a USB thumb drive. Select the appropriate drive, and then press **Enter**.

Tech Tip

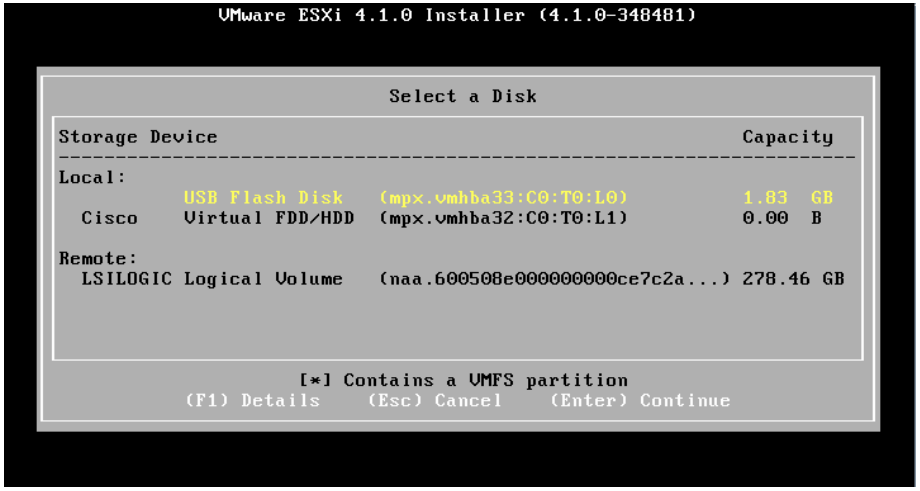
The system alerts you that any existing data on the target drive will be overwritten.

Figure 6 - Cisco UCS C-Series local disk drive



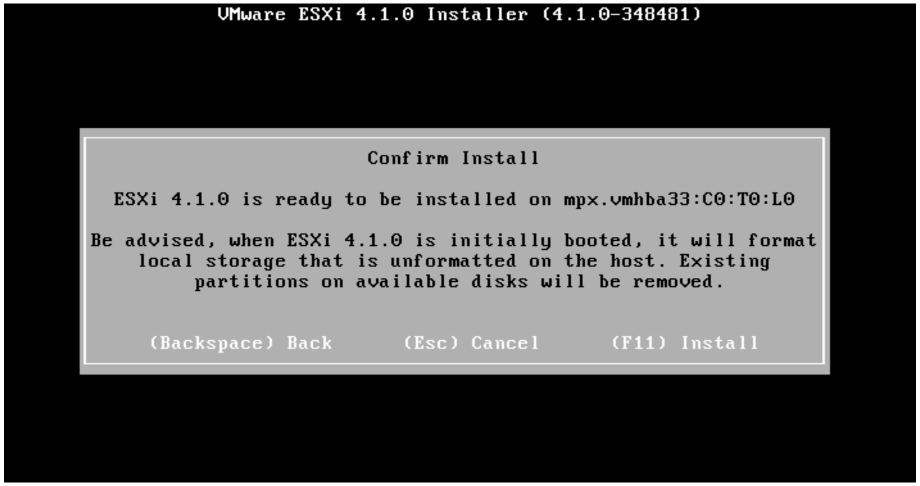
```
                   VMware ESXi 4.1.0 Installer (4.1.0-348481)

                              Select a Disk

 Storage Device                                                   Capacity
 ---------------------------------------------------------------------------
 Local:
   Cisco    Virtual FDD/HDD  (mpx.vmhba32:C0:T0:L1)               0.00  B

 Remote:
   LSILOGIC Logical Volume   (naa.600508e000000000ce7c2a...) 278.46 GB

                        [*] Contains a VMFS partition
              (F1) Details    (Esc) Cancel    (Enter) Continue
```

Figure 7 - Cisco UCS C-Series USB thumb drive



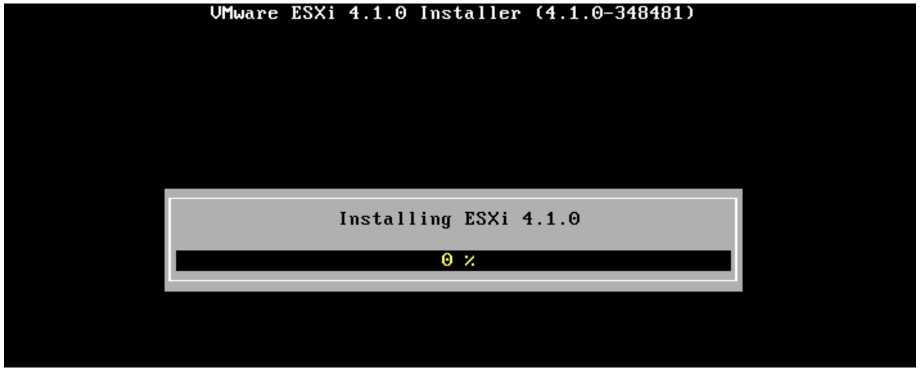
```
                   VMware ESXi 4.1.0 Installer (4.1.0-348481)

                              Select a Disk

 Storage Device                                                   Capacity
 ---------------------------------------------------------------------------
 Local:
            USB Flash Disk   (mpx.vmhba33:C0:T0:L0)               1.83  GB
   Cisco    Virtual FDD/HDD  (mpx.vmhba32:C0:T0:L1)               0.00  B

 Remote:
   LSILOGIC Logical Volume   (naa.600508e000000000ce7c2a...) 278.46 GB

                        [*] Contains a VMFS partition
              (F1) Details    (Esc) Cancel    (Enter) Continue
```

Step 4: Review the Confirm Install screen, and then press **F11**.



```
VMware ESXi 4.1.0 Installer (4.1.0-348481)

                    Confirm Install

  ESXi 4.1.0 is ready to be installed on mpx.vmhba33:C0:T0:L0

Be advised, when ESXi 4.1.0 is initially booted, it will format
    local storage that is unformatted on the host. Existing
         partitions on available disks will be removed.

     (Backspace) Back       (Esc) Cancel       (F11) Install
```

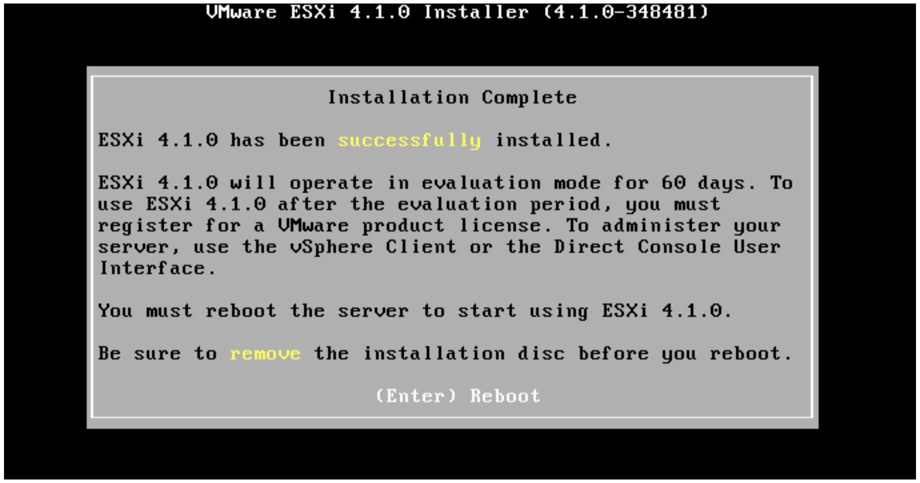
VMware ESXi installation begins and displays a status window.



```
VMware ESXi 4.1.0 Installer (4.1.0-348481)

          Installing ESXi 4.1.0
                   0 %
```

Step 5: When the Installation Complete screen is displayed, on the KVM Virtual Media window, next to the ISO file you loaded in the previous procedure, clear the **Mapped** check box. This removes the installation disk.

Step 6: On the Installation Complete screen, press **Enter**. The server reboots.



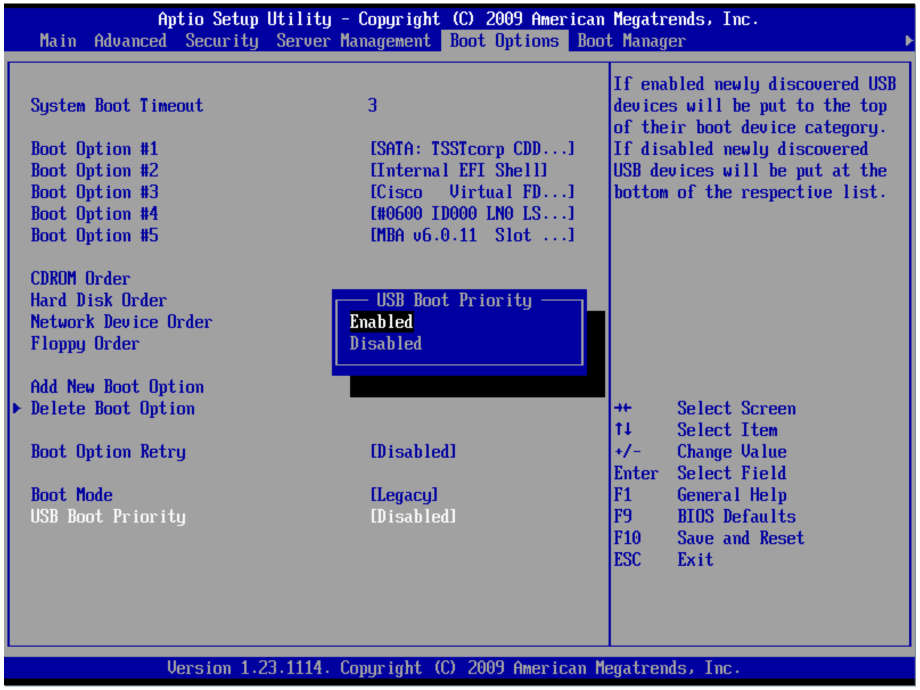
```
VMware ESXi 4.1.0 Installer (4.1.0-348481)

                  Installation Complete

ESXi 4.1.0 has been successfully installed.

ESXi 4.1.0 will operate in evaluation mode for 60 days. To
use ESXi 4.1.0 after the evaluation period, you must
register for a VMware product license. To administer your
server, use the vSphere Client or the Direct Console User
Interface.

You must reboot the server to start using ESXi 4.1.0.

Be sure to remove the installation disc before you reboot.

                      (Enter) Reboot
```

Step 7: If you are using the UCS B-Series Server or the UCS C-Series server with the boot-from-local-drive option, proceed to the next process "Configuring the ESXi Console."

If you are using the Cisco UCS C-Series server with the boot-from-USB-thumb-drive option, continue with this procedure.

Step 8: When the server boots, press **F2**. BIOS setup opens, where you can modify the BIOS boot order so the USB option is listed first.

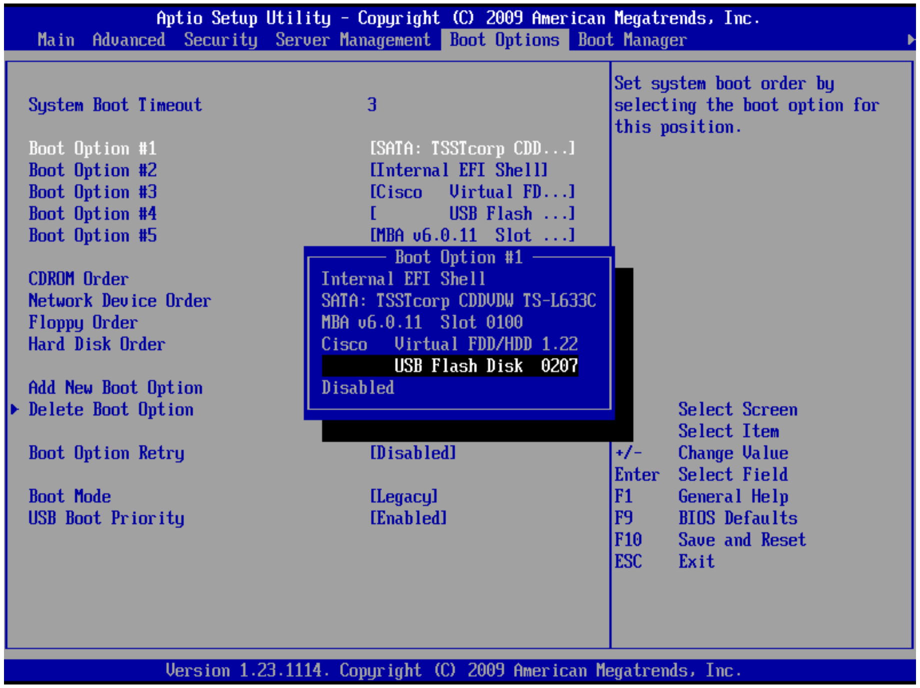
Step 9: Use the arrow keys to choose the Boot Options tab. Ensure that USB Boot Priority is **Enabled**. This ensures that the server attempts to boot from a USB device if one is available.



```
        Aptio Setup Utility - Copyright (C) 2009 American Megatrends, Inc.
  Main  Advanced  Security  Server Management  Boot Options  Boot Manager

  System Boot Timeout               3                    If enabled newly discovered USB
                                                         devices will be put to the top
  Boot Option #1                    [SATA: TSSTcorp CDD...]  of their boot device category.
  Boot Option #2                    [Internal EFI Shell]     If disabled newly discovered
  Boot Option #3                    [Cisco   Virtual FD...]  USB devices will be put at the
  Boot Option #4                    [#0600 ID000 LN0 LS...]  bottom of the respective list.
  Boot Option #5                    [MBA v6.0.11  Slot ...]

  CDROM Order
  Hard Disk Order              -- USB Boot Priority --
  Network Device Order          Enabled
  Floppy Order                  Disabled

  Add New Boot Option
► Delete Boot Option                                     →←    Select Screen
                                                         ↑↓    Select Item
  Boot Option Retry                 [Disabled]           +/-   Change Value
                                                         Enter Select Field
  Boot Mode                         [Legacy]             F1    General Help
  USB Boot Priority                 [Disabled]           F9    BIOS Defaults
                                                         F10   Save and Reset
                                                         ESC   Exit

        Version 1.23.1114. Copyright (C) 2009 American Megatrends, Inc.
```

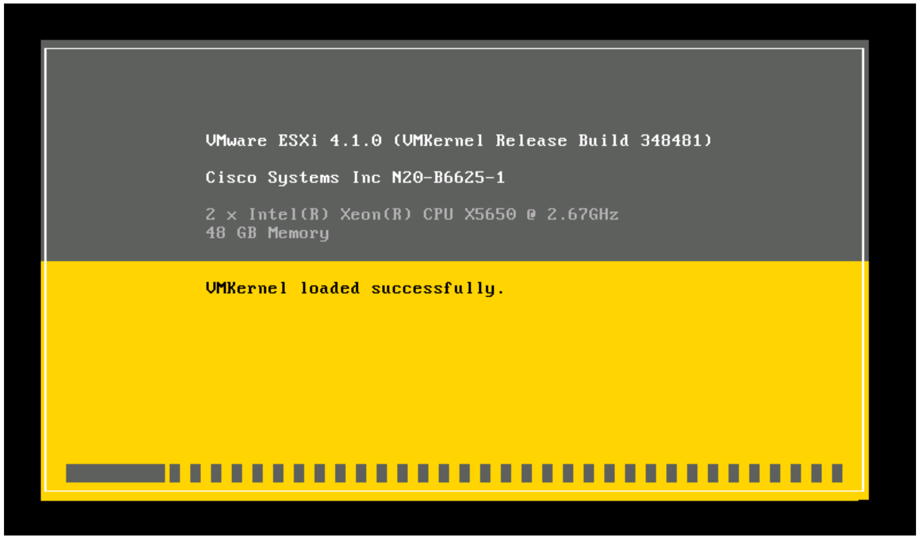
Step 10: In the Boot Options screen, use the arrow keys to select **Boot Option #1**, and then press **Enter**.

Step 11: Use the arrow keys to choose the USB device installed on your server, and then press **F10**. This saves your changes and reboots the server.



```
        Aptio Setup Utility - Copyright (C) 2009 American Megatrends, Inc.
  Main  Advanced  Security  Server Management  Boot Options  Boot Manager

                                                         Set system boot order by
  System Boot Timeout               3                    selecting the boot option for
                                                         this position.
  Boot Option #1                    [SATA: TSSTcorp CDD...]
  Boot Option #2                    [Internal EFI Shell]
  Boot Option #3                    [Cisco   Virtual FD...]
  Boot Option #4                    [        USB Flash ...]
  Boot Option #5                    [MBA v6.0.11  Slot ...]
                              -------- Boot Option #1 --------
  CDROM Order                  Internal EFI Shell
  Network Device Order         SATA: TSSTcorp CDDVDW TS-L633C
  Floppy Order                 MBA v6.0.11  Slot 0100
  Hard Disk Order              Cisco   Virtual FDD/HDD 1.22
                                         USB Flash Disk  0207
  Add New Boot Option          Disabled
► Delete Boot Option                                           Select Screen
                                                               Select Item
  Boot Option Retry                 [Disabled]           +/-   Change Value
                                                         Enter Select Field
  Boot Mode                         [Legacy]             F1    General Help
  USB Boot Priority                 [Enabled]            F9    BIOS Defaults
                                                         F10   Save and Reset
                                                         ESC   Exit

        Version 1.23.1114. Copyright (C) 2009 American Megatrends, Inc.
```

After the server reboots, the ESXi operating system is loaded.



```
VMware ESXi 4.1.0 (VMKernel Release Build 348481)

Cisco Systems Inc N20-B6625-1

2 x Intel(R) Xeon(R) CPU X5650 @ 2.67GHz
48 GB Memory

VMKernel loaded successfully.
```

Process

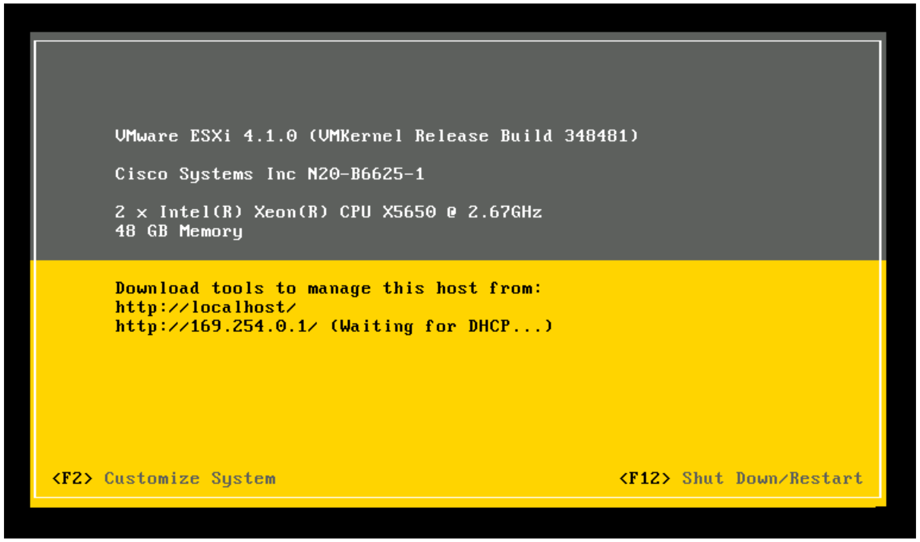
Configuring the ESXi Console

1. Configure the login password
2. Configure the management network
3. Configure DNS address
4. Test the configuration

Procedure 1 Configure the login password

After the ESXi host has rebooted, the KVM console should look like the following figure. Note that the console is waiting for DHCP to provide an IP address. This procedure assigns static IP addressing to the ESXi console.

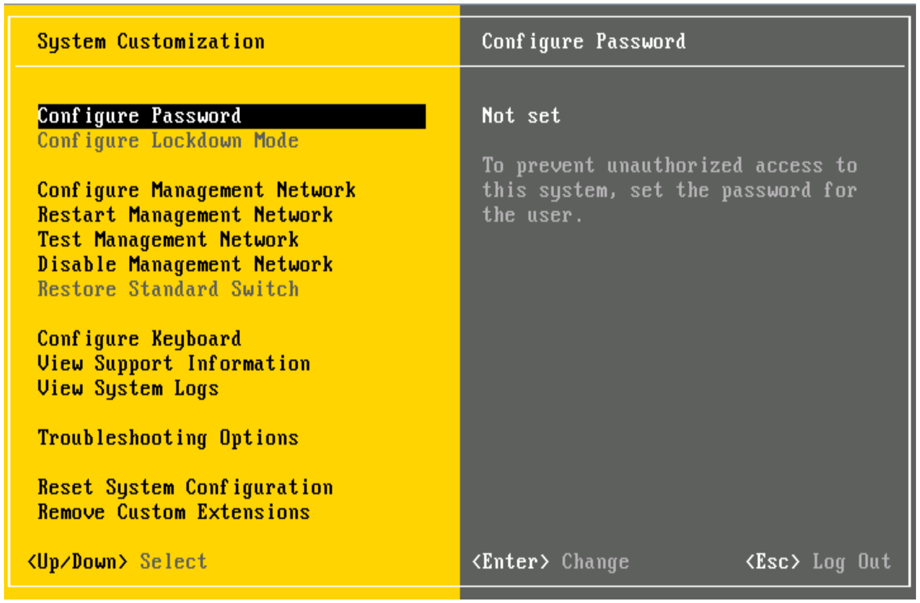
Step 1: Press **F2**.



```
VMware ESXi 4.1.0 (VMKernel Release Build 348481)

Cisco Systems Inc N20-B6625-1

2 x Intel(R) Xeon(R) CPU X5650 @ 2.67GHz
48 GB Memory

Download tools to manage this host from:
http://localhost/
http://169.254.0.1/ (Waiting for DHCP...)

<F2> Customize System                          <F12> Shut Down/Restart
```

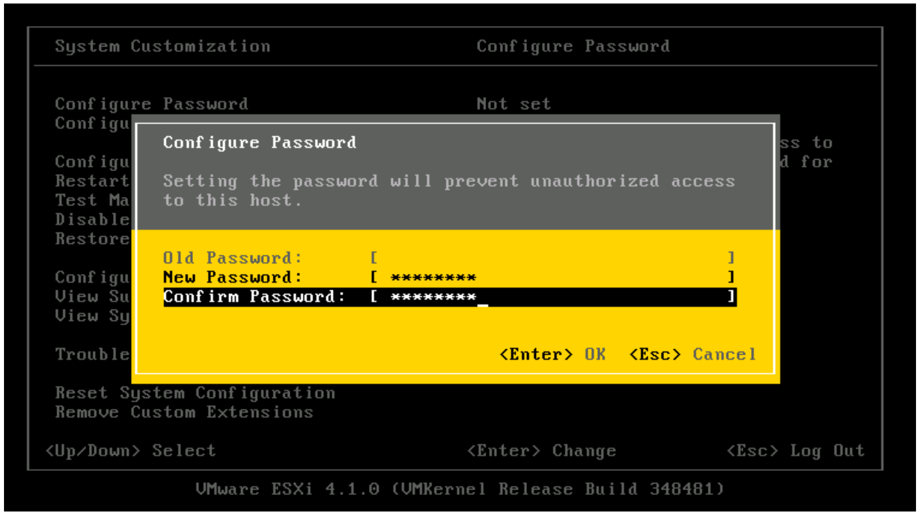
Step 2: On the Authentication Required screen, press **Enter**. By default, Password is an empty field.

Step 3: Use the arrow keys to choose **Configure Password**, and then press **Enter**.



```
System Customization                  Configure Password

Configure Password                    Not set
Configure Lockdown Mode
                                      To prevent unauthorized access to
Configure Management Network          this system, set the password for
Restart Management Network            the user.
Test Management Network
Disable Management Network
Restore Standard Switch

Configure Keyboard
View Support Information
View System Logs

Troubleshooting Options

Reset System Configuration
Remove Custom Extensions

<Up/Down> Select                      <Enter> Change          <Esc> Log Out
```

Step 4: When prompted, enter a new password, and then press **Enter**.



```
System Customization                  Configure Password

Configure Password                    Not set

   Configure Password

   Setting the password will prevent unauthorized access
   to this host.

   Old Password:      [                                  ]
   New Password:      [ ********                         ]
   Confirm Password:  [ ********_                        ]

                                   <Enter> OK   <Esc> Cancel

Reset System Configuration
Remove Custom Extensions

<Up/Down> Select                      <Enter> Change          <Esc> Log Out
              VMware ESXi 4.1.0 (VMKernel Release Build 348481)
```

Reader Tip

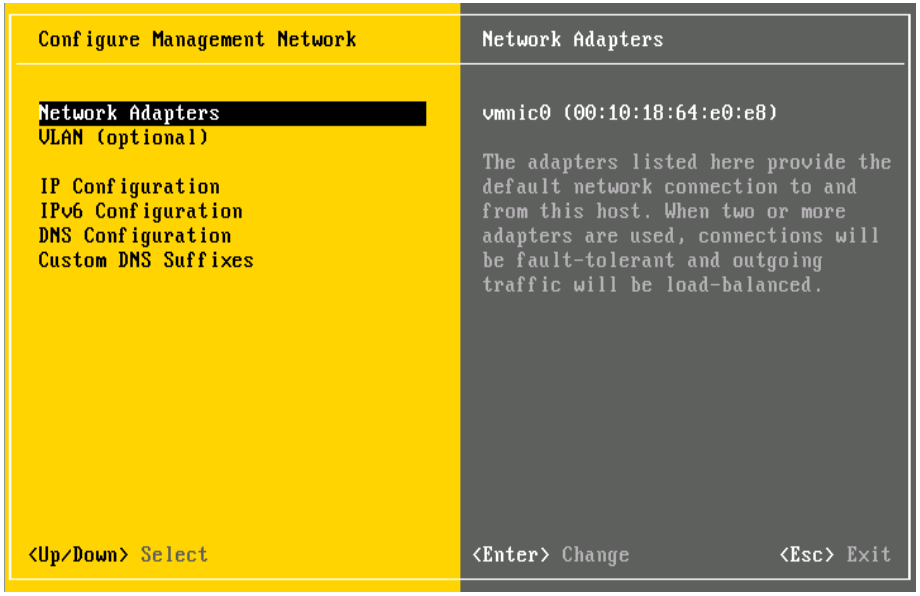
You can modify the Troubleshooting Options field to allow configuration of remote troubleshooting via SSH or directly from the console. Please refer to VMware KB Article: 1017910 for more information: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1017910

Procedure 2 Configure the management network

In this procedure, you configure management access to VMware ESXi on the server. When deciding to share an Ethernet port (or to dedicate one to management), be aware of traffic requirements of virtual machines. The best practice is to have a separate Ethernet port for management.

Step 1: On the System Customization screen, choose Configure Management Network.

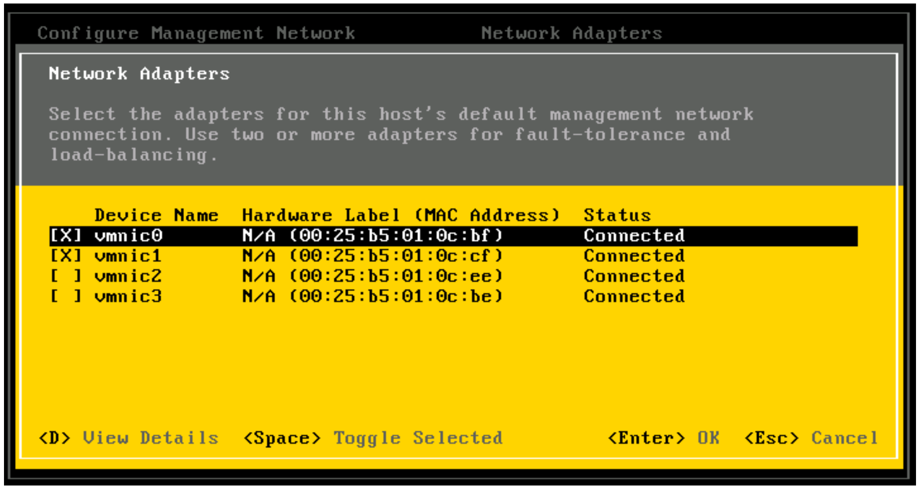
Step 2: On the Configure Management Network screen, choose Network Adapters, and then press Enter.



```
Configure Management Network                Network Adapters

Network Adapters                            vmnic0 (00:10:18:64:e0:e8)
VLAN (optional)
                                            The adapters listed here provide the
IP Configuration                            default network connection to and
IPv6 Configuration                          from this host. When two or more
DNS Configuration                           adapters are used, connections will
Custom DNS Suffixes                         be fault-tolerant and outgoing
                                            traffic will be load-balanced.

<Up/Down> Select                            <Enter> Change            <Esc> Exit
```

Step 3: Press the Space bar to select vmnics, and then press Enter.

Step 4: Select the adapter interfaces that will manage the ESXi host. Adapters are listed with their VMware name (vmnic0 through vmnic3), MAC addresses, and link status. In this setup, vmnic 0 and vmnic 1 are used for management.



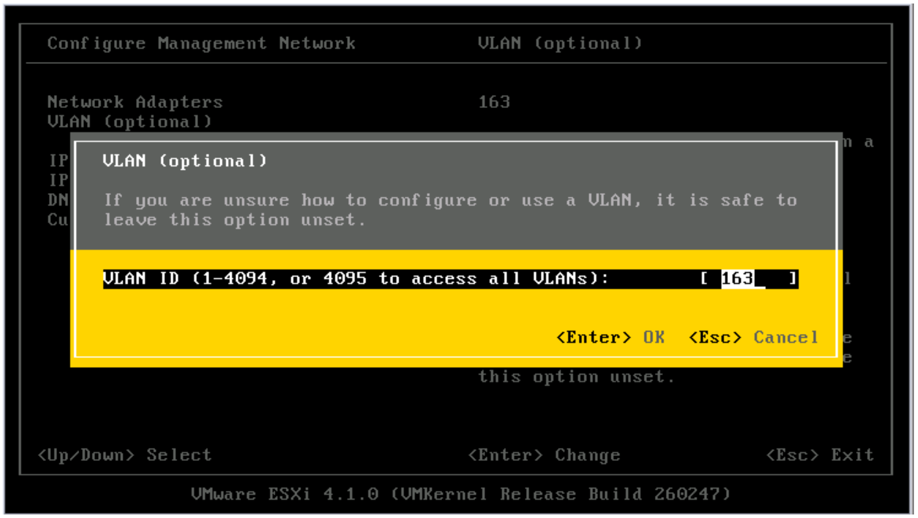
```
Configure Management Network              Network Adapters

 Network Adapters

 Select the adapters for this host's default management network
 connection. Use two or more adapters for fault-tolerance and
 load-balancing.

     Device Name  Hardware Label (MAC Address)  Status
 [X] vmnic0       N/A (00:25:b5:01:0c:bf)       Connected
 [X] vmnic1       N/A (00:25:b5:01:0c:cf)       Connected
 [ ] vmnic2       N/A (00:25:b5:01:0c:ee)       Connected
 [ ] vmnic3       N/A (00:25:b5:01:0c:be)       Connected

<D> View Details  <Space> Toggle Selected       <Enter> OK  <Esc> Cancel
```

If you are using the Cisco UCS B-Series server, use a trunk port and specify the management VLAN. This procedure shows how to tag traffic with VLANs on a trunk.

If you are using a Cisco UCS C-Series server with multiple NICs and you are using separate physical NICs for management with a single VLAN on this vmnic, skip to Step 7.

Step 5: On the Configure Management Network screen, choose **VLAN**, and then press **Enter**.

Step 6: Enter the management VLAN number **163**, and then press **Enter**. The Cisco SBA data center foundation design uses VLAN 163.



```
Configure Management Network              VLAN (optional)

Network Adapters                          163
VLAN (optional)
IP  VLAN (optional)
IP
DN  If you are unsure how to configure or use a VLAN, it is safe to
Cu  leave this option unset.

    VLAN ID (1-4094, or 4095 to access all VLANs):      [ 163_  ]

                                        <Enter> OK  <Esc> Cancel
                                          this option unset.

<Up/Down> Select                   <Enter> Change           <Esc> Exit

            VMware ESXi 4.1.0 (VMKernel Release Build 260247)
```

Step 7: On the Configuration Management Network screen, choose **IP Configuration**, and then press **Enter**.

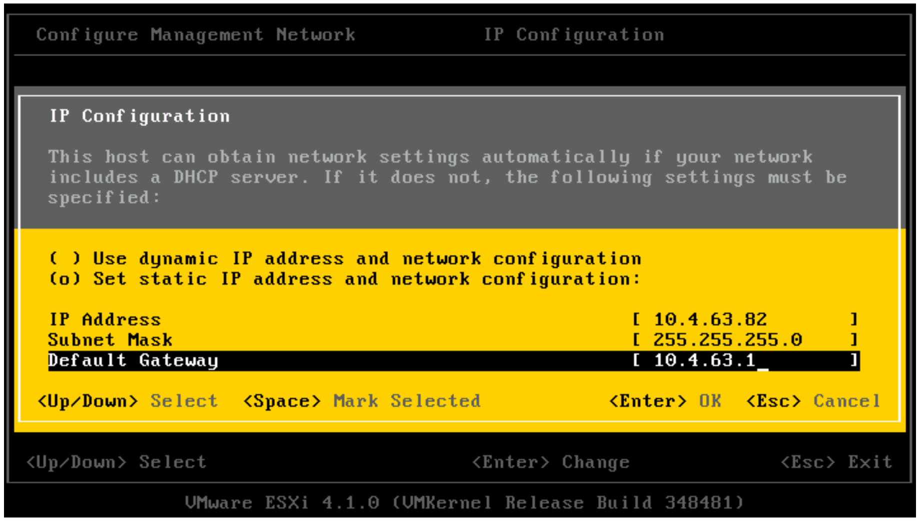
Step 8: On the IP Configuration screen, choose **Set static IP address and network configuration**.

Step 9: Use the arrow keys to move between the IP address fields, enter the following values for the following ESXi management interface settings, and then press **Enter**:

- IP address—10.4.63.82
- Subnet mask—255.255.255.0
- Default gateway—10.4.63.1

Tech Tip

Be careful to use the up and down arrows to navigate this screen. If you press **Enter** before you have entered all of the information required, you will return to the Configuration Management screen and will have to return to this screen to complete entering all required information.



```
Configure Management Network              IP Configuration

IP Configuration

This host can obtain network settings automatically if your network
includes a DHCP server. If it does not, the following settings must be
specified:

( ) Use dynamic IP address and network configuration
(o) Set static IP address and network configuration:

IP Address                                    [ 10.4.63.82      ]
Subnet Mask                                   [ 255.255.255.0   ]
Default Gateway                               [ 10.4.63.1_      ]

<Up/Down> Select  <Space> Mark Selected            <Enter> OK  <Esc> Cancel

<Up/Down> Select                       <Enter> Change             <Esc> Exit
            VMware ESXi 4.1.0 (VMKernel Release Build 348481)
```

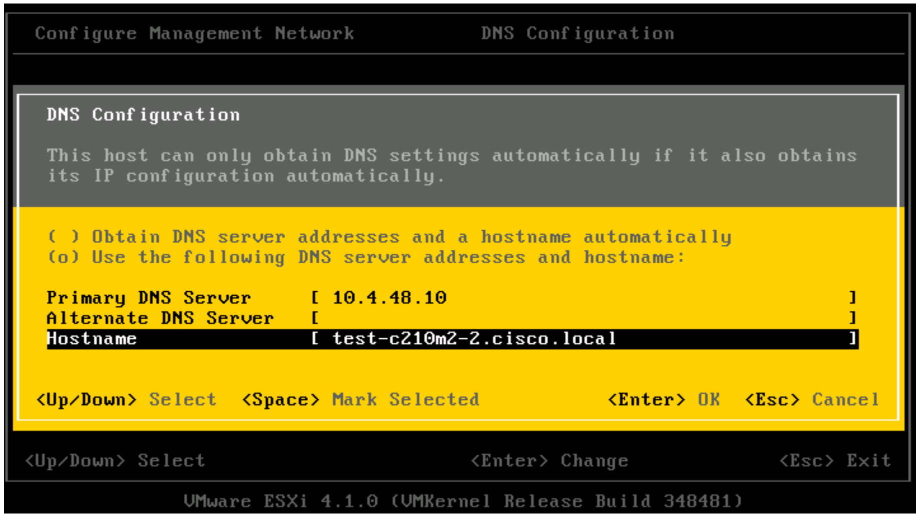
Procedure 3 Configure DNS address

Domain Name Service (DNS) provides for IP address-to-name resolution for ESXi system management. This is a critical service for VMware.

Step 1: On the Configure Management Network screen, choose **DNS Configuration**.

Step 2: Enter values for the following settings, and then press **Enter**:

- Primary DNS server
- Backup (or alternate) DNS server
- A fully qualified host name for this node

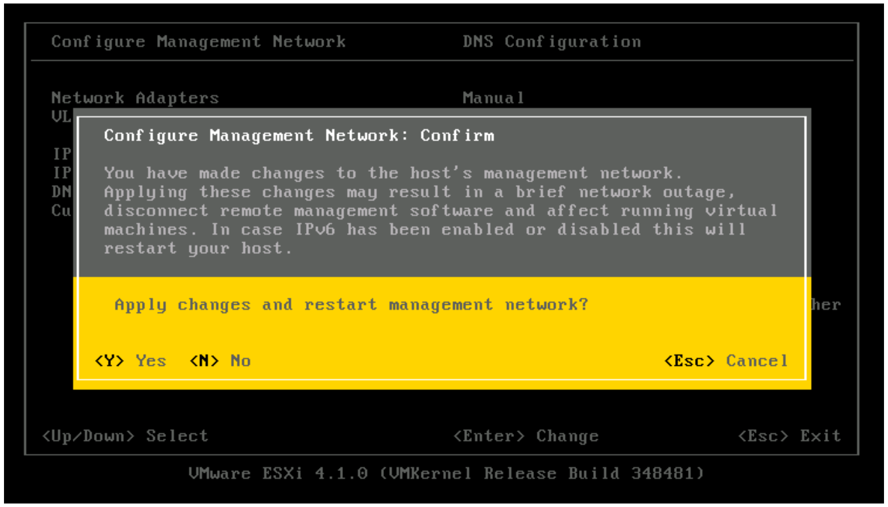


```
Configure Management Network              DNS Configuration

DNS Configuration

This host can only obtain DNS settings automatically if it also obtains
its IP configuration automatically.

( ) Obtain DNS server addresses and a hostname automatically
(o) Use the following DNS server addresses and hostname:

Primary DNS Server      [ 10.4.48.10                                ]
Alternate DNS Server    [                                           ]
Hostname                [ test-c210m2-2.cisco.local                 ]

<Up/Down> Select  <Space> Mark Selected            <Enter> OK  <Esc> Cancel

<Up/Down> Select                       <Enter> Change             <Esc> Exit
            VMware ESXi 4.1.0 (VMKernel Release Build 348481)
```

This completes the programming of the ESXi management parameters.

Step 3: Press **Esc**. Configuration is now complete.

Step 4: Press Y. This accepts the changes and restarts the management network.



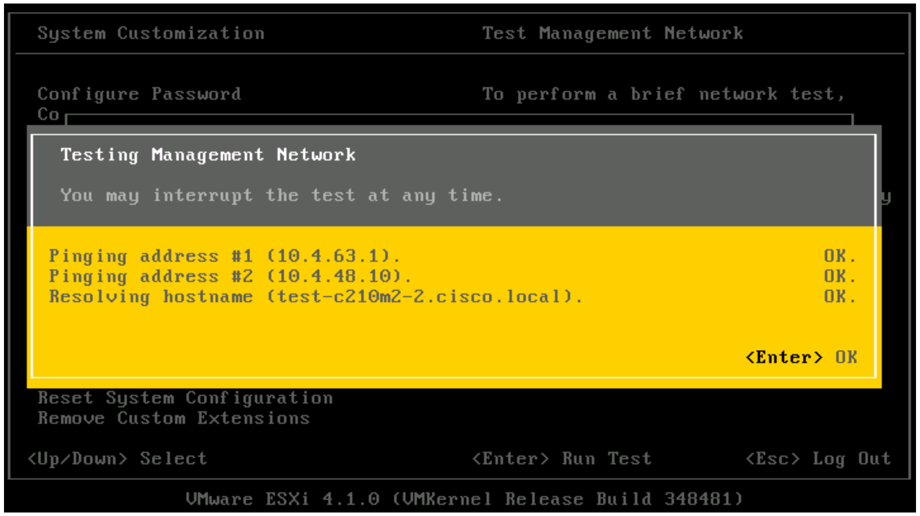
```
Configure Management Network                DNS Configuration

Network Adapters                            Manual
VL
     Configure Management Network: Confirm
IP
IP   You have made changes to the host's management network.
DN   Applying these changes may result in a brief network outage,
Cu   disconnect remote management software and affect running virtual
     machines. In case IPv6 has been enabled or disabled this will
     restart your host.

      Apply changes and restart management network?                    her

   <Y> Yes  <N> No                                      <Esc> Cancel

<Up/Down> Select                           <Enter> Change        <Esc> Exit
                VMware ESXi 4.1.0 (VMKernel Release Build 348481)
```

Procedure 4 Test the configuration

Now that you have completed configuration, it is recommended that you test for proper communication. Testing ensures that the ESXi management interface can reach its DNS servers and default gateway, as well as fully resolve its host name.

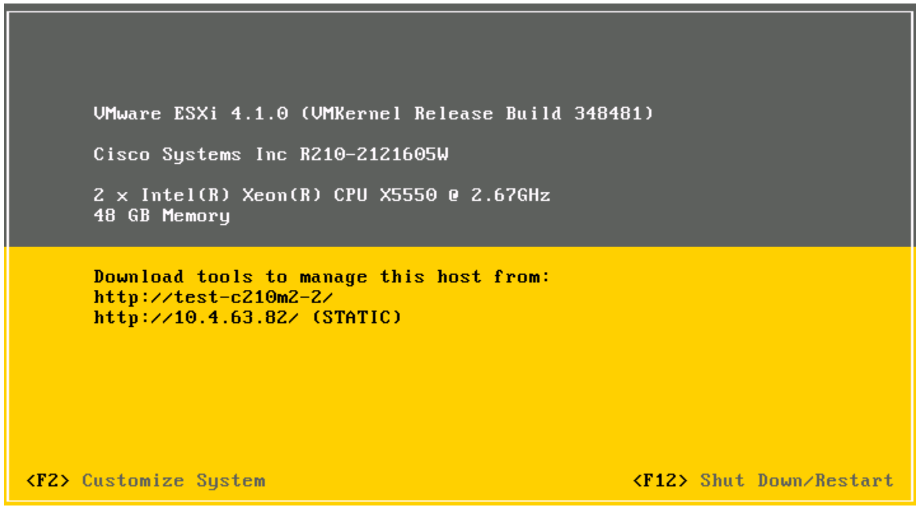
Step 1: On the main ESXi configuration screen, choose Test Management Network, and then press Enter.

Step 2: If the test is successful, the system marks the test OK.



```
System Customization                  Test Management Network

Configure Password                    To perform a brief network test,
Co
  Testing Management Network

  You may interrupt the test at any time.                              y

 Pinging address #1 (10.4.63.1).                                   OK.
 Pinging address #2 (10.4.48.10).                                  OK.
 Resolving hostname (test-c210m2-2.cisco.local).                   OK.

                                                            <Enter> OK
Reset System Configuration
Remove Custom Extensions

<Up/Down> Select                      <Enter> Run Test        <Esc> Log Out
           VMware ESXi 4.1.0 (VMKernel Release Build 348481)
```

Step 3: Press Enter, and then press Esc. The final welcome screen appears.



```
       VMware ESXi 4.1.0 (VMKernel Release Build 348481)

       Cisco Systems Inc R210-2121605W

       2 x Intel(R) Xeon(R) CPU X5550 @ 2.67GHz
       48 GB Memory

       Download tools to manage this host from:
       http://test-c210m2-2/
       http://10.4.63.82/ (STATIC)




<F2> Customize System                            <F12> Shut Down/Restart
```

Process

Installing vSphere Client

1. Install vSphere Client

VMware vCenter Server can be installed either on a virtual machine or on a physical machine. The procedure flow in this guide, which begins with installing the vSphere Client, is based on deploying VMware vCenter Server on a virtual machine.

Deploying vCenter Server on a virtual machine has following benefits:

- You can migrate the virtual machine running vCenter Server from one host to another, enabling non-disruptive maintenance.
- You can provide high availability by using VMware HA. In case of a host failure, the virtual machine running vCenter Server can be restarted elsewhere in the cluster.
- You can take snapshots, enabling data protection for the virtual machine running vCenter Server. You can use tools like VMware Data Recovery to provide speedy backup and recovery of virtual machines.
- You do not need to dedicate a physical server for vCenter Server.

If you prefer to install vCenter Server on a physical machine, do the following:

1. On a standalone server, install the Windows operating system.
2. Install a database (Oracle DB or Microsoft SQL Server) based on how many ESX/ESXi hosts and virtual machines you plan to install and manage in your environment. Consult VMware for guidance.
3. Install vCenter Server on the same machine on which you installed the database or on a different physical machine.
4. Install vSphere Client on any machine that has network access to vCenter Server and the ESX/ESXi hosts.
5. Using vSphere Client, access vCenter Server and start managing your hosts and virtual machines.

In this guide, you use Microsoft SQL Server 2005 Express Edition (which comes bundled with vCenter Server) as the database server. For smaller environments, this choice works well, and you can upgrade to a more full-featured version of SQL Server as you grow your environment.

Procedure 1 Install vSphere Client

Now that you installed ESXi in the previous process, you can download vSphere Client from the newly installed host.

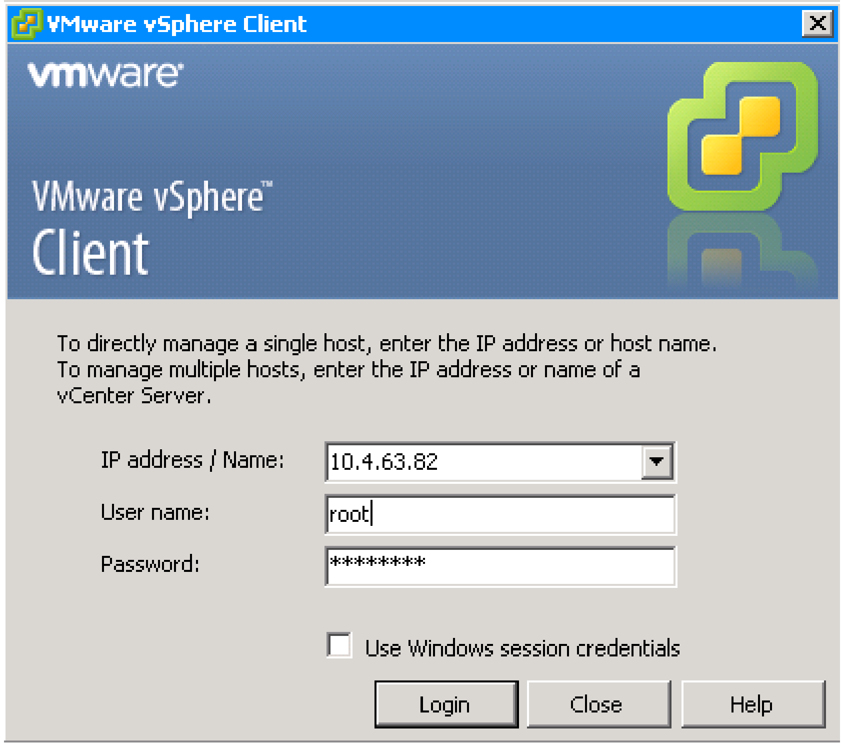
Step 1: In the address field of your web browser, enter the IP address used for the ESXi host management interface (Example: http://10.4.63.82/). VSphere Client is automatically available for download.

Tech Tip

VSphere Client is adaptive, and it only shows what the ESXi host knows how to do. VSphere Client is also used for access to vCenter (which will be covered later), allowing for vMotion and other functions. Be aware of what destination you are connecting to. ESXi hosts and vCenter have different abilities available to the client.

Step 2: Download and install vSphere Client.

Step 3: Start vSphere Client, enter the address of the ESXi server you just installed, along with the username **root** and the ESXi console login password, and then click **Login**.



To directly manage a single host, enter the IP address or host name.
To manage multiple hosts, enter the IP address or name of a vCenter Server.

IP address / Name: 10.4.63.82

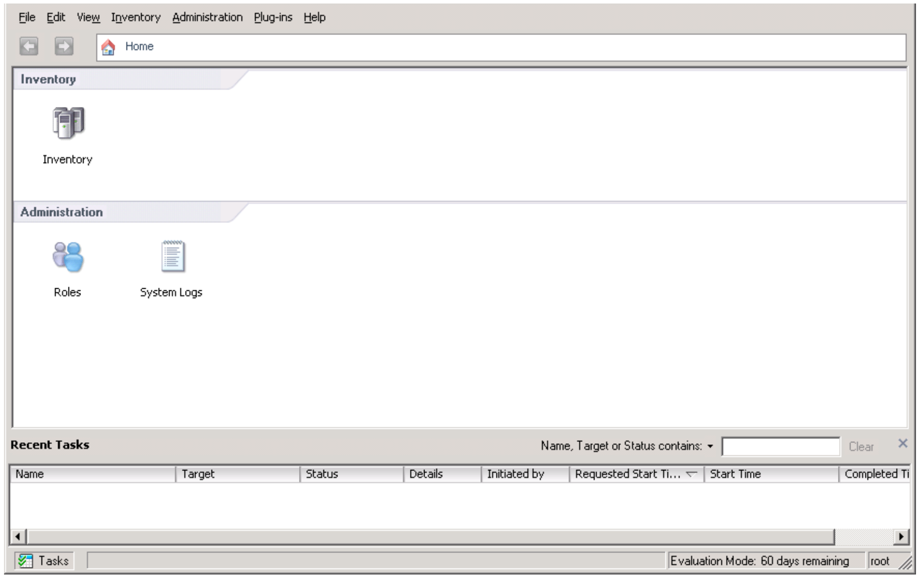
User name: root

Password: *********

☐ Use Windows session credentials

Step 4: On the security warning for an untrusted SSL certificate from the new ESXi host, click **Accept**.

After you log in, you are presented with a screen like the following. Since you have just installed, you are also prompted with a license notice. ESXi has a 60-day evaluation license. You will need to acquire proper licenses from VMware and install them in the vCenter.



Process

Adding Networking for Virtual Machines

1. Run the Add Network Wizard

The ESXi host links local VMs to each other and to the external enterprise network via a software virtual switch (vSwitch), which runs in the context of the kernel. Virtual switches are key networking components in ESXi.

A vSwitch, as implemented in the vSphere hypervisor, works in much the same way as a modern Ethernet switch. A vSwitch:

- Maintains a MAC address and port-forwarding table.
- Looks up each frame's destination MAC when the value arrives.
- Forwards a frame to one or more ports for transmission.
- Avoids unnecessary deliveries (in other words, it is not a hub).

Although it is recommended that the management console and VMkernel get their own respective dedicated virtual machine NIC (VMNIC), it is likely that in many deployments they will share the same VMNICs.

Multiple Gigabit Ethernet links can be connected to the ESXi host. In this example, the two onboard NICs are used for management. The following VLANs will be used:

- **Management console**—VLAN 163
- **VMkernel iSCSI**—VLAN 162
- **VMs**—VLAN 148
- **VMkernel vMotion**—VLAN 161

Reader Tip

The leading practice uses separate VLANs for the VMkernel interfaces, management interfaces, and virtual machines. For more information about load balancing and port groups with multiple VLANs, see the VMware documentation.

A vSwitch is required to configure access to a vSphere hypervisor. VSwitch 0 was created during the ESXi setup process when the management interface of the vSphere hypervisor was installed. A new vSwitch needs to be created to carry virtual machine, storage, and vMotion traffic.

Tech Tip

The vCenter or Virtual Infrastructure Client uses the management console to manage the ESXi server. Carefully review any change to the management console configuration in order to avoid losing management access to the ESXi server.

You need to perform the following procedure for each VLAN you add to the vSwitch.

Procedure 1 Run the Add Network Wizard

Step 1: Using vSphere Client, log in to the ESXi host.

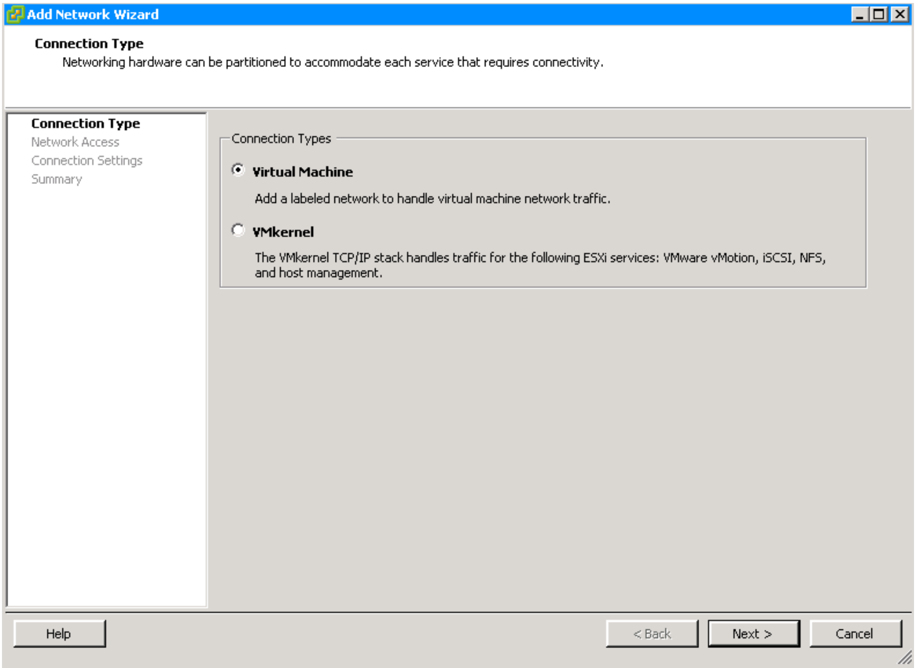
Step 2: Ignore the License warning. Licensing is be covered in its own process in this guide.

Step 3: Click the **Inventory** icon.

Step 4: In the left column, select the ESXi host, click the Configuration tab, and then select **Networking**.

Step 5: Click **Add Networking**.

Step 6: In the Add Network Wizard, select **Virtual Machine**, and then click **Next**.



Connection Type

Networking hardware can be partitioned to accommodate each service that requires connectivity.

Connection Types

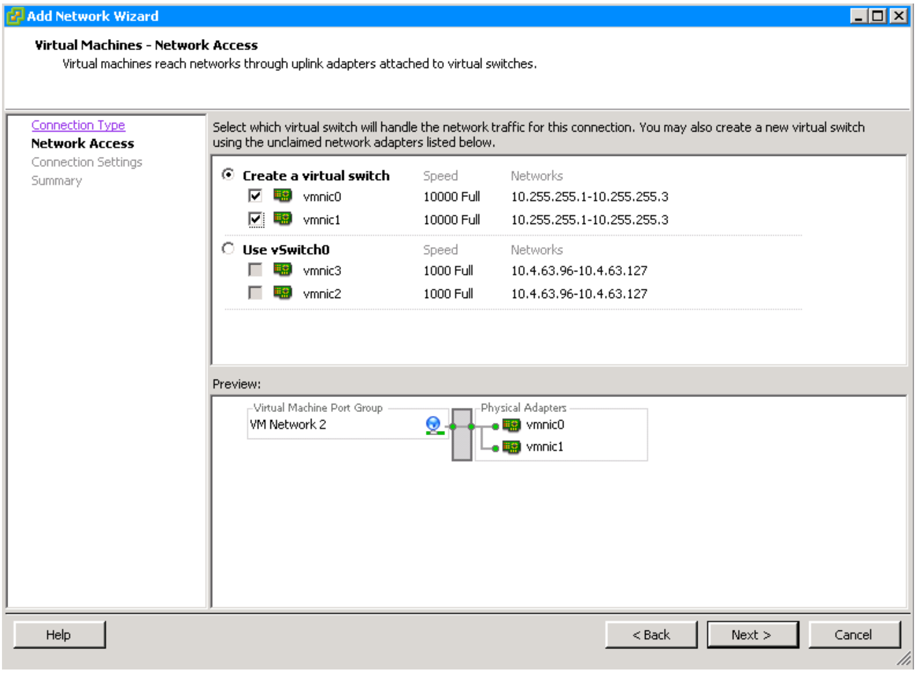
● **Virtual Machine**

Add a labeled network to handle virtual machine network traffic.

○ **VMkernel**

The VMkernel TCP/IP stack handles traffic for the following ESXi services: VMware vMotion, iSCSI, NFS, and host management.

Step 7: Select the desired VMNIC physical interfaces to use on the new vSwitch. These interfaces are the uplinks from the server to the data center network, which will carry production traffic.



Virtual Machines - Network Access

Virtual machines reach networks through uplink adapters attached to virtual switches.

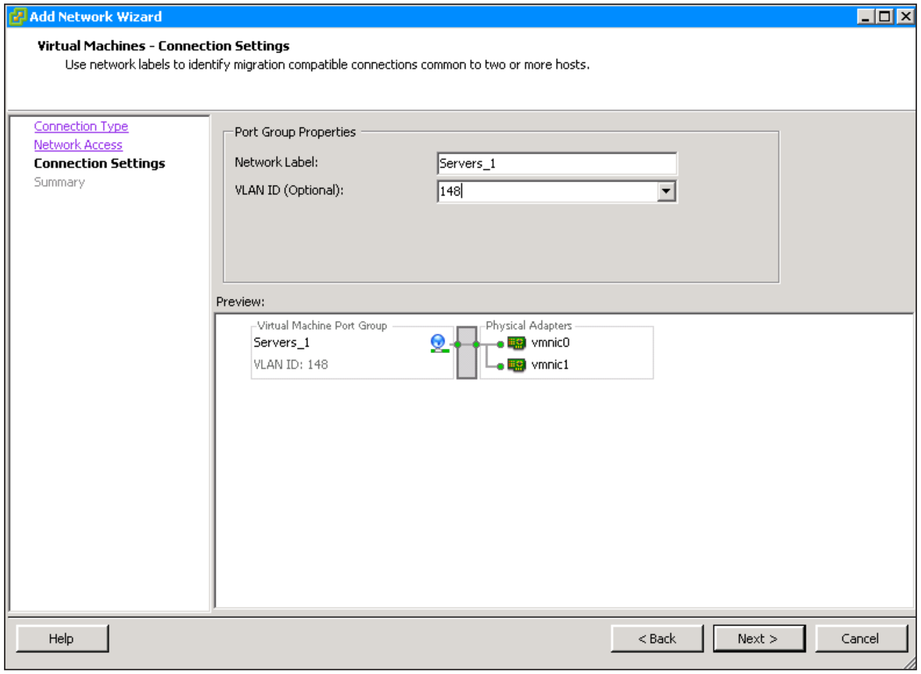
Select which virtual switch will handle the network traffic for this connection. You may also create a new virtual switch using the unclaimed network adapters listed below.

		Speed	Networks
● **Create a virtual switch**			
☑	vmnic0	10000 Full	10.255.255.1-10.255.255.3
☑	vmnic1	10000 Full	10.255.255.1-10.255.255.3
○ **Use vSwitch0**			
□	vmnic3	1000 Full	10.4.63.96-10.4.63.127
□	vmnic2	1000 Full	10.4.63.96-10.4.63.127

Tech Tip

If you are limited to two NIC cards, you can scroll down and add your VM VLAN to the existing vSwitch0.

Step 8: Name the VLAN, and then select the VLAN ID (Example: 148).



Virtual Machines - Connection Settings

Use network labels to identify migration compatible connections common to two or more hosts.

Port Group Properties

Network Label: Servers_1

VLAN ID (Optional): 148

Preview:

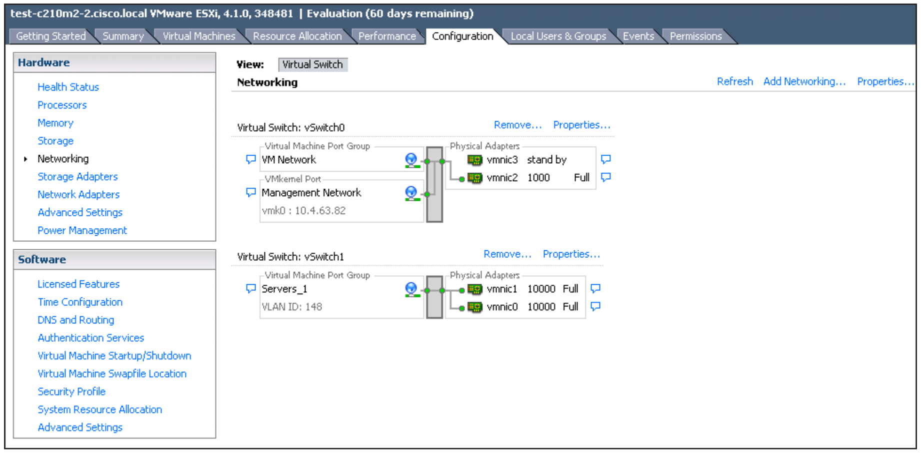
Virtual Machine Port Group: Servers_1, VLAN ID: 148

Physical Adapters: vmnic0, vmnic1

Tech Tip

The vSwitches in this example are set up for trunking, which allows for expansion in the future to multiple separate VLANs without your having to reconfigure interfaces.

Step 9: When prompted, review your settings, and then click **Finish**. The networking window shows the following configuration. The network is now created and available for future VMs.



test-c210m2-2.cisco.local VMware ESXi, 4.1.0, 348481 | Evaluation (60 days remaining)

View: Virtual Switch

Networking

Virtual Switch: vSwitch0

Virtual Machine Port Group: VM Network

VMkernel Port: Management Network, vmk0 : 10.4.63.82

Physical Adapters:

vmnic3 stand by

vmnic2 1000 Full

Virtual Switch: vSwitch1

Virtual Machine Port Group: Servers_1, VLAN ID: 148

Physical Adapters:

vmnic1 10000 Full

vmnic0 10000 Full

Process

Configuring Data Storage for the ESXi Host

1. Download and install vNIC drivers
2. Set up shared storage
3. Add a datastore to ESXi hosts

After you connect to the ESXi host using VMware vSphere Client, you may be presented with the message “The VMware ESX Server does not have persistent storage.” This message is generated when an ESXi host does not have a VMware Virtual Machine File System (VMFS) datastore. You have several options for adding storage; ESXi supports iSCSI, Fibre Channel, FCoE, and local storage.

This process will guide you through the following procedures:

- Updating your Ethernet and Fibre Channel drivers for Cisco UCS virtual interface cards.
- Setting up shared storage with iSCSI or Fibre Channel transport.
- Adding VMware data stores or "persistent storage" for your virtual machines.

Procedure 1 Download and install vNIC drivers

If you are using FCoE SAN connectivity for your server , you must install FCoE drivers on the ESXi 4.1 U1 operating system. The VMware ESX/ESXi driver CD for FCoE connected network adapters can be downloaded directly from the VMware website or from the Cisco website. If you are only using Ethernet connectivity on your server, it is still recommended to upgrade to the latest drivers for your server, or if you have existing UCS servers, upgrade to the reference version of drivers for your organization

In this procedure, you upgrade the Ethernet and Fibre Channel drivers for a Cisco UCS C-Series server by using a Cisco P81E VIC. If you are updating drivers for a UCS B-Series server with a Cisco UCS M81KR VIC, you follow the same steps but select drivers for the UCS M81KR instead.

Tech Tip

When using VMware ESXi version 4.1U1and boot from USB flash you may experience issues when updating software or drivers on the server due to unavailable scratch space. For more information and resolution refer to the VMware KB article 1037190: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1037190

Step 1: Using a web browser, navigate to the Cisco website, navigate to **Downloads > Unified Computing and Servers**, and then choose the Cisco UCS C-Series rack-mount server software corresponding to your type of UCS C-Series server.

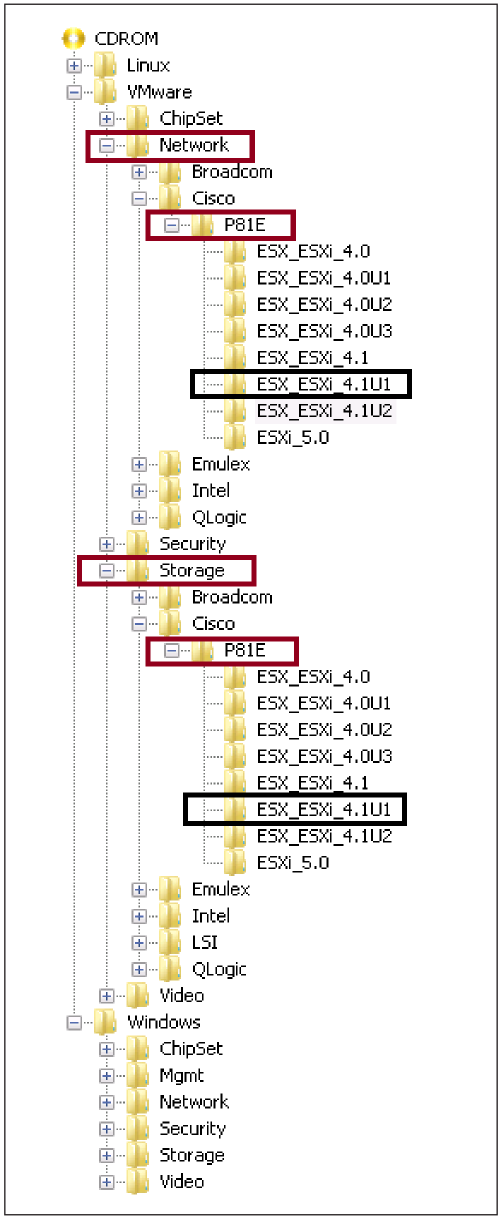
Step 2: Download the driver package ISO image file, and then save it on your local disk drive (Example: ucs-cxxx-drivers.1.4.2c.iso).

Tech Tip

If you are upgrading for a Cisco UCS B-Series M81KR VIC adapter, select that folder and load that ISO image. At the time of testing for this document, the drivers for the Cisco UCS P81E VIC adapter are the same as the drivers for the Cisco UCS M81KR adapter.

Step 3: Use an ISO extraction tool to extract the contents of the ISO image. There are various ISO image extraction tools available for download on the web.

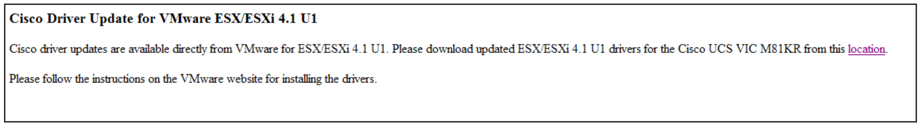
Figure 8 - Expanded directory structure of ISO file



```
CDROM
  Linux
  VMware
    ChipSet
    Network
      Broadcom
      Cisco
        P81E
          ESX_ESXi_4.0
          ESX_ESXi_4.0U1
          ESX_ESXi_4.0U2
          ESX_ESXi_4.0U3
          ESX_ESXi_4.1
          ESX_ESXi_4.1U1
          ESX_ESXi_4.1U2
          ESXi_5.0
      Emulex
      Intel
      QLogic
    Security
    Storage
      Broadcom
      Cisco
        P81E
          ESX_ESXi_4.0
          ESX_ESXi_4.0U1
          ESX_ESXi_4.0U2
          ESX_ESXi_4.0U3
          ESX_ESXi_4.1
          ESX_ESXi_4.1U1
          ESX_ESXi_4.1U2
          ESXi_5.0
      Emulex
      Intel
      LSI
      QLogic
    Video
  Windows
    ChipSet
    Mgmt
    Network
    Security
    Storage
    Video
```

Step 4: Browse through the folders **VMware > Storage > Cisco > P81E > ESX_ESXi_4.1U1**, and then download the FNIC driver labeled **fnic_driver_1.4...iso**.

If you find only a readme file, open the readme file, find the link that points to the location that has the driver, and click the link. The link in the readme file takes you to VMware website from where you can download the **fnic_driver_1.4...iso** file.



Cisco Driver Update for VMware ESX/ESXi 4.1 U1

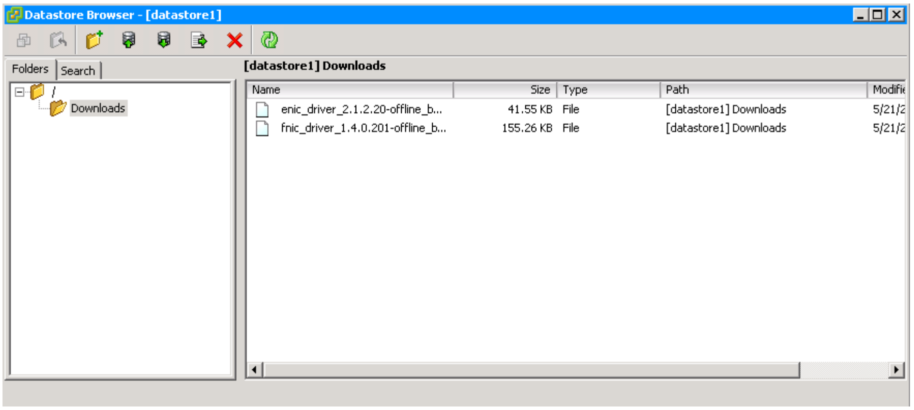
Cisco driver updates are available directly from VMware for ESX/ESXi 4.1 U1. Please download updated ESX/ESXi 4.1 U1 drivers for the Cisco UCS VIC M81KR from this location.

Please follow the instructions on the VMware website for installing the drivers.

Step 5: Browse through the folders **VMware > Network > Cisco > P81E > ESX_ESXi_4.1U1**, and then download the ENIC driver labeled **enic_driver_2.1....iso**.

Step 6: After you have saved both ENIC and FNIC drivers on your local disk, upload these drivers to the server's storage system by following these steps:

1. Select the host from vSphere Client.
2. Navigate to **Configuration > Storage**.
3. Right click the datastore, and then click **Browse Datastore**.
4. In the Datastore Browser window, on the Folders tab, create a folder named **Downloads**.
5. Double click the **Downloads** folder, and then click the **Upload Files to this datastore** icon.
6. Select both the ENIC and FNIC files, and then make sure both the files have been uploaded.



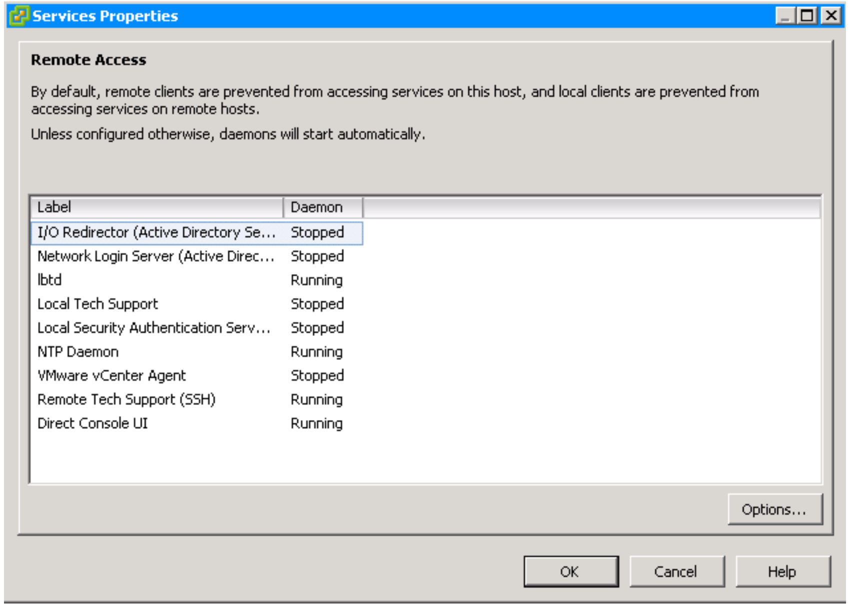
[datastore1] Downloads

Name	Size	Type	Path	Modifie
enic_driver_2.1.2.20-offline_b...	41.55 KB	File	[datastore1] Downloads	5/21/2
fnic_driver_1.4.0.201-offline_b...	155.26 KB	File	[datastore1] Downloads	5/21/2

Step 7: On the Configuration tab, from the Software list, choose **Security Profile**, and then on the Security Profile screen, click **Properties**.

Step 8: If the status of Remote Tech Support is Running, skip to the next step.

If the status of Remote Tech Support is Stopped, select the **Remote Tech Support** label, click **Options**, and under Startup Policy, select **Start and Stop manually**. Also you can enable Local Tech support mode in the same way. Remote Tech Support mode allows you to login to the ESXi server remotely via SSH. Local Tech Support allows you to login directly on the ESXi server console.



Remote Access

By default, remote clients are prevented from accessing services on this host, and local clients are prevented from accessing services on remote hosts.

Unless configured otherwise, daemons will start automatically.

Label	Daemon
I/O Redirector (Active Directory Se...	Stopped
Network Login Server (Active Direc...	Stopped
lbtd	Running
Local Tech Support	Stopped
Local Security Authentication Serv...	Stopped
NTP Daemon	Running
VMware vCenter Agent	Stopped
Remote Tech Support (SSH)	Running
Direct Console UI	Running

Step 9: Open an SSH client, and then log in to the ESXi server.

Step 10: Install the FNIC driver.

```
# cd /vmfs/volumes/datastore1/Downloads
# esxupdate --nosigcheck --maintenancemode --bundle /vmfs/
volumes/datastore1/Downloads/fnic_driver_1.4.0.201-offline_
bundle-491446.zip update
```

Step 11: Install the ENIC driver.

```
# cd /vmfs/volumes/datastore1/Downloads
# esxupdate --nosigcheck --maintenancemode --bundle /vmfs/
volumes/datastore1/Downloads/enic_driver_2.1.2.20-offline_
bundle-51242.zip update
```

Step 12: After the installation is complete, reboot the system.

Procedure 2 Set up shared storage

If you are not configuring shared storage, skip this procedure. If you are configuring access to shared storage for Cisco UCS B-Series and C-Series servers, complete the appropriate option:

- The first option shows how to set up your server for iSCSI storage array access.
- The second option shows how to set up storage for a Fibre Channel or FCoE attached storage array. A Cisco UCS B-Series server which may be running as a diskless server requires this procedure for SAN boot as well as centralized storage for any VMs running on the server. The UCS C-Series servers doing local boot, can still use this procedure for setting up shared storage for the VMs running on the server.

Option 1. Using iSCSI storage

Successful deployment of an iSCSI storage target requires that:

- A VMkernel interface exists with a valid IP address.
- The interface is enabled for the ESXi host.
- The iSCSI initiator is configured.
- The iSCSI VLAN is enabled on the data center core and the VLAN is allowed on the switch ports connected to the initiator and target devices.
- The iSCSI target is configured and reachable.

The VMkernel interface has an IP address on the ESXi host itself. The interface implements the iSCSI protocol in software for the ESXi host.

This allows for datastores to be created with iSCSI storage. After the iSCSI connectivity is established to the storage array, a new datastore can be added.

Reader Tip

The VMware best practice is to have a separate VLAN for the VMkernel interface.

Step 1: Using vSphere Client, establish a connection to the ESXi host.

Step 2: In the work pane, click the **Configuration** tab, and then in the Hardware menu list, choose **Networking**.

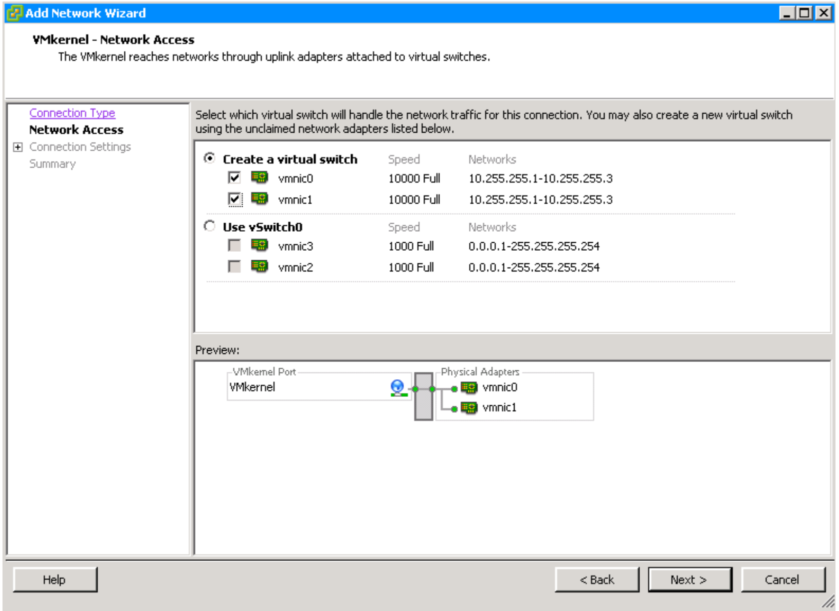
Step 3: Click **Add Networking.** This starts the Add Network Wizard.

Step 4: Select **VMkernel** as the Connection Type.

Step 5: If you are creating a new vSwitch, select the network adapters to be assigned to the new vSwitch, and then click **Next**.

If the vSwitch has already been created, select the appropriate vSwitch that will carry iSCSI traffic, and then click **Next**.

Figure 9 - Create a new virtual switch



Add Network Wizard

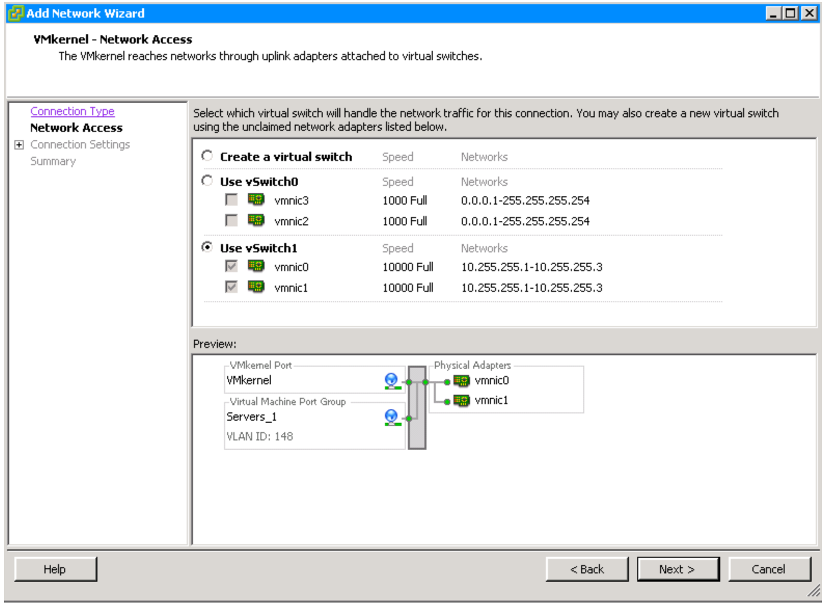
VMkernel - Network Access

The VMkernel reaches networks through uplink adapters attached to virtual switches.

Select which virtual switch will handle the network traffic for this connection. You may also create a new virtual switch using the unclaimed network adapters listed below.

	Speed	Networks
● **Create a virtual switch**	Speed	Networks
☑ vmnic0	10000 Full	10.255.255.1-10.255.255.3
☑ vmnic1	10000 Full	10.255.255.1-10.255.255.3
○ **Use vSwitch0**	Speed	Networks
□ vmnic3	1000 Full	0.0.0.1-255.255.255.254
□ vmnic2	1000 Full	0.0.0.1-255.255.255.254

Figure 10 - Use existing virtual switch



Add Network Wizard

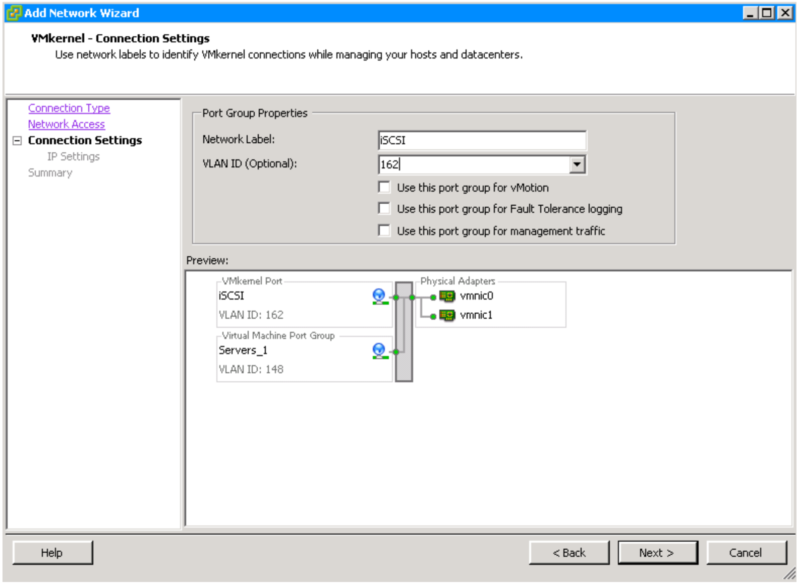
VMkernel - Network Access

The VMkernel reaches networks through uplink adapters attached to virtual switches.

Select which virtual switch will handle the network traffic for this connection. You may also create a new virtual switch using the unclaimed network adapters listed below.

	Speed	Networks
○ **Create a virtual switch**	Speed	Networks
○ **Use vSwitch0**	Speed	Networks
□ vmnic3	1000 Full	0.0.0.1-255.255.255.254
□ vmnic2	1000 Full	0.0.0.1-255.255.255.254
● **Use vSwitch1**	Speed	Networks
☑ vmnic0	10000 Full	10.255.255.1-10.255.255.3
☑ vmnic1	10000 Full	10.255.255.1-10.255.255.3

Step 6: Enter a value for the **Network Label**, and in **VLAN ID**, enter 162 for the VMkernel port that will be used to service iSCSI, network attached storage, or network file server traffic, ensure that all check boxes are cleared, and then click **Next**.



Add Network Wizard

VMkernel - Connection Settings

Use network labels to identify VMkernel connections while managing your hosts and datacenters.

Port Group Properties

Network Label: iSCSI

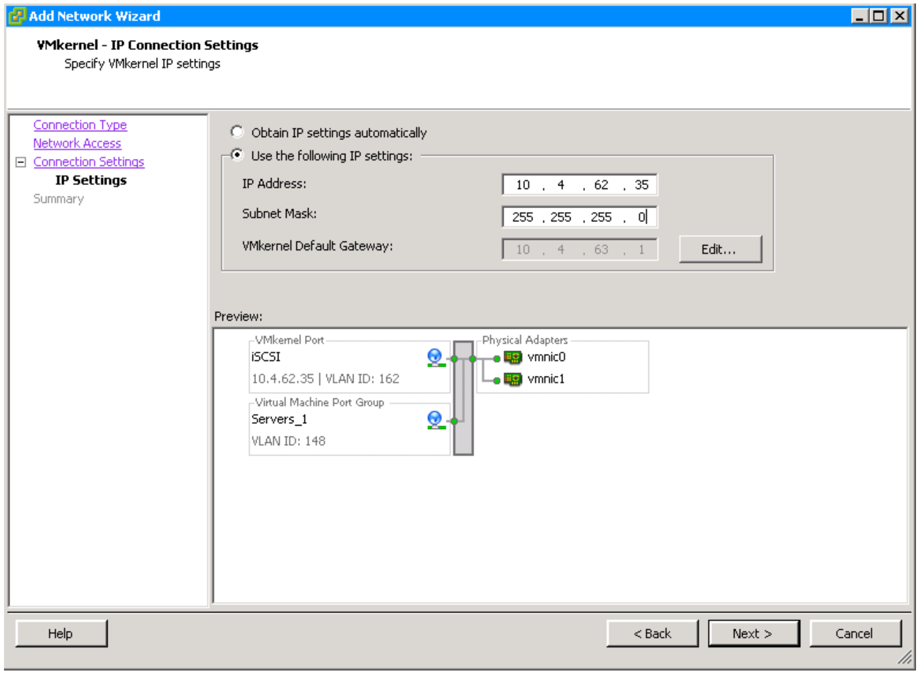
VLAN ID (Optional): 162

□ Use this port group for vMotion

□ Use this port group for Fault Tolerance logging

□ Use this port group for management traffic

Step 7: Enter an IP address (10.4.62.35) and proper subnet mask for the iSCSI interface for this ESXi host, and then click **Next**. This deployment guide uses VLAN 162 and IP subnet 10.4.62.X for iSCSI connectivity.



Add Network Wizard

VMkernel - IP Connection Settings
Specify VMkernel IP settings

○ Obtain IP settings automatically
● Use the following IP settings:

IP Address: 10 . 4 . 62 . 35
Subnet Mask: 255 . 255 . 255 . 0
VMkernel Default Gateway: 10 . 4 . 63 . 1

Preview:

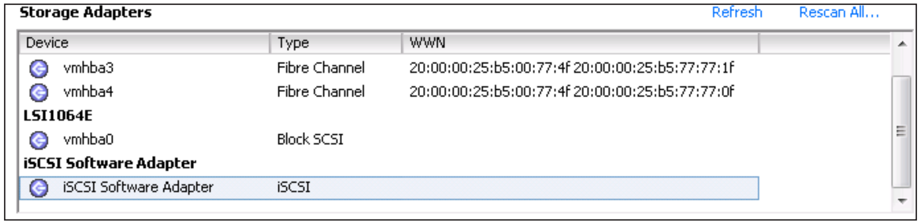
VMkernel Port
iSCSI
10.4.62.35 | VLAN ID: 162

Virtual Machine Port Group
Servers_1
VLAN ID: 148

Physical Adapters
vmnic0
vmnic1

Step 8: Click **Next**, and then click **Finish**.

Step 9: Under **Configuration > Storage Adapters**, scroll until you see the iSCSI software adapter, as illustrated below.



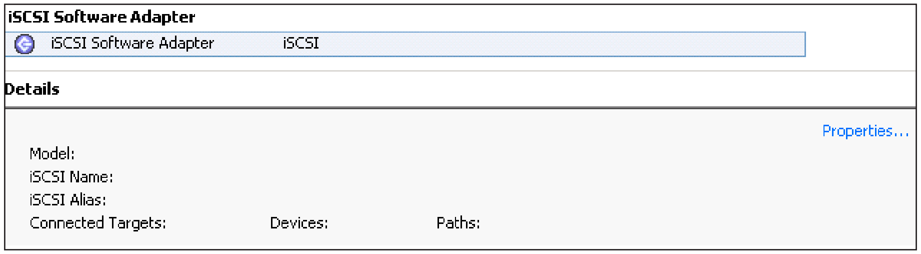
Storage Adapters

Device	Type	WWN
vmhba3	Fibre Channel	20:00:00:25:b5:00:77:4f 20:00:00:25:b5:77:77:1f
vmhba4	Fibre Channel	20:00:00:25:b5:00:77:4f 20:00:00:25:b5:77:77:0f
LSI1064E		
vmhba0	Block SCSI	
iSCSI Software Adapter		
iSCSI Software Adapter	iSCSI	

Tech Tip

If you use hardware-accelerated iSCSI adapters, the configuration is similar but located under the hardware interface.

Step 10: Select **iSCSI Software Adapter**, and then click **Properties**.



iSCSI Software Adapter

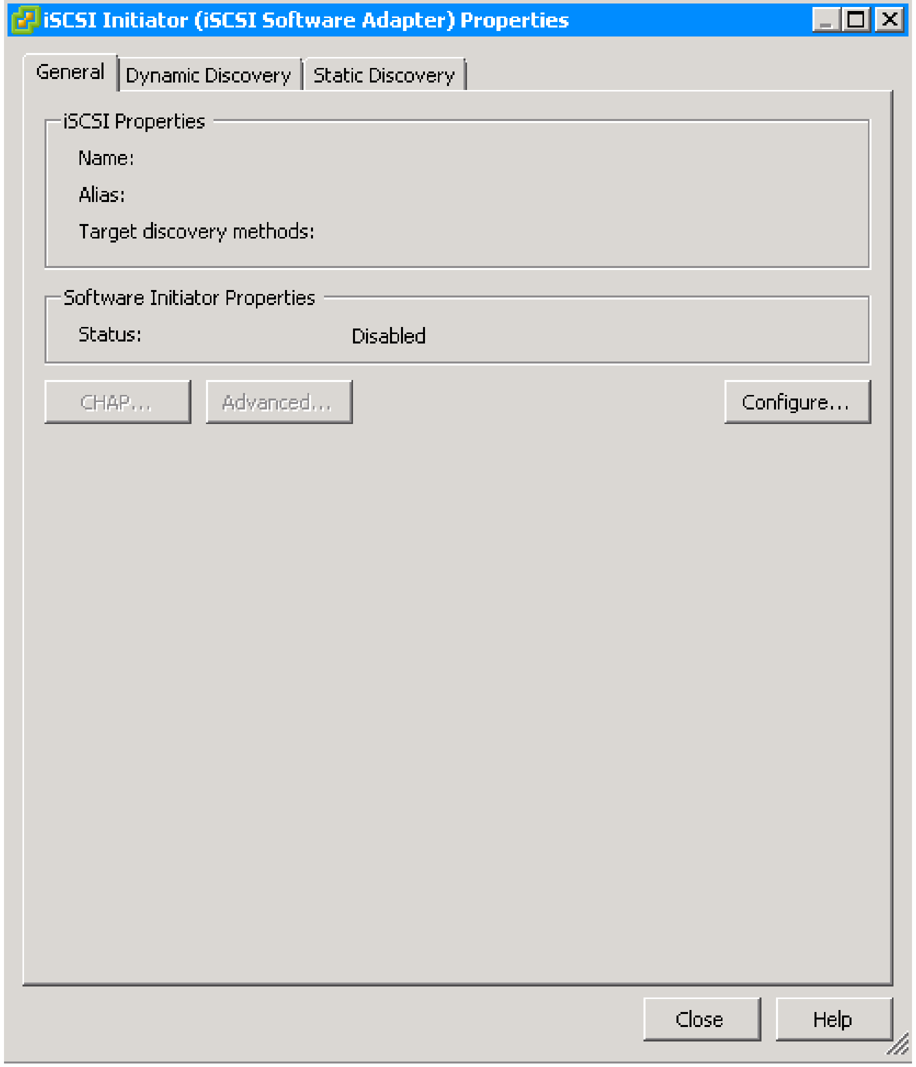
iSCSI Software Adapter iSCSI

Details

Model:
iSCSI Name:
iSCSI Alias:
Connected Targets: Devices: Paths:

The iSCSI Initiator Properties dialog box appears.

Step 11: In the iSCSI Initiator Properties dialog box, click **Configure**.



iSCSI Initiator (iSCSI Software Adapter) Properties

General | Dynamic Discovery | Static Discovery

iSCSI Properties

Name:

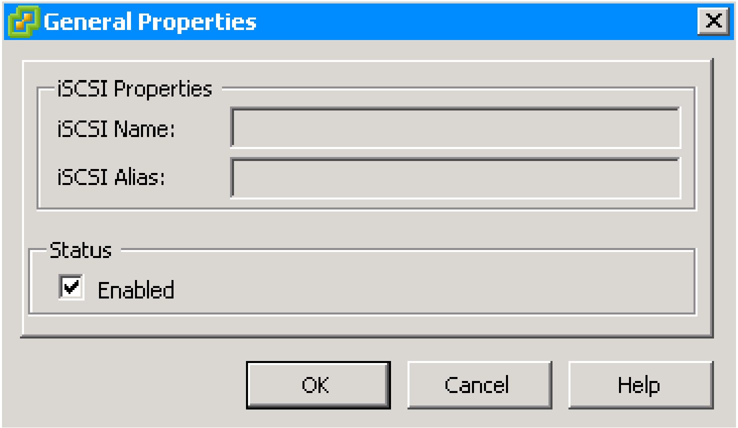
Alias:

Target discovery methods:

Software Initiator Properties

Status: Disabled

Step 12: Select the **Enabled** check box, and then click **OK**.



General Properties

iSCSI Properties

iSCSI Name:

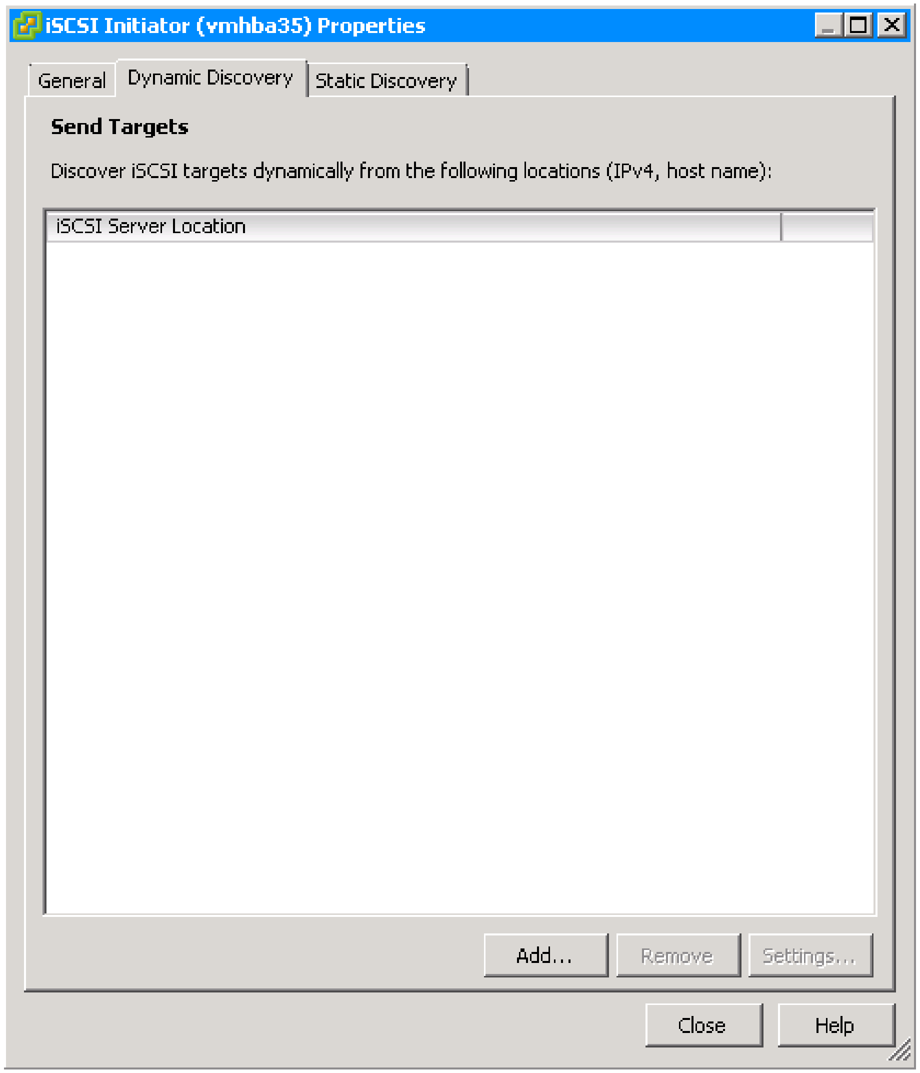
iSCSI Alias:

Status

☑ Enabled

The iSCSI name self-creates. If you need to change the name for your setup, click **Configure** again and edit the name.

Step 13: Click the Dynamic Discovery tab, and then click **Add**.



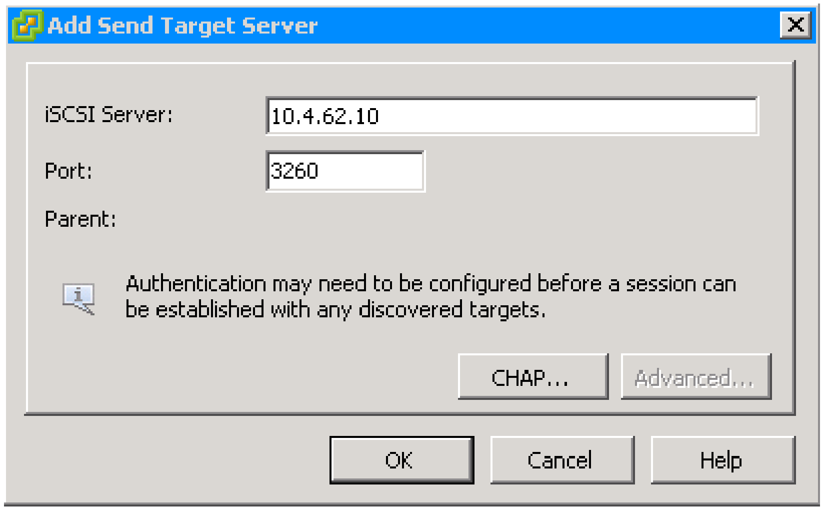
iSCSI Initiator (vmhba35) Properties

Send Targets

Discover iSCSI targets dynamically from the following locations (IPv4, host name):

iSCSI Server Location

Step 14: Enter the IP address of your iSCSI target array and verify that the port matches the array configuration, and then click **OK**.



Add Send Target Server

iSCSI Server: 10.4.62.10

Port: 3260

Parent:

Authentication may need to be configured before a session can be established with any discovered targets.

Step 15: On the properties window, click **Close**.

Step 16: When you are prompted to rescan the iSCSI software adapter, click **Yes**.

Step 17: If your array is properly masked for your ESXi host, after the scan is complete, your new iSCSI LUN is available, and you can add it as a datastore. For more information about adding a datastore, see the next procedure , “Add a datastore to ESXi hosts”.

If the storage array is not properly masked, you will not see the new storage. If this is the case, verify the mask settings on the storage array.

Option 2. Using Fibre Channel or FCoE storage

This procedure sets up access to shared storage for Cisco UCS B-Series and C-Series servers for a Fibre Channel or FCoE attached storage array. The Cisco UCS B-Series servers, which may be running as a diskless server, require this procedure for SAN boot as well as centralized storage for any VMs running on the server. The Cisco UCS C-Series servers doing local boot can use this procedure for setting up shared storage for the VMs running on the server.

VMware ESXi supports most Fibre Channel adapters. To verify support for your adapters, see the VMware Compatibility Guide at the following URL: http://www.vmware.com/resources/compatibility/search.php

Before you can add Fibre Channel storage, you must have prepared the network and storage array for the Fibre Channel target by completing Procedure 1 “Configure a storage array” and Procedure 2 “Configure SAN zones” of the Process “Preparing the Environment for Server Access to SAN.”

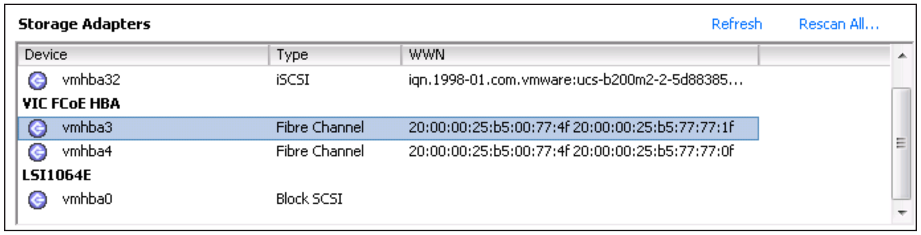
Also, FCoE vHBA and storage connectivity must have been deployed on the server as detailed in the *Cisco SBA—Data Center Unified Computing System Deployment Guide*.

Step 1: In vSphere Client, in the Host and Clusters tree, select the **ESXi host**, and then click the **Configuration** tab.

Step 2: Under **Configuration > Storage Adapters**, note the worldwide node name and worldwide port name of the HBAs. You must properly zone and mask the ports and their corresponding worldwide names to your particular array.

Reader Tip

For more information on configuring a SAN or storage array, see the *Data Center Deployment Guide* and the *NetApp Storage Deployment Guide*.



Storage Adapters

Device	Type	WWN
vmhba32	iSCSI	iqn.1998-01.com.vmware:ucs-b200m2-2-5d88385...
VIC FCoE HBA		
vmhba3	Fibre Channel	20:00:00:25:b5:00:77:4f 20:00:00:25:b5:77:77:1f
vmhba4	Fibre Channel	20:00:00:25:b5:00:77:4f 20:00:00:25:b5:77:77:0f
LSI1064E		
vmhba0	Block SCSI	

Step 3: After you have properly zoned and masked the Fibre Channel HBA, select **Rescan**.

After the scan is complete, your new Fibre Channel LUN is available, and you can add it as a datastore in the same manner as local storage. For more information, see the next procedure, ”Add a datastore to ESXi hosts”

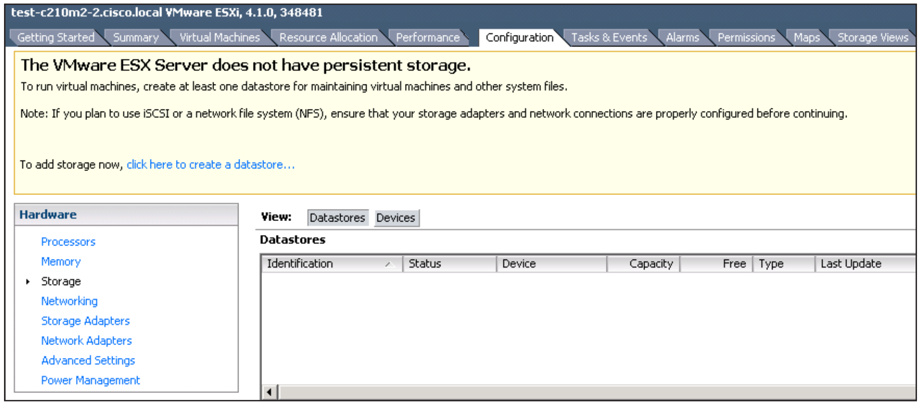
Procedure 3 Add a datastore to ESXi hosts

In this procedure, you will add storage for the virtual machines to use, as well as other system files. The storage can be a disk drive physically located on the server, or a Disk or LUN located on a shared storage array.

Step 1: Using vSphere Client, log in to the ESXi host.

Step 2: On the Configuration tab, in the Hardware work pane click on Storage.

If your ESXi host does not have a provisioned virtual machine file system (VMFS), you will see "The VMware ESX Server does not have persistent storage" message in the main window, click **Click here to create a datastore**.



The VMware ESX Server does not have persistent storage.

To run virtual machines, create at least one datastore for maintaining virtual machines and other system files.

Note: If you plan to use iSCSI or a network file system (NFS), ensure that your storage adapters and network connections are properly configured before continuing.

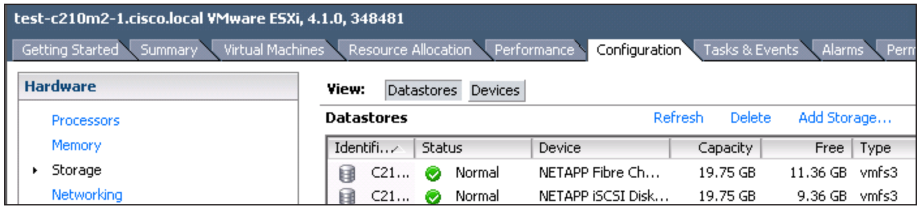
To add storage now, click here to create a datastore...

Datastores

Identification	Status	Device	Capacity	Free	Type	Last Update

If you have existing VMFS provisioned storage on your ESXi host, you will see the details of the storage system under the Configuration > Storage Adapters as shown in Table 2. To create a new datastore, in the Datastores workpane, click **Add Storage**.

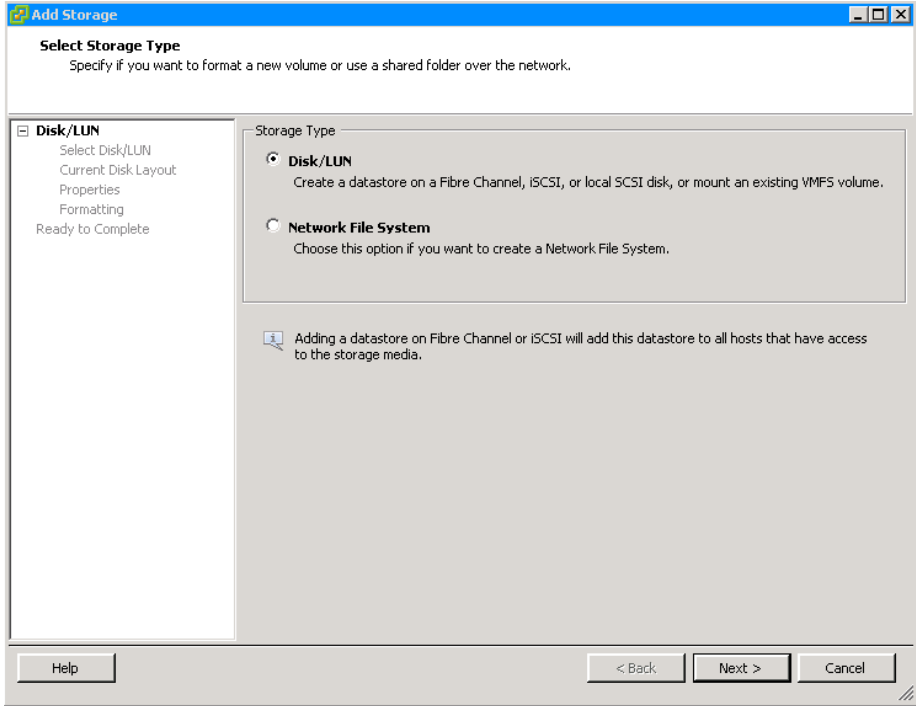
Figure 11 - Existing VMFS datastores on ESXi host



Datastores

Identifi...	Status	Device	Capacity	Free	Type
C21...	✓ Normal	NETAPP Fibre Ch...	19.75 GB	11.36 GB	vmfs3
C21...	✓ Normal	NETAPP iSCSI Disk...	19.75 GB	9.36 GB	vmfs3

Step 3: In the Add Storage wizard, select **Disk/LUN**, and then click **Next**.



Select Storage Type

Specify if you want to format a new volume or use a shared folder over the network.

Storage Type

● Disk/LUN

Create a datastore on a Fibre Channel, iSCSI, or local SCSI disk, or mount an existing VMFS volume.

○ Network File System

Choose this option if you want to create a Network File System.

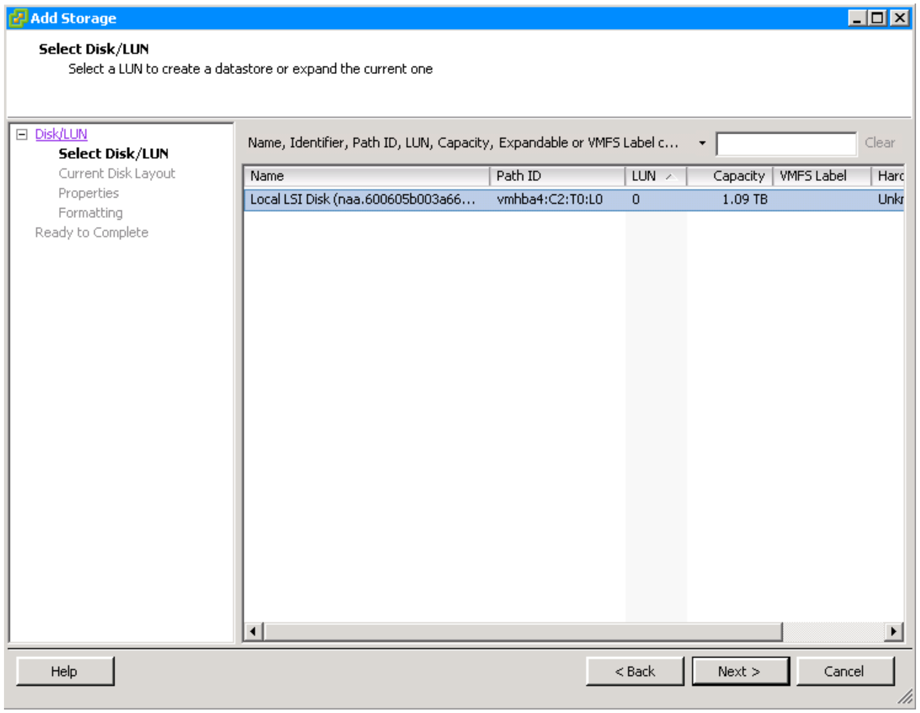
Adding a datastore on Fibre Channel or iSCSI will add this datastore to all hosts that have access to the storage media.

Step 4: On the Select Disk/LUN page, select the local disk or shared storage LUN, and then click **Next**. This list provides all data storage available to the ESXi host, including local hard disks installed in the machine and any remote data storage available to the host.

Tech Tip

When iSCSI or Fibre Channel storage is configured, their LUNs appear in the list on the Select Disk/LUN page, as illustrated in Step 5.

Figure 12 - Local disk drive



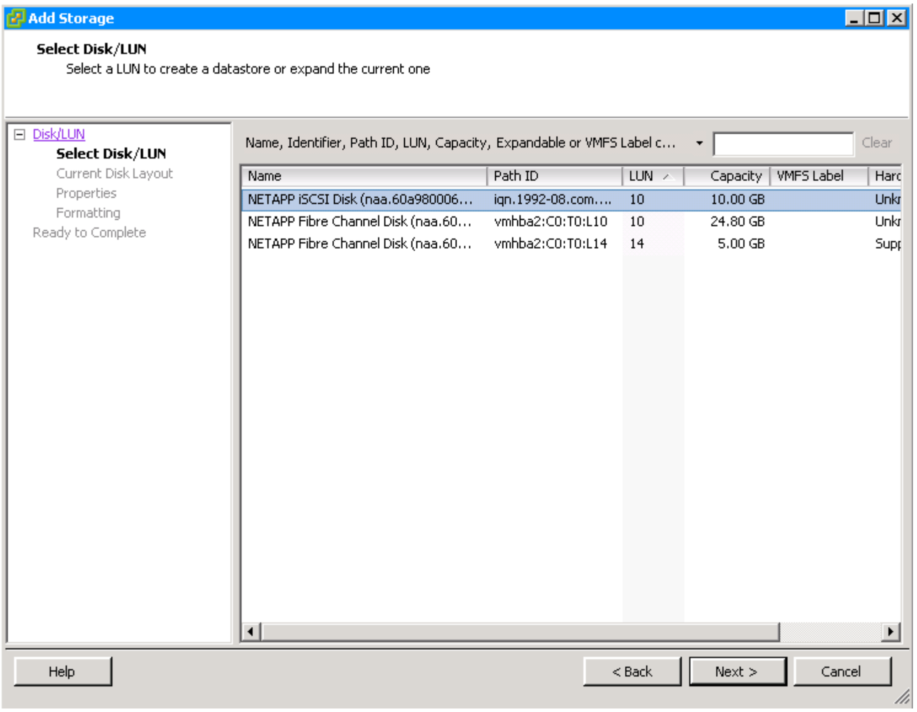
Add Storage

Select Disk/LUN

Select a LUN to create a datastore or expand the current one

Name	Path ID	LUN	Capacity	VMFS Label	Harc
Local LSI Disk (naa.600605b003a66…	vmhba4:C2:T0:L0	0	1.09 TB		Unkr

Figure 13 - Shared iSCSI and Fibre Channel LUNs



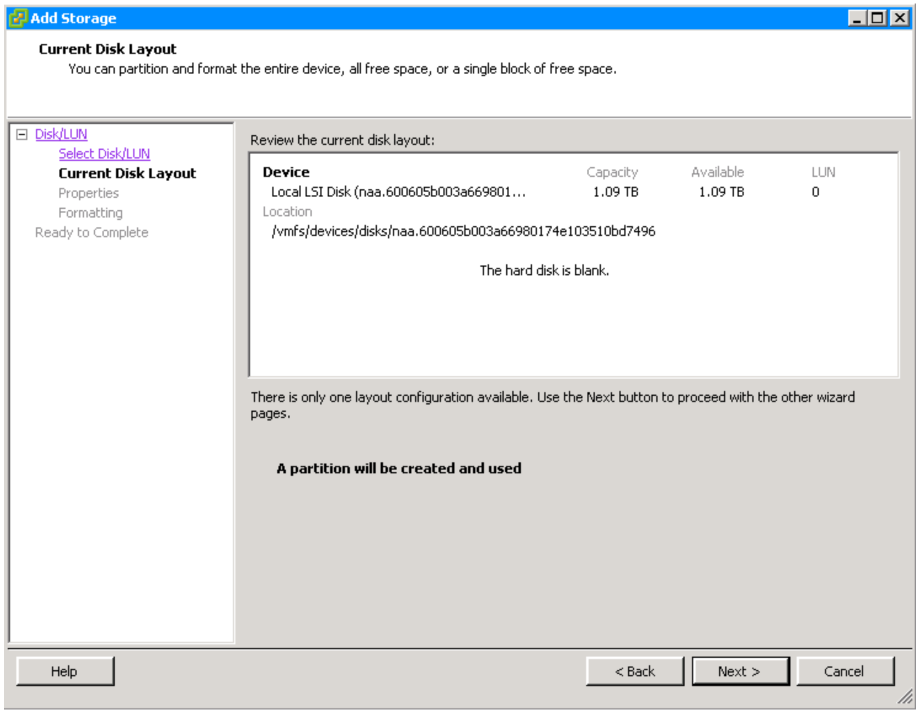
Add Storage

Select Disk/LUN

Select a LUN to create a datastore or expand the current one

Name	Path ID	LUN	Capacity	VMFS Label	Harc
NETAPP iSCSI Disk (naa.60a980006…	iqn.1992-08.com.…	10	10.00 GB		Unkr
NETAPP Fibre Channel Disk (naa.60…	vmhba2:C0:T0:L10	10	24.80 GB		Unkr
NETAPP Fibre Channel Disk (naa.60…	vmhba2:C0:T0:L14	14	5.00 GB		Supp

Step 5: Review the disk capacity and partition information, and then click **Next**.


Add Storage

Current Disk Layout

You can partition and format the entire device, all free space, or a single block of free space.

Review the current disk layout:

Device	Capacity	Available	LUN
Local LSI Disk (naa.600605b003a669801...	1.09 TB	1.09 TB	0

Location

/vmfs/devices/disks/naa.600605b003a66980174e103510bd7496

The hard disk is blank.

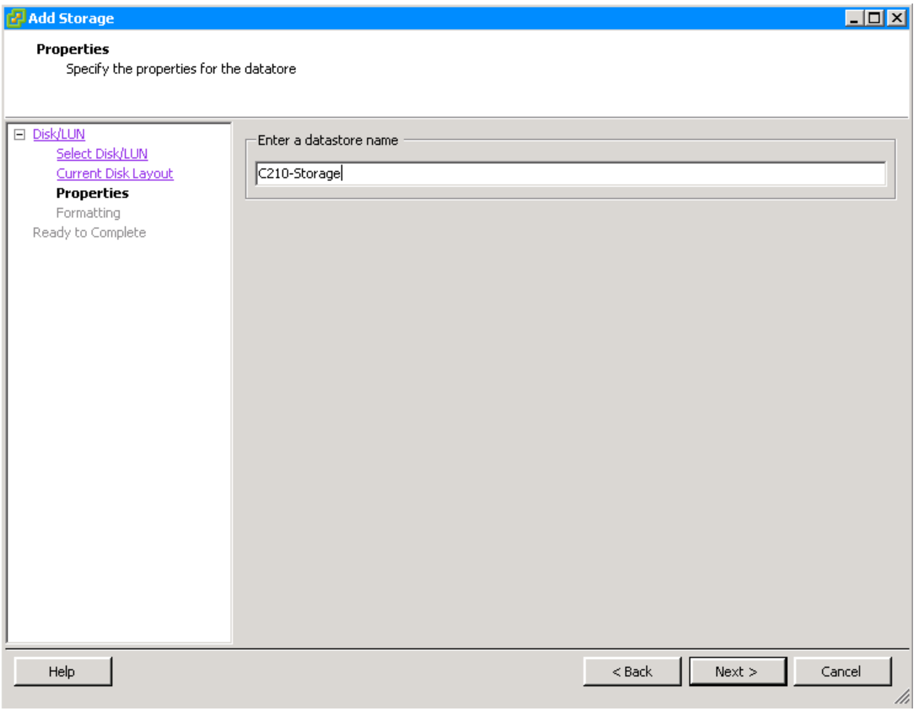
There is only one layout configuration available. Use the Next button to proceed with the other wizard pages.

A partition will be created and used

Step 6: Enter a datastore name, and then click **Next**.

Tech Tip

Use a descriptive name for the datastore, to help you identify which datastore is which when you add more of them.


Add Storage

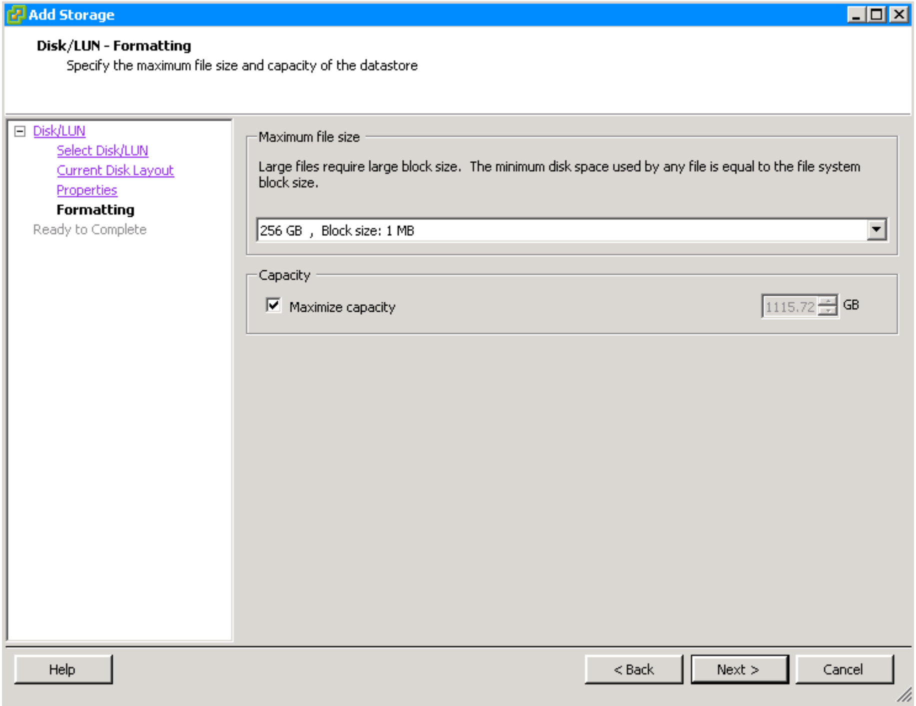
Properties

Specify the properties for the datatore

Enter a datastore name

C210-Storage

Step 7: On the Disk/LUN Formatting page, note that the default block size is 1 MB. The largest virtual disk that is supported on VMFS-3 with a block size of 1 MB is 256 GB. The block size should be carefully chosen based on the size of the largest file that must be stored. In this setup, accept the defaults by clicking **Next**.



Add Storage

Disk/LUN - Formatting

Specify the maximum file size and capacity of the datastore

Maximum file size

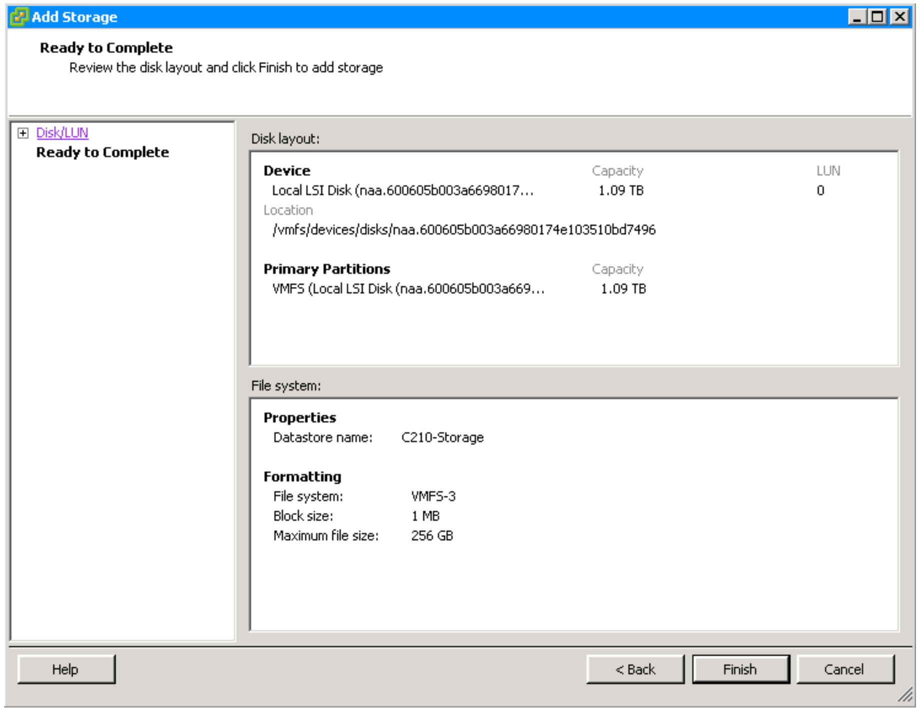
Large files require large block size. The minimum disk space used by any file is equal to the file system block size.

256 GB , Block size: 1 MB

Capacity

☑ Maximize capacity 1115.72 GB

Step 8: Click **Finish**. The Add Storage wizard is completed.



Add Storage

Ready to Complete

Review the disk layout and click Finish to add storage

Disk layout:

Device Capacity LUN

Local LSI Disk (naa.600605b003a6698017... 1.09 TB 0

Location

/vmfs/devices/disks/naa.600605b003a66980174e103510bd7496

Primary Partitions Capacity

VMFS (Local LSI Disk (naa.600605b003a669... 1.09 TB

File system:

Properties

Datastore name: C210-Storage

Formatting

File system: VMFS-3

Block size: 1 MB

Maximum file size: 256 GB

Process

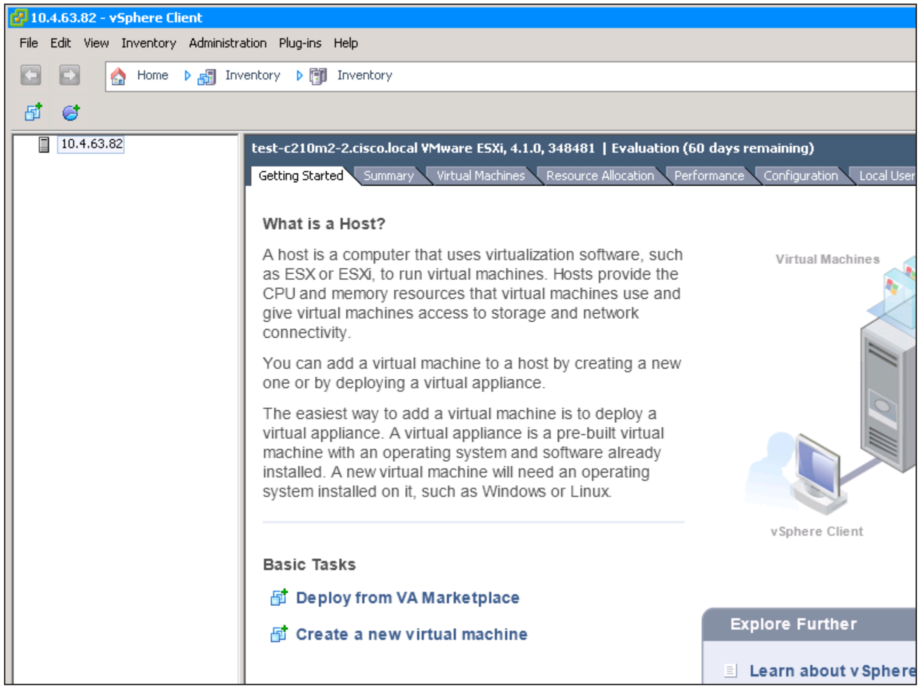
Creating a Virtual Machine

1. Run the Create Virtual Machine wizard
2. Edit virtual machine settings
3. Install a guest operating system
4. Install VMware tools

With ESXi installed, vSphere Client installed and connected, and the datastore created, it is now time to create a virtual machine. This first virtual machine will support vSphere vCenter. This requires a 64-bit operating system. For this example, Windows Server 2008 64-bit is used.

Procedure 1 Run the Create Virtual Machine wizard

Step 1: In vSphere Client, on the Getting Started tab, click **Create a new virtual machine**.



test-c210m2-2.cisco.local VMware ESXi, 4.1.0, 348481 | Evaluation (60 days remaining)

What is a Host?

A host is a computer that uses virtualization software, such as ESX or ESXi, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and give virtual machines access to storage and network connectivity.

You can add a virtual machine to a host by creating a new one or by deploying a virtual appliance.

The easiest way to add a virtual machine is to deploy a virtual appliance. A virtual appliance is a pre-built virtual machine with an operating system and software already installed. A new virtual machine will need an operating system installed on it, such as Windows or Linux.

Basic Tasks

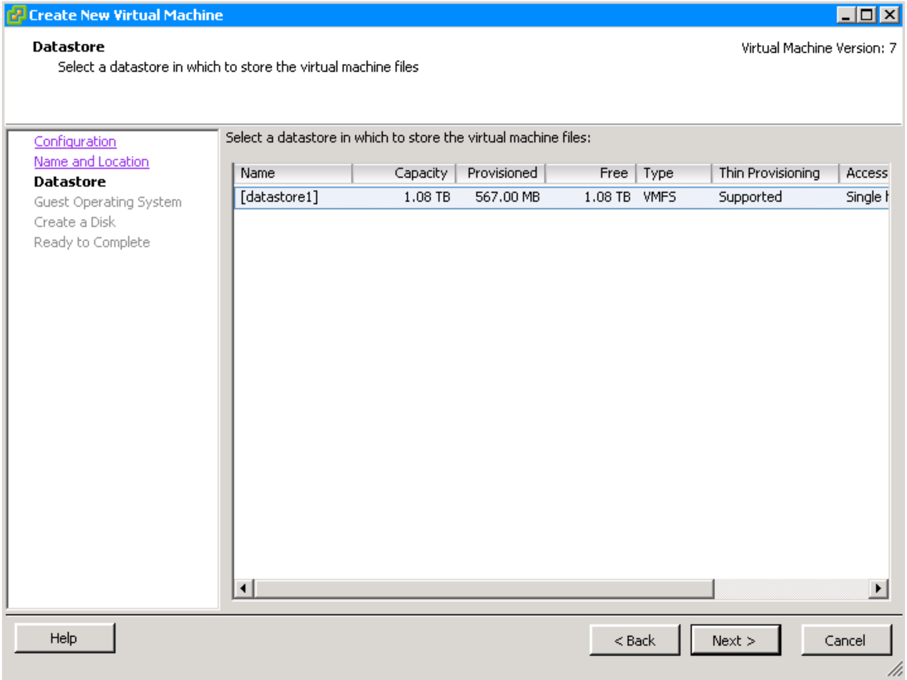
Deploy from VA Marketplace

Create a new virtual machine

Step 2: On the Configuration page, select **Typical**, and then click **Next**.

Step 3: Name the virtual machine, and then click **Next**.

Step 4: Select the datastore created previously, and then click **Next**.



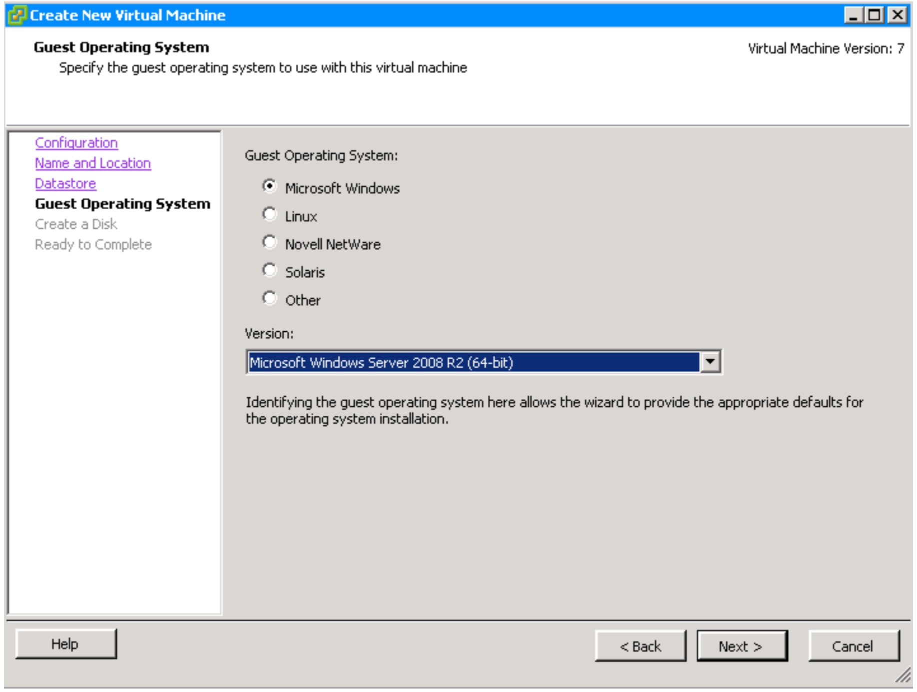
Datastore
Select a datastore in which to store the virtual machine files

Virtual Machine Version: 7

Select a datastore in which to store the virtual machine files:

Name	Capacity	Provisioned	Free	Type	Thin Provisioning	Access
[datastore1]	1.08 TB	567.00 MB	1.08 TB	VMFS	Supported	Single h

Step 5: Select the guest operating system for the virtual machine, and then click **Next**.



Guest Operating System

Specify the guest operating system to use with this virtual machine

Virtual Machine Version: 7

Guest Operating System:

● Microsoft Windows
○ Linux
○ Novell NetWare
○ Solaris
○ Other

Version: Microsoft Windows Server 2008 R2 (64-bit)

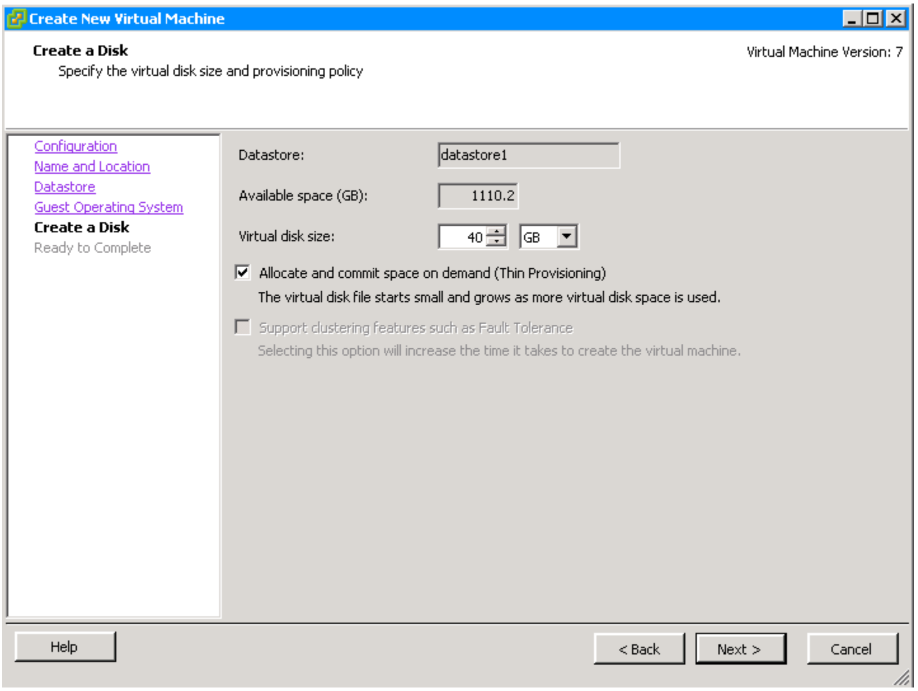
Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Tech Tip

Be careful that you select the correct operating system (64-bit, 32-bit, etc.) because this aligns the data partitions for the operating system for optimum efficiency. If you install a different operating system than what was selected, performance issues can arise.

Step 6: On the Create a Disk page, enter a virtual disk size, and then click **Next**. Ensure that the disk size matches your operating system requirements and does not exceed the available datastore.

In the following figure, the default disk size of 40 Gb is used. The example uses thin provisioning in order to conserve actual datastore used versus what is provisioned. With thin provisioning, VMware VMFS starts the actual provisioned disk space on the storage system small and then increases the storage as the system requires more storage.



Create a Disk

Specify the virtual disk size and provisioning policy

Virtual Machine Version: 7

Datastore: datastore1

Available space (GB): 1110.2

Virtual disk size: 40 GB

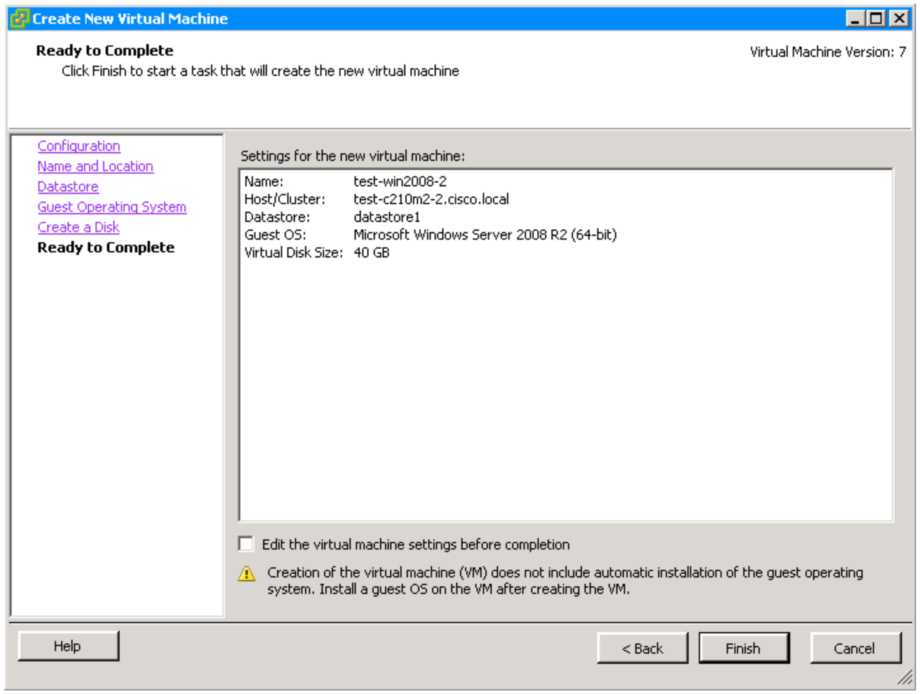
☑ Allocate and commit space on demand (Thin Provisioning)

The virtual disk file starts small and grows as more virtual disk space is used.

□ Support clustering features such as Fault Tolerance

Selecting this option will increase the time it takes to create the virtual machine.

Step 7: On the Ready to Complete page, review the information, and then click **Finish**. The virtual machine is created.



Ready to Complete

Click Finish to start a task that will create the new virtual machine

Virtual Machine Version: 7

Settings for the new virtual machine:

Name:	test-win2008-2
Host/Cluster:	test-c210m2-2.cisco.local
Datastore:	datastore1
Guest OS:	Microsoft Windows Server 2008 R2 (64-bit)
Virtual Disk Size:	40 GB

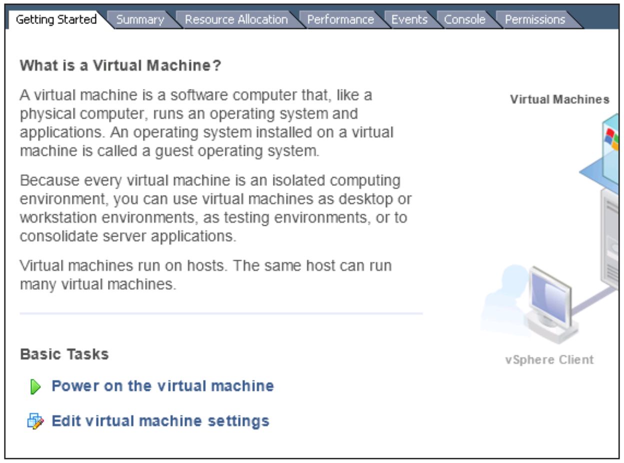
□ Edit the virtual machine settings before completion

⚠ Creation of the virtual machine (VM) does not include automatic installation of the guest operating system. Install a guest OS on the VM after creating the VM.

Procedure 2 Edit virtual machine settings

In this procedure, you configure settings for the virtual machine that were not available in the Create New Virtual Machine Wizard, such as memory, number of dedicated CPUs, and network connectivity.

Step 1: In vSphere Client, in the tree, select the newly created virtual machine, and then on the General tab, click **Edit virtual machine settings**.



What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

Virtual machines run on hosts. The same host can run many virtual machines.

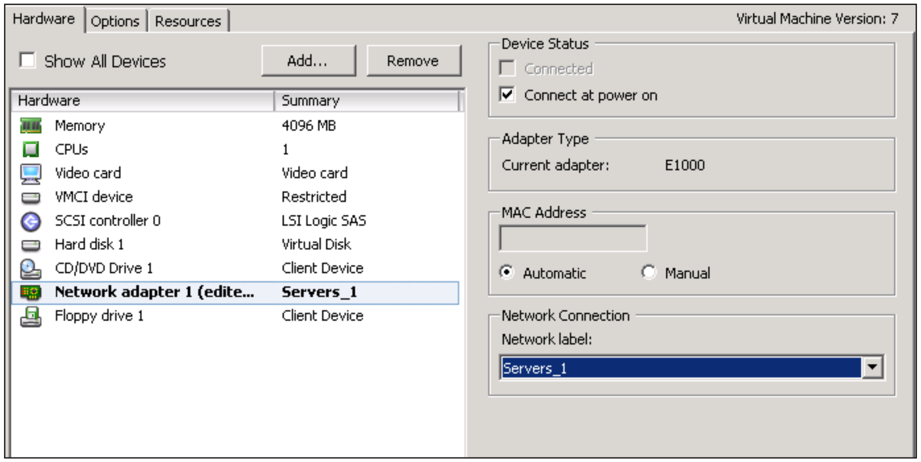
Basic Tasks

Power on the virtual machine

Edit virtual machine settings

Step 2: On the Virtual Machine Properties dialog box, in the list, select **Network Adapter 1**.

Step 3: In the **Network label** drop-down list, choose the network you configured in Step 8 of the “Run the Add Networking Wizard” procedure.



Virtual Machine Version: 7

□ Show All Devices

Hardware	Summary
Memory	4096 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk
CD/DVD Drive 1	Client Device
Network adapter 1 (edite...	**Servers_1**
Floppy drive 1	Client Device

Device Status

□ Connected

☑ Connect at power on

Adapter Type

Current adapter: E1000

MAC Address

● Automatic ○ Manual

Network Connection

Network label: Servers_1

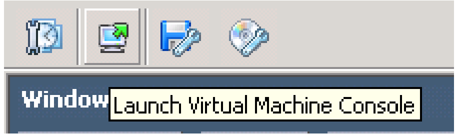
Procedure 3 Install a guest operating system

Now the virtual machine is ready for its guest operating system. There are several ways to connect to the installation media for the operating system:

- DVD local to the ESXi host
- DVD mounted on your local vSphere Client host
- ISO image on a ESXi datastore
- ISO image is present on the local disk drive of the vSphere Client host

For this procedure, an ISO image is present on the disk drive of the local machine running vSphere Client. In such cases, you must power on the virtual machine before you can attach a disk or start the installation.

Step 1: In the vSphere Client, in the tree, select your virtual machine, and then in the toolbar, click **Launch Virtual Machine Console**. A separate console window opens.

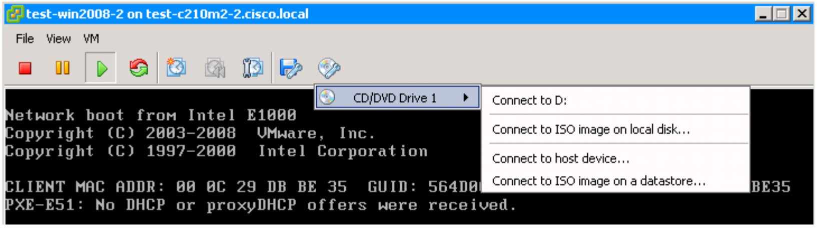


Tech Tip

A Console tab appears in the work pane when the virtual machine is highlighted in the navigation pane. This is the same console, just in a smaller window.

Step 2: Press the **Play** button (green triangle).

Step 3: Click the **CD/DVD** icon in the toolbar, choose **Connect to ISO image on local disk**, and then specify the appropriate image.


test-win2008-2 on test-c210m2-2.cisco.local
File View VM
CD/DVD Drive 1
Connect to D:
Connect to ISO image on local disk...
Connect to host device...
Connect to ISO image on a datastore...

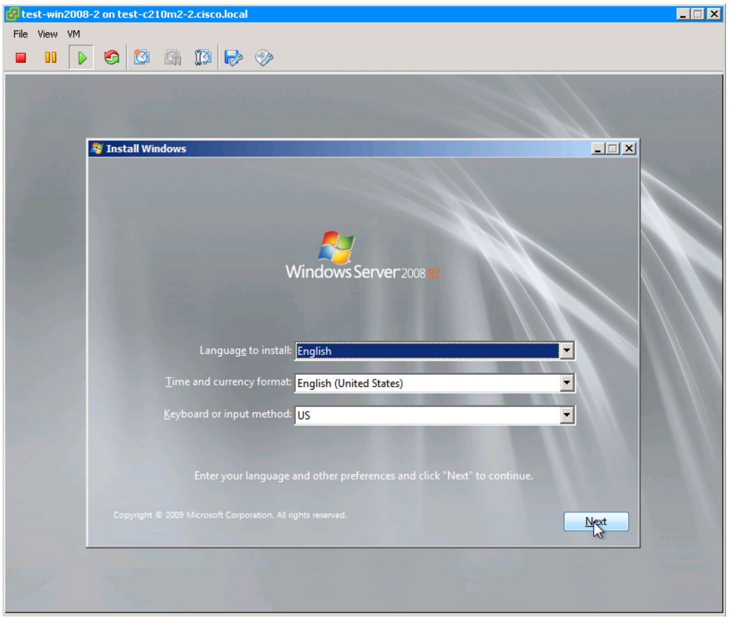
```
Network boot from Intel E1000
Copyright (C) 2003-2008  VMware, Inc.
Copyright (C) 1997-2000  Intel Corporation

CLIENT MAC ADDR: 00 0C 29 DB BE 35  GUID: 564D0                  BE35
PXE-E51: No DHCP or proxyDHCP offers were received.
```

Tech Tip

To regain control of the mouse from a console window, press **Ctrl-Alt**, and the mouse will be released.

Step 4: Click the VM tab, and then **select VM > Guest > Send Key > Ctrl-Alt-Del.** The virtual machine reboots to the attached ISO file.

The Install Windows dialog box for Windows 2008 is shown in the following figure. Other operating system installations work similarly; Windows Server 2008 was chosen arbitrarily.



Language to install: English

Time and currency format: English (United States)

Keyboard or input method: US

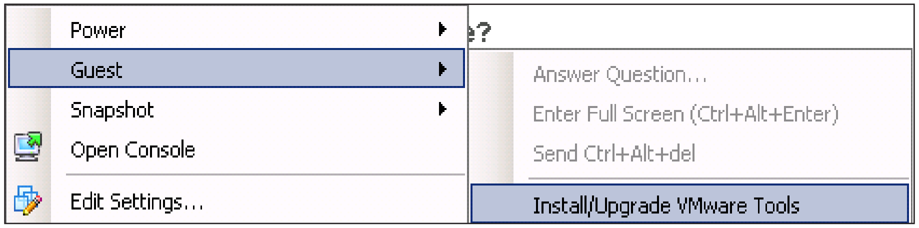
Enter your language and other preferences and click "Next" to continue.

Copyright © 2009 Microsoft Corporation. All rights reserved.

Procedure 4 Install VMware tools

VMware tools greatly enhance graphics and mouse performance in the virtual machine console. VMware tools also help with power-up and power-down of virtual machines from vSphere Client. When the operating system installation is complete, you can install VMware tools.

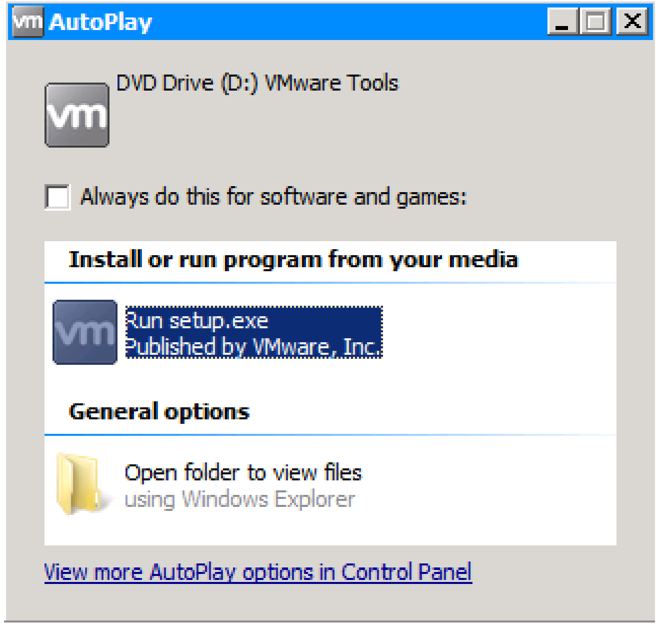
Step 1: In vSphere Client, in the tree, right-click the virtual machine, and then choose **Guest > Install/Upgrade VMware Tools**.



ESXi now installs the VMware tools on the host operating system by mounting the tools to the operating system as an attached disk. The operating system—whether it is Windows, Red Hat, or any other supported operating system—then initiates installation and prompts the user to install the tools.

Step 2: Follow the prompts.

Figure 14 - Tools install prompt in Windows Server 2008


AutoPlay
DVD Drive (D:) VMware Tools
□ Always do this for software and games:
Install or run program from your media
Run setup.exe
Published by VMware, Inc.
General options
Open folder to view files
using Windows Explorer
View more AutoPlay options in Control Panel

Tech Tip

Make sure to update VMware tools after each ESXi upgrade.

Process

Installing and Configuring VMware vCenter

1. Install VMware vCenter
2. Create a data center
3. Create a cluster
4. Add an ESXi server to the data center
5. License vCenter
6. License ESXi hosts

Previous sections described how to manage a single server with vSphere Client connected directly to the ESXi host. In order to manage multiple servers running ESXi and get the other features like vMotion, DRS, or HA, you must set up a vCenter. This requires connecting the vSphere Client to a vCenter to manage the hosts.

Procedure 1 Install VMware vCenter

Step 1: Using operating-system administrative tools, add the user who will own the vCenter process. For this example, the Windows user vCenter owner was added with administrator privileges.

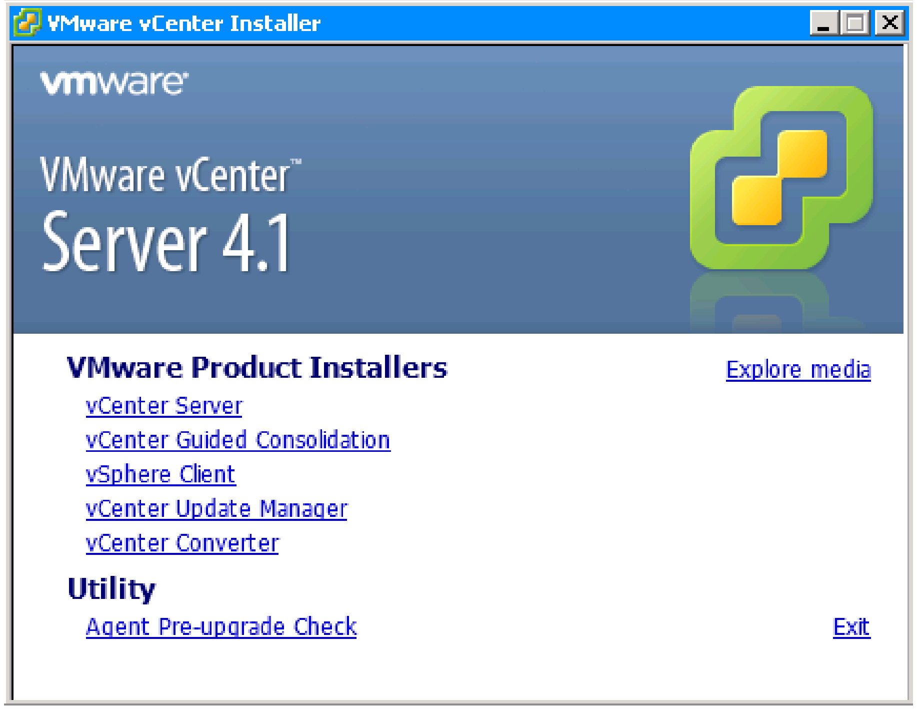
Tech Tip

To function properly, vCenter Server 4.1 requires a 64-bit operating system.

Step 2: Obtain the vCenter Server image (from a disc, ISO, download, etc.) and copy it to your server.

Step 3: Unzip the vCenter image on the new virtual machine you created in the previous process, "Creating a Virtual Machine."

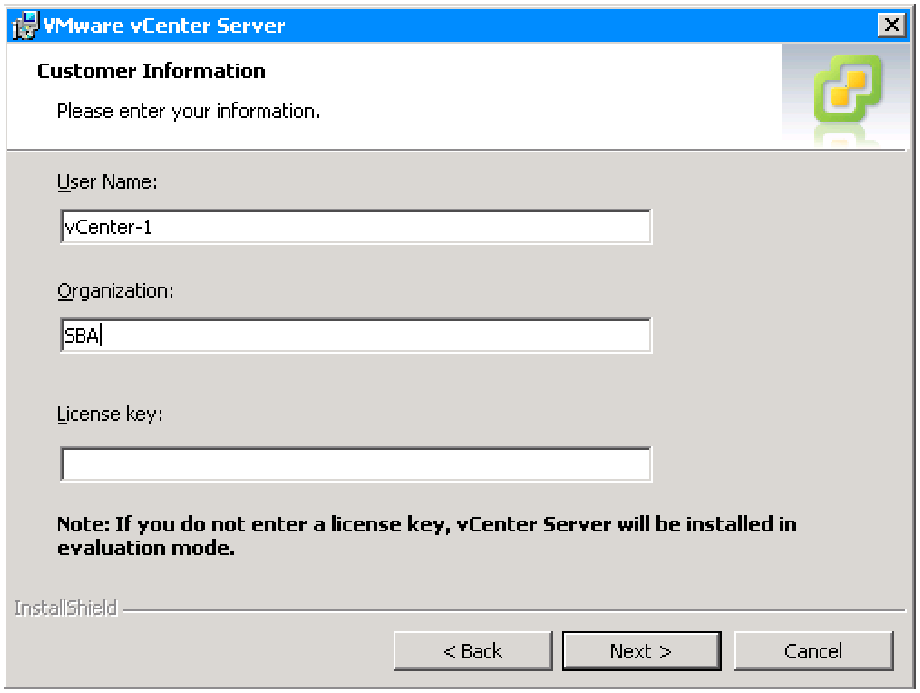
Step 4: Run the VMware vCenter Installer. The following screen appears.



Step 5: Click **vCenter Server**. The VMware vCenter Server wizard starts.

Step 6: Follow the instructions in the wizard. Note the following:

- On the Customer Information page, enter your username and organization, and then click **Next**. This installation uses an evaluation mode license, which is valid for 60 days. If a valid license came with a purchase of vCenter, it can be entered now or after the installation.



VMware vCenter Server

Customer Information

Please enter your information.

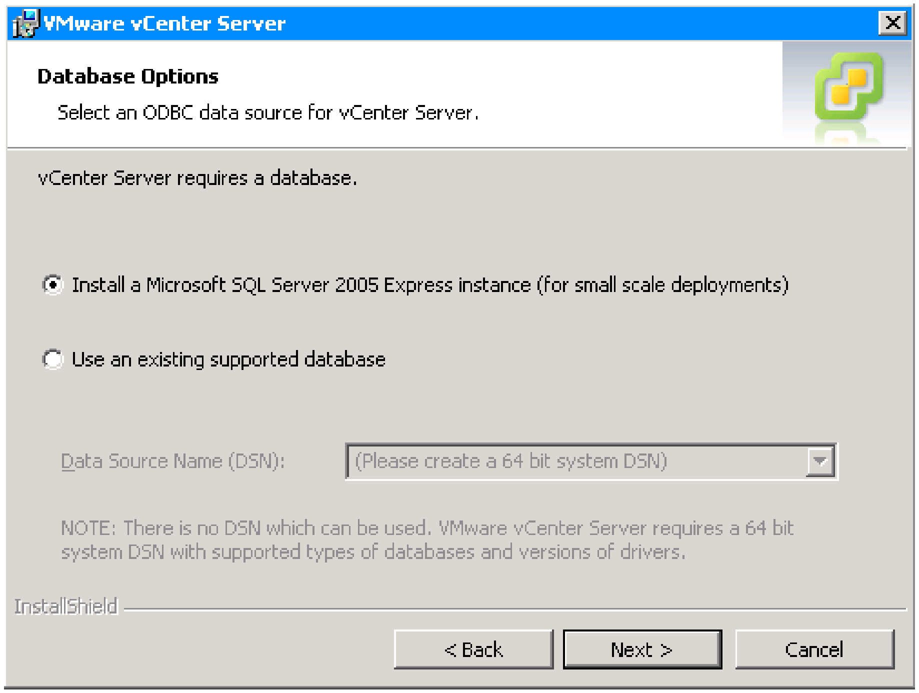
User Name: vCenter-1

Organization: SBA

License key:

Note: If you do not enter a license key, vCenter Server will be installed in evaluation mode.

- On the Database Options page, choose an ODBC data source for vCenter Server, and then click **Next**.



VMware vCenter Server

Database Options

Select an ODBC data source for vCenter Server.

vCenter Server requires a database.

● Install a Microsoft SQL Server 2005 Express instance (for small scale deployments)

○ Use an existing supported database

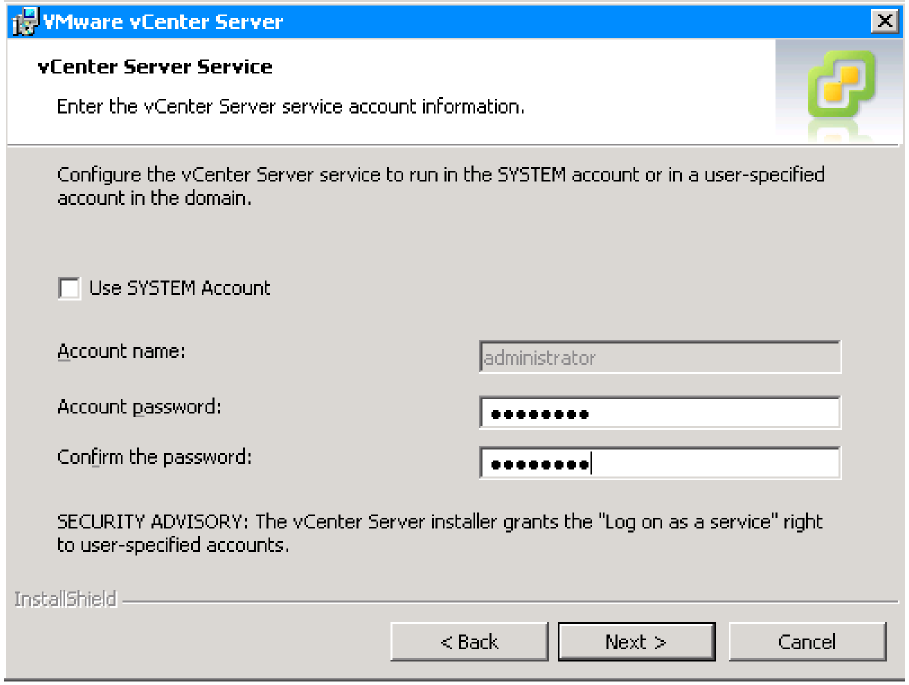
Data Source Name (DSN): (Please create a 64 bit system DSN)

NOTE: There is no DSN which can be used. VMware vCenter Server requires a 64 bit system DSN with supported types of databases and versions of drivers.

Tech Tip

Many customers purchase their own SQL database for this use. This example uses Microsoft SQL Server 2005 Express, which is included in the vCenter software package and is only suited for smaller VMware environments. For larger implementations, other databases are supported. Refer to the VMware website for specific information on database sizing.

- On the vCenter Server Service page, the best practice is for you to clear the **Use System Account** check box, and create a separate user account—specifically for vCenter—with proper services privileges.



VMware vCenter Server

vCenter Server Service

Enter the vCenter Server service account information.

Configure the vCenter Server service to run in the SYSTEM account or in a user-specified account in the domain.

□ Use SYSTEM Account

Account name: administrator

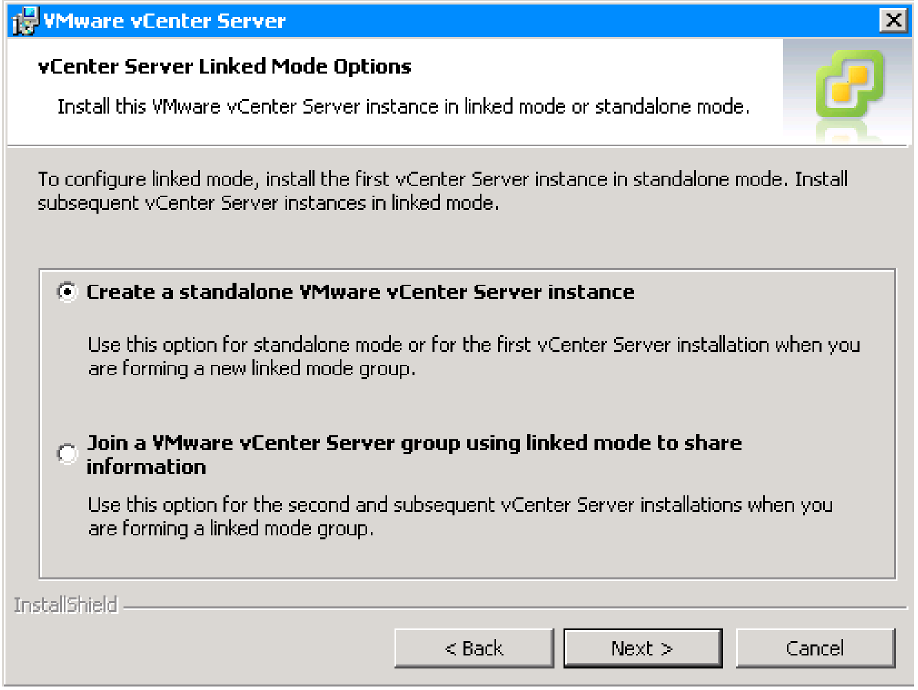
Account password: ●●●●●●●●●

Confirm the password: ●●●●●●●●●

SECURITY ADVISORY: The vCenter Server installer grants the "Log on as a service" right to user-specified accounts.

Click **Next**, and continue to follow the instructions in the wizard.

- On the vCenter Server Linked Mode Options page, for this example, select **Create a standalone VMware vCenter Server instance**, and then click **Next**.



VMware vCenter Server

vCenter Server Linked Mode Options

Install this VMware vCenter Server instance in linked mode or standalone mode.

To configure linked mode, install the first vCenter Server instance in standalone mode. Install subsequent vCenter Server instances in linked mode.

● **Create a standalone VMware vCenter Server instance**

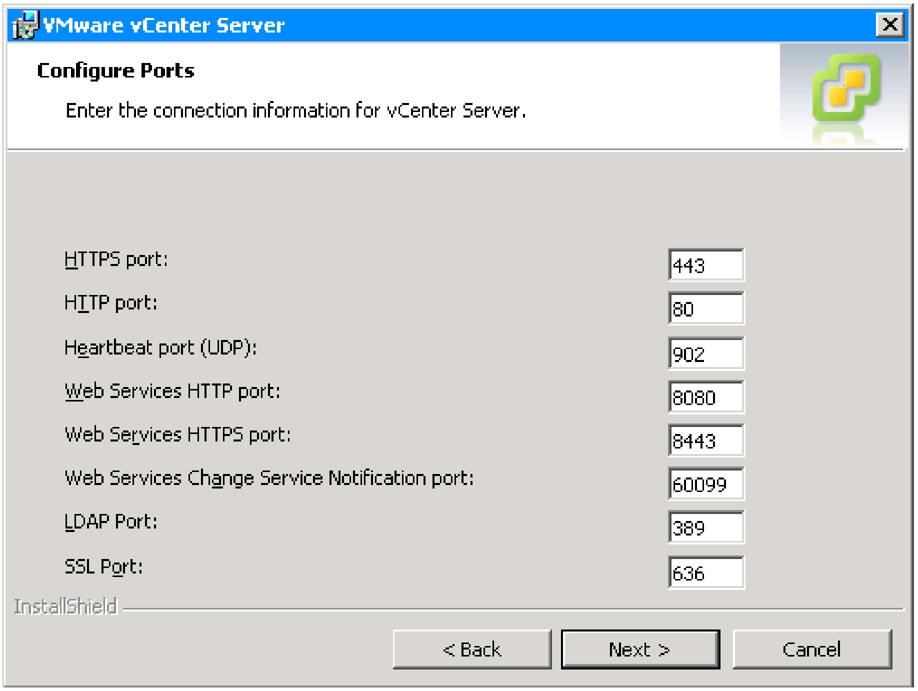
Use this option for standalone mode or for the first vCenter Server installation when you are forming a new linked mode group.

○ **Join a VMware vCenter Server group using linked mode to share information**

Use this option for the second and subsequent vCenter Server installations when you are forming a linked mode group.

- If vCenter services need to run on different ports for security or policy reasons, on the Configure Ports page, enter the appropriate ports, and then click **Next**.

  If the services can run on the default ports, click **Next**.



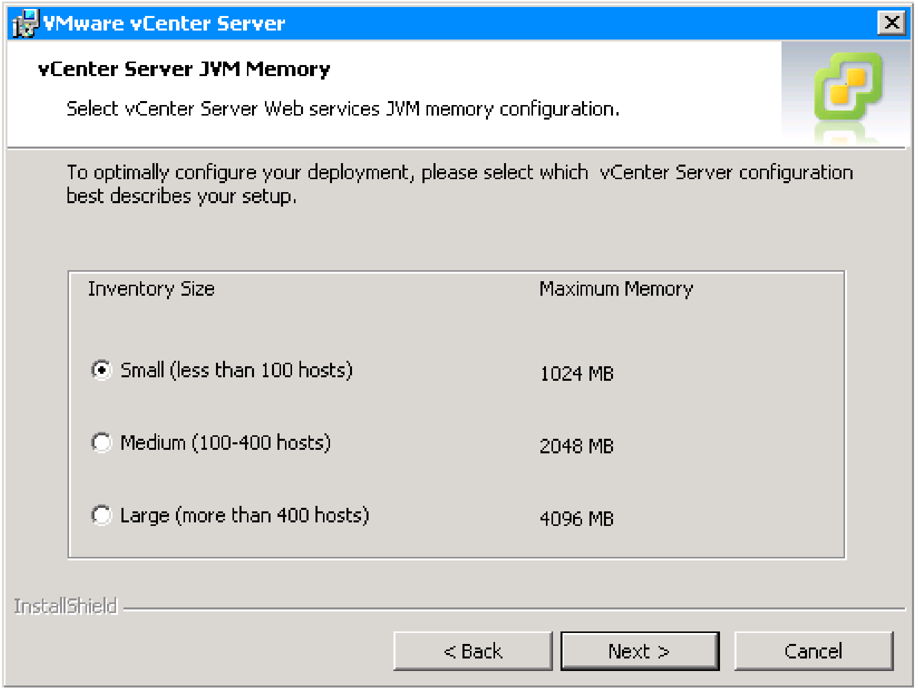
VMware vCenter Server

Configure Ports

Enter the connection information for vCenter Server.

HTTPS port:	443
HTTP port:	80
Heartbeat port (UDP):	902
Web Services HTTP port:	8080
Web Services HTTPS port:	8443
Web Services Change Service Notification port:	60099
LDAP Port:	389
SSL Port:	636

Step 7: Select **Small**, and then click **Next**. This installation is for less than 100 hosts.



VMware vCenter Server

vCenter Server JVM Memory

Select vCenter Server Web services JVM memory configuration.

To optimally configure your deployment, please select which vCenter Server configuration best describes your setup.

Inventory Size	Maximum Memory
● Small (less than 100 hosts)	1024 MB
○ Medium (100-400 hosts)	2048 MB
○ Large (more than 400 hosts)	4096 MB

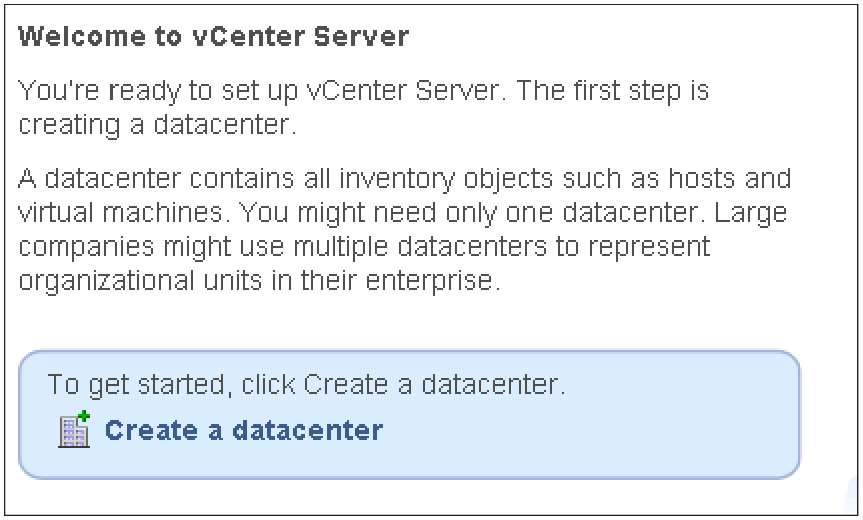
Step 8: Continue following the instructions in the wizard, accepting default values, until it finishes.

Procedure 2 Create a data center

Now that vCenter is installed, you must configure it to manage the previously installed ESXi hosts. To do so, you must first create the data center to which you will add the ESXi hosts.

Step 1: Start vSphere Client, and then enter the IP address and login credentials of the newly installed vCenter Server.

Step 2: On the screen that appears, click **Create a datacenter**.



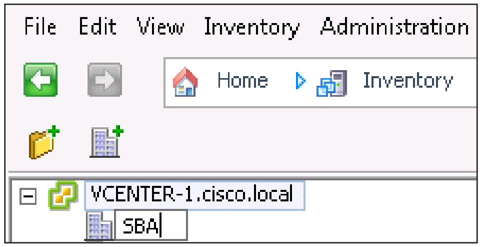
Welcome to vCenter Server

You're ready to set up vCenter Server. The first step is creating a datacenter.

A datacenter contains all inventory objects such as hosts and virtual machines. You might need only one datacenter. Large companies might use multiple datacenters to represent organizational units in their enterprise.

To get started, click Create a datacenter.

Step 3: In the tree, enter a name for the new data center.



VCENTER-1.cisco.local

SBA

Procedure 3 Create a cluster

(Optional)

A *cluster* is a collection of multiple ESX/ESXi hosts and associated virtual machines with shared resources and a shared management interface. When you add an ESX/ESXi host to a cluster, the host's resources become part of the cluster's resources. You can further enhance your environment by enabling features like VMware HA and DRS. VMware HA provides high availability for applications running in virtual machines. When a server failure occurs, affected virtual machines are automatically restarted on other servers that have spare capacity. DRS can provide migration recommendations or can migrate virtual machines based on continuously monitoring the distribution and usage of CPU and memory resources on all hosts and virtual machines in a cluster, resulting in a balanced cluster workload

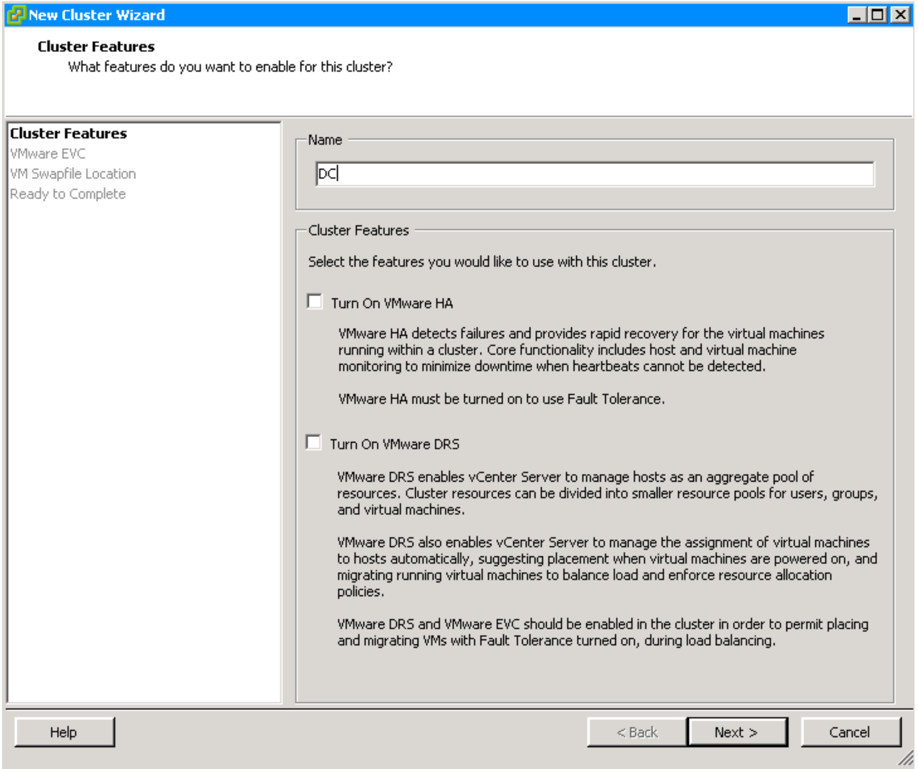
Step 1: In the Inventory tree, right-click **Datacenter**, and then click **New Cluster.**

Step 2: Enter an appropriate name for the cluster, and then click **Next**.

Tech Tip

You can use turn on VMware HA or VMware DRS by selecting the check boxes next to the feature names Setting up these advanced features is not discussed in this guide.

For more information, please see the following:
http://www.vmware.com/pdf/vmware_ha_wp.pdf



Cluster Features

What features do you want to enable for this cluster?

Name: DC

Cluster Features

Select the features you would like to use with this cluster.

☐ Turn On VMware HA

VMware HA detects failures and provides rapid recovery for the virtual machines running within a cluster. Core functionality includes host and virtual machine monitoring to minimize downtime when heartbeats cannot be detected.

VMware HA must be turned on to use Fault Tolerance.

☐ Turn On VMware DRS

VMware DRS enables vCenter Server to manage hosts as an aggregate pool of resources. Cluster resources can be divided into smaller resource pools for users, groups, and virtual machines.

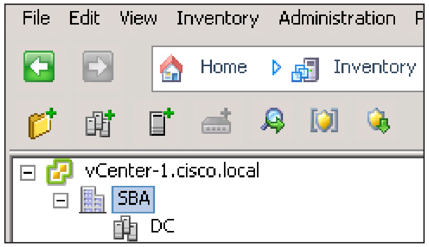
VMware DRS also enables vCenter Server to manage the assignment of virtual machines to hosts automatically, suggesting placement when virtual machines are powered on, and migrating running virtual machines to balance load and enforce resource allocation policies.

VMware DRS and VMware EVC should be enabled in the cluster in order to permit placing and migrating VMs with Fault Tolerance turned on, during load balancing.

Step 3: Leave the VMware EVC set to default, and then click **Next.**

Step 4: Leave the Swapfile Policy for Virtual Machines set to default, and then click **Next.**

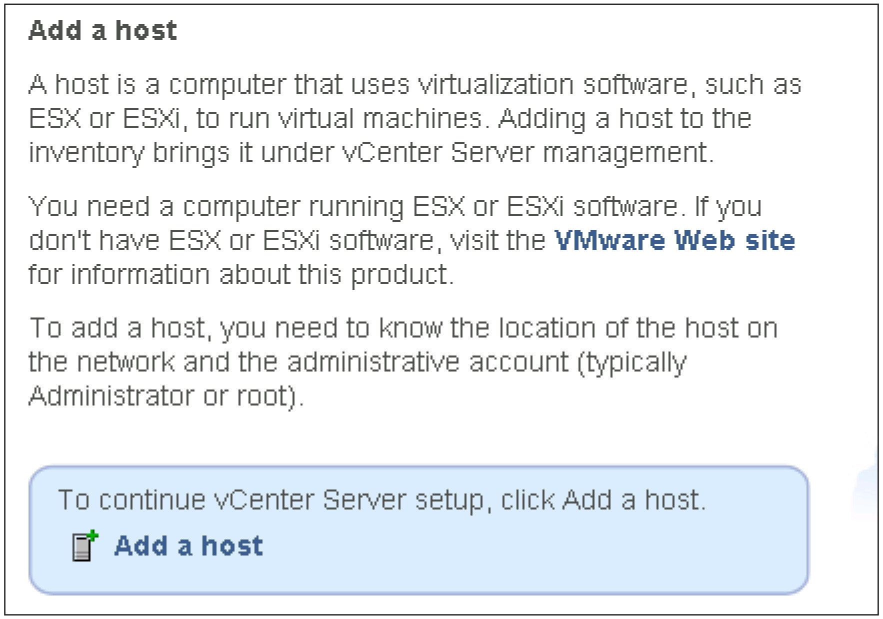
Step 5: Click **Finish.** This completes the creation of a cluster. When a cluster has been created, the ESXi hosts can be added to the cluster by dragging the host into the cluster in the navigation pane.



Procedure 4 Add an ESXi server to the data center

With the data center created, ESXi servers now can be added.

Step 1: Click **Add a Host**.



Add a host

A host is a computer that uses virtualization software, such as ESX or ESXi, to run virtual machines. Adding a host to the inventory brings it under vCenter Server management.

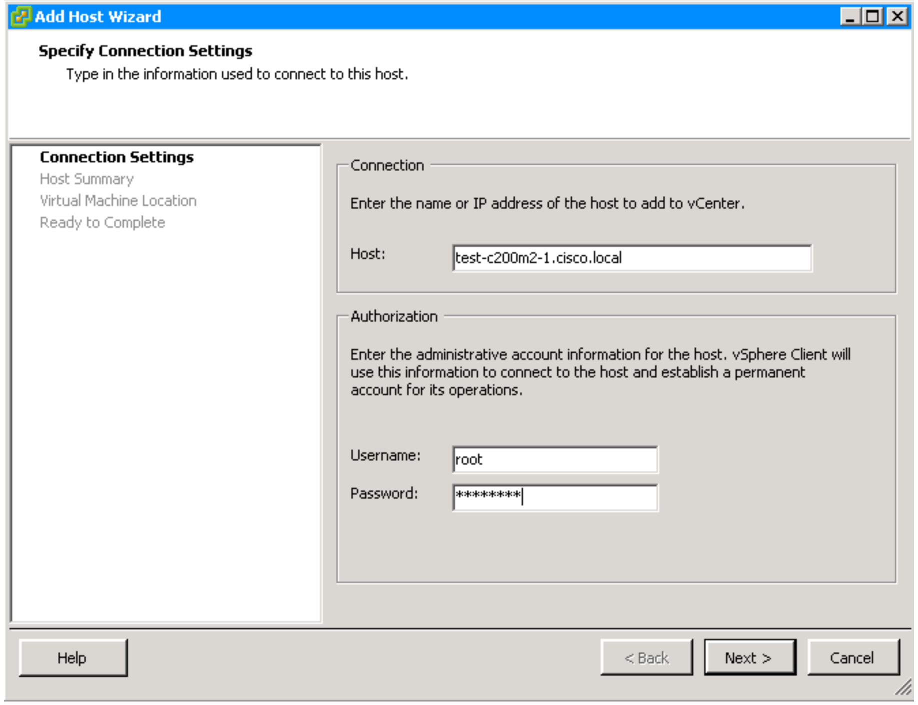
You need a computer running ESX or ESXi software. If you don't have ESX or ESXi software, visit the **VMware Web site** for information about this product.

To add a host, you need to know the location of the host on the network and the administrative account (typically Administrator or root).

To continue vCenter Server setup, click Add a host.

Add a host

Step 2: In the Add Host Wizard, enter the Name or IP address, username, and password you configured in the "Mapping the ESXi ISO file using virtual KVM" process, and then click **Next**.



Add Host Wizard

Specify Connection Settings

Type in the information used to connect to this host.

Connection Settings
Host Summary
Virtual Machine Location
Ready to Complete

Connection

Enter the name or IP address of the host to add to vCenter.

Host: test-c200m2-1.cisco.local

Authorization

Enter the administrative account information for the host. vSphere Client will use this information to connect to the host and establish a permanent account for its operations.

Username: root

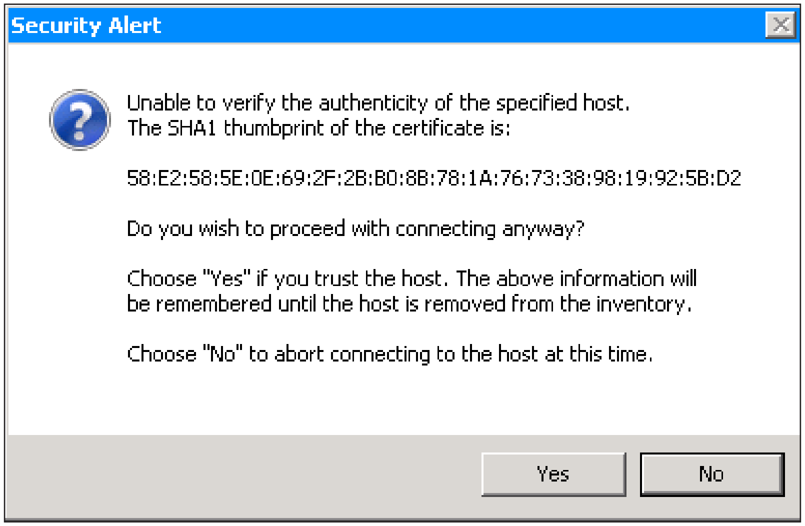
Password: *********

Help | < Back | Next > | Cancel

Tech Tip

To have a host appear by name, be sure to add the host into your DNS and add the host to vCenter by name instead of by IP address. To change a host after it has been added, you have to remove it and then add it again.

Step 3: On the security warning that appears, click **Yes**. The warning appears because this is the first time this host has been seen by the vCenter.



Security Alert

Unable to verify the authenticity of the specified host.
The SHA1 thumbprint of the certificate is:

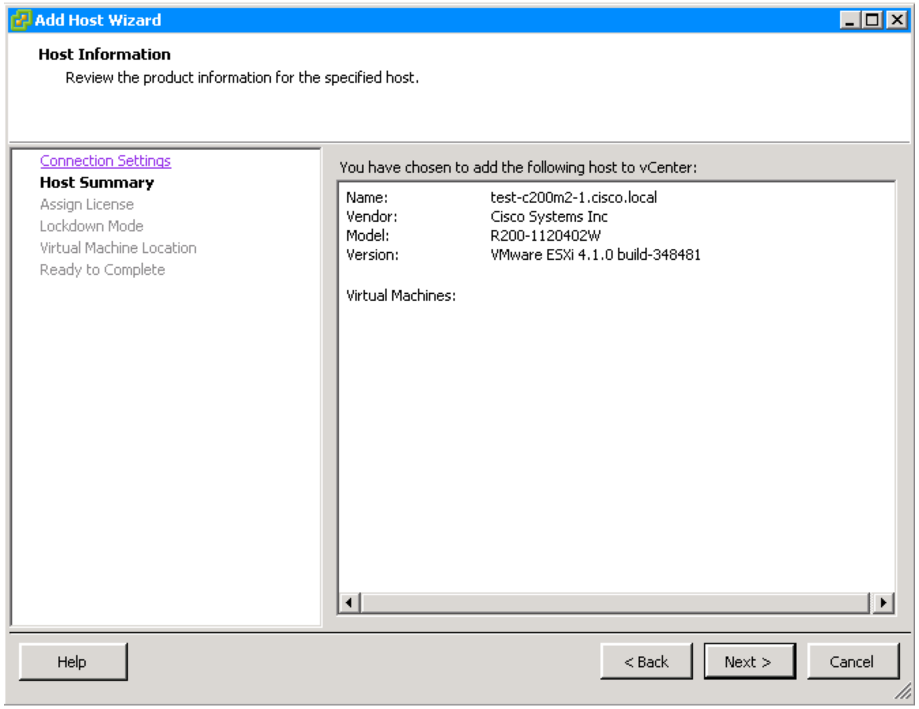
58:E2:58:5E:0E:69:2F:2B:B0:8B:78:1A:76:73:38:98:19:92:5B:D2

Do you wish to proceed with connecting anyway?

Choose "Yes" if you trust the host. The above information will be remembered until the host is removed from the inventory.

Choose "No" to abort connecting to the host at this time.

Step 4: Verify that this is the correct host, and then click **Next**.



Add Host Wizard

Host Information

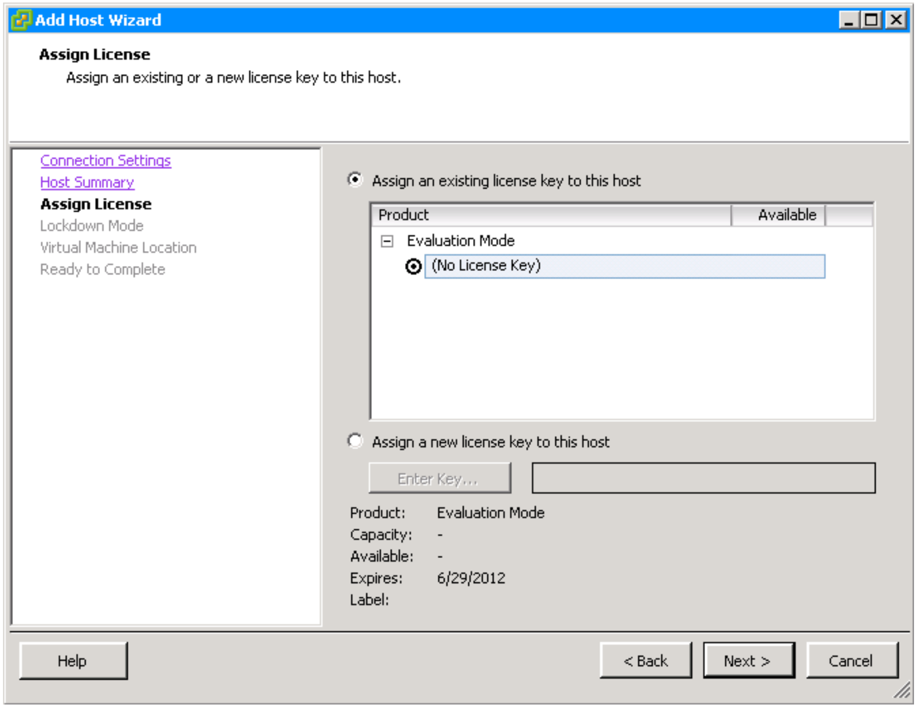
Review the product information for the specified host.

You have chosen to add the following host to vCenter:

```
Name:      test-c200m2-1.cisco.local
Vendor:    Cisco Systems Inc
Model:     R200-1120402W
Version:   VMware ESXi 4.1.0 build-348481

Virtual Machines:
```

Step 5: If you have a license to assign to this host, select **Assign a new license key to this host**, enter the key, and then click **Next**.

If you want to add the key later in vCenter, under Evaluation Mode select **No License Key**, and then click **Next**.



Add Host Wizard

Assign License

Assign an existing or a new license key to this host.

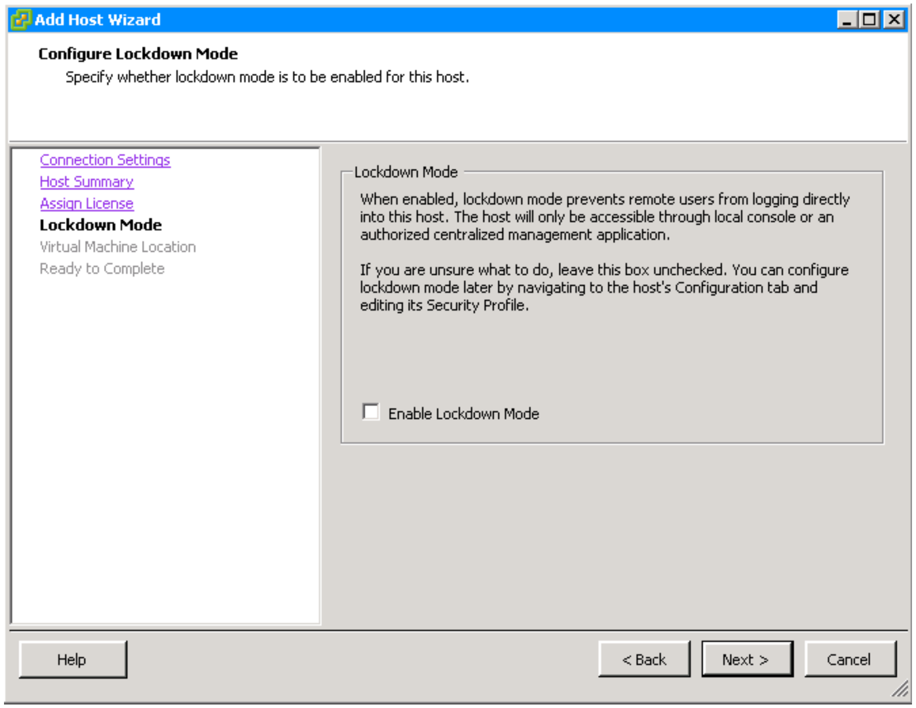
● Assign an existing license key to this host

Product	Available
⊟ Evaluation Mode	
● (No License Key)	

○ Assign a new license key to this host

Product:	Evaluation Mode
Capacity:	-
Available:	-
Expires:	6/29/2012
Label:	

Step 6: On the Configure Lockdown Mode page, click **Next**. For this example, lockdown mode is not used.



Add Host Wizard

Configure Lockdown Mode

Specify whether lockdown mode is to be enabled for this host.

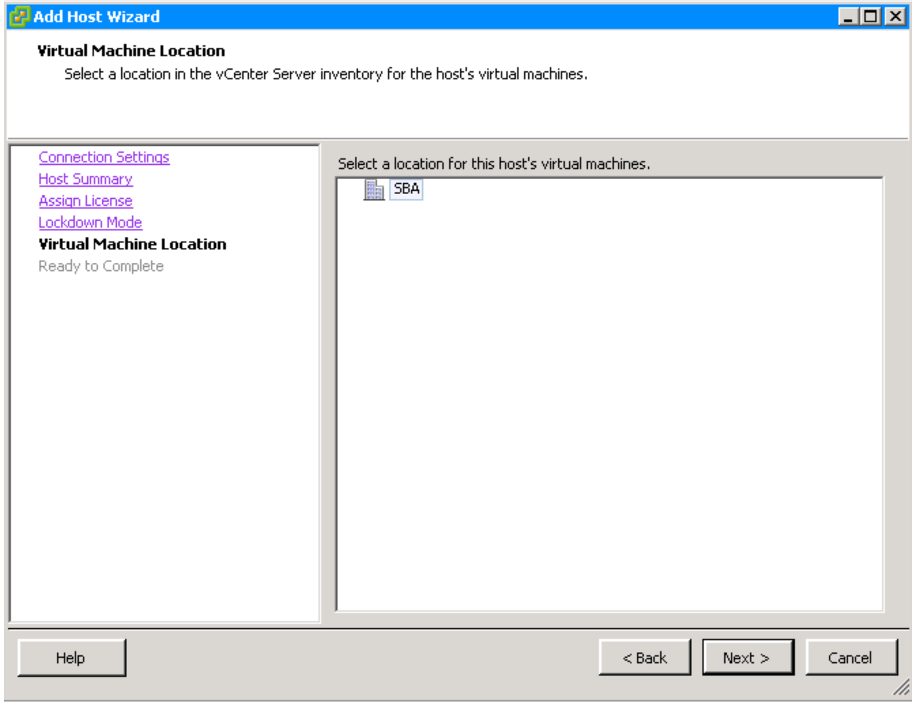
Lockdown Mode

When enabled, lockdown mode prevents remote users from logging directly into this host. The host will only be accessible through local console or an authorized centralized management application.

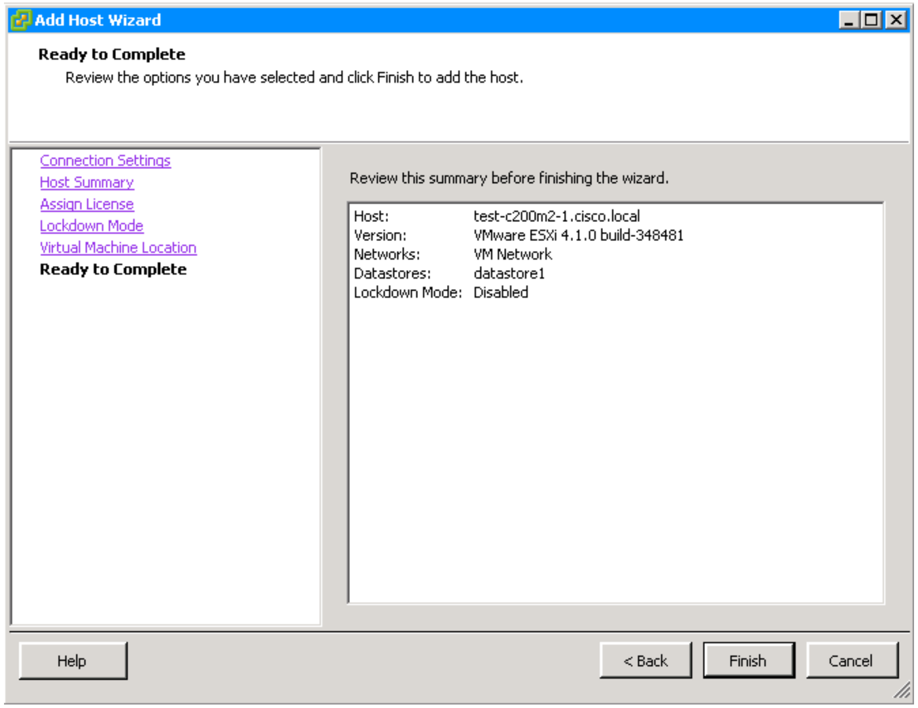
If you are unsure what to do, leave this box unchecked. You can configure lockdown mode later by navigating to the host's Configuration tab and editing its Security Profile.

☐ Enable Lockdown Mode

Step 7: On the Virtual Machine Location page, select the data center you created previously, and then click **Next**. The virtual machine location is where the machine resides in vCenter.



Step 8: Review the information, and then click **Finish**. VCenter is ready to add the ESXi host into its inventory.



Ready to Complete

Review the options you have selected and click Finish to add the host.

Review this summary before finishing the wizard.

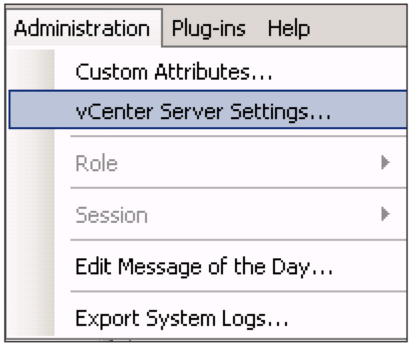
```
Host:           test-c200m2-1.cisco.local
Version:        VMware ESXi 4.1.0 build-348481
Networks:       VM Network
Datastores:     datastore1
Lockdown Mode:  Disabled
```

The wizard is finished. In the vCenter tree, a new host appears under the data center you created earlier.

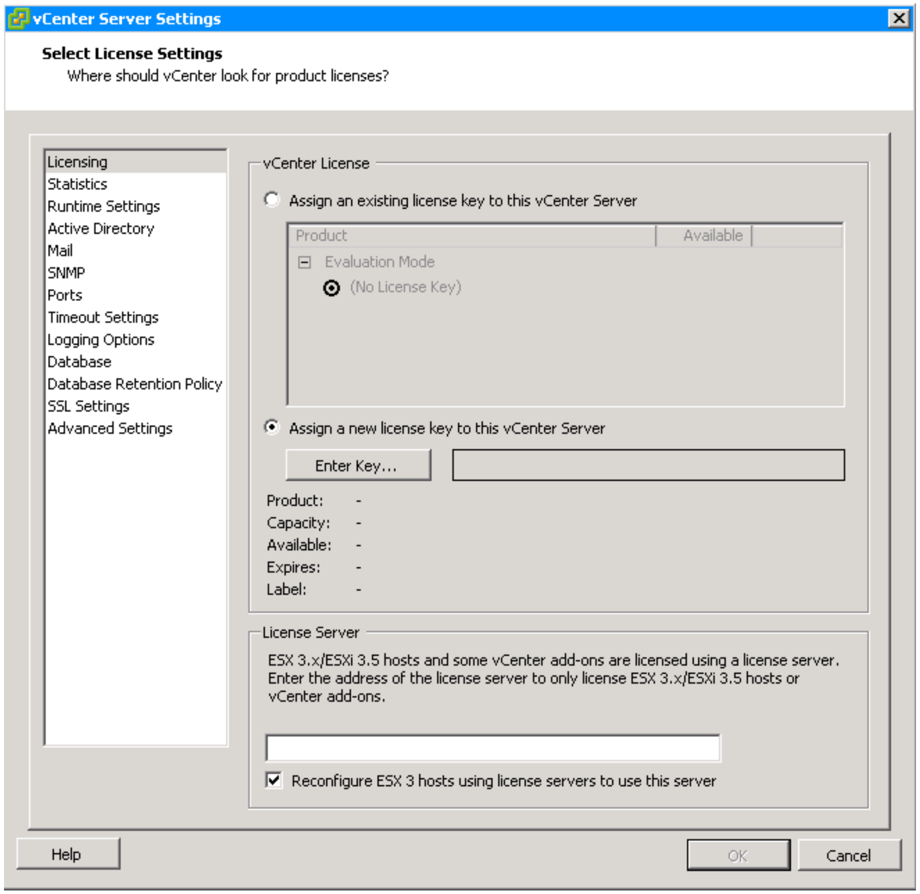
Procedure 5 License vCenter

If you initially configured vCenter with a license key, skip to the next procedure. If you are using the 60-day default evaluation license, complete this procedure to license vCenter. Be sure you are using a license for vCenter and not for ESXi.

Step 1: On the top menu bar in vCenter, navigate to **Administration > vCenter Server Settings**.



Step 2: In the navigation pane, choose **Licensing**, and in the work pane, select **Assign a new license key to this vCenter Server,** and then click **Enter Key**.



Select License Settings

Where should vCenter look for product licenses?

vCenter License

○ Assign an existing license key to this vCenter Server

Product	Available
⊟ Evaluation Mode	
● (No License Key)	

● Assign a new license key to this vCenter Server

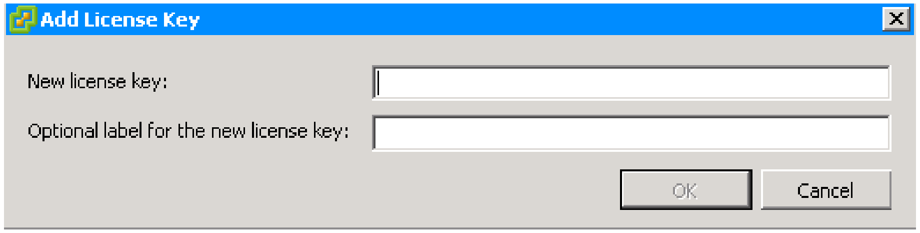
Product: -
Capacity: -
Available: -
Expires: -
Label: -

License Server

ESX 3.x/ESXi 3.5 hosts and some vCenter add-ons are licensed using a license server. Enter the address of the license server to only license ESX 3.x/ESXi 3.5 hosts or vCenter add-ons.

☑ Reconfigure ESX 3 hosts using license servers to use this server

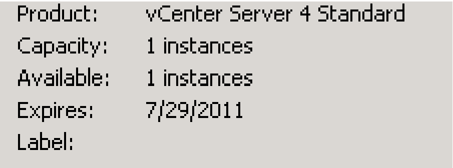
Step 3: Enter the license key (including dashes), and then click **OK**.



New license key:

Optional label for the new license key:

The new license can be seen in the main licensing window shown in Step 2.



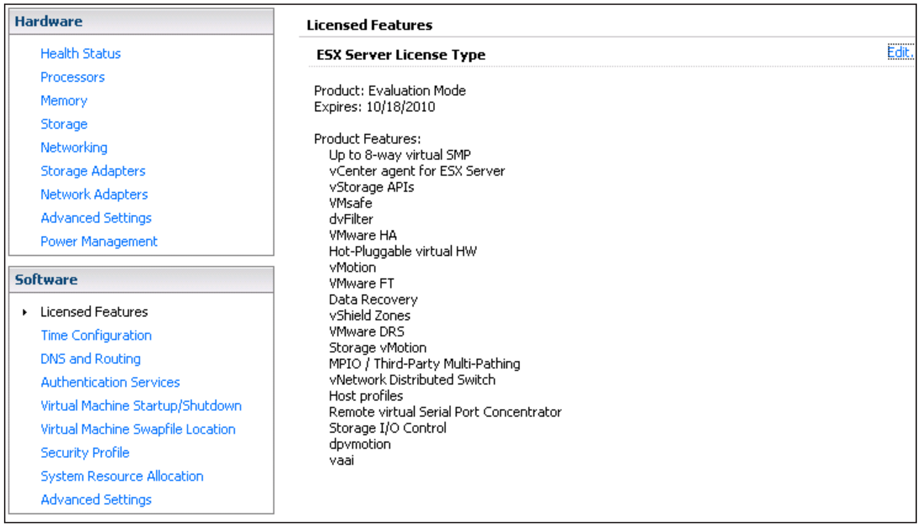
Product:	vCenter Server 4 Standard
Capacity:	1 instances
Available:	1 instances
Expires:	7/29/2011
Label:	

Procedure 6 License ESXi hosts

If you have already licensed the ESXi hosts, skip this procedure. VMware allows ESXi hosts to run for 60 days on an evaluation license. To run your host longer, you must acquire and provide a new license key. For more information, see the VMware documentation. Be sure you are using a license for ESXi and not for the vCenter.

Step 1: In the main inventory window, select the ESXi host.

Step 2: On the Configuration tab, in the Software list, select **Licensed Features**, and then in the upper right corner, click **Edit**.



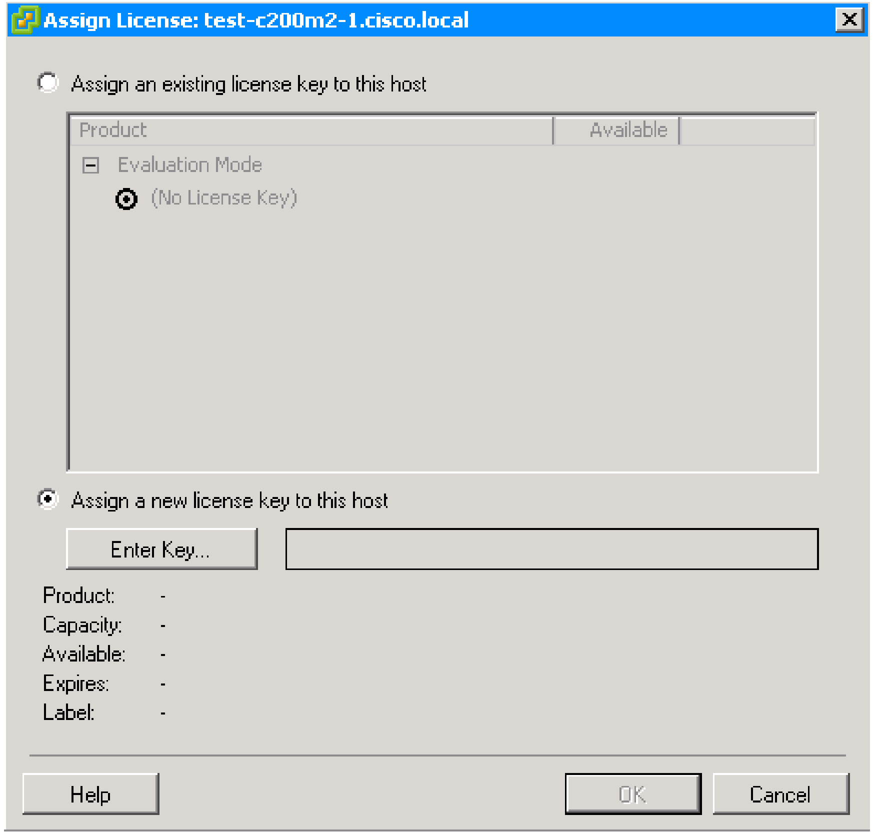
Licensed Features

ESX Server License Type

Product: Evaluation Mode
Expires: 10/18/2010

Product Features:
- Up to 8-way virtual SMP
- vCenter agent for ESX Server
- vStorage APIs
- VMsafe
- dvFilter
- VMware HA
- Hot-Pluggable virtual HW
- vMotion
- VMware FT
- Data Recovery
- vShield Zones
- VMware DRS
- Storage vMotion
- MPIO / Third-Party Multi-Pathing
- vNetwork Distributed Switch
- Host profiles
- Remote virtual Serial Port Concentrator
- Storage I/O Control
- dpvmotion
- vaai

Step 3: Select **Assign a new license key to this host**, and then click **Enter Key**.



Assign License: test-c200m2-1.cisco.local

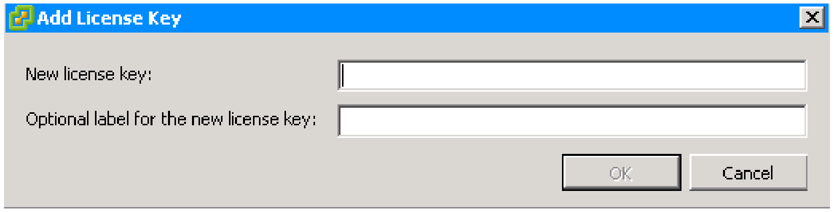
○ Assign an existing license key to this host

Product	Available
⊟ Evaluation Mode	
● (No License Key)	

● Assign a new license key to this host

Product: -
Capacity: -
Available: -
Expires: -
Label: -

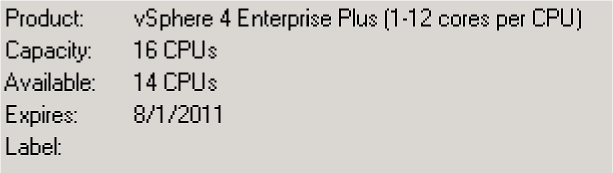
Step 4: Enter the license key (including dashes), and then click **OK**.



Add License Key

New license key:
Optional label for the new license key:

The new license can be seen in the main licensing window shown in Step 4.



Product: vSphere 4 Enterprise Plus (1-12 cores per CPU)
Capacity: 16 CPUs
Available: 14 CPUs
Expires: 8/1/2011
Label:

Process

Installing VMware vCenter Update Manager

1. Install VUM
2. Install vCenter Update Manager plug-in
3. Configure VUM

VMware vCenter Update Manager (VUM) is a tool that streamlines the process of scanning and applying patches or upgrades to VMware ESX/ESXi hosts, virtual machines, and virtual appliances. VUM runs as a plug-in on the vSphere Client and can be installed on the same server running vCenter Server or on a different server. VUM downloads patches and updates from the VMware website; and based on the policies you set up, it can scan and remediate (update) ESX/ESXi hosts, virtual machines, and templates. Updating your virtual machines, appliances, and ESX/ESXi hosts can make your environment more secure. In a later module in this guide, VUM plays an integral part in installing and updating the Cisco Nexus 1000V distributed virtual switch.

Before proceeding with this procedure, please visit the VMware web site and review the hardware requirements needed on a system to run VUM.

Before installing VUM, you need to set up Oracle or Microsoft SQL Server database. VUM uses a database server to store patch metadata. You need to decide whether to use SQL Server Express Edition, which is included in the VMware vCenter media, or SQL Server 2005, SQL Server 2008, or Oracle 10g/11g databases. The decision depends on how large you plan to scale your environment. For environments with more than five hosts and 50 virtual machines, create an Oracle or SQL Server database for VUM. Refer to the VMware vCenter Update Manager Performance and Best Practices website for more information.

Procedure 1 Install VUM

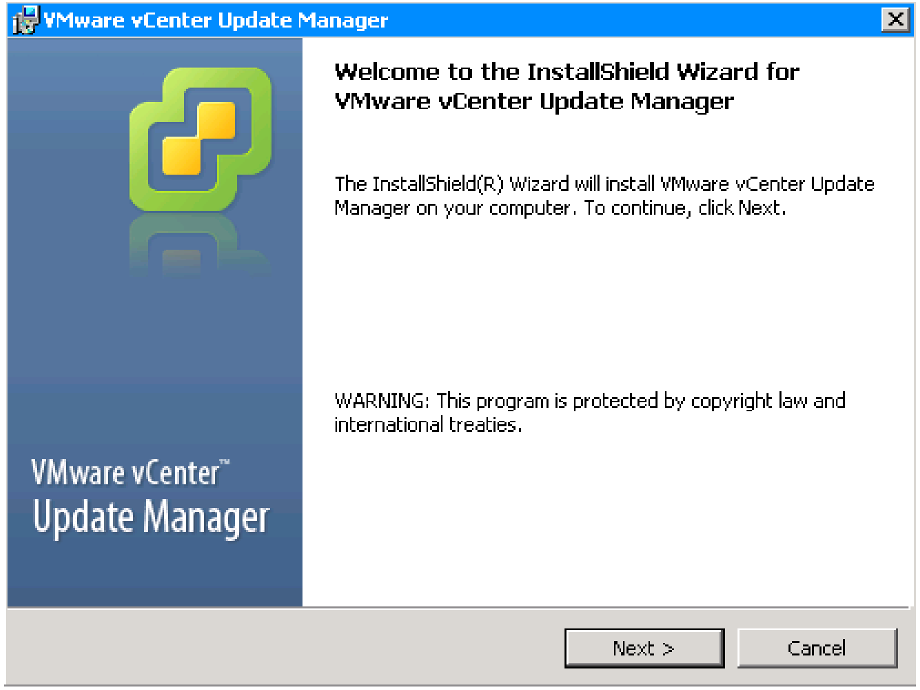
In this procedure, you install VUM by using an instance of SQL Server 2005 Express Edition.

Step 1: Copy the vCenter Server image to your server, unzip the contents, and then run the VMware vCenter Installer.

Step 2: Under the VMware Product Installers, select **vCenter Update Manager.**

Step 3: Choose the correct language for the installation, and then click **OK.**

Step 4: On the Welcome to the InstallShield Wizard for VMware vCenter Update Manager page, click **Next**.



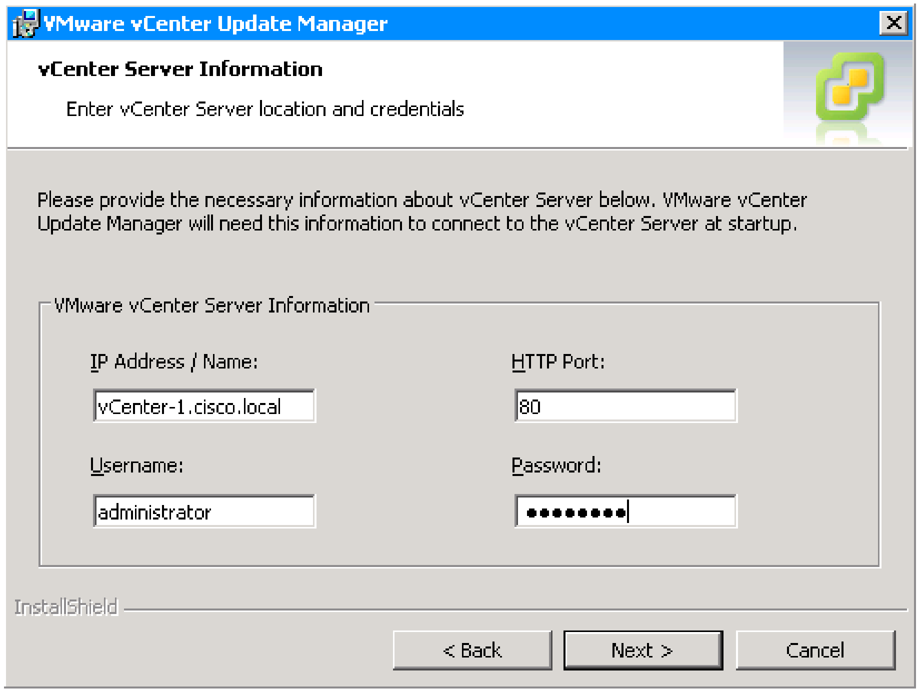
Welcome to the InstallShield Wizard for VMware vCenter Update Manager

The InstallShield(R) Wizard will install VMware vCenter Update Manager on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Step 5: Read and accept the VMware End User License Agreement, and then click **Next**.

Step 6: Enter the IP address, username, password, and HTTP port of the vCenter Server instance to which you want to associate this VUM, and then click **Next**.



VMware vCenter Update Manager

vCenter Server Information

Enter vCenter Server location and credentials

Please provide the necessary information about vCenter Server below. VMware vCenter Update Manager will need this information to connect to the vCenter Server at startup.

VMware vCenter Server Information

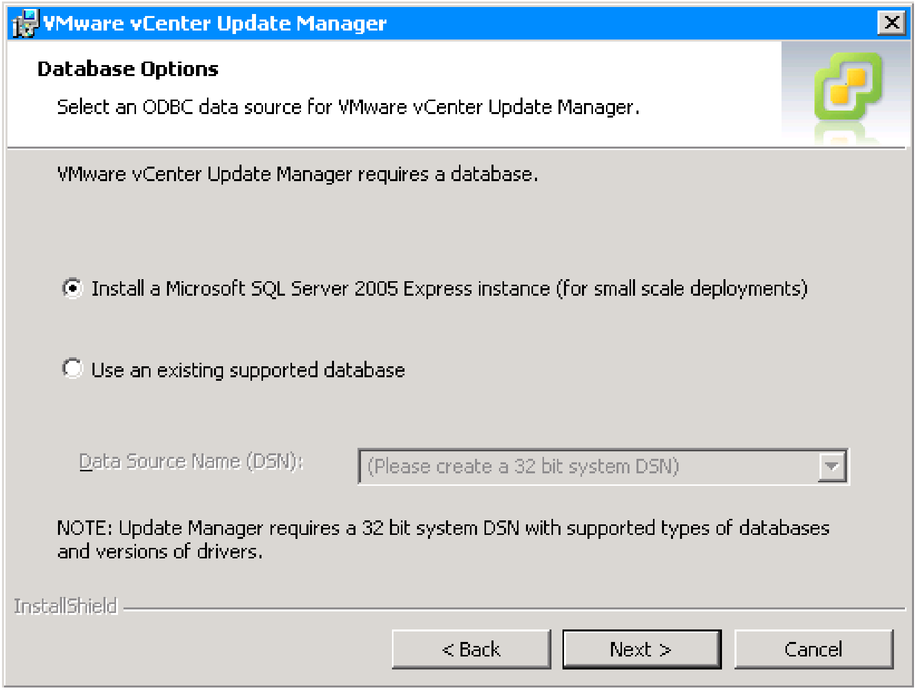
IP Address / Name: vCenter-1.cisco.local

HTTP Port: 80

Username: administrator

Password: ●●●●●●●●●

Step 7: Select **Install a Microsoft SQL Server 2005 Express instance (for small scale deployments)**, and then click **Next**.



VMware vCenter Update Manager

Database Options

Select an ODBC data source for VMware vCenter Update Manager.

VMware vCenter Update Manager requires a database.

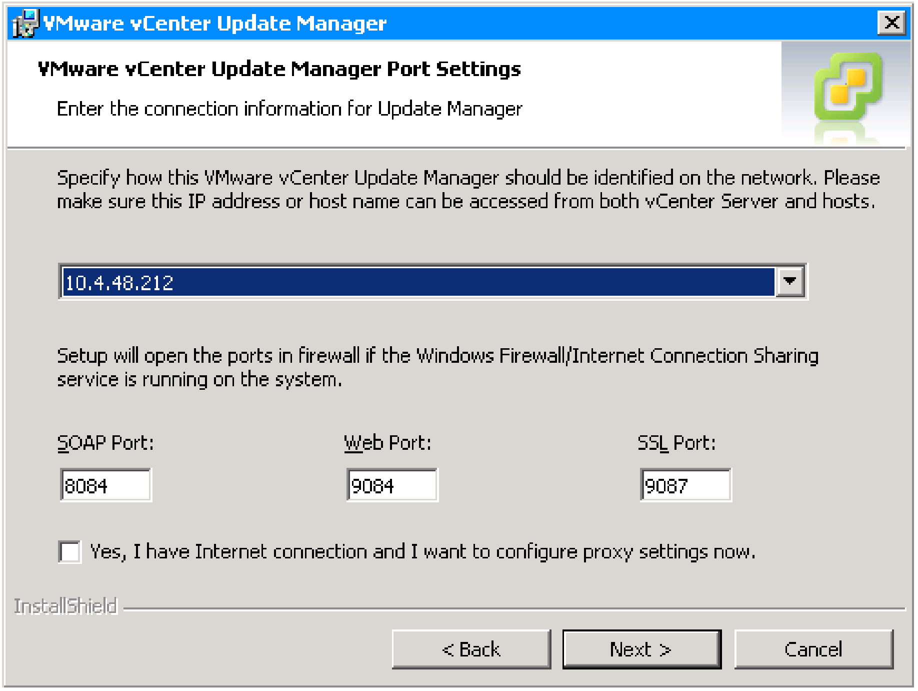
● Install a Microsoft SQL Server 2005 Express instance (for small scale deployments)

○ Use an existing supported database

Data Source Name (DSN): (Please create a 32 bit system DSN)

NOTE: Update Manager requires a 32 bit system DSN with supported types of databases and versions of drivers.

Step 8: On the VMware vCenter Update Manager Port Settings screen, leave the default settings, and then click **Next**.


VMware vCenter Update Manager

VMware vCenter Update Manager Port Settings

Enter the connection information for Update Manager

Specify how this VMware vCenter Update Manager should be identified on the network. Please make sure this IP address or host name can be accessed from both vCenter Server and hosts.

10.4.48.212

Setup will open the ports in firewall if the Windows Firewall/Internet Connection Sharing service is running on the system.

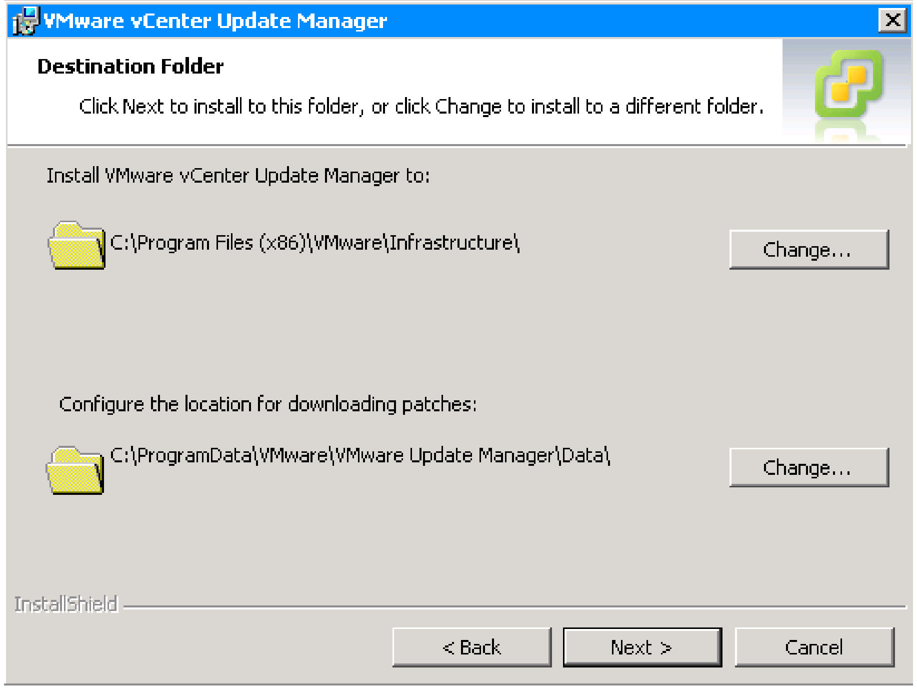
SOAP Port: 8084

Web Port: 9084

SSL Port: 9087

☐ Yes, I have Internet connection and I want to configure proxy settings now.

Step 9: On the Destination Folder screen, click **Next**. You are allowed to specify the directory path where you want to install VUM and store the patches, but leave it at the default for now.


VMware vCenter Update Manager

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

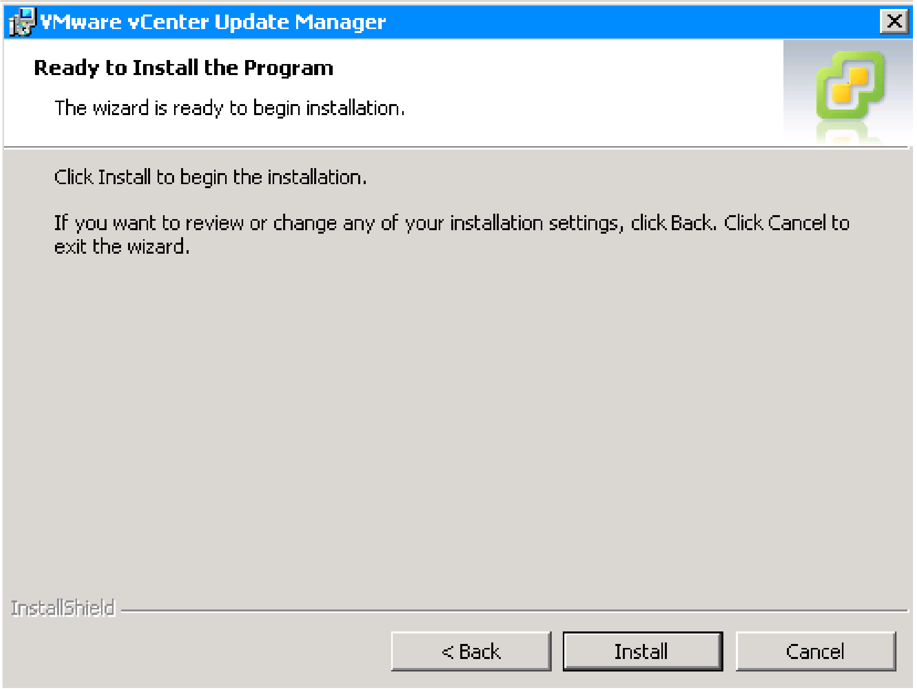
Install VMware vCenter Update Manager to:

C:\Program Files (x86)\VMware\Infrastructure\

Configure the location for downloading patches:

C:\ProgramData\VMware\VMware Update Manager\Data\

Step 10: Click **Install**.



VMware vCenter Update Manager

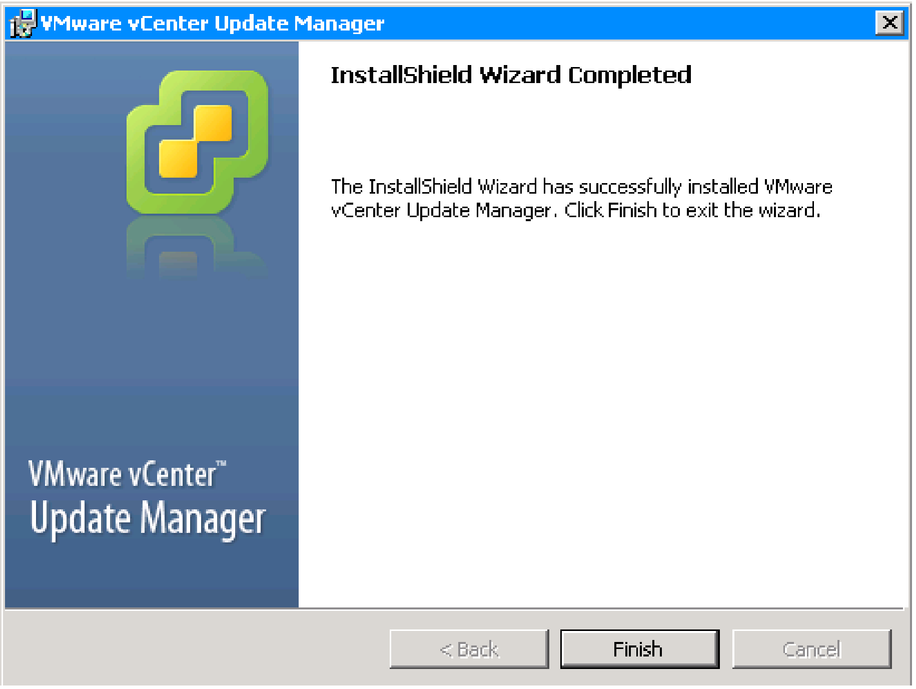
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Step 11: When the installation is complete, click **Finish**.



VMware vCenter Update Manager

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed VMware vCenter Update Manager. Click Finish to exit the wizard.

Step 12: From the computer where VUM was installed, run **services.msc** from a command prompt, and then click **OK**. This launches the Services console.

Step 13: Scroll down to the VMware Update Manager Service, and make sure the service is running. If it is not, right-click the Update Manager Service, and then click Start.

Procedure 2 Install vCenter Update Manager plug-in

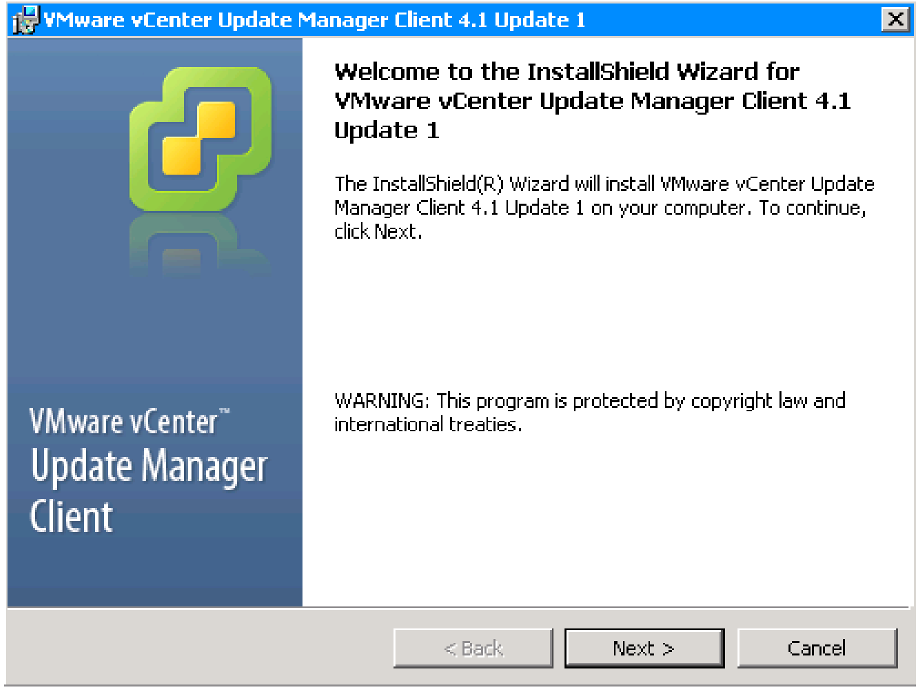
To manage VUM, you install the Update Manager Client plug-in for vSphere Client.

Step 1: Launch vSphere Client, and then connect to your vCenter Server instance.

Step 2: Navigate to **Plug-ins > Manage Plug-ins**.

Step 3: In the Plug-in Manager window, for the VMware vCenter Update Manager extension, click **Download and install**.

Step 4: In the InstallShield Wizard for VMware vCenter Update Manager Client, click **Next**.



Welcome to the InstallShield Wizard for VMware vCenter Update Manager Client 4.1 Update 1

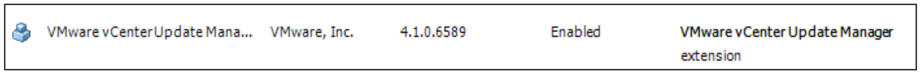
The InstallShield(R) Wizard will install VMware vCenter Update Manager Client 4.1 Update 1 on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Step 5: Click **Install**.

Step 6: After installation is complete, click **Finish**.

Step 7: In the Plug-in Manager window, under Installed Plug-ins, make sure the Update Manager extension is displayed as **Enabled**, and then click **Close**.



VMware vCenter Update Mana...	VMware, Inc.	4.1.0.6589	Enabled	VMware vCenter Update Manager extension

Procedure 3 Configure VUM

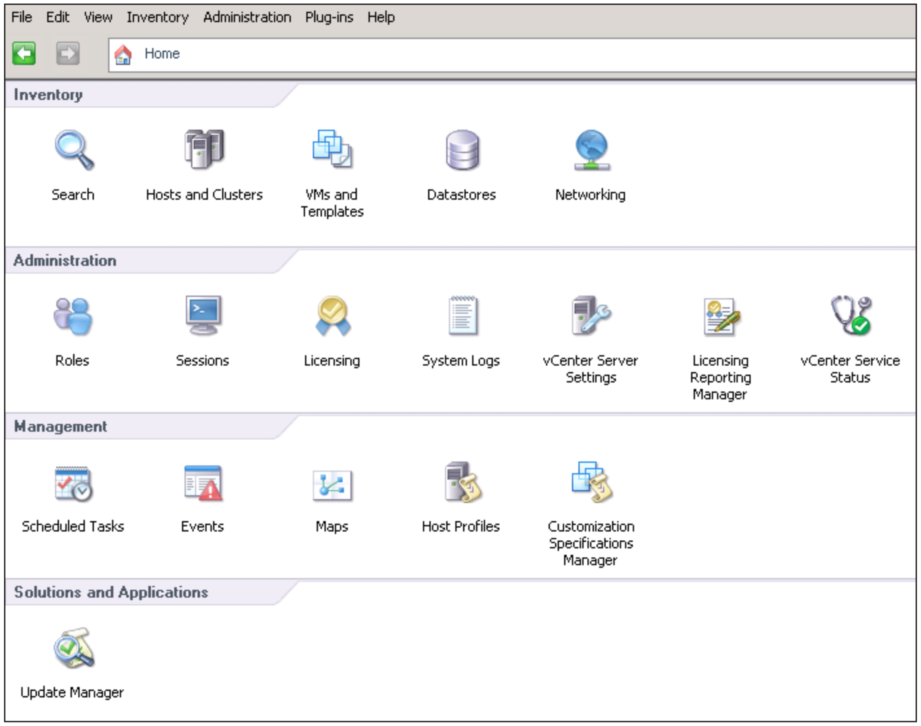
Update Manager includes many default baselines that can be used to scan any virtual machine, virtual appliance or host in order to determine if they have all patches applied or if they need to be upgraded to latest version.

Baselines are collections of one or more updates such as service packs, patches, extensions, upgrades, or bug fixes. Baselines can be divided into three categories:

- Patch baselines can be used to define a list of patches that need to be applied to ESX/ESXi host or guest operating system.
- Upgrade baselines can be used to define the versions to which ESX/ESXi hosts, VMware tools, or virtual appliances can be upgraded.
- Extension baselines define third-party software that must be applied to a given host.

In this procedure, you check whether ESX/ESXi hosts are compliant with all critical and optional patches. Also, you apply patches for non-complying hosts.

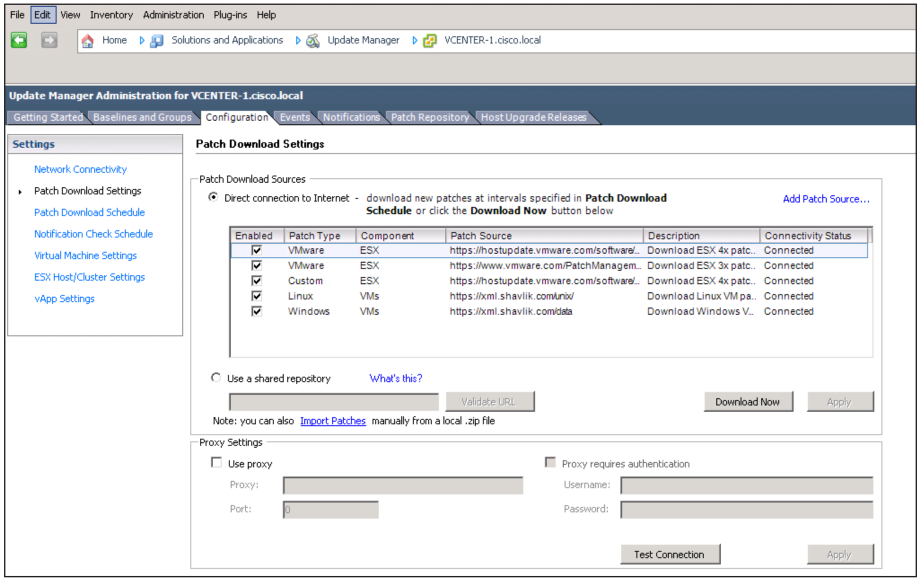
Step 1: Launch vSphere Client, navigate to Home, and under Solutions and Applications, click **Update Manager**.



Step 2: Navigate to the Configuration tab, select **Patch download schedule**, and then make sure the **State** check box is selected.

Step 3: If you want to modify how frequently the patch definitions are downloaded, click **Edit Patch Downloads**.

Step 4: Navigate to **Configuration > Patch Download Settings**, and check whether the connectivity status is Connected. This step assumes that your setup has connectivity to the Internet.



Patch Download Settings

Patch Download Sources

● Direct connection to Internet - download new patches at intervals specified in **Patch Download Schedule** or click the **Download Now** button below

Enabled	Patch Type	Component	Patch Source	Description	Connectivity Status
☑	VMware	ESX	https://hostupdate.vmware.com/software/...	Download ESX 4x patc..	Connected
☑	VMware	ESX	https://www.vmware.com/PatchManagem...	Download ESX 3x patc..	Connected
☑	Custom	ESX	https://hostupdate.vmware.com/software/...	Download ESX 4x patc..	Connected
☑	Linux	VMs	https://xml.shavlik.com/unix/	Download Linux VM pa..	Connected
☑	Windows	VMs	https://xml.shavlik.com/data	Download Windows V...	Connected

○ Use a shared repository

Note: you can also Import Patches manually from a local .zip file

Proxy Settings

□ Use proxy

Proxy:

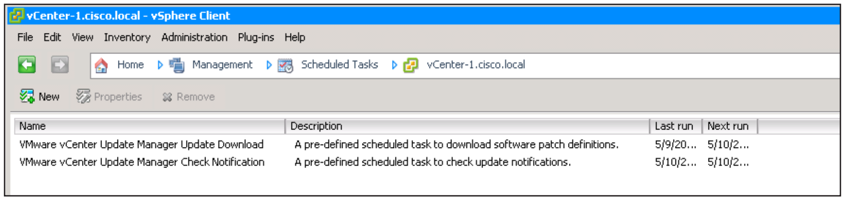
Port: 0

□ Proxy requires authentication

Username:

Password:

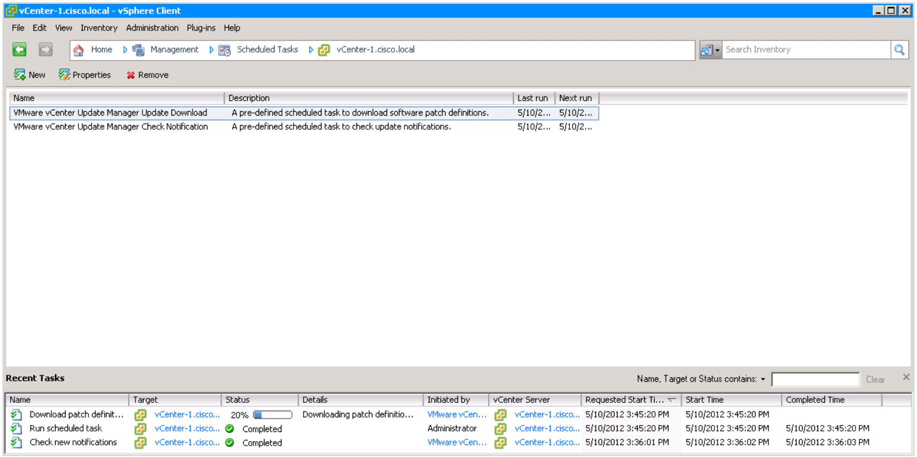
Step 5: Navigate to **Home > Management**, and then click **Schedule Task**. This shows when you are scheduled to download patch definitions. In the next step, you manually run this task.


vCenter-1.cisco.local - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home
Management
Scheduled Tasks
vCenter-1.cisco.local
New
Properties
Remove

Name	Description	Last run	Next run
VMware vCenter Update Manager Update Download	A pre-defined scheduled task to download software patch definitions.	5/9/20...	5/10/2...
VMware vCenter Update Manager Check Notification	A pre-defined scheduled task to check update notifications.	5/10/2...	5/10/2...

Step 6: Right-click **VMware vCenter Update Manager Update Download**, and then click **Run**. This downloads the patch definitions from the VMware site.

Step 7: In the Recent Tasks pane, notice that the patch definitions are downloaded from the VMware site.

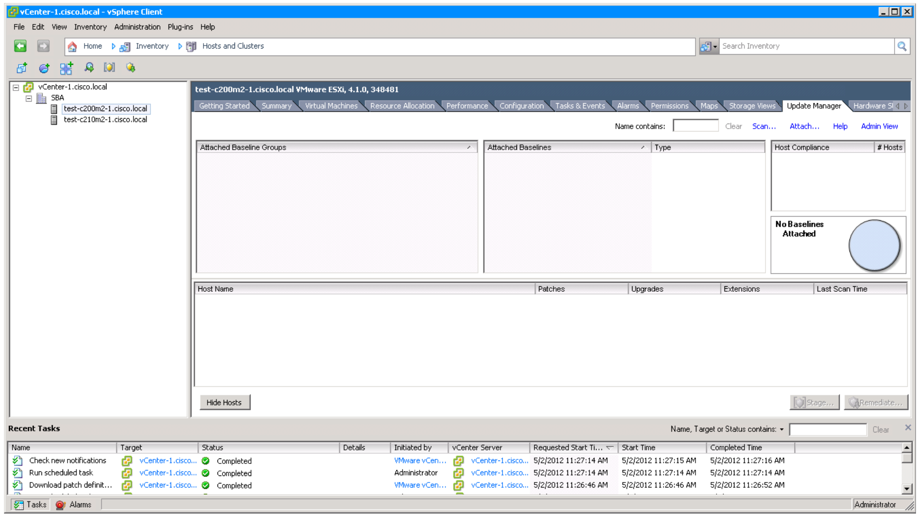


Name	Description	Last run	Next run
VMware vCenter Update Manager Update Download	A pre-defined scheduled task to download software patch definitions.	5/10/2...	5/10/2...
VMware vCenter Update Manager Check Notification	A pre-defined scheduled task to check update notifications.	5/10/2...	5/10/2...

Recent Tasks

Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Ti...	Start Time	Completed Time
Download patch definit...	vCenter-1.cisco...	20%	Downloading patch definitio...	VMware vCen...	vCenter-1.cisco...	5/10/2012 3:45:20 PM	5/10/2012 3:45:20 PM	
Run scheduled task	vCenter-1.cisco...	Completed		Administrator	vCenter-1.cisco...	5/10/2012 3:45:20 PM	5/10/2012 3:45:20 PM	5/10/2012 3:45:20 PM
Check new notifications	vCenter-1.cisco...	Completed		VMware vCen...	vCenter-1.cisco...	5/10/2012 3:36:01 PM	5/10/2012 3:36:02 PM	5/10/2012 3:36:03 PM

Step 8: Navigate to **Home > Inventory > Hosts and Clusters**, select the host on which you want to install the patches, navigate to the Update Manager tab, and then click **Attach.**



test-c200m2-1.cisco.local VMware ESXi, 4.1.0, 348481

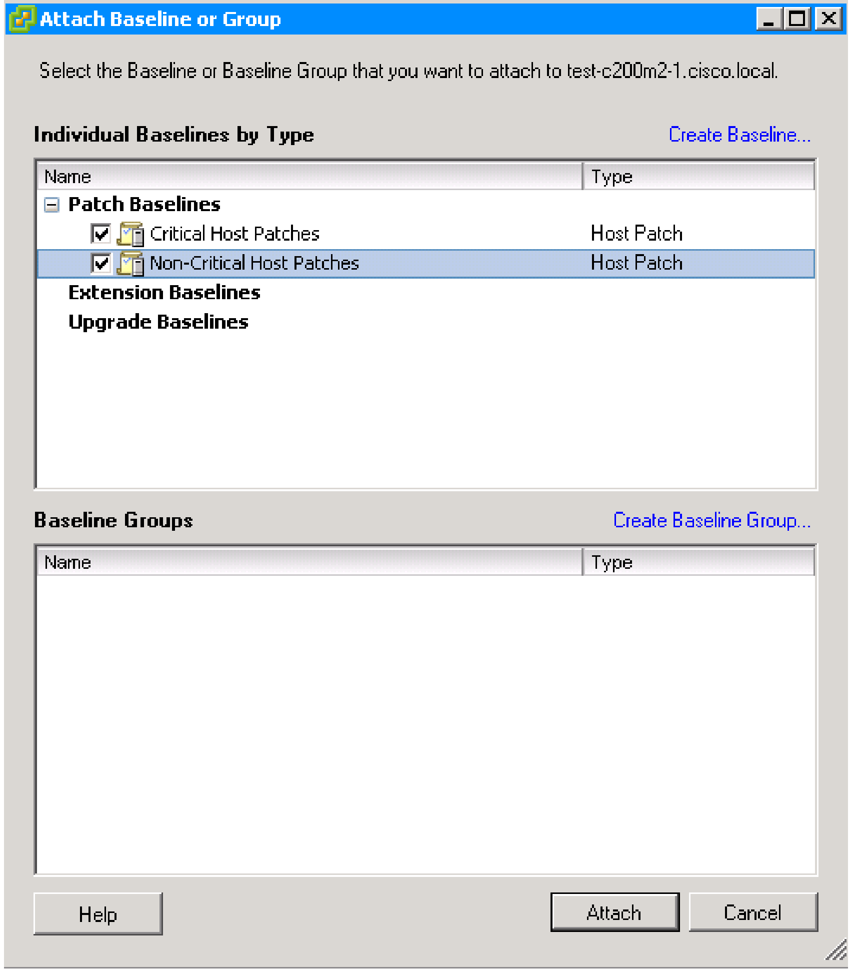
Recent Tasks

Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Ti...	Start Time	Completed Time
Check new notifications	vCenter-1.cisco...	Completed		VMware vCen...	vCenter-1.cisco...	5/2/2012 11:27:14 AM	5/2/2012 11:27:15 AM	5/2/2012 11:27:16 AM
Run scheduled task	vCenter-1.cisco...	Completed		Administrator	vCenter-1.cisco...	5/2/2012 11:27:14 AM	5/2/2012 11:27:14 AM	5/2/2012 11:27:14 AM
Download patch definit...	vCenter-1.cisco...	Completed		VMware vCen...	vCenter-1.cisco...	5/2/2012 11:26:46 AM	5/2/2012 11:26:46 AM	5/2/2012 11:26:52 AM

Step 9: Under Patch Baselines, select **Critical Host Patches** and **Non-Critical Host Patches,** and then click **Attach**.

Reader Tip

Notice that you can create your own Baseline and Baseline groups. Refer to the *VMware vCenter Update Manager Installation and Administration Guide* documentation for information about how to create custom baseline groups.



Attach Baseline or Group

Select the Baseline or Baseline Group that you want to attach to test-c200m2-1.cisco.local.

Individual Baselines by Type

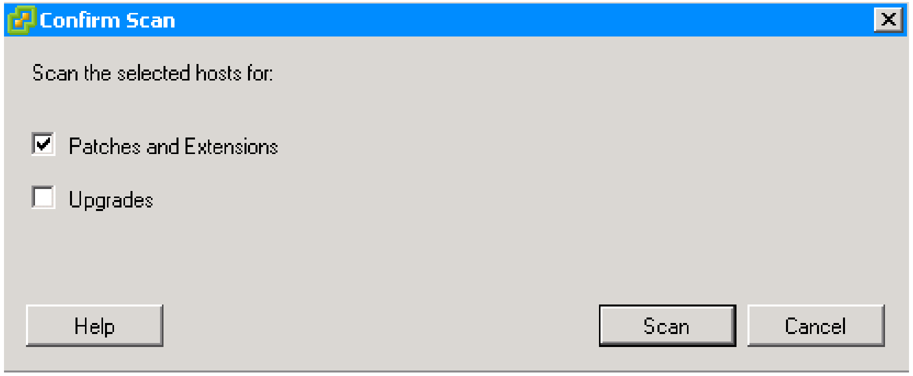
Name	Type
⊟ Patch Baselines	
☑ Critical Host Patches	Host Patch
☑ Non-Critical Host Patches	Host Patch
Extension Baselines	
Upgrade Baselines	

Baseline Groups

Name	Type

Step 10: Right-click the host to which you attached the default patch baselines, and then choose **Scan for Updates**.

Step 11: In the Confirm Scan window, select **Patches and Extensions**, and then click **Scan**.

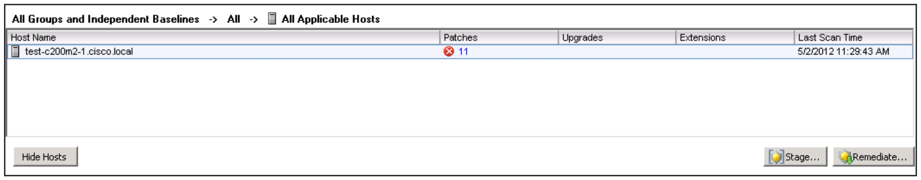


Scan the selected hosts for:

☑ Patches and Extensions

□ Upgrades

When the scan is complete, the system lists the number of patches missing on the ESX/ESXi host.



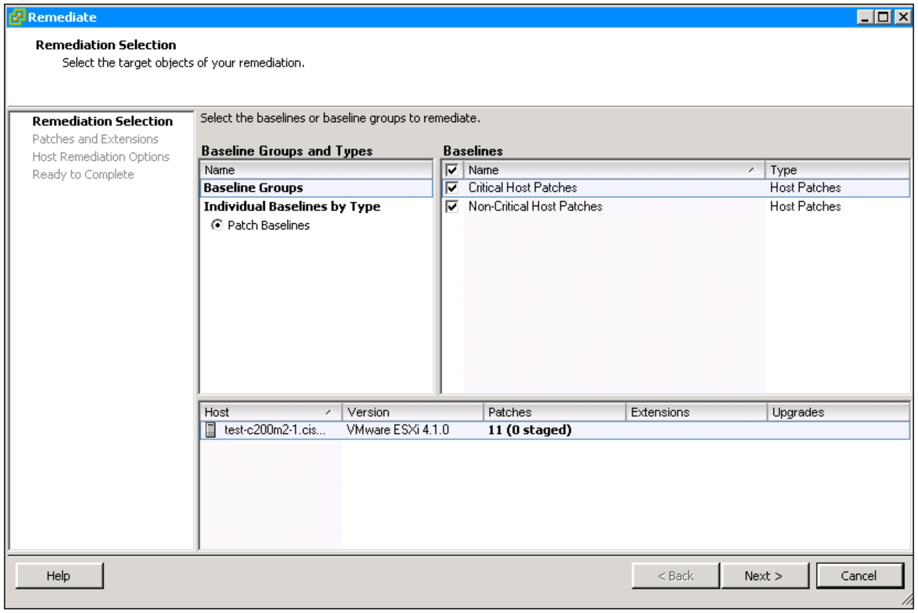
All Groups and Independent Baselines -> All -> All Applicable Hosts

Host Name	Patches	Upgrades	Extensions	Last Scan Time
test-c200m2-1.cisco.local	⊗ 11			5/2/2012 11:29:43 AM

Step 12: For patches to be remediated onto the host you must power off the virtual machines, or move them to a different host, using vMotion as described in "Migrate VM to another ESXi host". Patches are installed on a host by putting the host in maintenance mode which will disrupt any active VMs on the host.

Step 13: Right-click the host on which you want to remediate the patches, and then click **Remediate**.

Step 14: In the Remediation Selection window, select **Critical Host Patches** and **Non-Critical Host Patches**, and then click **Next**.



Remediation Selection

Select the target objects of your remediation.

Select the baselines or baseline groups to remediate.

Baseline Groups and Types

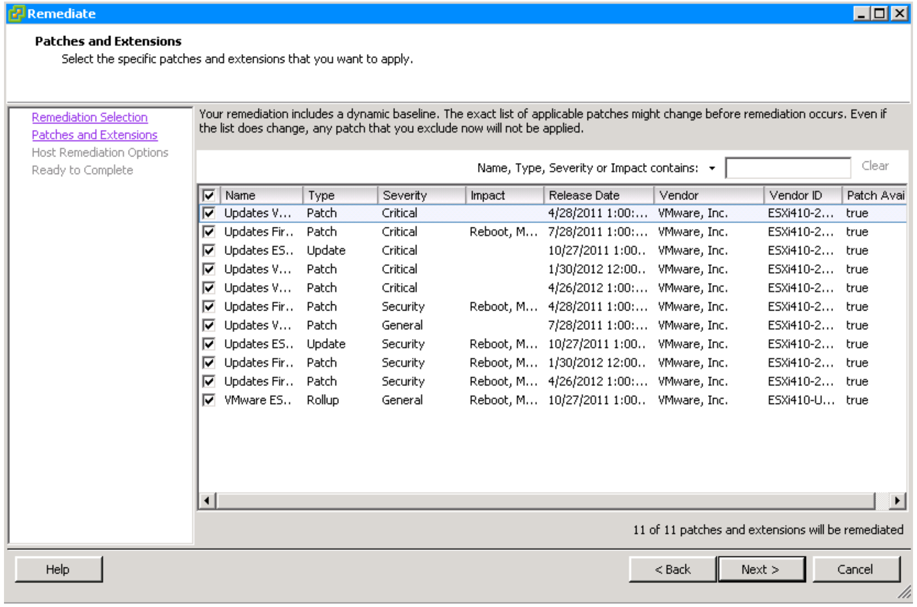
Name
Baseline Groups
Individual Baselines by Type
● Patch Baselines

Baselines

☑	Name	Type
☑	Critical Host Patches	Host Patches
☑	Non-Critical Host Patches	Host Patches

Host	Version	Patches	Extensions	Upgrades
test-c200m2-1.cis...	VMware ESXi 4.1.0	**11 (0 staged)**		

Step 15: In the Patches and Extensions screen, select all of the patches you wish to apply, and then click **Next**.



Patches and Extensions

Select the specific patches and extensions that you want to apply.

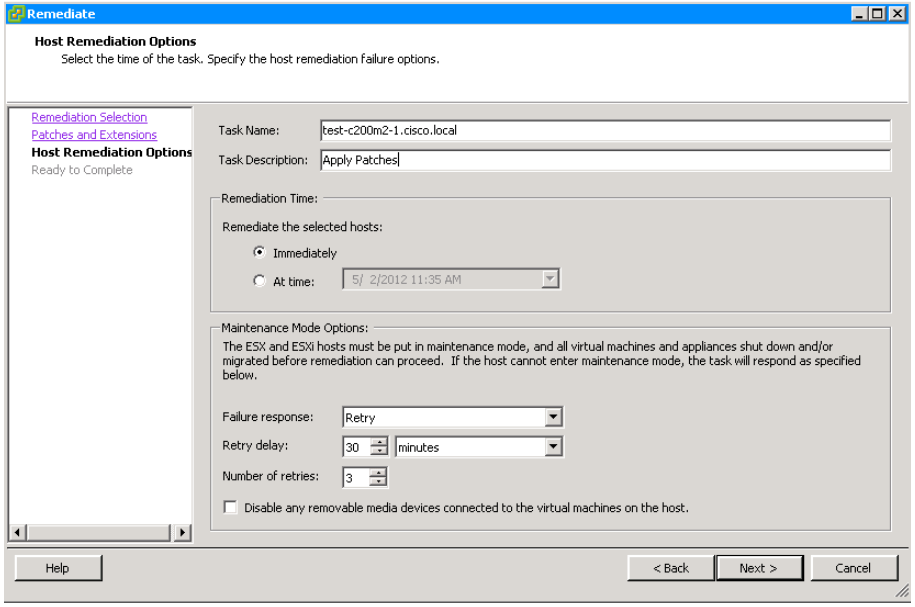
Your remediation includes a dynamic baseline. The exact list of applicable patches might change before remediation occurs. Even if the list does change, any patch that you exclude now will not be applied.

Name, Type, Severity or Impact contains:

☑	Name	Type	Severity	Impact	Release Date	Vendor	Vendor ID	Patch Avai
☑	Updates V...	Patch	Critical		4/28/2011 1:00:...	VMware, Inc.	ESXi410-2...	true
☑	Updates Fir..	Patch	Critical	Reboot, M...	7/28/2011 1:00:...	VMware, Inc.	ESXi410-2...	true
☑	Updates ES..	Update	Critical		10/27/2011 1:00..	VMware, Inc.	ESXi410-2...	true
☑	Updates V...	Patch	Critical		1/30/2012 12:00..	VMware, Inc.	ESXi410-2...	true
☑	Updates V...	Patch	Critical		4/26/2012 1:00:...	VMware, Inc.	ESXi410-2...	true
☑	Updates Fir..	Patch	Security	Reboot, M...	4/28/2011 1:00:...	VMware, Inc.	ESXi410-2...	true
☑	Updates V...	Patch	General		7/28/2011 1:00:...	VMware, Inc.	ESXi410-2...	true
☑	Updates ES..	Update	Security	Reboot, M...	10/27/2011 1:00..	VMware, Inc.	ESXi410-2...	true
☑	Updates Fir..	Patch	Security	Reboot, M...	1/30/2012 12:00..	VMware, Inc.	ESXi410-2...	true
☑	Updates Fir..	Patch	Security	Reboot, M...	4/26/2012 1:00:...	VMware, Inc.	ESXi410-2...	true
☑	VMware ES..	Rollup	General	Reboot, M...	10/27/2011 1:00..	VMware, Inc.	ESXi410-U...	true

11 of 11 patches and extensions will be remediated

Step 16: Enter a description for the task, select **Immediately**, and then click **Next**.



Host Remediation Options

Select the time of the task. Specify the host remediation failure options.

Task Name: test-c200m2-1.cisco.local

Task Description: Apply Patches

Remediation Time:

Remediate the selected hosts:

● Immediately

○ At time: 5/ 2/2012 11:35 AM

Maintenance Mode Options:

The ESX and ESXi hosts must be put in maintenance mode, and all virtual machines and appliances shut down and/or migrated before remediation can proceed. If the host cannot enter maintenance mode, the task will respond as specified below.

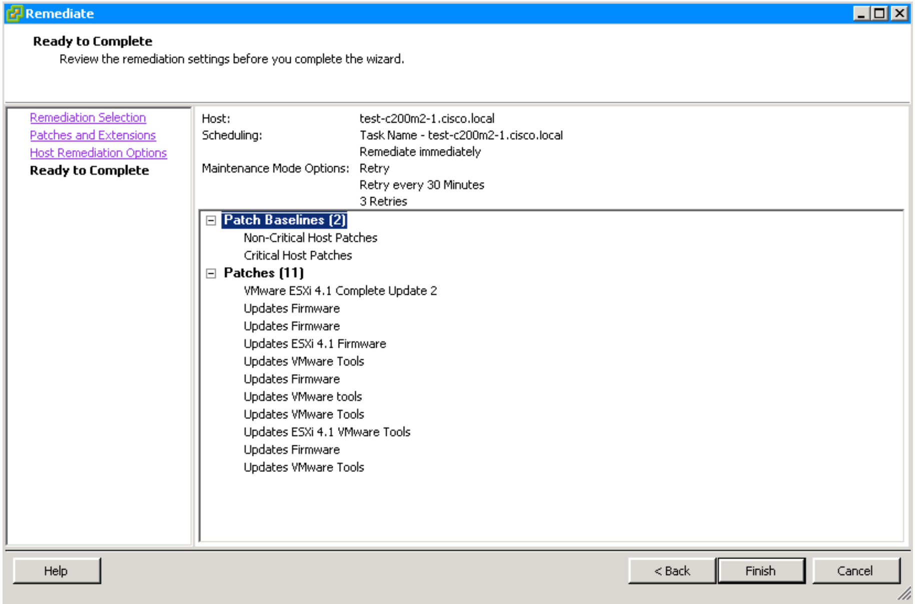
Failure response: Retry

Retry delay: 30 minutes

Number of retries: 3

☐ Disable any removable media devices connected to the virtual machines on the host.

Step 17: Review your configurations, and then click **Finish**.



Ready to Complete

Review the remediation settings before you complete the wizard.

Host: test-c200m2-1.cisco.local

Scheduling: Task Name - test-c200m2-1.cisco.local
Remediate immediately

Maintenance Mode Options: Retry
Retry every 30 Minutes
3 Retries

Patch Baselines (2)
- Non-Critical Host Patches
- Critical Host Patches

Patches (11)
- VMware ESXi 4.1 Complete Update 2
- Updates Firmware
- Updates Firmware
- Updates ESXi 4.1 Firmware
- Updates VMware Tools
- Updates Firmware
- Updates VMware tools
- Updates VMware Tools
- Updates ESXi 4.1 VMware Tools
- Updates Firmware
- Updates VMware Tools

VUM downloads patches from the VMware website and remediates the host. Your host will likely be rebooted after remediation is finished. Check the Recent Tasks pane for the progress.

Process

Migrating Virtual Machine Storage and Virtual Machines

1. Migrate virtual machine storage
2. Migrate VM to another ESXi host

If you have an Enterprise or Enterprise Plus license for your VMware environment you can use vMotion to migrate virtual machines and virtual machine storage from one location to another. This process shows how VMware can migrate virtual machine storage from one location to another and how virtual machines can be migrated from one server to another. VMware vMotion requires an Enterprise or Enterprise Plus license. If you have a Standard license, skip this process.

Procedure 1 Migrate virtual machine storage

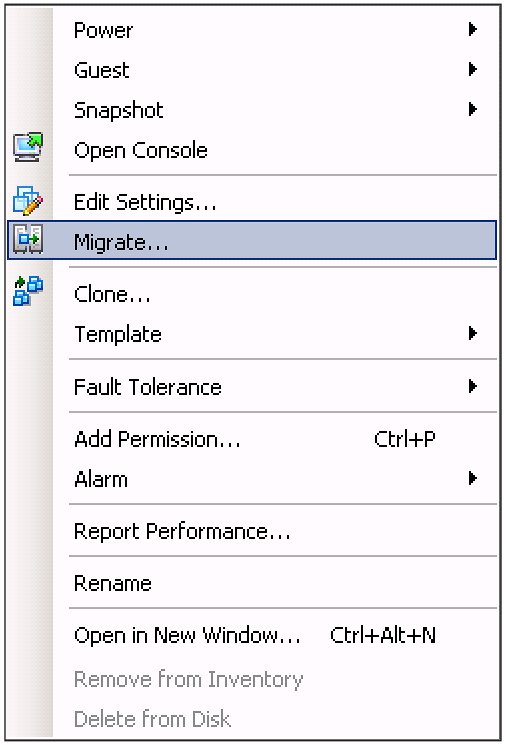
You can move storage from local ESXi server datastores to Fibre Channel or iSCSI datastores. If you installed your new VM as described earlier in this guide, it is located on a local datastore on the ESXi host. To maximize flexibility and enable the ability to use vMotion to move the VM, the storage needs to be located on the SAN storage array.

Many guest virtual disks are allocated more storage than they truly need. Moving these disks from one datastore to another using storage vMotion provides an opportunity for a storage administrator to choose the virtual disk format from thick to thin, thereby reclaiming any unused storage space. Alternatively, the storage administrator can go from thin format to thick (eagerzeroedthick) using storage vMotion. In the thick format, the size of the VMDK file in the datastore is same as the size of the virtual disk which you have chosen when you created the Virtual Machine. The full storage space allocated for the virtual machine is consumed immediately in your storage system. If you do not wish to change the format at the destination, choose the option "Same format as source." For more information on thin provisioned format and thick format, visit the VMware website.

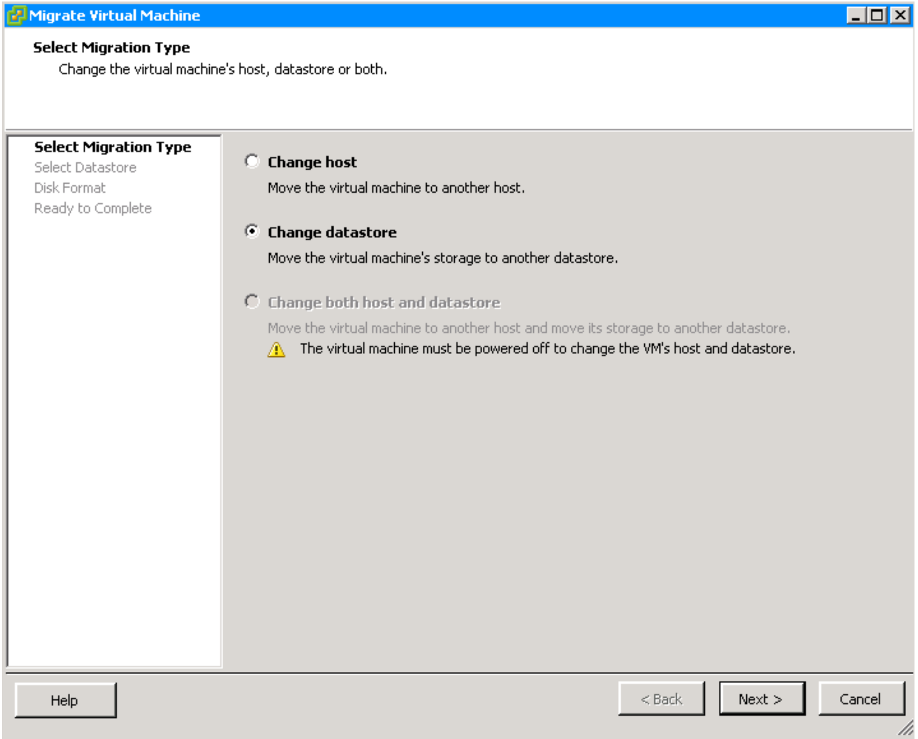
Tech Tip

Before using VMware Storage vMotion, make sure you have sufficient storage bandwidth between the ESXi host where the VM is running and both the source and destination storage arrays. This is necessary because the VM continues to read from and write to the source storage array; while at the same time, the virtual disk to be moved is being read from the source storage array and written to the destination storage array. If there is insufficient storage bandwidth, Storage vMotion can fail. If bandwidth is barely sufficient, Storage vMotion might succeed, but its performance will be poor.

Step 1: In vSphere Client, in the tree, right-click the virtual machine, and then click **Migrate**.



Step 2: Select **Change Datastore**.



Select Migration Type

Change the virtual machine's host, datastore or both.

○ Change host

Move the virtual machine to another host.

● Change datastore

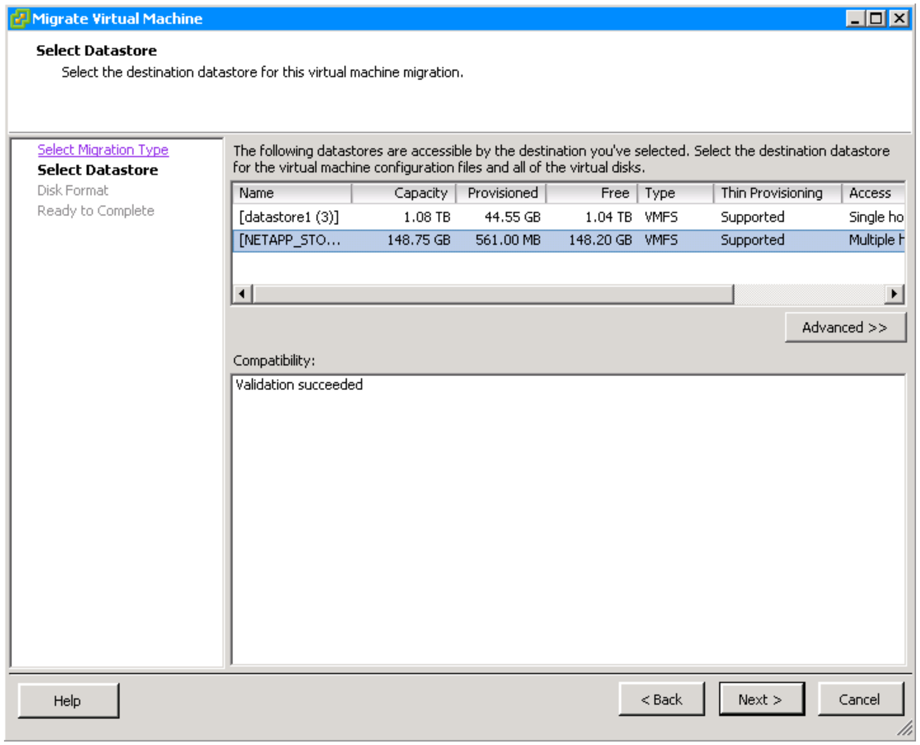
Move the virtual machine's storage to another datastore.

○ Change both host and datastore

Move the virtual machine to another host and move its storage to another datastore.

⚠ The virtual machine must be powered off to change the VM's host and datastore.

Step 3: Select the destination datastore, and then in the left pane, click **Disk Format**.



Select Datastore

Select the destination datastore for this virtual machine migration.

The following datastores are accessible by the destination you've selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Provisioned	Free	Type	Thin Provisioning	Access
[datastore1 (3)]	1.08 TB	44.55 GB	1.04 TB	VMFS	Supported	Single ho
[NETAPP_STO...	148.75 GB	561.00 MB	148.20 GB	VMFS	Supported	Multiple h

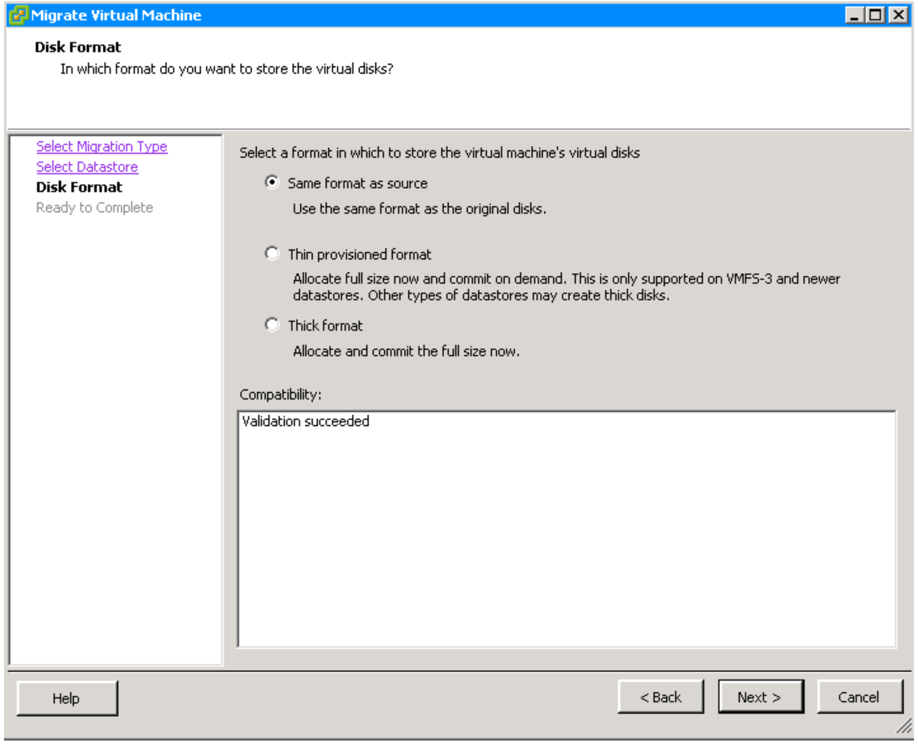
Compatibility:

Validation succeeded

Step 4: Select a disk format, and then click **Next**.

There are three choices:

- Same as source (this is the default setting)
- Thin provisioned format
- Thick format



Disk Format

In which format do you want to store the virtual disks?

Select a format in which to store the virtual machine's virtual disks

● Same format as source

Use the same format as the original disks.

○ Thin provisioned format

Allocate full size now and commit on demand. This is only supported on VMFS-3 and newer datastores. Other types of datastores may create thick disks.

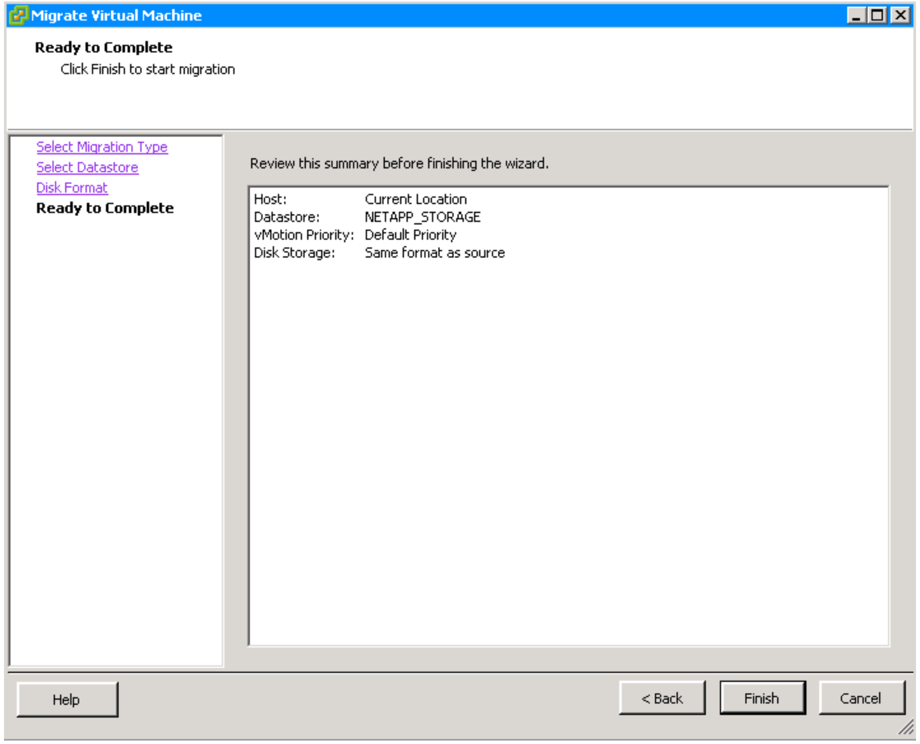
○ Thick format

Allocate and commit the full size now.

Compatibility:

Validation succeeded

Step 5: Click **Finish**. The status of the migration is displayed in the Recent Tasks pane at the bottom of the vSphere Client window.



Migrate Virtual Machine

Ready to Complete

Click Finish to start migration

Review this summary before finishing the wizard.

```
Host:              Current Location
Datastore:         NETAPP_STORAGE
vMotion Priority:  Default Priority
Disk Storage:      Same format as source
```

Procedure 2 Migrate VM to another ESXi host

Migration with vMotion allows you to move a powered-on virtual machine to a new host, without any interruption in the availability of the virtual machine.

In order to successfully use vMotion, you must first configure your hosts correctly:

- Each host must be correctly licensed for vMotion.
- Each host virtual machine's datastore must reside on shared storage, either iSCSI, network file server (NFS), or Fibre Channel.
- Host networking for the ESXi host must have a VMkernel interface configured with an IP address, have vMotion selected, and be located on the same IP subnet as the destination host.

Migration with vMotion cannot be used to move virtual machines from one data center to another or move virtual machines across Layer 3 boundaries.

Tech Tip

VMotion can use up the bandwidth of an entire interface. Use caution when configuring it on a port that includes other services such as management, iSCSI, or virtual machine traffic. VMkernel configuration is identical to iSCSI, with the exception of the check box for vMotion.

Step 1: Launch the vSphere Client and login to the vCenter Server.

Step 2: In the inventory tree, **select** the ESXi host on which you plan to enable vMotion.

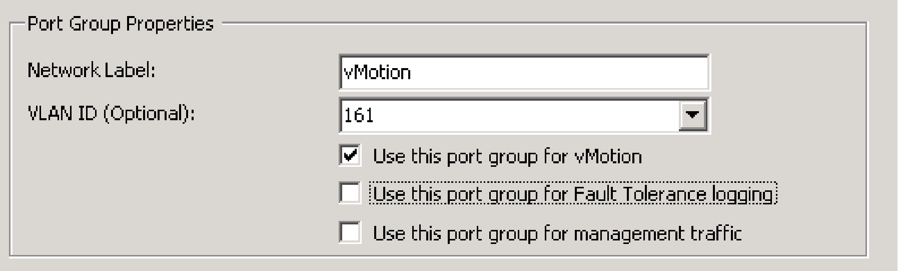
Step 3: Select the Configuration tab, and then in the Hardware menu list, choose **Networking**.

Step 4: Click **Add Networking**.

Step 5: Select Connection Type **VMkernel**.

Step 6: If you are creating a new vSwitch, select the network adapters to be assigned to the new vSwitch, and then click **Next**. If the vSwitch has already been created, select the appropriate vSwitch that will carry vMotion traffic, and then click **Next**.

Step 7: Enter a value for the Network Label, and in VLAN ID (161) for the VMkernel port that will be used to service vMotion traffic, ensure that “Use this port group for vMotion” check box is checked, and then click **Next**.



Port Group Properties

Network Label: vMotion

VLAN ID (Optional): 161

☑ Use this port group for vMotion

☐ Use this port group for Fault Tolerance logging

☐ Use this port group for management traffic

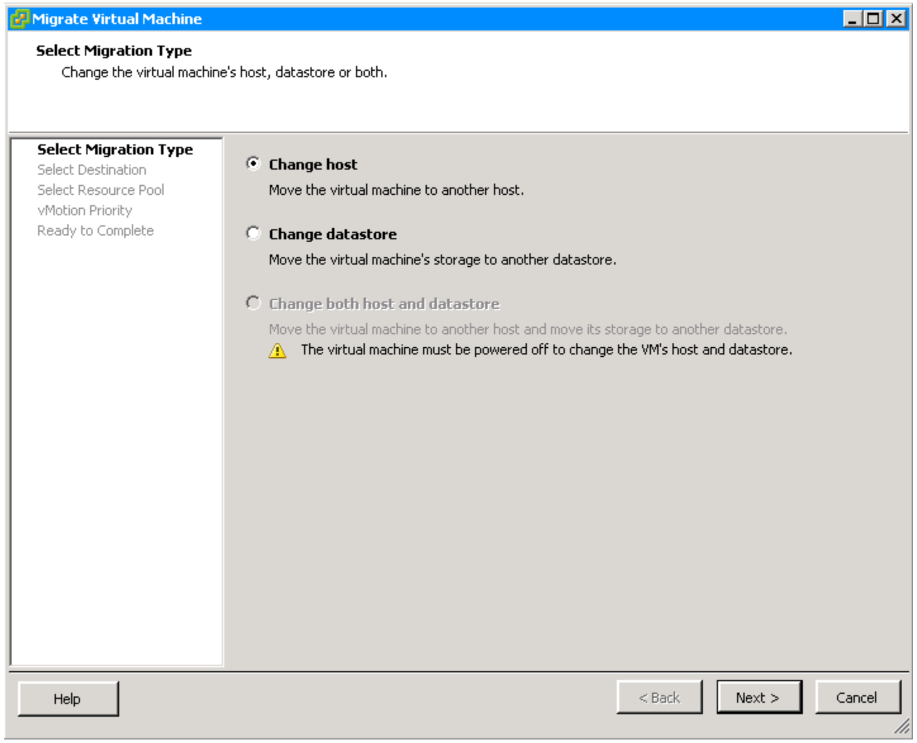
Step 8: Specify an IP address and subnet mask for this VMkernel interface and click **Next**.

Step 9: Review the configuration on the Summary page and then click **Finish**.

Step 10: Repeat Step 1 through Step 9 for all of the ESXi hosts you plan to enable vMotion on.

Step 11: In vSphere Client, in the tree, right-click the virtual machine you want to migrate, and then click **Migrate**.

Step 12: Select **Change host**. You are prompted for a destination.



Select Migration Type

Change the virtual machine's host, datastore or both.

● Change host

Move the virtual machine to another host.

○ Change datastore

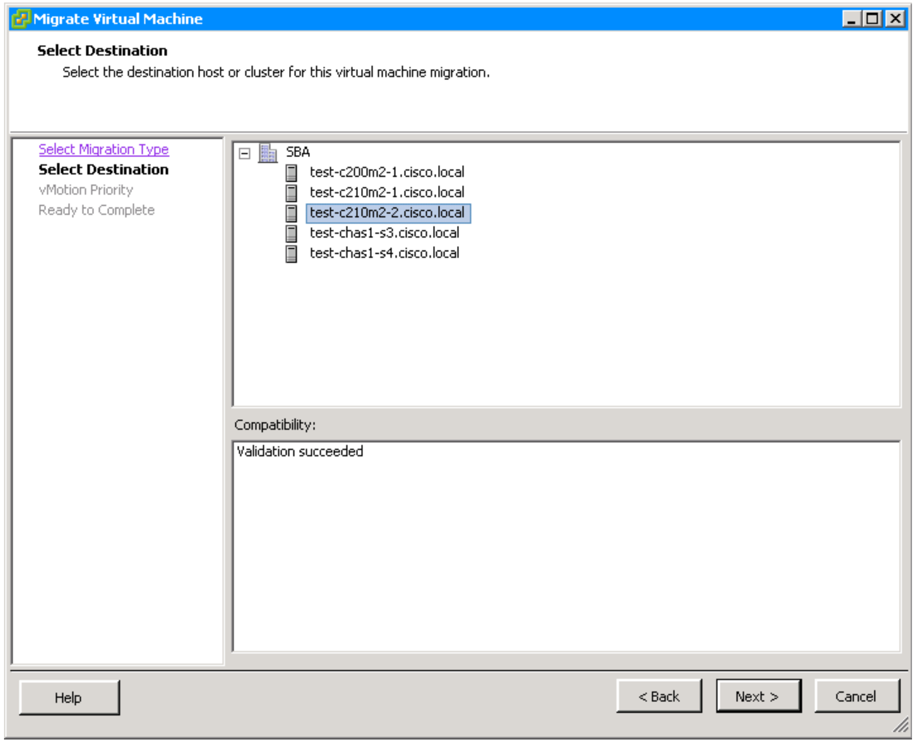
Move the virtual machine's storage to another datastore.

○ Change both host and datastore

Move the virtual machine to another host and move its storage to another datastore.

⚠ The virtual machine must be powered off to change the VM's host and datastore.

Step 13: Choose the correct destination host, and then click **Next**.



Migrate Virtual Machine

Select Destination

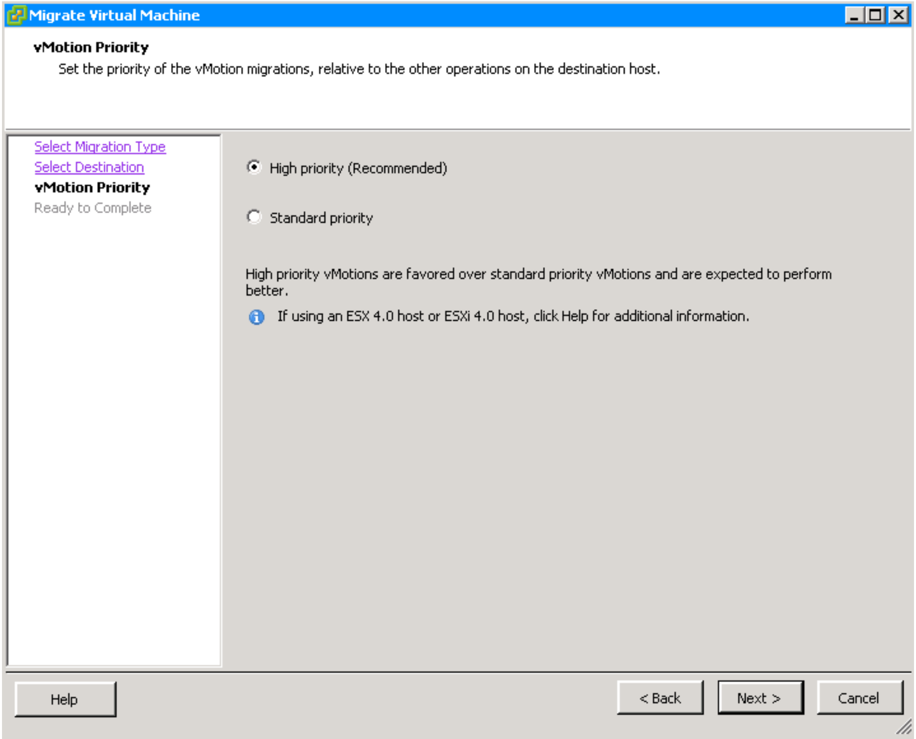
Select the destination host or cluster for this virtual machine migration.

- SBA
  - test-c200m2-1.cisco.local
  - test-c210m2-1.cisco.local
  - test-c210m2-2.cisco.local
  - test-chas1-s3.cisco.local
  - test-chas1-s4.cisco.local

Compatibility:

Validation succeeded

Step 14: Choose the reservation priority for the ESXi host CPU, and then click **Next**.



Migrate Virtual Machine

vMotion Priority

Set the priority of the vMotion migrations, relative to the other operations on the destination host.

● High priority (Recommended)

○ Standard priority

High priority vMotions are favored over standard priority vMotions and are expected to perform better.

If using an ESX 4.0 host or ESXi 4.0 host, click Help for additional information.

Step 15: Click **Finish**. Live migration of virtual machines from one ESXi host to another occurs without any service interruption.

When migration is complete, the virtual machine is displayed under the new ESXi host you selected. You can monitor the status of the migration in the Recent Tasks pane while the vMotion is in progress.

Cisco Nexus 1000V Series Switch Installation and Deployment

The Cisco Nexus 1000V Series Switch is a virtual distributed switch that runs in software on the virtualized host. The value of using Cisco Nexus 1000V is that it extends the same Cisco NX-OS operating system to the hypervisor that you are familiar with in the Nexus 5500 Series switches that make up the Cisco SBA Data Center core. Using Cisco Nexus 1000V in your VMware ESXi environment provides ease of operation with a consistent CLI and feature set for the VMware distributed switch environment.

The Cisco Nexus 1000V Virtual Supervisor Module (VSM) is the central control for distributed Virtual Ethernet Modules (VEMs). In a typical modular Ethernet switch, the supervisor module controls all of the control plane protocols, enables central configuration of line cards and ports, and provides statistics on packet counts, among other supervisory tasks. In the Nexus 1000V distributed switch, the VSM controls the distributed virtual switches, or VEMs, on the VMware servers.

You can install the Cisco Nexus 1000V VSM on a VMware ESXi host as a virtual machine, and you can install a secondary VSM on a second ESXi host for resiliency. For the ultimate in resiliency and scalability in controlling a Nexus 1000V environment, you can deploy the Cisco Nexus 1010 Virtual Services Appliance.

Reader Tip

This deployment guide is based on the best practices for Cisco Nexus 1000V Series Switches:
http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9902/white_paper_c11-558242.html

The following process installs the Cisco Nexus 1000V Series Switch on virtual machines.

Process

Deploying Cisco Nexus 1000V VSM as a VM on an ESXi Host

1. Install the first VSM
2. Configure the primary VSM
3. Install and setup the secondary VSM

This process walks you through deploying a primary and secondary Cisco Nexus 1000V VSM installed on VMware virtual machines for resiliency. You will install VSM using an Open Virtualization Format (OVF) template provided in the download for the Cisco Nexus 1000V code.

Each Cisco Nexus 1000V VSM in an active-standby pair is required to run on a separate VMware ESX/ESXi host. This requirement helps ensure high availability even if one of the VMware ESX/ESXi servers fails. It is recommended that you disable Distributed Resource Scheduling (DRS) for both active and standby VSMs, which prevents the VSMs from ending up on the same server. If you do not disable DRS, you must use the VMware anti-affinity rules to ensure that the two virtual machines are never on the same host. If the VSMs end up on the same host due to VMware High Availability, VMware DRS posts a five-star recommendation to move one of the VSMs.

The Virtual Ethernet Module (VEM) provides Cisco Nexus 1000V Series with network connectivity and forwarding capabilities. Each instance of Cisco Nexus 1000V Series is composed of two VSMs and one or more VEMs.

The VSM and VEM can communicate over a Layer 2 network or Layer 3 network. Layer 3 mode is the recommended option, as it is easier to troubleshoot Layer 3 communication problems between VSM and VEM. This deployment guide uses the Layer 3 mode of operation for VSM-to-VEM communication.

Procedure 1 Install the first VSM

The Cisco Nexus 1000V VSM is a virtual machine that, during installation, creates three virtual network interface cards (vNICs):

- The control interface handles low-level control packets, such as heartbeats, as well as any configuration data that needs to be exchanged between the VSM and VEM. VSM active/standby synchronization is done via this interface.
- The management interface is used to maintain the connection between the VSM and the VMware vCenter Server. This interface allows access to VSM via HTTP and Secure Shell (SSH) Protocol.
- The packet interface is used to carry packets that need to be processed by the VSM. This interface is mainly used for two types of traffic: Cisco Discovery Protocol and Internet Group Management Protocol (IGMP) control packets. The VSM presents a unified Cisco Discovery Protocol view to the network administrator through the Cisco NX-OS CLI. When a VEM receives a Cisco Discovery Protocol packet, the VEM retransmits that packet to the VSM so that the VSM can parse the packet and populate the Cisco Discovery Protocol entries in the CLI. The packet interface is also used to coordinate IGMP across multiple servers. For example, when a server receives an IGMP join request, that request is sent to the VSM, which coordinates the request across all the modules in the switch. The packet interface is always the third interface on the VSM and is usually labeled “Network Adapter 3” in the virtual machine network properties. The packet interface is used in Layer 2 mode to carry network packets that need to be coordinated across the entire Cisco Nexus 1000V Series switch. In Layer 3 mode this vNIC is not used, and the control and packets frames are encapsulated in User Datagram Packets (UDP).

With Cisco Nexus 1000V running in Layer 3 mode, the control and packet frames between the VSM and the VEMs are encapsulated in UDP. This process requires configuration of the VMware VMkernel interface on each VMware ESX host. Ideally, this is the management interface that the ESXi host uses to communicate with the vCenter Server. This alleviates the need to consume another VMkernel interface and another IP address for Layer 3 communication between VSM and VEM. Cisco Nexus 1000V running in Layer 3 mode also eliminates the need for a separate Packet VLAN. The control interface on the VSMs is used for high availability communication between VSMs over IP, however it does not require a switched virtual interface on the data center core for routing beyond the data center. You must ensure that the control and management VLANs are configured on the upstream data center core switches. You can use the same VLAN for control and management; however, using separate VLANs provides flexibility.

Table 2 - VLANs used for Cisco Nexus 1000V VSM installation

VLAN	IP Address Range	Description
160	10.4.60.0/24	Nexus 1000V Control
163	10.4.63.0/24	Data Center Management Traffic

Table 3 - Additional VLANs defined in the SBA data center design

VLANs	Description
148-155	Virtual Machine Network Data
161	vMotion
162	iSCSI

Step 1: Download the zipped Cisco Nexus 1000V software image, save it on the local drive of the machine from where you are launching vSphere Client, and then extract the contents of the software image onto your local drive. The extraction will contain VSM files with a .ova extension and an OVF folder with the .ovf extension file. This procedure will use the file with the .ova extension.

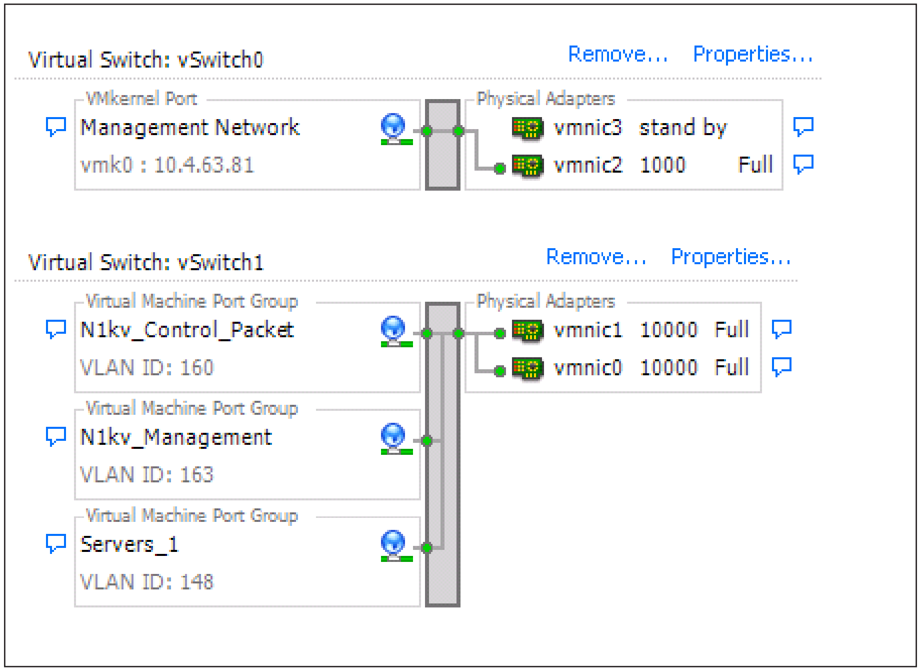
Tech Tip

You can install the software from the OVA or OVF image. Here you use the OVA installation file, because it allows you to apply initial configurations to the VSM, including the VSM domain ID, admin user password, management IP address, subnet mask and IP gateway.

Step 2: Log in to your vCenter Server via the VMware vSphere Client, with the domain administrator username and password.

Step 3: Navigate to Home > Inventory > Hosts and Clusters, and then choose the host on which you plan to install the VSM VM.

Step 4: Navigate to **Configuration > Networking > Virtual Switch**, and then ensure that the control and management port groups are configured with correct VLANs, as shown in .



Virtual Switch: vSwitch0 Remove... Properties...

VMkernel Port
Management Network
vmk0 : 10.4.63.81

Physical Adapters
vmnic3 stand by
vmnic2 1000 Full

Virtual Switch: vSwitch1 Remove... Properties...

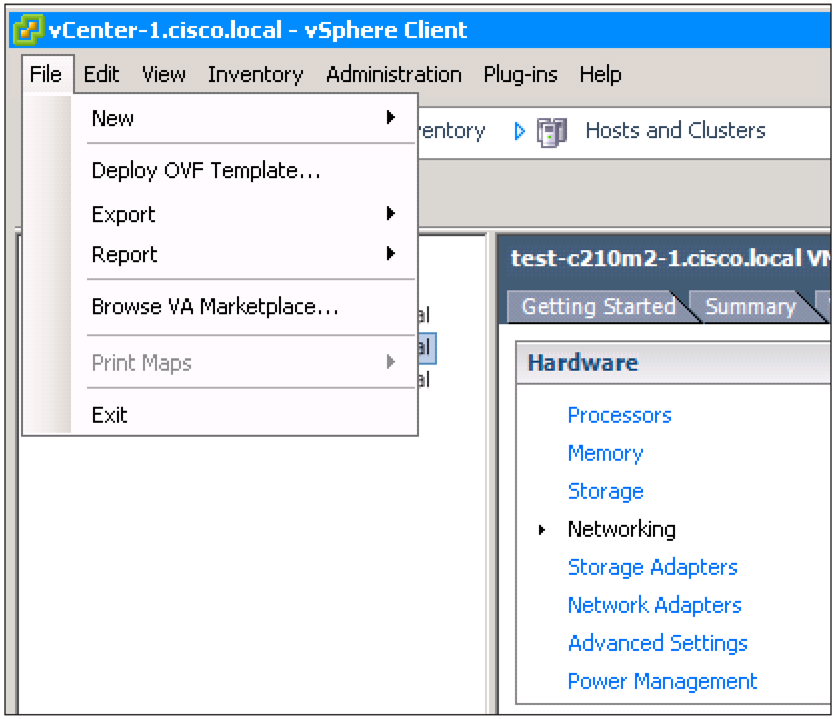
Virtual Machine Port Group
N1kv_Control_Packet
VLAN ID: 160

Virtual Machine Port Group
N1kv_Management
VLAN ID: 163

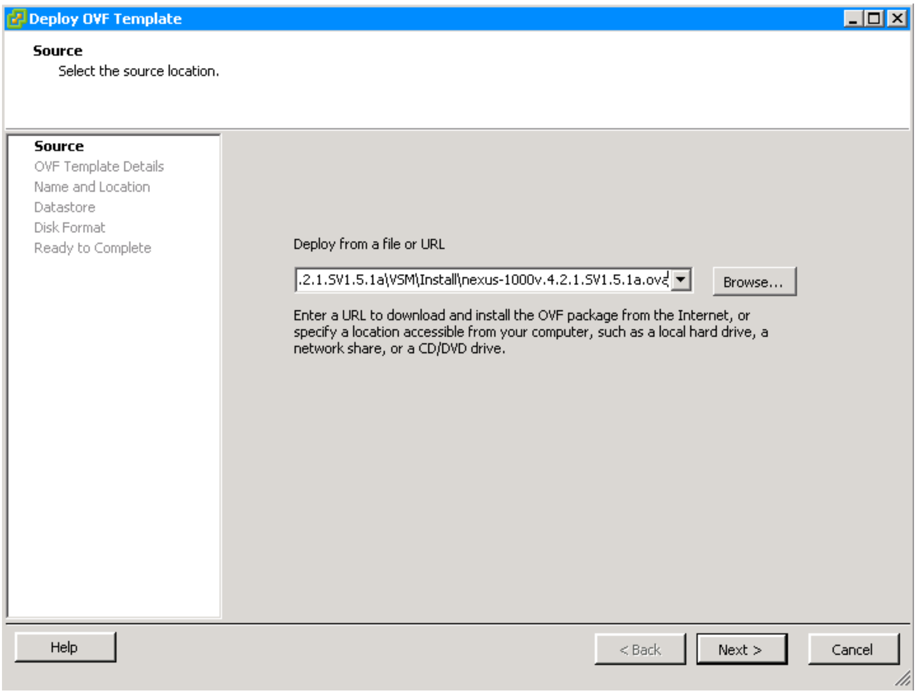
Virtual Machine Port Group
Servers_1
VLAN ID: 148

Physical Adapters
vmnic1 10000 Full
vmnic0 10000 Full

Step 5: In the vSphere Client, from the File menu, choose **Deploy OVF Template**.



Step 6: Choose **Deploy from file option**, browse to the location where you have downloaded the OVA file, and then click **Next**.



Source

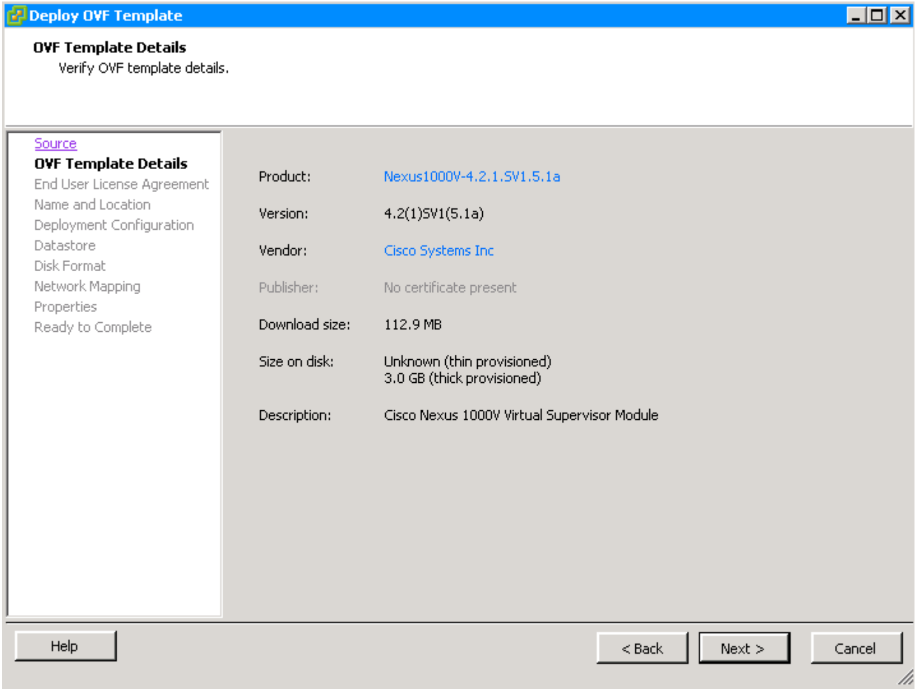
Select the source location.

Deploy from a file or URL

.2.1.SV1.5.1a\VSM\Install\nexus-1000v.4.2.1.SV1.5.1a.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

Step 7: You are presented with product information, size of the file, and the size of VM disk. Verify that you have selected the correct version and product, and then click **Next**.



OVF Template Details

Verify OVF template details.

Product: Nexus1000V-4.2.1.SV1.5.1a

Version: 4.2(1)SV1(5.1a)

Vendor: Cisco Systems Inc

Publisher: No certificate present

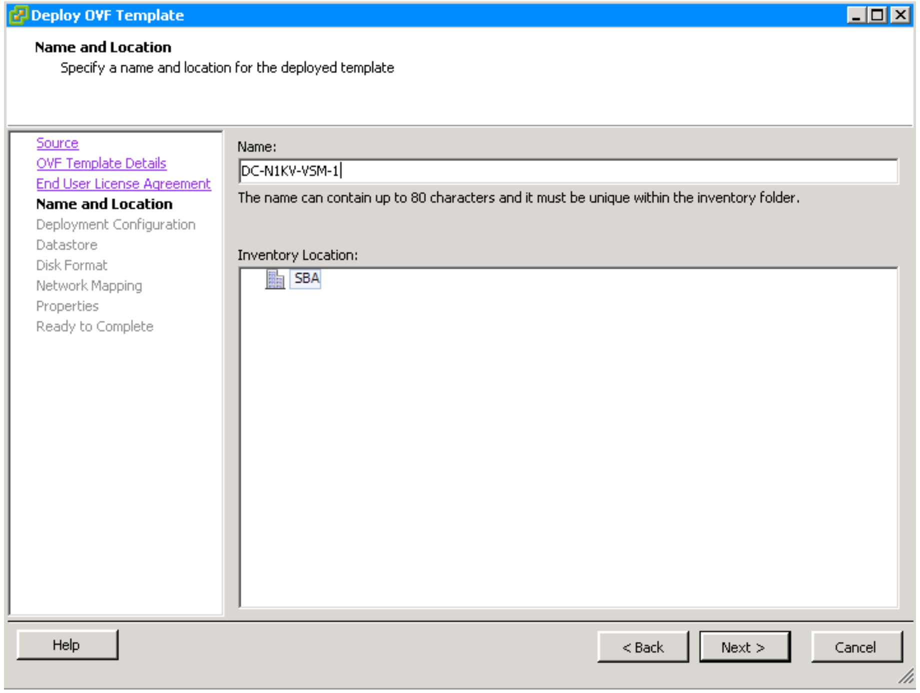
Download size: 112.9 MB

Size on disk: Unknown (thin provisioned)
3.0 GB (thick provisioned)

Description: Cisco Nexus 1000V Virtual Supervisor Module

Step 8: Accept the Cisco Nexus 1000V License Agreement, and then click **Next**.

Step 9: Specify the name of your VSM, choose the location, and then click **Next**.



Deploy OVF Template

Name and Location

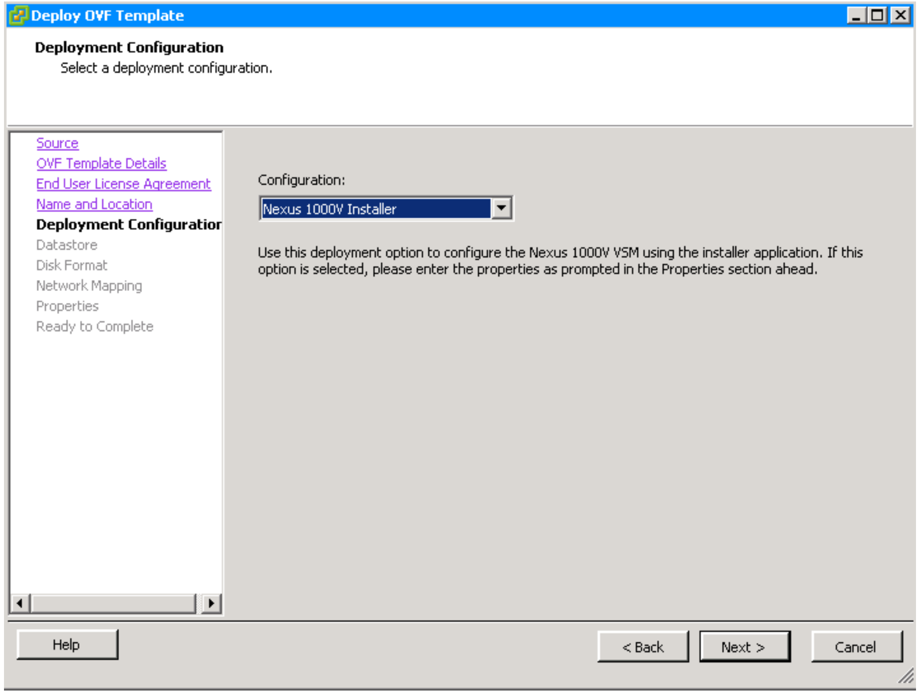
Specify a name and location for the deployed template

Name: DC-N1KV-VSM-1

The name can contain up to 80 characters and it must be unique within the inventory folder.

Inventory Location: SBA

Step 10: In the Configuration list, choose **Nexus 1000V Installer**, and then click **Next**.



Deploy OVF Template

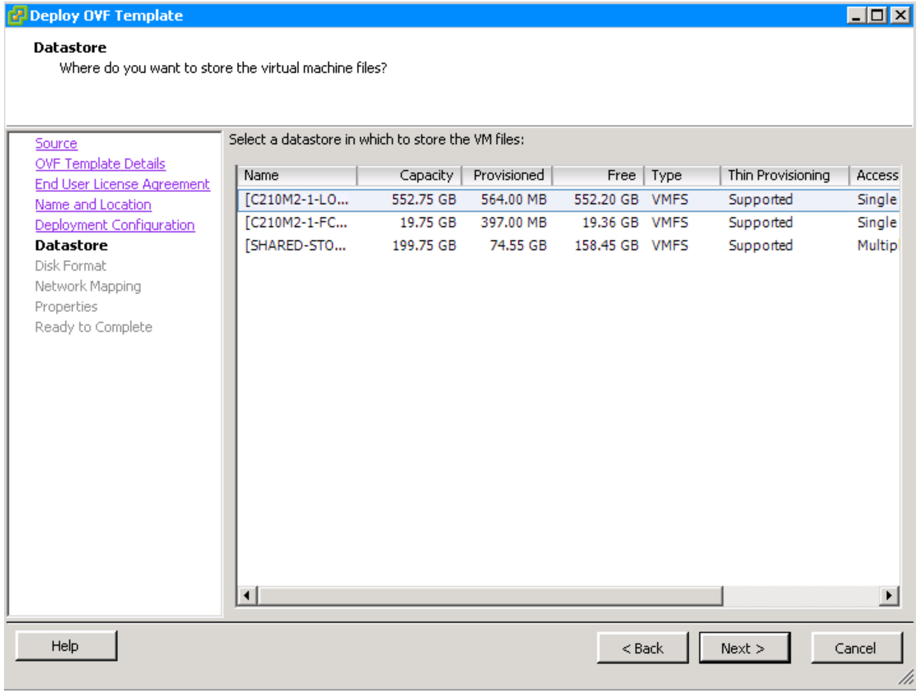
Deployment Configuration

Select a deployment configuration.

Configuration: Nexus 1000V Installer

Use this deployment option to configure the Nexus 1000V VSM using the installer application. If this option is selected, please enter the properties as prompted in the Properties section ahead.

Step 11: Choose the datastore you want the VSM to use, and then click **Next**.



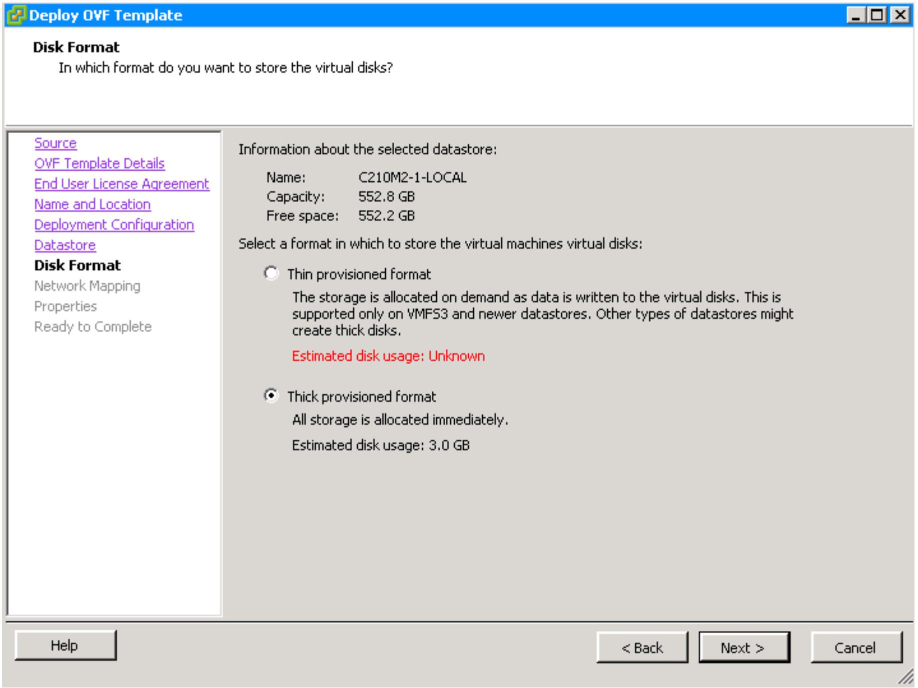
Datastore

Where do you want to store the virtual machine files?

Select a datastore in which to store the VM files:

Name	Capacity	Provisioned	Free	Type	Thin Provisioning	Access
[C210M2-1-LO...	552.75 GB	564.00 MB	552.20 GB	VMFS	Supported	Single
[C210M2-1-FC...	19.75 GB	397.00 MB	19.36 GB	VMFS	Supported	Single
[SHARED-STO...	199.75 GB	74.55 GB	158.45 GB	VMFS	Supported	Multip

Step 12: Select **Thick provisioned format**, and then click **Next**. This allocates all storage needed to store the virtual machine virtual disks. The size of the VSM will be approximately 3 GB.



Disk Format

In which format do you want to store the virtual disks?

Information about the selected datastore:

Name: C210M2-1-LOCAL
Capacity: 552.8 GB
Free space: 552.2 GB

Select a format in which to store the virtual machines virtual disks:

○ Thin provisioned format

The storage is allocated on demand as data is written to the virtual disks. This is supported only on VMFS3 and newer datastores. Other types of datastores might create thick disks.

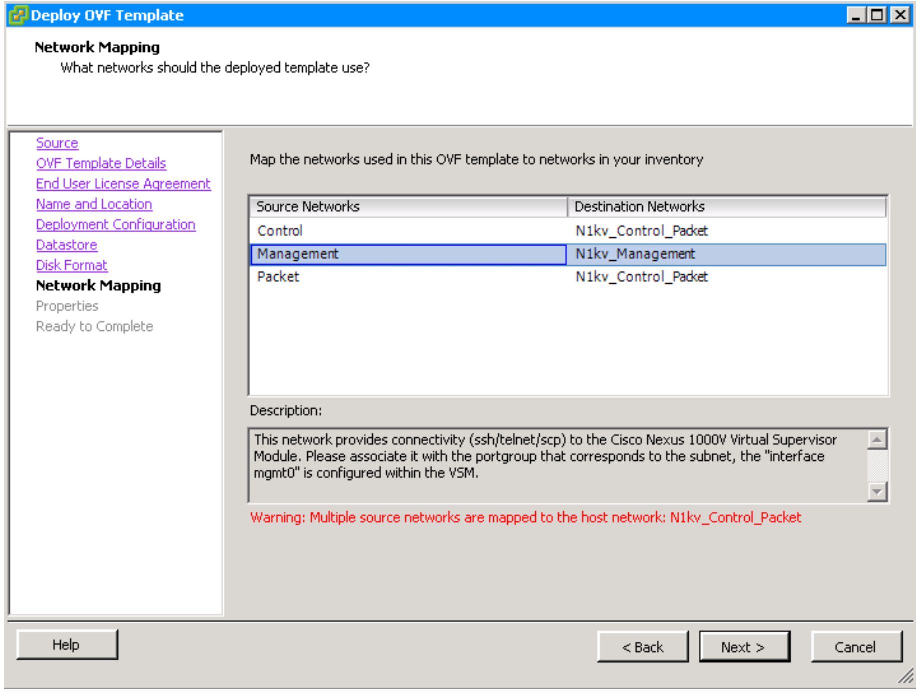
Estimated disk usage: Unknown

● Thick provisioned format

All storage is allocated immediately.

Estimated disk usage: 3.0 GB

Step 13: In the Layer 3 control mode, the packet NIC does not get used on the VM. The VM still expects the packet nic to be present. On the Network Mapping screen, in the **Destination Network** list, map the Control port-group for the Control Source network and the Packet Source network, and the Management port-group for the Management Source network. Click **Next**.



Network Mapping

What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
Control	N1kv_Control_Packet
Management	N1kv_Management
Packet	N1kv_Control_Packet

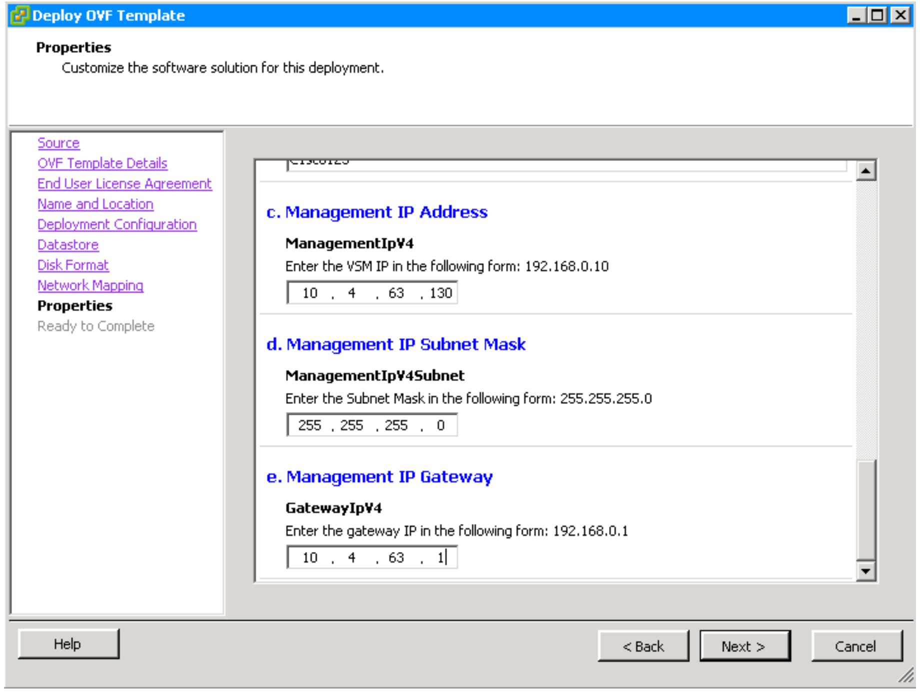
Description:

This network provides connectivity (ssh/telnet/scp) to the Cisco Nexus 1000V Virtual Supervisor Module. Please associate it with the portgroup that corresponds to the subnet, the "interface mgmt0" is configured within the VSM.

Warning: Multiple source networks are mapped to the host network: N1kv_Control_Packet

Step 14: Specify the following properties for your primary VSM, and then click **Next**.

- VSM Domain ID
- Nexus 1000V Admin User Password
- Management IP Address
- Management IP Subnet mask
- Management IP Gateway



Properties

Customize the software solution for this deployment.

c. Management IP Address

ManagementIpV4

Enter the VSM IP in the following form: 192.168.0.10

10 . 4 . 63 . 130

d. Management IP Subnet Mask

ManagementIpV4Subnet

Enter the Subnet Mask in the following form: 255.255.255.0

255 . 255 . 255 . 0

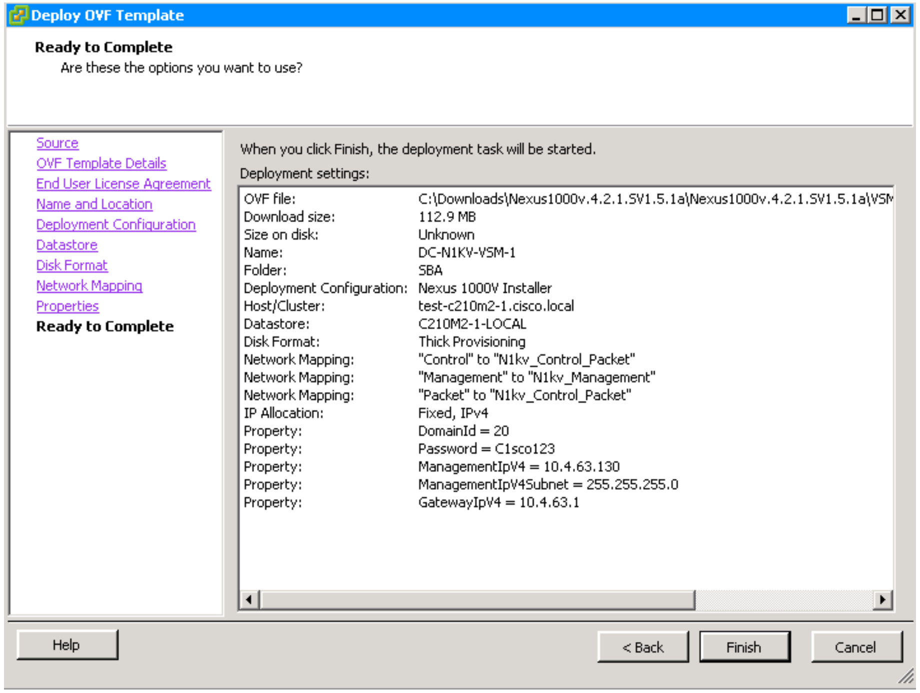
e. Management IP Gateway

GatewayIpV4

Enter the gateway IP in the following form: 192.168.0.1

10 . 4 . 63 . 1

Step 15: Verify that your configuration settings are correct, and then click **Finish**. VMware starts to deploy your VSM.



Deploy OVF Template

Ready to Complete

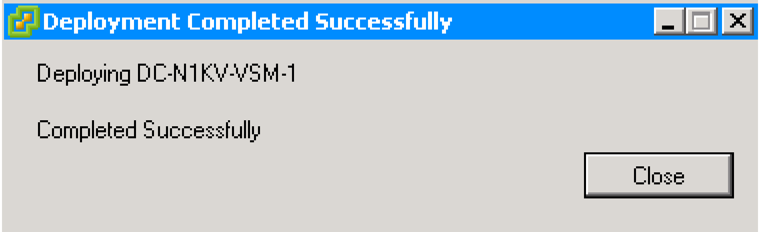
Are these the options you want to use?

When you click Finish, the deployment task will be started.

Deployment settings:

```
OVF file:                    C:\Downloads\Nexus1000v.4.2.1.SV1.5.1a\Nexus1000v.4.2.1.SV1.5.1a\VSM
Download size:               112.9 MB
Size on disk:                Unknown
Name:                        DC-N1KV-VSM-1
Folder:                      SBA
Deployment Configuration:    Nexus 1000V Installer
Host/Cluster:                test-c210m2-1.cisco.local
Datastore:                   C210M2-1-LOCAL
Disk Format:                 Thick Provisioning
Network Mapping:             "Control" to "N1kv_Control_Packet"
Network Mapping:             "Management" to "N1kv_Management"
Network Mapping:             "Packet" to "N1kv_Control_Packet"
IP Allocation:               Fixed, IPv4
Property:                    DomainId = 20
Property:                    Password = C1sco123
Property:                    ManagementIpV4 = 10.4.63.130
Property:                    ManagementIpV4Subnet = 255.255.255.0
Property:                    GatewayIpV4 = 10.4.63.1
```

Step 16: On the "Deployment Completed Successfully" message that appears, click **Close**.

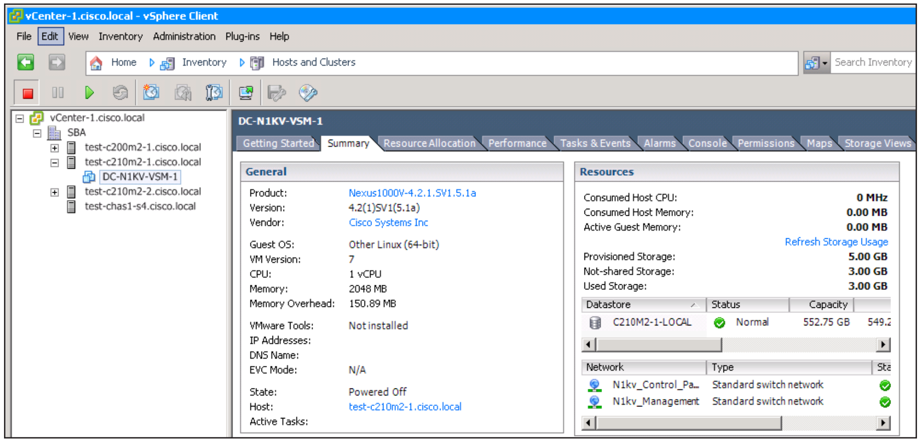


Deployment Completed Successfully

Deploying DC-N1KV-VSM-1

Completed Successfully

You can find the VSM in the inventory window under the machine it was installed on. Notice that the VSM is in a powered-off state.



vCenter-1.cisco.local - vSphere Client

DC-N1KV-VSM-1

General

```
Product:            Nexus1000V-4.2.1.SV1.5.1a
Version:            4.2(1)SV1(5.1a)
Vendor:             Cisco Systems Inc

Guest OS:           Other Linux (64-bit)
VM Version:         7
CPU:                1 vCPU
Memory:             2048 MB
Memory Overhead:    150.89 MB

VMware Tools:       Not installed
IP Addresses:
DNS Name:
EVC Mode:           N/A

State:              Powered Off
Host:               test-c210m2-1.cisco.local
Active Tasks:
```

Resources

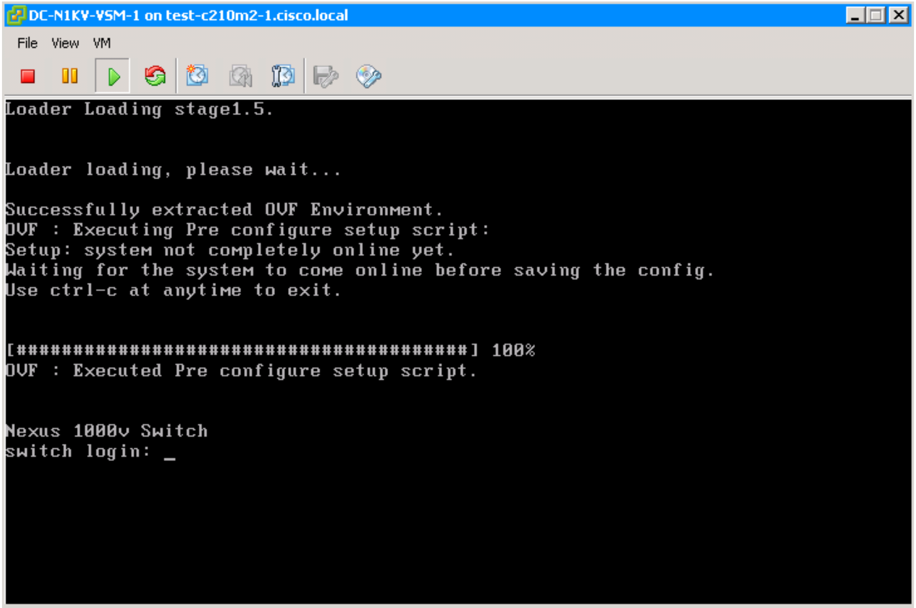
```
Consumed Host CPU:         0 MHz
Consumed Host Memory:    0.00 MB
Active Guest Memory:     0.00 MB
              Refresh Storage Usage
Provisioned Storage:     5.00 GB
Not-shared Storage:      3.00 GB
Used Storage:            3.00 GB
```

Datastore	Status	Capacity	
C210M2-1-LOCAL	✓ Normal	552.75 GB	549.2

Network	Type	Sta
N1kv_Control_Pa...	Standard switch network	✓
N1kv_Management	Standard switch network	✓

Step 17: Right click the VSM VM, point to **Power**, and then click **Power On**.

Step 18: Right-click the VSM, choose **Open Console**, and then wait for the VSM to finish the boot process and display the login prompt.



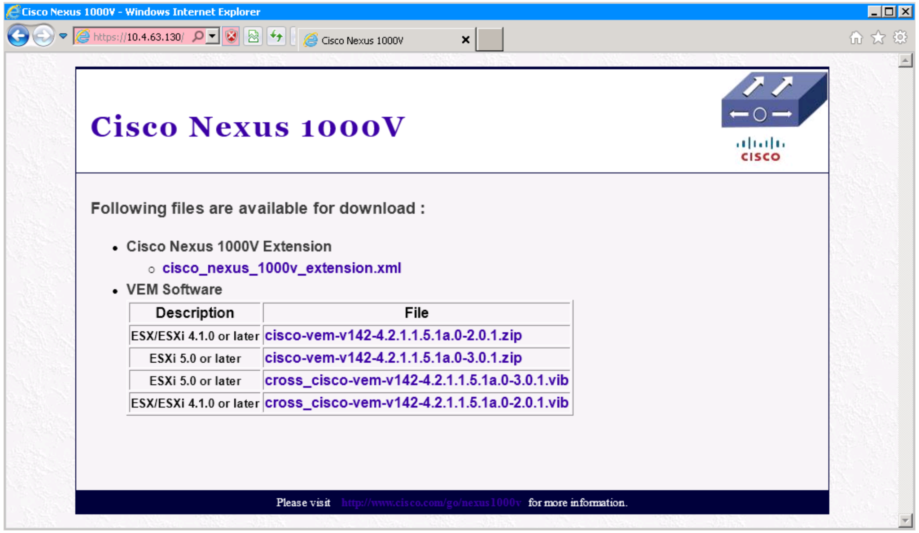
```
Loader Loading stage1.5.


Loader loading, please wait...

Successfully extracted OVF Environment.
OVF : Executing Pre configure setup script:
Setup: system not completely online yet.
Waiting for the system to come online before saving the config.
Use ctrl-c at anytime to exit.


[########################################] 100%
OVF : Executed Pre configure setup script.


Nexus 1000v Switch
switch login: _
```

Procedure 2 Configure the primary VSM

In this procedure, you perform the following:

- Install the Nexus 1000V extension in the vCenter
- Set the transport mode of VSM from Layer 2 to Layer 3
- Connect the VSM to vCenter Server
- Verify the connectivity from the VSM to the vCenter
- Configure the VSM as Primary VSM

Step 1: Launch a web browser, and then browse to the IP address of the VSM (http://10.4.63.130).



Cisco Nexus 1000V

Following files are available for download :

- Cisco Nexus 1000V Extension
  - cisco_nexus_1000v_extension.xml
- VEM Software

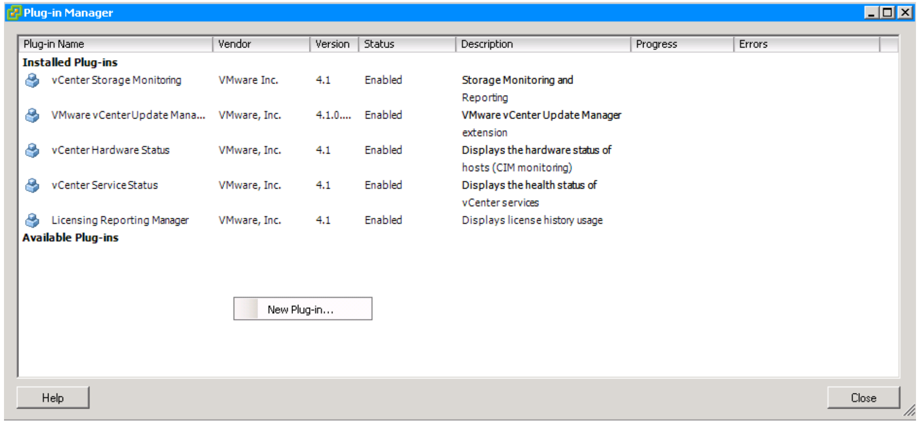
Description	File
ESX/ESXi 4.1.0 or later	cisco-vem-v142-4.2.1.1.5.1a.0-2.0.1.zip
ESXi 5.0 or later	cisco-vem-v142-4.2.1.1.5.1a.0-3.0.1.zip
ESXi 5.0 or later	cross_cisco-vem-v142-4.2.1.1.5.1a.0-3.0.1.vib
ESX/ESXi 4.1.0 or later	cross_cisco-vem-v142-4.2.1.1.5.1a.0-2.0.1.vib

Please visit http://www.cisco.com/go/nexus1000v for more information.

Step 2: Under the Cisco Nexus 1000V Extension, right click on the cisco_nexus_1000v_extension.xml file, select the **Save target as** option, and then save the xml file to the local directory of the machine from where you launch vSphere Client.

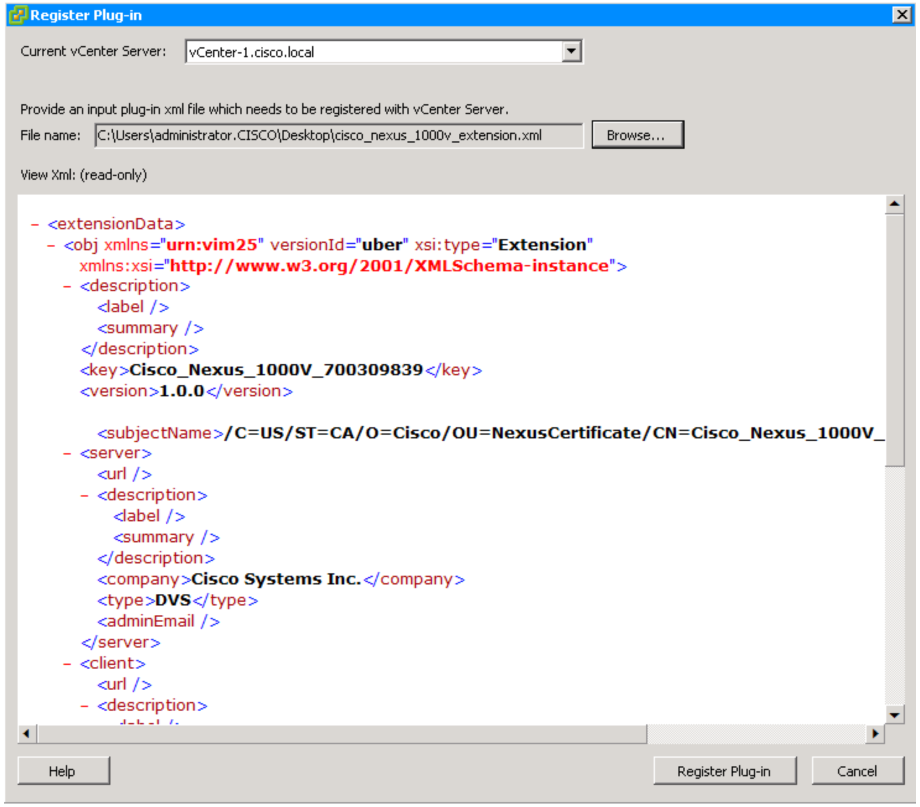
Step 3: In the vSphere Client, from the **Plug-ins** menu, choose **Manage Plug-ins**. The Plug-in Manager screen pops up.

Step 4: On the Plug-in Manager screen, under the Available Plug-ins section, right click, and then select **New Plug-in**.



Plug-in Name	Vendor	Version	Status	Description	Progress	Errors
Installed Plug-ins						
vCenter Storage Monitoring	VMware Inc.	4.1	Enabled	Storage Monitoring and Reporting		
VMware vCenter Update Mana...	VMware, Inc.	4.1.0....	Enabled	VMware vCenter Update Manager extension		
vCenter Hardware Status	VMware, Inc.	4.1	Enabled	Displays the hardware status of hosts (CIM monitoring)		
vCenter Service Status	VMware, Inc.	4.1	Enabled	Displays the health status of vCenter services		
Licensing Reporting Manager	VMware, Inc.	4.1	Enabled	Displays license history usage		
Available Plug-ins						

Step 5: In the Register Plug-in screen, browse to the location where you have stored the Cisco Nexus 1000V extension xml file that was downloaded in Step 2, and then click **Register Plug-in**.



Current vCenter Server: vCenter-1.cisco.local

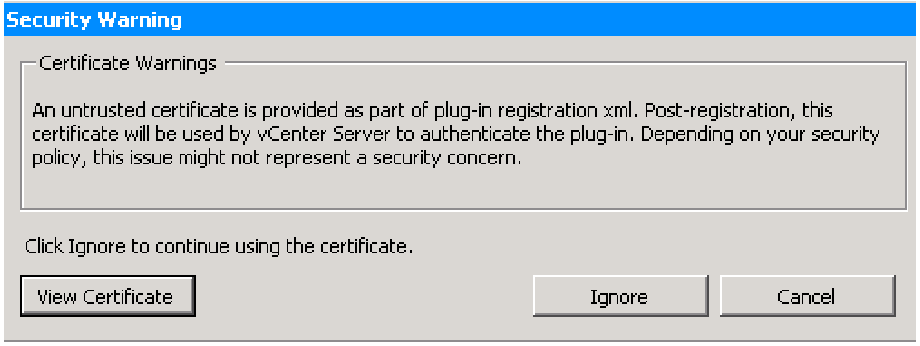
Provide an input plug-in xml file which needs to be registered with vCenter Server.

File name: C:\Users\administrator.CISCO\Desktop\cisco_nexus_1000v_extension.xml

View Xml: (read-only)

```
- <extensionData>
  - <obj xmlns="urn:vim25" versionId="uber" xsi:type="Extension"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    - <description>
        <label />
        <summary />
      </description>
      <key>Cisco_Nexus_1000V_700309839</key>
      <version>1.0.0</version>

        <subjectName>/C=US/ST=CA/O=Cisco/OU=NexusCertificate/CN=Cisco_Nexus_1000V_
    - <server>
        <url />
      - <description>
          <label />
          <summary />
        </description>
        <company>Cisco Systems Inc.</company>
        <type>DVS</type>
        <adminEmail />
      </server>
    - <client>
        <url />
      - <description>
```

Step 6: In the Security warning screen, click **Ignore**.



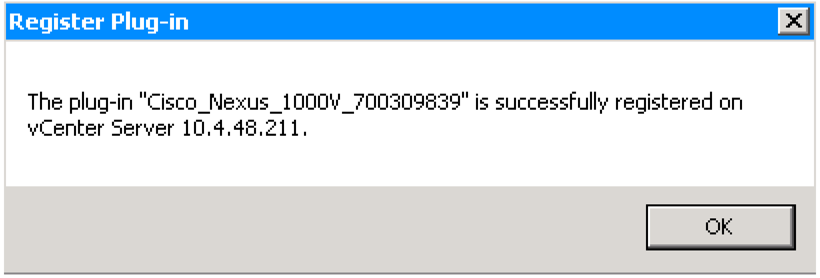
Security Warning

Certificate Warnings

An untrusted certificate is provided as part of plug-in registration xml. Post-registration, this certificate will be used by vCenter Server to authenticate the plug-in. Depending on your security policy, this issue might not represent a security concern.

Click Ignore to continue using the certificate.

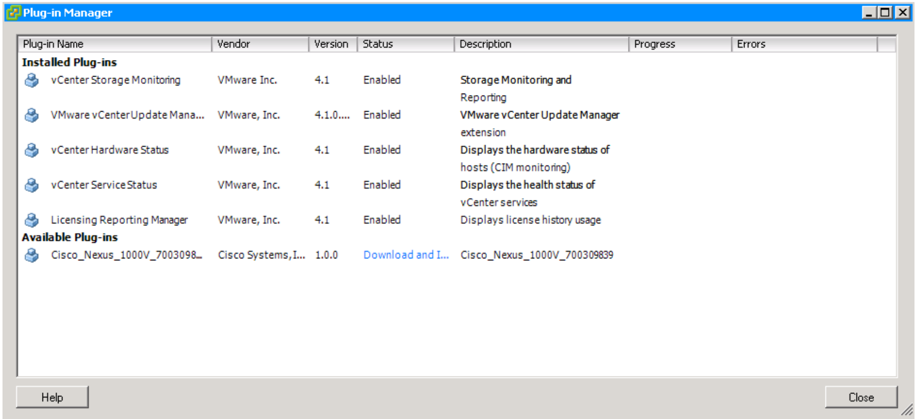
A message confirms that the plug-in has registered successfully with the vCenter Server. The VSM maintains a link to the vCenter Server to maintain the definition of Cisco Nexus 1000V Series within VMware vCenter Server and also to propagate port profiles.



Register Plug-in

The plug-in "Cisco_Nexus_1000V_700309839" is successfully registered on vCenter Server 10.4.48.211.

Step 7: Do not attempt to download and install the plug-in, as this capability is currently not available for the Cisco Nexus 1000V plug-in. In the Plug-in Manager screen, click **Close**.



Plug-in Manager

Plug-in Name	Vendor	Version	Status	Description	Progress	Errors
Installed Plug-ins						
vCenter Storage Monitoring	VMware Inc.	4.1	Enabled	Storage Monitoring and Reporting		
VMware vCenter Update Mana...	VMware, Inc.	4.1.0....	Enabled	VMware vCenter Update Manager extension		
vCenter Hardware Status	VMware, Inc.	4.1	Enabled	Displays the hardware status of hosts (CIM monitoring)		
vCenter Service Status	VMware, Inc.	4.1	Enabled	Displays the health status of vCenter services		
Licensing Reporting Manager	VMware, Inc.	4.1	Enabled	Displays license history usage		
Available Plug-ins						
Cisco_Nexus_1000V_7003098...	Cisco Systems, I...	1.0.0	Download and I...	Cisco_Nexus_1000V_700309839		

Step 8: In the vSphere Client window, right-click the VSM VM, choose **Open Console**, and then log in to the VSM using the default username (admin) and the password you provided during the VSM installation.

Step 9: Configure the device hostname.

```
hostname [hostname]
```

Step 10: In this step, you set the transport mode of the VSM from Layer 2 to Layer 3 for the VSM domain control and packet traffic.

When setting up the Layer 3 control mode you have two options:

- Layer 3 packet transport through the VSM mgmt0 interface
- Layer 3 packet transport through the VSM control0 interface

Setup the Layer 3 packet transport to use the VSM mgmt0 interface.

```
svs-domain
no control vlan
no packet vlan
svs mode L3 interface mgmt0
```

Tech Tip

If you want to isolate your control and management packet transport to the VSM VM, you can use a dedicated control interface.

Step 11: Configure a connection, and then connect the VSM to vCenter Server.

```
svs connection [name]
  protocol vmware-vim
  remote ip address [vCenter Server IP address] port 80
  vmware dvs datacenter-name [Datacenter name in vCenter Server]
  connect
```

Step 12: Verify that communication with vCenter Server is working.

```
DC-N1kv-VSM# show svs connections

connection vcenter:
    ip address: 10.4.48.211
    remote port: 80
    protocol: vmware-vim https
    certificate: default
    datacenter name: SBA
    admin:
    max-ports: 8192
    DVS uuid: f8 cc 2b 50 64 f3 84 e3-57 57 ed 05 24 66 d3 20
    config status: Enabled
    operational status: Connected
    sync status: Complete
```

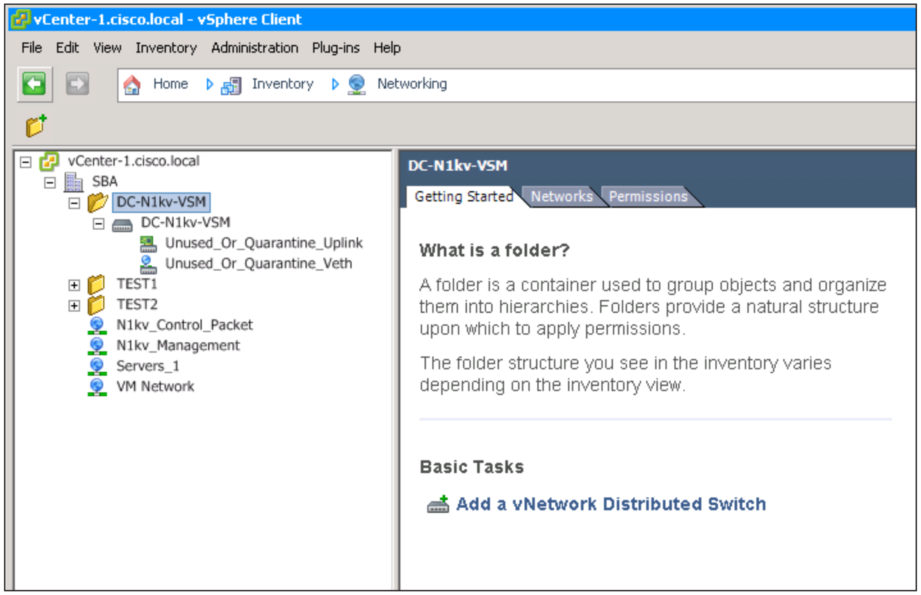
Step 13: After the installation of VSM, it is left in a standalone mode. The best practice for deployment of VSM is in an HA pair. Convert the VSM standalone role to primary role.

```
DC-N1kv-VSM# system redundancy role primary
```

Step 14: Save the running configuration to the startup configuration.

```
copy running-config startup-config
```

Step 15: In your vSphere Client, navigate to **Home > Inventory > Networking**, and then verify that your Cisco Nexus 1000V switch is created.



What is a folder?

A folder is a container used to group objects and organize them into hierarchies. Folders provide a natural structure upon which to apply permissions.

The folder structure you see in the inventory varies depending on the inventory view.

Procedure 3 Install and setup the secondary VSM

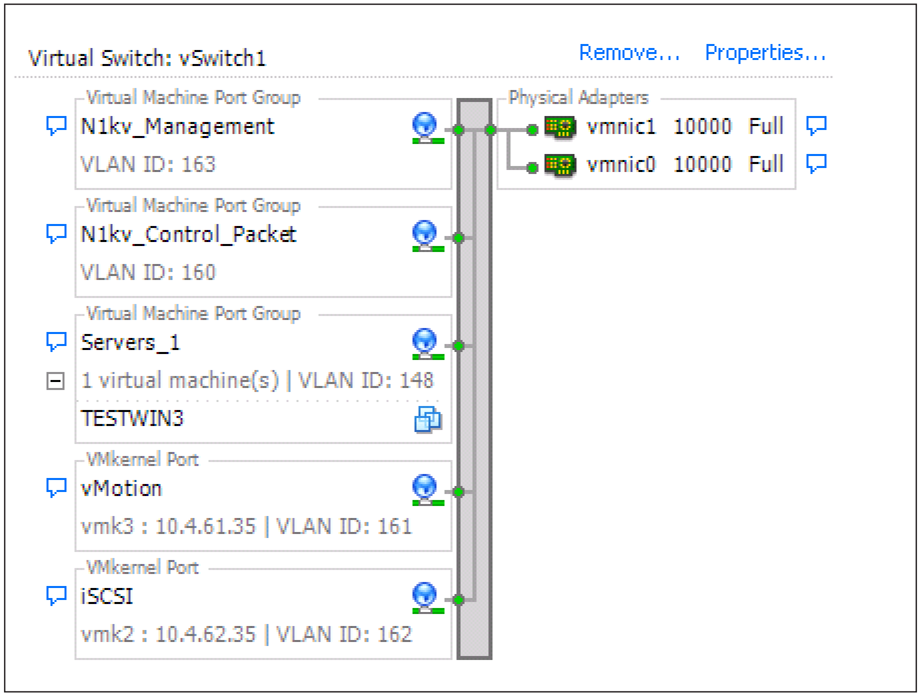
Step 1: Select the host on which you plan to run the secondary VSM VM.

Tech Tip

Do not install the secondary VSM on the same host with the primary VSM. By installing the VSMs on separate hosts, you help ensure high availability, even if one of the VMware ESXi hosts fails.

Step 2: Navigate to **Configuration > Networking > Virtual Switch**, and then ensure that the control and management port groups are configured with correct VLANs, as shown in .

Step 3: For consistency, give the same port-group names you gave for the primary VSM's control, management and packet interfaces.

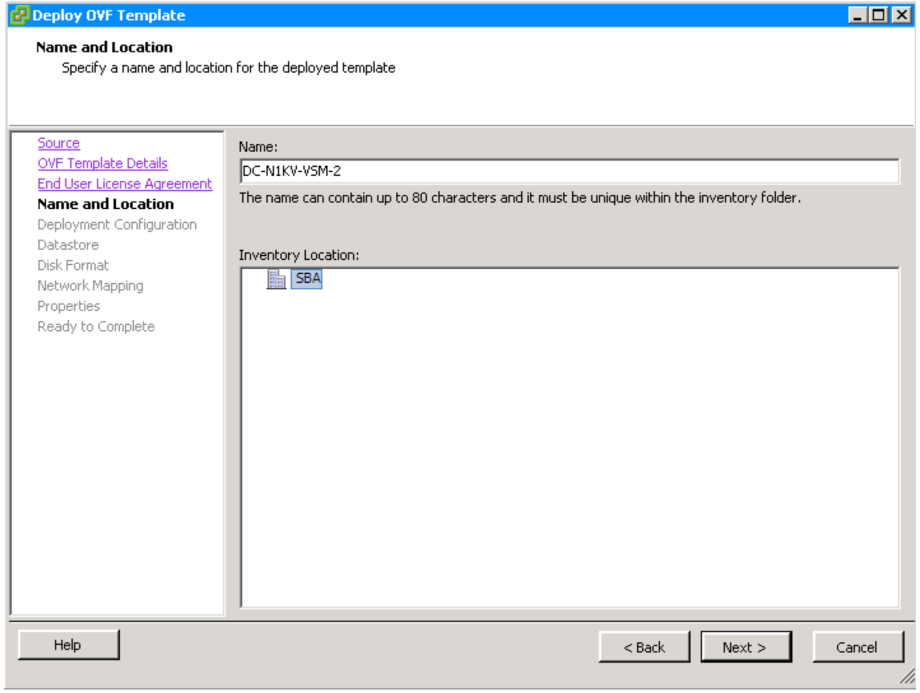


Step 4: In the vSphere Client, from the **File** menu, choose **Deploy OVF Template**, browse to the location where you have downloaded the Cisco Nexus 1000V installation files, choose the OVA file, and then click **Next**.

Step 5: On the OVF Template Details page, you are presented with product information, size of the file, and the size of VM disk. Verify that you have selected the same version and product as the primary VSM, and then click **Next**.

Step 6: Accept the Cisco Nexus 1000V License Agreement, and then click **Next**.

Step 7: On the Name and Location screen, give a unique name to your secondary VSM, choose the inventory location, and then click **Next**.



Deploy OVF Template

Name and Location

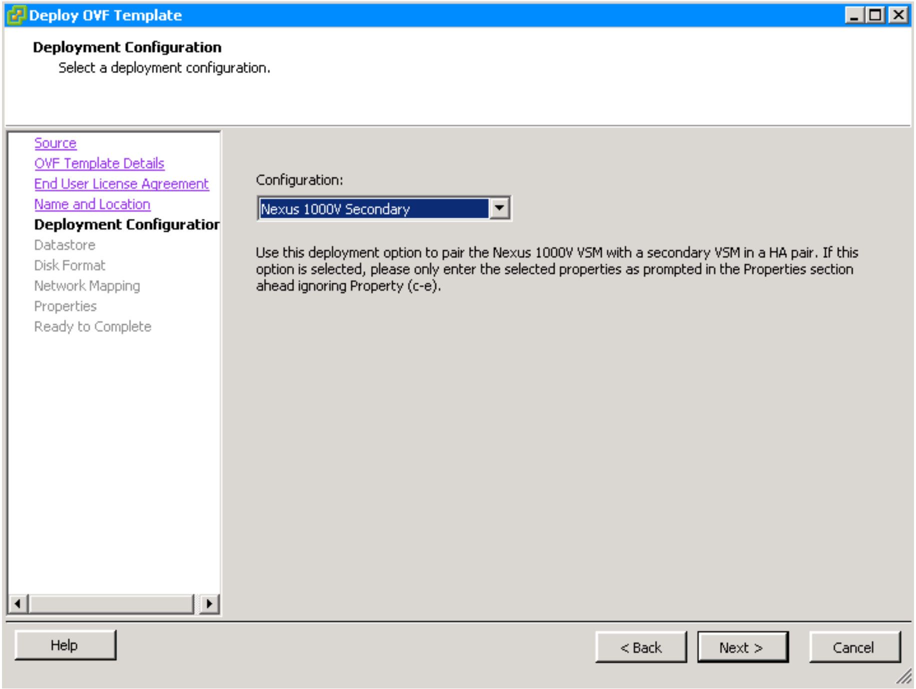
Specify a name and location for the deployed template

Name: DC-N1KV-VSM-2

The name can contain up to 80 characters and it must be unique within the inventory folder.

Inventory Location: SBA

Step 8: On the Deployment Configuration screen, in the **Configuration** list, choose **Nexus 1000V Secondary**, and then click **Next**.



Deploy OVF Template

Deployment Configuration

Select a deployment configuration.

Configuration: Nexus 1000V Secondary

Use this deployment option to pair the Nexus 1000V VSM with a secondary VSM in a HA pair. If this option is selected, please only enter the selected properties as prompted in the Properties section ahead ignoring Property (c-e).

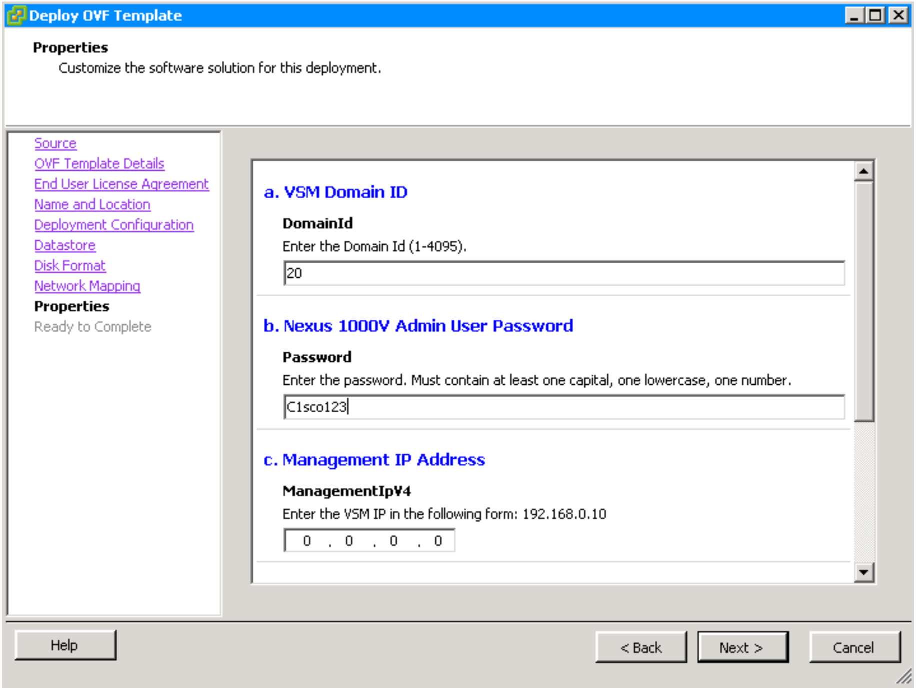
Notice that you are told to ignore section (c-e) in the Properties section

Step 9: On the Datastore screen, choose the datastore you want the VSM to use, and then click **Next**.

Step 10: On the Disk Format screen, select **Thick provisioned format**, and then click **Next**.

Step 11: On the Network Mapping screen, in the **Destination Network** list, map the Control port-group for the Control Source network and the Packet Source network, and the Management port-group for the Management Source network, and then click **Next**.

Step 12: On the Properties screen, enter the same VSM domain ID and Cisco Nexus 1000V admin user password that you used for the primary VSM (in Step 14 in the "The Cisco Nexus 1000V VSM is a virtual machine that, during installation, creates three virtual network interface cards (vNICs):" procedure earlier in this process), skip sections C through E, and then click **Next**.



Properties

Customize the software solution for this deployment.

a. VSM Domain ID

DomainId

Enter the Domain Id (1-4095).

20

b. Nexus 1000V Admin User Password

Password

Enter the password. Must contain at least one capital, one lowercase, one number.

C1sco123

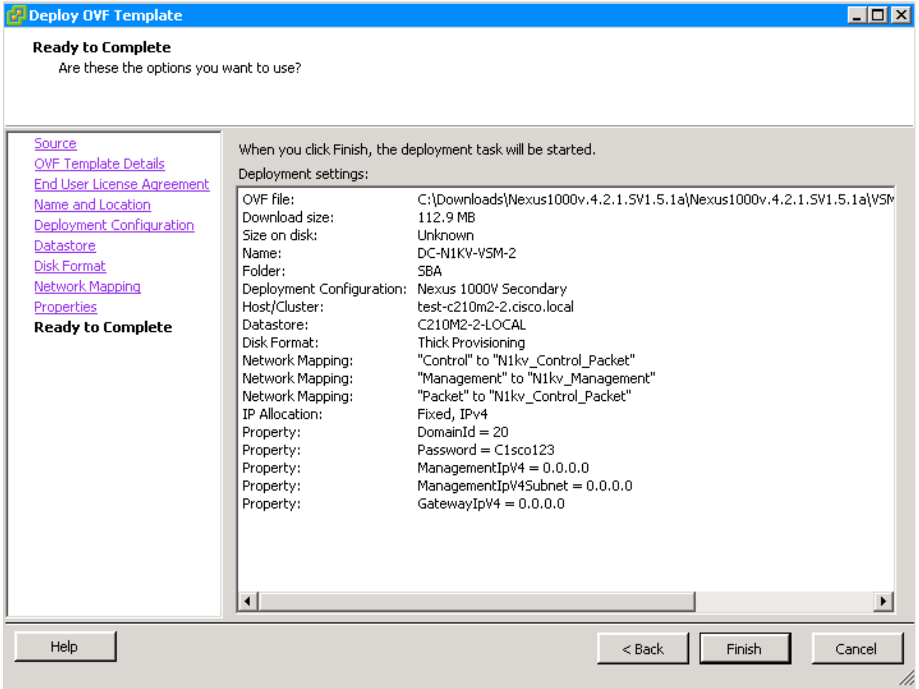
c. Management IP Address

ManagementIpV4

Enter the VSM IP in the following form: 192.168.0.10

0 . 0 . 0 . 0

Step 13: Review your settings, and then click **Finish**.



Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

Deployment settings:

```
OVF file:                  C:\Downloads\Nexus1000v.4.2.1.SV1.5.1a\Nexus1000v.4.2.1.SV1.5.1a\VSM
Download size:             112.9 MB
Size on disk:              Unknown
Name:                      DC-N1KV-VSM-2
Folder:                    SBA
Deployment Configuration:  Nexus 1000V Secondary
Host/Cluster:              test-c210m2-2.cisco.local
Datastore:                 C210M2-2-LOCAL
Disk Format:               Thick Provisioning
Network Mapping:           "Control" to "N1kv_Control_Packet"
Network Mapping:           "Management" to "N1kv_Management"
Network Mapping:           "Packet" to "N1kv_Control_Packet"
IP Allocation:             Fixed, IPv4
Property:                  DomainId = 20
Property:                  Password = C1sco123
Property:                  ManagementIpV4 = 0.0.0.0
Property:                  ManagementIpV4Subnet = 0.0.0.0
Property:                  GatewayIpV4 = 0.0.0.0
```

Step 14: Right click the VM for the secondary VSM, and then select **Power > Power ON**.

Step 15: Right-click the VSM VM in the vSphere Client window, choose **Open Console**, and then wait for the secondary VSM to finish the boot process and display the login prompt.

Step 16: To verify that the secondary VSM has joined the high-availability (HA) cluster along with the primary VSM, open a SSH client, and then log on to the Management IP address of the primary VSM set in Step 14 of the "Install the first VSM" procedure (10.4.63.130).

Step 17: Verify that the system is in HA mode, and verify that Sup-1 and Sup-2 have been detected and are in Active or Standby state.

```
DC-N1kv-VSM# show system redundancy status
Redundancy role
---------------
      administrative:   primary
         operational:   primary

Redundancy mode
---------------
      administrative:   HA
         operational:   HA

This supervisor (sup-1)
-----------------------
    Redundancy state:   Active
    Supervisor state:   Active
      Internal state:   Active with HA standby

Other supervisor (sup-2)
------------------------
    Redundancy state:   Standby
    Supervisor state:   HA standby
      Internal state:   HA standby
DC-N1kv-VSM# 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(5.1a)     0.0
2    4.2(1)SV1(5.1a)     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    10.4.63.130      NA                           NA
2    10.4.63.130      NA                           NA
```

Process

Configuring Virtualized Hosts to use the Cisco Nexus 1000V switch

1. Configure port profiles
2. Prepare Cisco UCS B-Series server for VEM
3. Install VEM using VMware Update Manager

In this process, you configure port profiles and deploy Virtual Ethernet Modules (VEMs) by configuring the virtual machines to use the Cisco Nexus 1000V switch.

You use port profiles to configure interfaces, and you can apply similar configurations to multiple interfaces by associating port profiles to the interfaces. In VMware vCenter Server, port profiles are represented as port groups. Port profiles are created on the VSM and are propagated to the VMware vCenter Server as VMware port groups. After propagation, port profiles appear within the VMware vSphere Client. These include uplink port profiles for the physical uplinks and port profiles for virtual networks used by virtual machines and VMkernel ports.

The VEM is installed on each VMware ESX host as a kernel component; it is a lightweight software component that effectively replaces the virtual switch in the VMware environment. In the Cisco Nexus 1000V switch, traffic is switched between virtual machines locally at each VEM. Each VEM also interconnects the local virtual machine with the rest of the network through the upstream switch.

When a new VEM is installed, it is assigned the lowest available module number from 3 to 66. The VSM tracks the VEM by using the Unique User ID (UUID) of the VMware ESX server, thus ensuring that if the VMware ESX host reboots or loses connectivity for any reason, the VEM will retain its module number when the host comes back online. The VEM will load the system port profiles and pass traffic even if the VSM is not up. If there is a connectivity problem between VEM and VSM, the VEM will continue to switch packets in its last known good state. After communication is restored between VSM and VEM, the VEM is reprogrammed with the last-known good configuration from the VSM.

Procedure 1 Configure port profiles

You can apply a port profile on a virtual interface by using the **vethernet** keyword for the port-profile type or on a physical interface by using the **Ethernet** keyword for the port-profile type.

A system VLAN is used to configure and initialize the physical or vethernet ports before the VSM has established communications with the VEM. Interfaces that use the system port profile and that are members of one of the defined system VLANs are automatically enabled and can begin forwarding traffic, even if the VEM does not have communication with the VSM. Critical host functions can be enabled even if the VMware ESXi host starts and cannot communicate with the VSM.

Step 1: Launch an SSH client, and then log in to your VSM CLI by using the IP address, default username (admin), and password you set when you installed the VSM in Step 14 of the “The Cisco Nexus 1000V VSM is a virtual machine that, during installation, creates three virtual network interface cards (vNICs):” procedure (10.4.63.130).

Step 2: Create the VLANs required for your setup.

Table 4 - VLANs for Cisco Nexus 1000V

VLANs	Description
148-155	Virtual Machine Network Data
160	Cisco Nexus 1000V Control
161	vMotion
162	iSCSI
163	Data Center Management Traffic

```
DC-N1kv-VSM# configure terminal
DC-N1kv-VSM(config)# vlan 148
DC-N1kv-VSM(config-vlan)# name Servers_1
DC-N1kv-VSM(config-vlan)# vlan 149-155
DC-N1kv-VSM(config-vlan)# vlan 160
DC-N1kv-VSM(config-vlan)# name 1kv-Control
DC-N1kv-VSM(config-vlan)# vlan 161
DC-N1kv-VSM(config-vlan)# name vMotion
DC-N1kv-VSM(config-vlan)# vlan 162
DC-N1kv-VSM(config-vlan)# name iSCSI
DC-N1kv-VSM(config-vlan)# vlan 163
DC-N1kv-VSM(config-vlan)# name DC-Management
```

The control and management VLANs are defined as system VLANs, as are VMware VMkernel iSCSI VLANs connecting to storage and VLANs used with vMotion traffic. Port profiles that contain system VLANs are defined as *system port profiles*. In the deployment in this guide, the Cisco UCS C-Series server is physically connected to two different switches in a fabric extender (FEX) straight-through mode. In this setup, port-channel was not configured in the upstream switches. Therefore the deployment uses MAC-pinning, which enables Cisco Nexus 1000V to span across multiple switches and provides a port-channel–like setup, but does not require port-channel configurations to be made in the upstream switches. For a Cisco UCS B-Series server in the Cisco SBA design, the fabric interfaces are set up in end-host mode; therefore, MAC-pinning is used for UCS B-Series servers as well.

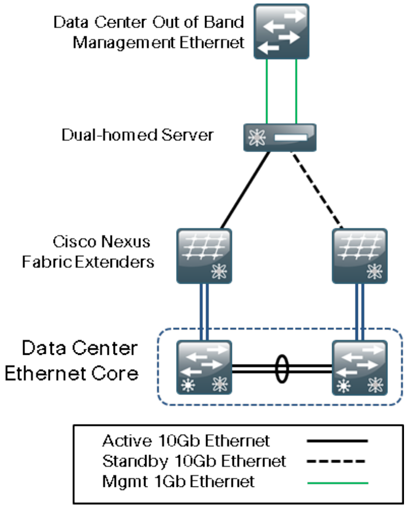
Step 3: Create an uplink port profile named System-Uplink.

```
port-profile type ethernet System-Uplink
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 148-155,160-163
  channel-group auto mode on mac-pinning
  no shutdown
  system vlan 160-163
  state enabled
```

The **channel-group auto mode on mac-pinning** command statically binds the virtual machine's vNICs to a given uplink port. If a failover occurs, the Cisco Nexus 1000V switch sends a gratuitous Address Resolution Protocol (ARP) packet to alert the upstream switch that the MAC address of the VEM that was learned on the previous link will now be learned on a different link, enabling failover in less than a second.

Step 4: If you have a Cisco UCS C-Series server that has separate physical interface connections to both an upstream management switch and physical interfaces for the data path, as shown in Figure 15, then you need to create a port profile for the VMware VMkernel management interface and a second upstream port profile for data traffic. An example of this scenario would be an ESXi management VMkernel interface connected to the management switch, and the rest of the data traffic is sent out of an interface connected to the Cisco Nexus 5500 Series switch.

Figure 15 - Cisco UCS C-Series server with separate management interfaces



The management console is controlled by the VMware vSwitch by default as part of the initial installation of the VMware ESXi. It is the management interface of the VMware vSphere Client, from which VMware vCenter Server configures and manages the server.

Create a port profile to carry the management console traffic.

```
port-profile type ethernet ESXi-Mgmnt-Uplink
  vmware port-group
  switchport mode access
  switchport access vlan 163
  channel-group auto mode on mac-pinning
  no shutdown
  system vlan 163
  description C-Series {Uplink for ESXi Management}
  state enabled
```

If you are using an installation where multiple Ethernet port profiles are active on the same VEM, it is recommended that they do not carry the same VLANs. The allowed VLAN list should be mutually exclusive.

Create a port profile that carries data traffic.

```
port-profile type ethernet 10G_CSeries
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 148-155,160-162
  channel-group auto mode on mac-pinning
  no shutdown
  system vlan 160-162
  state enabled
```

Tech Tip

It is recommended that you assign Control/Packet, IP Storage, Service Console, and Management Networks VLAN IDs as system VLANs.

Next configure port profiles for VMkernel ports and VMs.

Step 5: Configure the port profile for the virtual machine network to which all the servers in VLAN 148 will be associated.

```
port-profile type vethernet Servers_Vl148
  vmware port-group
  switchport mode access
  switchport access vlan 148
  no shutdown
  state enabled
```

Step 6: Configure the port profile for vMotion VMkernel ports.

```
port-profile type vethernet vMotion
  vmware port-group
  switchport mode access
  switchport access vlan 161
  no shutdown
  state enabled
```

Step 7: Configure the port profile for storage (iSCSI) VMkernel ports.

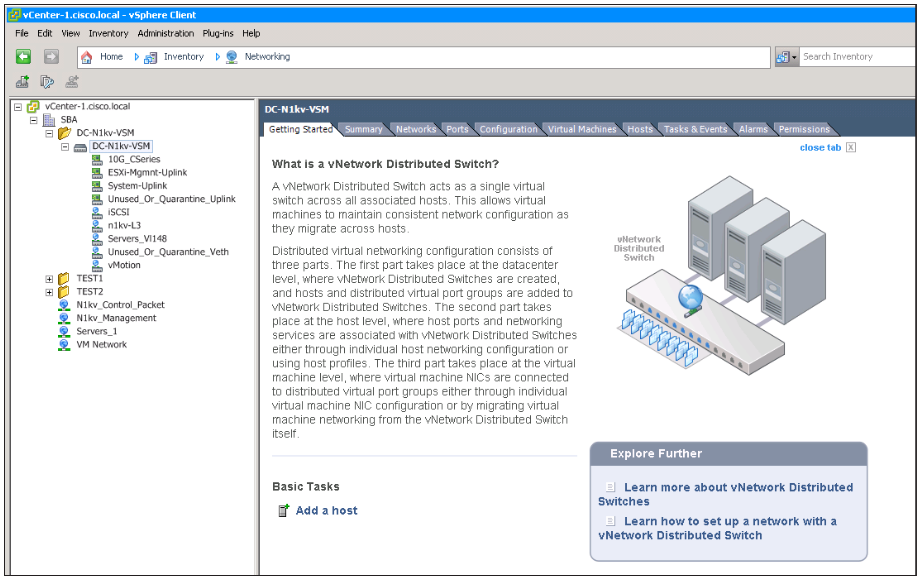
```
port-profile type vethernet iSCSI
  vmware port-group
  switchport mode access
  switchport access vlan 162
  no shutdown
  system vlan 162
  state enabled
```

Step 8: For Layer 3 communication between the VSM and VEM, a port profile of type vEthernet is needed that is capable of Layer 3 communication. Create a vethernet port profile for the VMkernel interfaces that will be used for L3 control. In this setup, since the VMkernel interface of the host is in VLAN 163, create the following port profile with **capability l3control** enabled.

```
port-profile type vethernet n1kv-L3
  capability l3control
  vmware port-group
  switchport mode access
  switchport access vlan 163
  no shutdown
  system vlan 163
  state enabled
```

Step 9: If you have other virtual machine traffic and VMkernel ports, you can configure additional port profiles in similar fashion.

Step 10: Once all the port profiles are created, launch the vSphere Client, connect to vCenter Server, navigate to **Home > Inventory > Networking**, and then verify that the port profiles have synced with vCenter.



What is a vNetwork Distributed Switch?

A vNetwork Distributed Switch acts as a single virtual switch across all associated hosts. This allows virtual machines to maintain consistent network configuration as they migrate across hosts.

Distributed virtual networking configuration consists of three parts. The first part takes place at the datacenter level, where vNetwork Distributed Switches are created, and hosts and distributed virtual port groups are added to vNetwork Distributed Switches. The second part takes place at the host level, where host ports and networking services are associated with vNetwork Distributed Switches either through individual host networking configuration or using host profiles. The third part takes place at the virtual machine level, where virtual machine NICs are connected to distributed virtual port groups either through individual virtual machine NIC configuration or by migrating virtual machine networking from the vNetwork Distributed Switch itself.

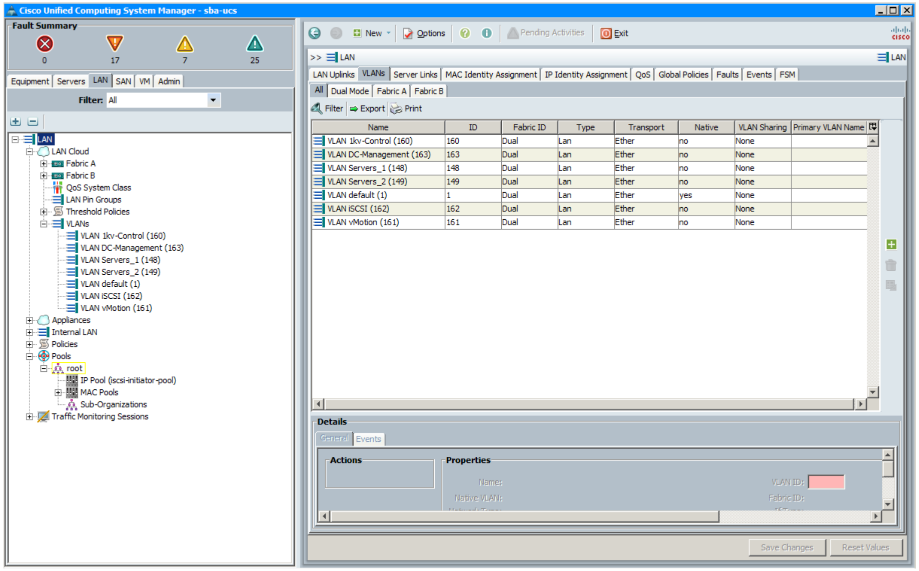
Procedure 2 Prepare Cisco UCS B-Series server for VEM

If you are installing a Cisco Nexus 1000V switch VEM on a Cisco UCS B-Series server, you must prepare the server for the VEM installation. If you are not installing a Cisco Nexus 1000V switch VEM on a Cisco UCS B-Series server you can skip this procedure.

Step 1: Launch Cisco UCS Manager.

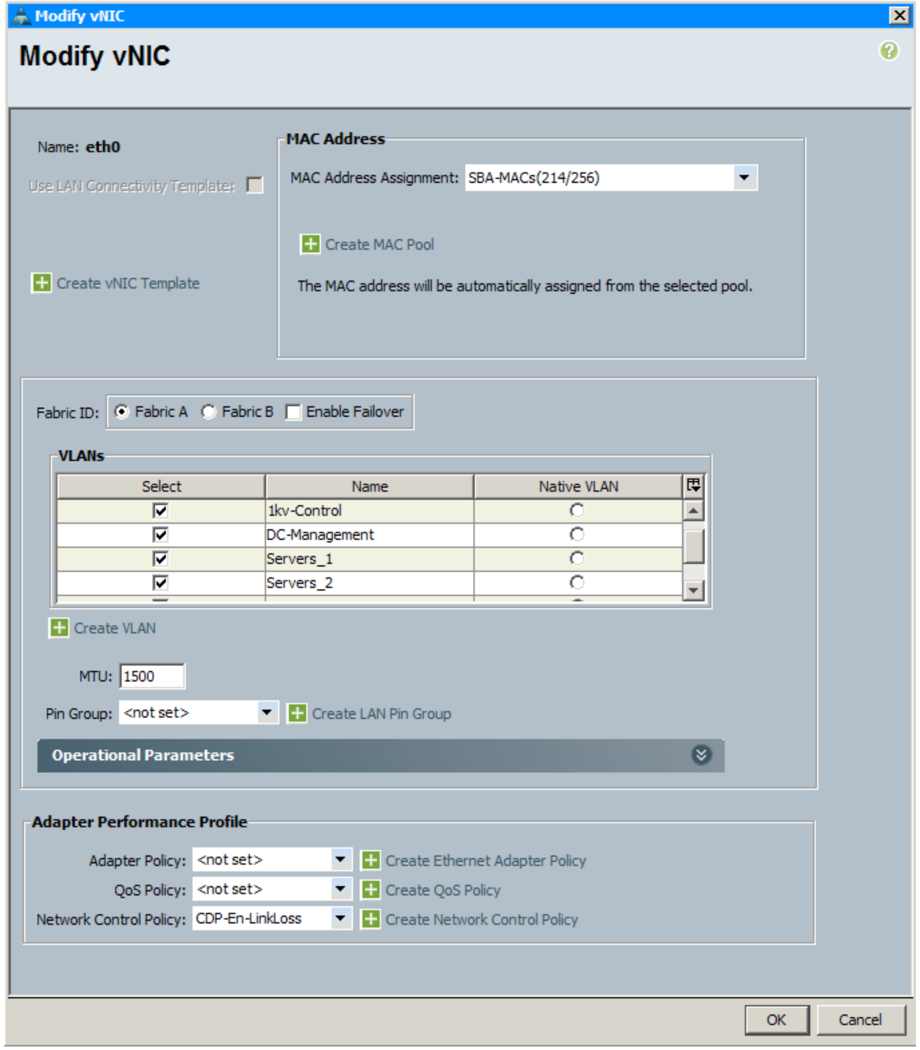
Step 2: In the navigation pane, navigate to the LAN tab, and then choose **VLANs**.

Step 3: Define the additional VLANs from Table 4 (VLANs 160 and 163) that need to be passed to the vNIC and to the Cisco Nexus 1000V switch. Ensure that the control and management VLANs used by the Nexus 1000V switch are defined and assigned to the vNICs on each of the server's service profiles, as shown in the following figure.



Name	ID	Fabric ID	Type	Transport	Native	VLAN Sharing	Primary VLAN Name
VLAN 1kv-Control (160)	160	Dual	Lan	Ether	no	None	
VLAN DC-Management (163)	163	Dual	Lan	Ether	no	None	
VLAN Servers_1 (148)	148	Dual	Lan	Ether	no	None	
VLAN Servers_2 (149)	149	Dual	Lan	Ether	no	None	
VLAN default (1)	1	Dual	Lan	Ether	yes	None	
VLAN iSCSI (162)	162	Dual	Lan	Ether	no	None	
VLAN vMotion (161)	161	Dual	Lan	Ether	no	None	

Step 4: For each vNIC that you map to the Cisco Nexus 1000V switch, click **Modify**, and then ensure that the **Enable Failover** check box is cleared.



Modify vNIC

Name: eth0

Use LAN Connectivity Template: □

MAC Address

MAC Address Assignment: SBA-MACs(214/256)

The MAC address will be automatically assigned from the selected pool.

Fabric ID: ● Fabric A ○ Fabric B □ Enable Failover

VLANs

Select	Name	Native VLAN
☑	1kv-Control	○
☑	DC-Management	○
☑	Servers_1	○
☑	Servers_2	○

MTU: 1500

Pin Group: <not set>

Adapter Performance Profile

Adapter Policy: <not set>

QoS Policy: <not set>

Network Control Policy: CDP-En-LinkLoss

Procedure 3 Install VEM using VMware Update Manager

There are several ways to install the VEM:

- Using SSH by connecting directly to the VMware ESXi host
- Using vSphere remote CLI
- Using VMware vCenter Update Manager (VUM)

When you use the VMware VUM, you do not have to manually install the Cisco Nexus 1000V VEM. VUM obtains the VEM software from the VSM through the web server hosted on the VSM. When you add a host to the Nexus 1000V switch, VUM installs the VEM software automatically.

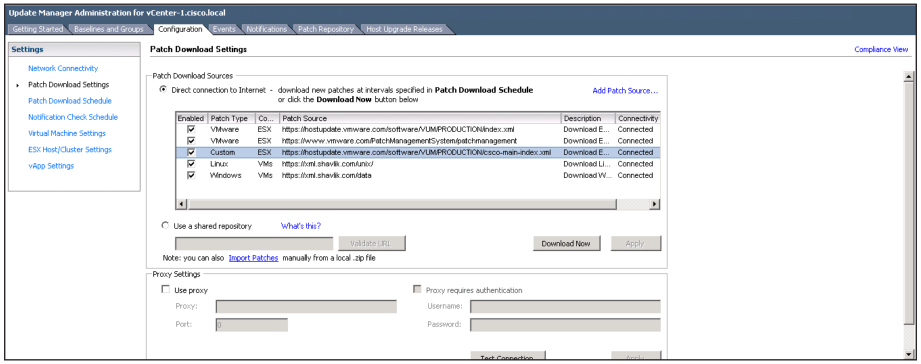
VMware vCenter Server sends opaque data containing the switch domain ID, switch name, control and packet VLAN IDs, and system port profiles to the VEM, which the VEM uses to establish communication with the VSM and download appropriate configuration data.

Each VEM has a control and packet interface. These interfaces are not manageable and configurable by the end user. The VEM uses the opaque data provided by the VMware vCenter Server to configure the control and packet interfaces with correct VLANs. The VEM then applies the correct uplink port profiles to the control and packet interfaces to establish connection with the VSM. There are two ways of communicating between the VSM and the VEM: Layer 2 mode or Layer 3 mode. Layer 3 mode is the recommended option, where the control and packet frames are encapsulated through UDP.

In the Layer 3 mode, you must associate the VMware VMkernel interface to the port profile configured with L3 control option. The L3 control configuration configures the VEM to use the VMkernel interface to send Layer 3 packets.

Step 1: In the vSphere Client, navigate to **Home**, and under Solutions and Applications, choose **Update Manager**.

Step 2: Navigate to the Configuration tab, choose **Patch Download Settings**, and then ensure that for the **Custom** Patch Type, **Enabled** is selected and the Connectivity status is Connected.



Patch Download Settings

Patch Download Sources

● Direct connection to Internet - download new patches at intervals specified in **Patch Download Schedule** or click the **Download Now** button below

Enabled	Patch Type	Co...	Patch Source	Description	Connectivity
☑	VMware	ESX	https://hostupdate.vmware.com/software/VUM/PRODUCTION/index.xml	Download E...	Connected
☑	VMware	ESX	https://www.vmware.com/PatchManagementSystem/patchmanagement	Download E...	Connected
☑	Custom	ESX	https://hostupdate.vmware.com/software/VUM/PRODUCTION/csco-main-index.xml	Download E...	Connected
☑	Linux	VMs	https://xml.shavlik.com/unix/	Download Li...	Connected
☑	Windows	VMs	https://xml.shavlik.com/data	Download W...	Connected

○ Use a shared repository

Note: you can also Import Patches manually from a local .zip file

Proxy Settings

☐ Use proxy

Proxy:

Port: 0

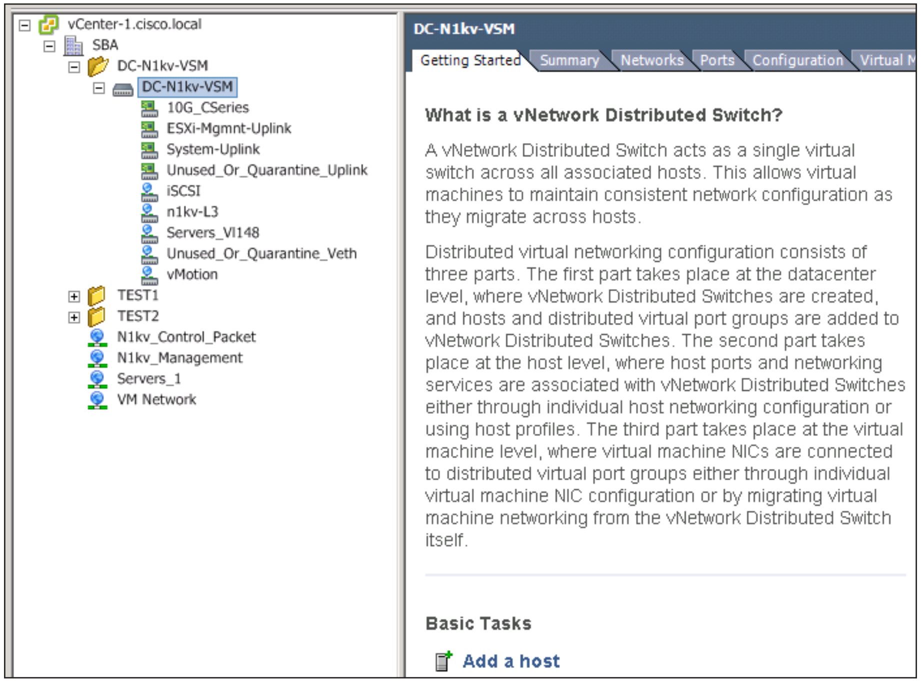
☐ Proxy requires authentication

Username:

Password:

At this point, you are ready to install a VEM.

Step 3: Navigate to **Home > Inventory > Networking**, select the Cisco Nexus 1000V switch you created, and in the work pane, on the Getting Started tab, click **Add a Host**.



What is a vNetwork Distributed Switch?

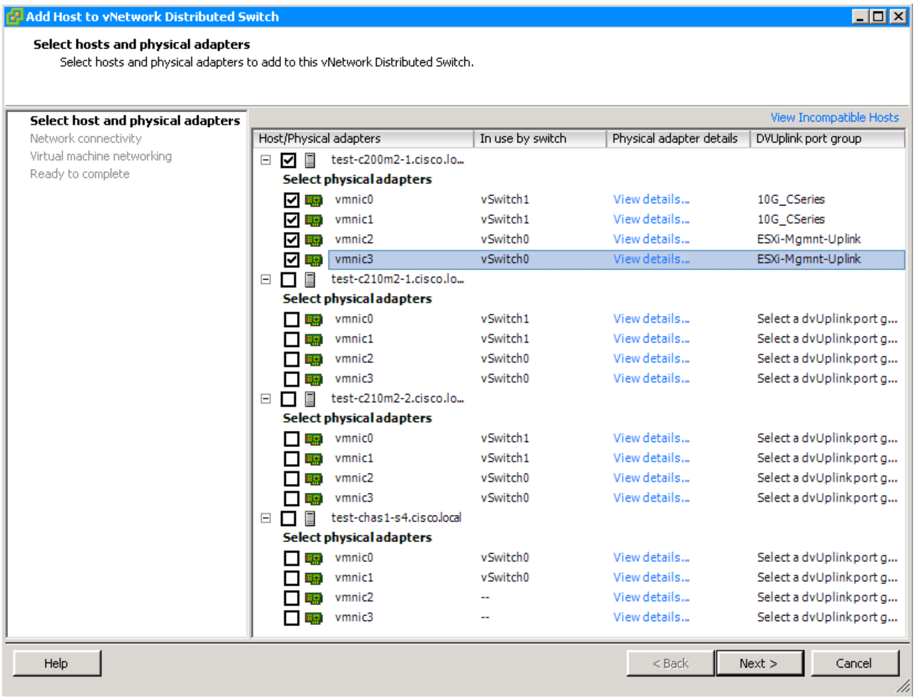
A vNetwork Distributed Switch acts as a single virtual switch across all associated hosts. This allows virtual machines to maintain consistent network configuration as they migrate across hosts.

Distributed virtual networking configuration consists of three parts. The first part takes place at the datacenter level, where vNetwork Distributed Switches are created, and hosts and distributed virtual port groups are added to vNetwork Distributed Switches. The second part takes place at the host level, where host ports and networking services are associated with vNetwork Distributed Switches either through individual host networking configuration or using host profiles. The third part takes place at the virtual machine level, where virtual machine NICs are connected to distributed virtual port groups either through individual virtual machine NIC configuration or by migrating virtual machine networking from the vNetwork Distributed Switch itself.

Basic Tasks

Add a host

Step 4: In the Add Host to vNetwork Distributed Switch screen, select the host on which you want to install VEM, select the check boxes next to the physical adapters to provide connectivity between the vDS and the host, and then under the **DVUplink port group** column, from the pull down list, choose the uplink port profile you created in Step 3 of "You can apply a port profile on a virtual interface by using the vethernet keyword for the port-profile type or on a physical interface by using the Ethernet keyword for the port-profile type.". Click **Next.**



Add Host to vNetwork Distributed Switch

Select hosts and physical adapters
Select hosts and physical adapters to add to this vNetwork Distributed Switch.

Select host and physical adapters
Network connectivity
Virtual machine networking
Ready to complete

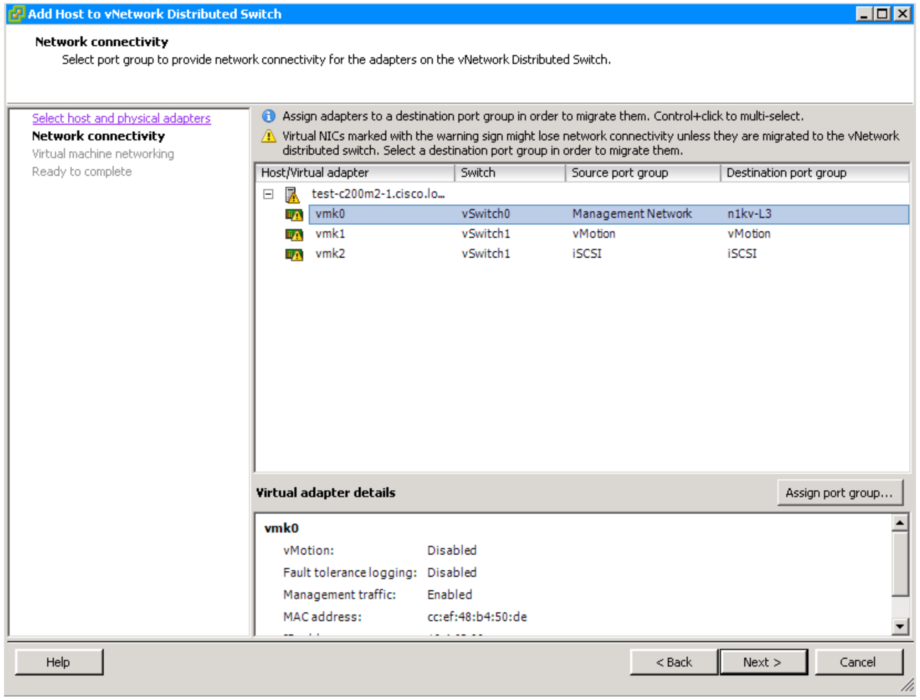
View Incompatible Hosts

Host/Physical adapters	In use by switch	Physical adapter details	DVUplink port group
☑ test-c200m2-1.cisco.lo...			
Select physical adapters			
☑ vmnic0	vSwitch1	View details...	10G_CSeries
☑ vmnic1	vSwitch1	View details...	10G_CSeries
☑ vmnic2	vSwitch0	View details...	ESXi-Mgmnt-Uplink
☑ vmnic3	vSwitch0	View details...	ESXi-Mgmnt-Uplink
□ test-c210m2-1.cisco.lo...			
Select physical adapters			
□ vmnic0	vSwitch1	View details...	Select a dvUplink port g...
□ vmnic1	vSwitch1	View details...	Select a dvUplink port g...
□ vmnic2	vSwitch0	View details...	Select a dvUplink port g...
□ vmnic3	vSwitch0	View details...	Select a dvUplink port g...
□ test-c210m2-2.cisco.lo...			
Select physical adapters			
□ vmnic0	vSwitch1	View details...	Select a dvUplink port g...
□ vmnic1	vSwitch1	View details...	Select a dvUplink port g...
□ vmnic2	vSwitch0	View details...	Select a dvUplink port g...
□ vmnic3	vSwitch0	View details...	Select a dvUplink port g...
□ test-chas1-s4.cisco.local			
Select physical adapters			
□ vmnic0	vSwitch0	View details...	Select a dvUplink port g...
□ vmnic1	vSwitch0	View details...	Select a dvUplink port g...
□ vmnic2	--	View details...	Select a dvUplink port g...
□ vmnic3	--	View details...	Select a dvUplink port g...

Step 5: On the Network connectivity screen, do the following, and then click **Next**:

- For vmk0, in the Destination port group lists, choose **n1kv-L3**.
- For vmk1, in the Destination port group lists, choose **vMotion**.
- For vmk2, in the Destination port group lists, choose **iSCSI**.

This step assigns virtual adapters to an appropriate port group for the traffic that they are carrying. Vmk0, Vmk1 and vmk2 are going to be migrated from VMware vSwitch to the Cisco Nexus 1000V vDS.



Add Host to vNetwork Distributed Switch

Network connectivity
Select port group to provide network connectivity for the adapters on the vNetwork Distributed Switch.

Select host and physical adapters
Network connectivity
Virtual machine networking
Ready to complete

Assign adapters to a destination port group in order to migrate them. Control+click to multi-select.
Virtual NICs marked with the warning sign might lose network connectivity unless they are migrated to the vNetwork distributed switch. Select a destination port group in order to migrate them.

Host/Virtual adapter	Switch	Source port group	Destination port group
test-c200m2-1.cisco.lo...			
vmk0	vSwitch0	Management Network	n1kv-L3
vmk1	vSwitch1	vMotion	vMotion
vmk2	vSwitch1	iSCSI	iSCSI

Virtual adapter details

vmk0

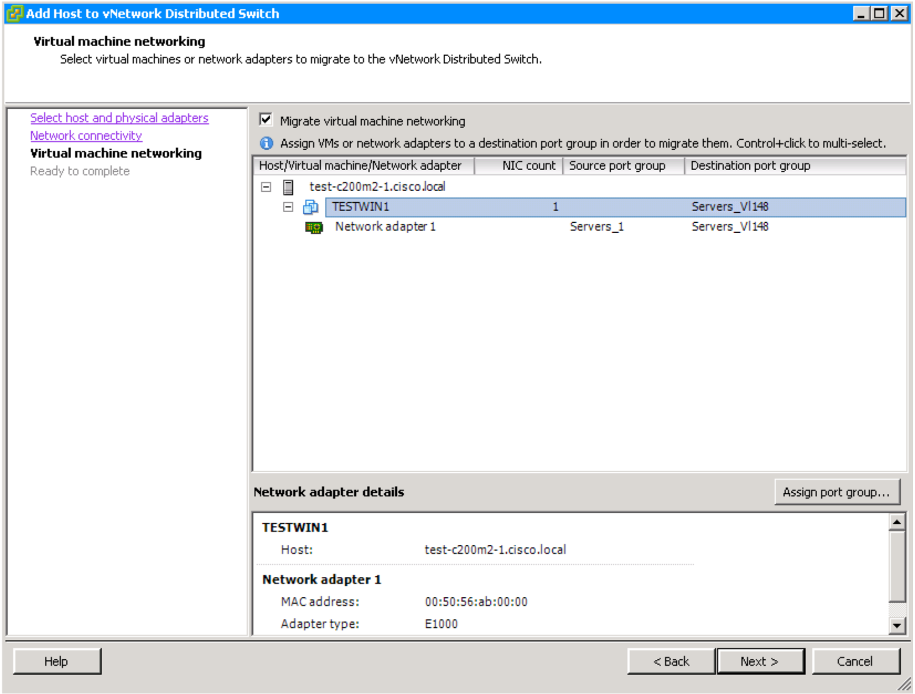
vMotion:	Disabled
Fault tolerance logging:	Disabled
Management traffic:	Enabled
MAC address:	cc:ef:48:b4:50:de

Step 6: If you have virtual machines already assigned to the host, select **Migrate virtual machine networking**, and in the **Destination port group** list for each virtual machine, choose the appropriate destination port group, and then click **Next**.

Tech Tip

If you do not currently have VMs running on this host, once you have created VMs on the host you can begin at this step to assign the Cisco Nexus 1000V virtual switch for the new VMs.

When a new virtual machine is provisioned, the server administrator selects the appropriate port profile. The Cisco Nexus 1000V Series creates a new switch port based on the policies defined by the port profile. The server administrator can reuse the port profile to provision similar virtual machines as needed.



Virtual machine networking
Select virtual machines or network adapters to migrate to the vNetwork Distributed Switch.

Select host and physical adapters
Network connectivity
Virtual machine networking
Ready to complete

☑ Migrate virtual machine networking

Assign VMs or network adapters to a destination port group in order to migrate them. Control+click to multi-select.

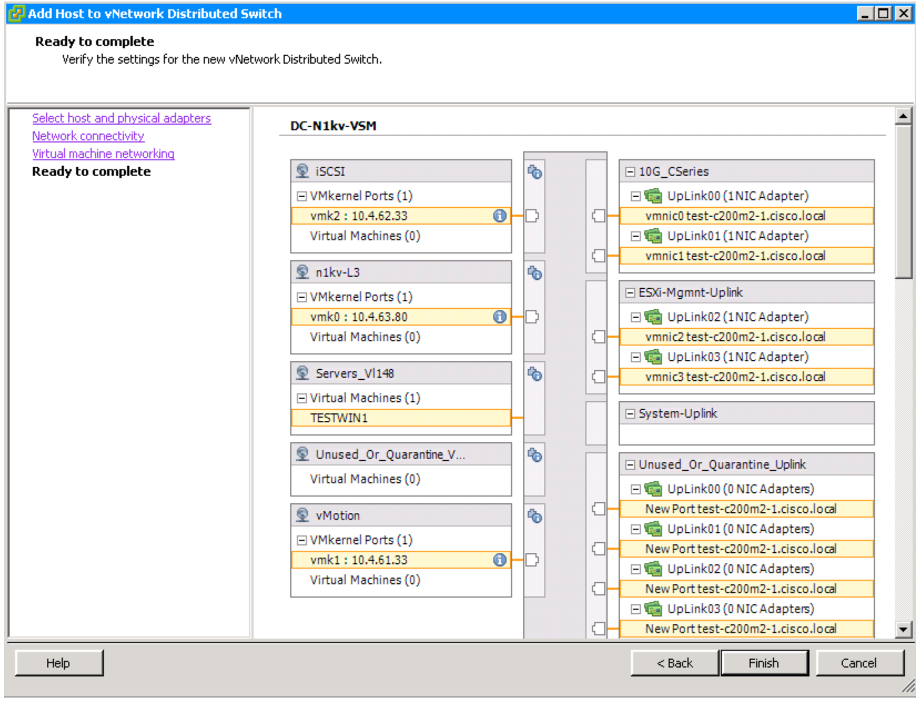
Host/Virtual machine/Network adapter	NIC count	Source port group	Destination port group
test-c200m2-1.cisco.local			
TESTWIN1	1		Servers_Vl148
Network adapter 1		Servers_1	Servers_Vl148

Network adapter details

TESTWIN1
Host: test-c200m2-1.cisco.local

Network adapter 1
MAC address: 00:50:56:ab:00:00
Adapter type: E1000

Step 7: On the Ready to complete screen, verify that the settings for the new vNetwork Distributed Switch are correct, and then click **Finish**. Existing interfaces from other hosts are included in the display, because it represents a switch that is distributed across multiple hosts.



Ready to complete
Verify the settings for the new vNetwork Distributed Switch.

Select host and physical adapters
Network connectivity
Virtual machine networking
Ready to complete

DC-N1kv-VSM

iSCSI
VMkernel Ports (1)
vmk2 : 10.4.62.33
Virtual Machines (0)

n1kv-L3
VMkernel Ports (1)
vmk0 : 10.4.63.80
Virtual Machines (0)

Servers_Vl148
Virtual Machines (1)
TESTWIN1

Unused_Or_Quarantine_V...
Virtual Machines (0)

vMotion
VMkernel Ports (1)
vmk1 : 10.4.61.33
Virtual Machines (0)

10G_CSeries
UpLink00 (1 NIC Adapter)
vmnic0 test-c200m2-1.cisco.local
UpLink01 (1 NIC Adapter)
vmnic1 test-c200m2-1.cisco.local

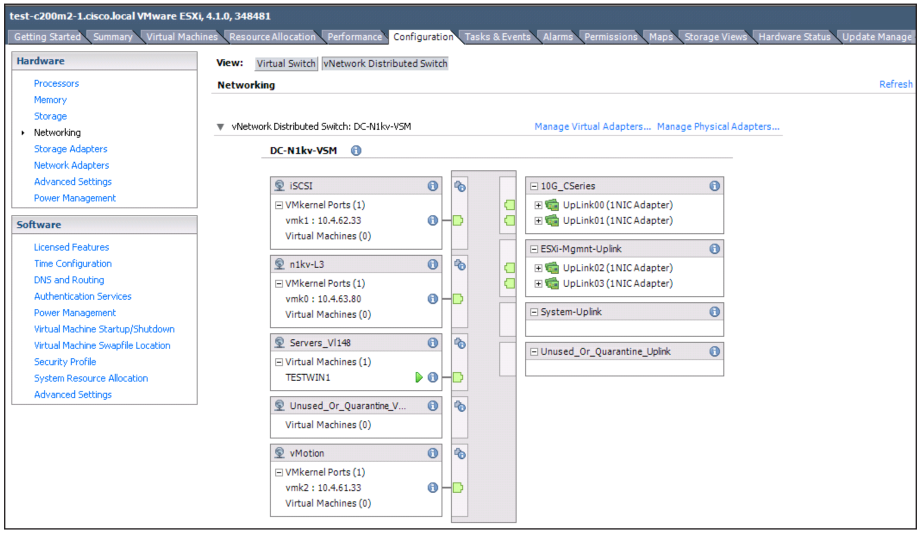
ESXi-Mgmnt-Uplink
UpLink02 (1 NIC Adapter)
vmnic2 test-c200m2-1.cisco.local
UpLink03 (1 NIC Adapter)
vmnic3 test-c200m2-1.cisco.local

System-Uplink

Unused_Or_Quarantine_Uplink
UpLink00 (0 NIC Adapters)
New Port test-c200m2-1.cisco.local
UpLink01 (0 NIC Adapters)
New Port test-c200m2-1.cisco.local
UpLink02 (0 NIC Adapters)
New Port test-c200m2-1.cisco.local
UpLink03 (0 NIC Adapters)
New Port test-c200m2-1.cisco.local

Step 8: In the vSphere Client, in the Recent Tasks window, monitor the remediation of the host.

Step 9: When the host has completed the Update Network Configuration task, navigate to **Inventory > Hosts and Clusters**, highlight the host name, navigate to the Configuration tab, choose **Networking**, and then click **vNetwork Distributed Switch**. View the results of the configuration.



Notes

Summary

Applications are the heartbeat of your business and provide rich business functionality; VMware virtualization is the heartbeat of an infrastructure that drives tangible benefits for both the business and the IT organization. With VMware as the platform underlying your application landscape, infrastructure and application teams are empowered to do their work more efficiently and with fewer administrative headaches throughout the hardware and software lifecycle, from development through production and maintenance.

More and more customers are taking advantage of the benefits of VMware infrastructure to build a dynamic, responsive infrastructure to support their applications. VMware virtualization enables efficient data-center resource pooling and maximized utilization of system resources. VMware virtualization technologies help customers achieve faster and more cost-efficient upgrades, while reducing risk to the business. By expediting and simplifying the application development and testing processes, customers experience faster time to production while maintaining high quality throughout. Implementing business continuity solutions for applications on VMware infrastructure delivers enhanced high availability while minimizing the need for duplicate hardware. Rapid provisioning and efficient change management in production environments increase IT flexibility, allowing timely response to sudden and changing business needs.

You can enhance the manageability of the VMware networking environment by installing Cisco Nexus 1000V. The configuration procedures that have been provided in this guide allow you to establish a basic, functional Nexus 1000V setup for your network. The virtual switch configuration and port profile allow for vastly simplified deployment of new virtual machines with consistent port configurations. For more details on Cisco Nexus 1000V configuration, please see the Cisco Nexus 1000V configuration guides on www.cisco.com.

Notes

Appendix A: Product List

Data Center Virtualization

Functional Area	Product Description	Part Numbers	Software
Virtual Switch	Nexus 1000V CPU License Qty-1	N1K-VLCPU-01=	4.2(1)SV1(5.1a)
	Nexus 1000V VSM on Physical Media	N1K-VSMK9-404S12=	
VMWare	ESXi	ESXi	4.1U1

Data Center Core

Functional Area	Product Description	Part Numbers	Software
Core Switch	Cisco Nexus 5596 up to 96-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5596UP-FA	NX-OS 5.1(3)N1(1a) Layer 3 License
	Cisco Nexus 5596 Layer 3 Switching Module	N55-M160L30V2	
	Cisco Nexus 5548 up to 48-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5548UP-FA	
	Cisco Nexus 5548 Layer 3 Switching Module	N55-D160L3	
Ethernet Extension	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T Fabric Extender	N2K-C2248TP-1GE	—
	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T (enhanced) Fabric Extender	N2K-C2248TP-E	
	Cisco Nexus 2000 Series 32 1/10 GbE SFP+, FCoE capable Fabric Extender	N2K-C2232PP-10GE	

Storage Network Extension

Functional Area	Product Description	Part Numbers	Software
Fibre-channel Switch	Cisco MDS 9148 Multilayer Fibre Channel Switch	DS-C9148D-8G16P-K9	NX-OS 5.0(7)
	Cisco MDS 9124 Multilayer Fibre Channel Switch	DS-C9124-K9	

Computing Resources

Functional Area	Product Description	Part Numbers	Software
UCS Fabric Interconnect	Cisco UCS up to 48-port Fabric Interconnect	UCS-FI-6248UP	2.0(2q) Cisco UCS Release
	Cisco UCS 20-port Fabric Interconnect	N10-S6100	
	Cisco UCS 6100 6-port Fibre Channel Expansion Module	N10-E0060	
UCS B-Series Blade Servers	Cisco UCS Blade Server Chassis	N20-C6508	2.0(2q) Cisco UCS Release
	Cisco UCS 8-port 10GbE Fabric Extender	UCS-IOM2208XP	
	Cisco UCS 4-port 10GbE Fabric Extender	UCS-IOM2204XP	
	Cisco UCS 4-port 10GbE First Generation Fabric Extender	N20-I6584	
	Cisco UCS B200 M2 Blade Server	N20-B6625-1	
	Cisco UCS B250 M2 Blade Server	N20-B6625-2	
	Cisco UCS M81KR Virtual Interface Card	N20-AC0002	
UCS C-Series Rack-mount Servers	Cisco UCS C200 M2 Rack Mount Server	R200-1120402W	1.4.1e Cisco UCS CIMC Release
	Cisco UCS C210 M2 Rack Mount Server	R210-2121605W	
	Cisco UCS C250 M2 Rack Mount Server	R250-2480805W	

Appendix B: Configuration Files

The following is the configuration from the deployed Cisco Nexus 1000V Virtual Supervisor Module.

```
DC-N1kv-VSM# show run
!Command: show running-config
version 4.2(1)SV1(5.1a)
no feature telnet
username admin password 5 *****  role network-admin
banner motd #Nexus 1000v Switch#
ssh key rsa 2048
ip domain-lookup
hostname DC-N1kv-VSM
vem 3
  host vmware id e71de724-e517-11e0-bd1d-ccef48b450da
snmp-server user admin network-admin auth md5 ***** priv *****
localizedkey
ntp server 10.4.48.17
!
vrf context management
  ip route 0.0.0.0/0 10.4.63.1
vlan 1,148-155,160-163
vlan 1
vlan 148
  name Servers_1
vlan 149-155
vlan 160
  name 1kv-Control
vlan 161
  name vMotion
vlan 162
  name iSCSI
vlan 163
  name DC-Management
!
port-channel load-balance ethernet source-mac
port-profile default max-ports 32
port-profile type ethernet Unused_Or_Quarantine_Uplink
  vmware port-group
  shutdown
  description Port-group created for Nexus1000V internal usage.
Do not use.
  state enabled
port-profile type vethernet Unused_Or_Quarantine_Veth
  vmware port-group
  shutdown
  description Port-group created for Nexus1000V internal usage.
Do not use.
  state enabled
port-profile type ethernet System-Uplink
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 148-155,160-163
  channel-group auto mode on mac-pinning
  no shutdown
  system vlan 160-163
  state enabled
port-profile type ethernet ESXi-Mgmnt-Uplink
  vmware port-group
  switchport mode access
  switchport access vlan 163
  channel-group auto mode on mac-pinning
  no shutdown
  system vlan 163
  description C-Series {Uplink for ESXi Management}
  state enabled
port-profile type ethernet 10G_CSeries
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 148-155,160-162
  channel-group auto mode on mac-pinning
  no shutdown
  system vlan 160-162
  state enabled
port-profile type vethernet Servers_Vl148
  vmware port-group
  switchport mode access
  switchport access vlan 148
  no shutdown
  state enabled
port-profile type vethernet iSCSI
  vmware port-group
  switchport mode access
  switchport access vlan 162
  no shutdown
  system vlan 162
  state enabled
port-profile type vethernet n1kv-L3
  capability l3control
  vmware port-group
  switchport mode access
  switchport access vlan 163
  no shutdown
  system vlan 163
  state enabled
port-profile type vethernet vMotion
  vmware port-group
  switchport mode access
  switchport access vlan 161
  no shutdown
  state enabled

vdc DC-N1kv-VSM id 1
  limit-resource vlan minimum 16 maximum 2049
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource vrf minimum 16 maximum 8192
```

```
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 1 maximum 1
  limit-resource u6route-mem minimum 1 maximum 1
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8
interface port-channel1
  inherit port-profile 10G_CSeries
  vem 3
interface port-channel2
  inherit port-profile ESXi-Mgmnt-Uplink
  vem 3
interface mgmt0
  ip address 10.4.63.130/24
interface Vethernet1
  inherit port-profile n1kv-L3
  description VMware VMkernel, vmk0
  vmware dvport 101 dvswitch uuid “f8 cc 2b 50 64 f3 84 e3-57 57
ed 05 24 66 d3 20”
  vmware vm mac CCEF.48B4.50DE
interface Vethernet2
  inherit port-profile iSCSI
  description VMware VMkernel, vmk1
  vmware dvport 65 dvswitch uuid “f8 cc 2b 50 64 f3 84 e3-57 57
ed 05 24 66 d3 20”
  vmware vm mac 0050.567D.4E79
interface Vethernet3
  inherit port-profile vMotion
  description VMware VMkernel, vmk2
  vmware dvport 129 dvswitch uuid “f8 cc 2b 50 64 f3 84 e3-57 57
ed 05 24 66 d3 20”
  vmware vm mac 0050.5672.53E5
interface Vethernet4
  inherit port-profile Servers_Vl148
  description TESTWIN1, Network Adapter 1
  vmware dvport 33 dvswitch uuid “f8 cc 2b 50 64 f3 84 e3-57 57
ed 05 24 66 d3 20”
  vmware vm mac 0050.56AB.0000
```

```
interface Ethernet3/1
  inherit port-profile 10G_CSeries
interface Ethernet3/2
  inherit port-profile 10G_CSeries
interface Ethernet3/3
  inherit port-profile ESXi-Mgmnt-Uplink
interface Ethernet3/4
  inherit port-profile ESXi-Mgmnt-Uplink
interface control0
clock timezone PST -8 0
clock summer-time PDT 2 Sunday march 02:00 1 Sunday nov 02:00 60
line console
boot kickstart bootflash:/nexus-1000v-kickstart-
mz.4.2.1.SV1.5.1a.bin sup-1
boot system bootflash:/nexus-1000v-mz.4.2.1.SV1.5.1a.bin sup-1
boot kickstart bootflash:/nexus-1000v-kickstart-
mz.4.2.1.SV1.5.1a.bin sup-2
boot system bootflash:/nexus-1000v-mz.4.2.1.SV1.5.1a.bin sup-2
svs-domain
  domain id 20
  control vlan 1
  packet vlan 1
  svs mode L3 interface mgmt0
svs connection vcenter
  protocol vmware-vim
  remote ip address 10.4.48.211 port 80
  vmware dvs uuid "f8 cc 2b 50 64 f3 84 e3-57 57 ed 05 24 66 d3 
20" datacenter-name SBA
  max-ports 8192
  connect
vsn type vsg global
  tcp state-checks
vnm-policy-agent
  registration-ip 0.0.0.0
  shared-secret **********
  log-level
```

Notes

Appendix C: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- We improved process and step flow in the "VMware vSphere Installation and Setup" section.
- We changed the Cisco Nexus 1000V configuration to use the Layer 3 mode of operation which is now the recommended mode. We updated the "Cisco Nexus 1000V Series Switch Installation and Deployment" to reflect new installation and configuration procedures for Layer 3 mode operation.
- We updated the Cisco Nexus 1000V software to a later image.

Notes

Feedback

Click here to provide feedback to Cisco SBA.

SMART BUSINESS ARCHITECTURE

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLiERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

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.