Newer Design Guide Available

Cisco Smart Business Architecture has become part of the Cisco Validated Designs program.

For up-to-date guidance on the designs described in this guide, see http://cvddocs.com/fw/Aug13-555

For information about the Cisco Validated Design program, go to http://www.cisco.com/go/cvd

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

SMART BUSINESS ARCHITECTURE

February 2013 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 February 2013 is the "February 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

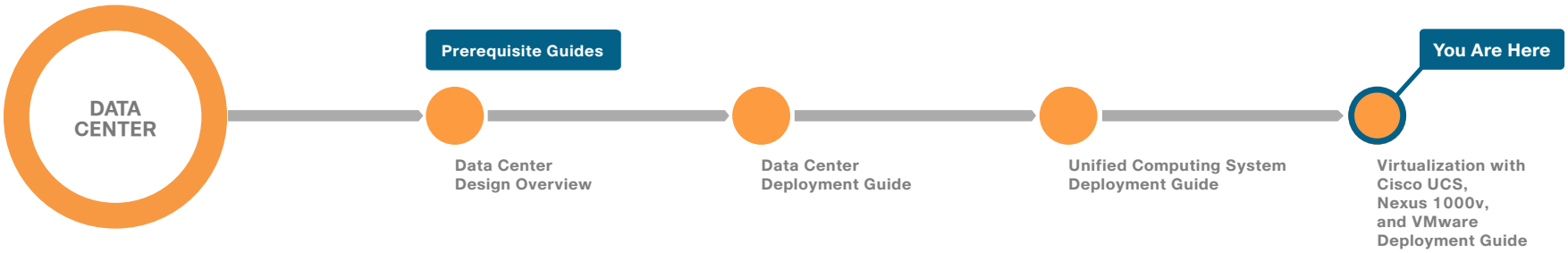
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- **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



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.

The Deployment Details chapter of this guide is divided into the following modules:

- Preparing the Environment for VMware—this module is useful for deployments that will use shared storage over a Fibre Channel SAN. This module includes an overview of the requirements of the storage array logical unit numbers (LUNs), and the Fibre Channel network zoning.
- VMware vSphere Installation and Setup—explains how to deploy VMware using version 5.0U1 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.
- Cisco Nexus 1000V Series Switch Installation and Deployment—explains how to install and deploy Cisco Nexus 1000V Series Switches running Cisco Nexus Operating System (NX-OS) version 4.2(1)SV2(1.1) software 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.
- Cisco Virtual Machine Fabric Extender Configuration and Deployment—explains how to deploy Cisco Virtual Machine Fabric Extender (VM-FEX) on a Cisco UCS B-Series server equipped with a Cisco virtual interface card (VIC) adapter. Cisco VM-FEX bypasses software-based switching of VM traffic by the hypervisor to use external hardware-based switching in the Cisco UCS fabric interconnects. This method reduces the load on the server CPU, provides faster switching, and enables you to apply a rich set of network management features to local and remote traffic.

Related Reading

The *Cisco SBA—Data Center Design Overview* provides an overview of the data center architecture. This guide discusses how the Cisco Smart Business Architecture (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 it includes 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.

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 high availability 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 Cisco Nexus 1000V

The Cisco Nexus 1000V Series switch is a software-based switch designed for hypervisor environments that implements the same Cisco NX-OS as the Cisco Nexus 5500 Series switching platforms that comprise the primary Ethernet switch fabric for the Cisco SBA data center architecture. This allows a consistent method of operation and support for both the physical and virtual switching environments. 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. Cisco Nexus 1000V is currently supported with hypervisor software from VMware as an integrated part of the vSphere server virtualization environment.

Cisco Nexus 1000V is now offered in two editions, Essential and Advanced:

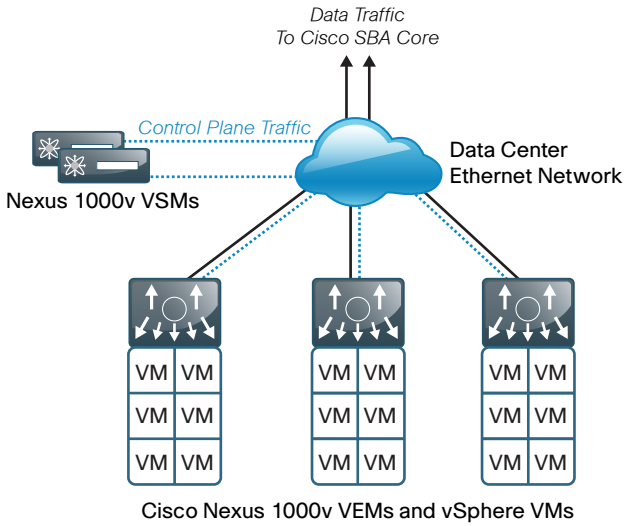
- Essential—Is a no-cost version that offers a rich set of services, including VLANs, loop prevention, port channels, Switched Port Analyzer (SPAN), Encapsulated Remote SPAN (ERSPAN), quality of service (QoS) control, Virtual Extensible Local Area Network (VXLAN), and Cisco vPath.
- Advanced—Includes the features in the Essential edition and adds Cisco Integrated Security Features, Cisco TrustSec security group access, and Cisco Virtual Security Gateway.

For more information on Cisco Nexus 1000V product-level offerings, see the following:
http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9902/data_sheet_c78-492971.html

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)SV2(1.1) and VMware ESXi version 5.0U1.

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 or 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



Cisco 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 vSphere 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 features, such as private VLAN, access control lists, port security, Dynamic Host Configuration Protocol (DHCP) snooping. Cisco TrustSec in Cisco Nexus 1000V combines with the Cisco Identity Services Engine, to make context-aware access control decisions.
- Monitoring functions, such as 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, Cisco 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 or 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 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.

Virtualized Network Services with Cisco vPath

In addition to virtual machine switching, Cisco Nexus 1000V Series supports Cisco vPath in order to provide a single architecture supporting multiple Layer 4 through 7 network services. In the Cisco vPath architecture, virtual service nodes can provide a variety of network services, such as virtual firewall, load balancing, and WAN acceleration. Specifically, the Cisco vPath architecture provides:

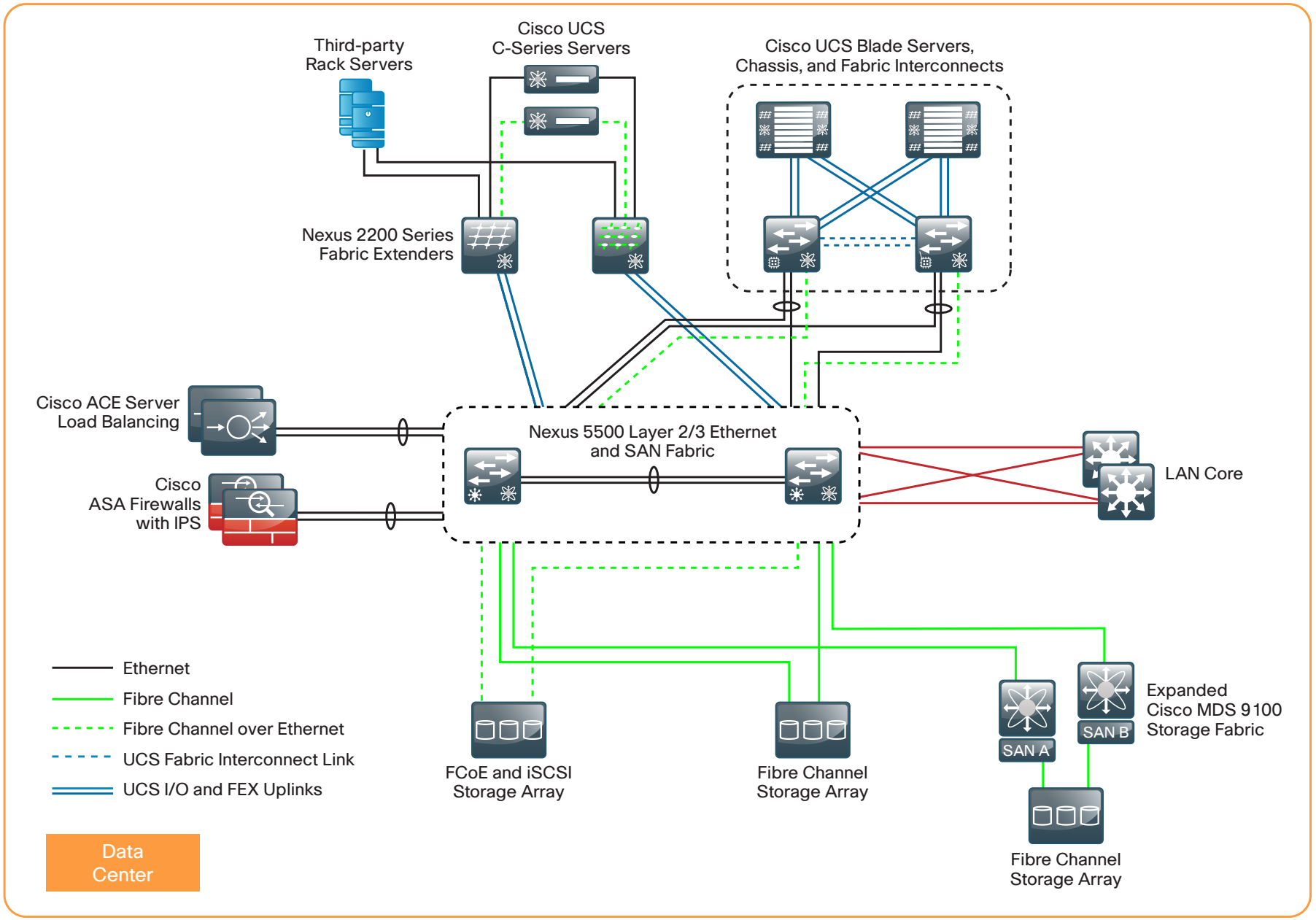
- Intelligent traffic steering—Redirect traffic from the server requesting a network service to the virtual service node (VSN), and extend port profiles to include the network service profile.
- Flexible deployment—Each VSN can serve multiple physical servers, and the VSN can be hosted on a separate or dedicated server.
- Network service acceleration—With Network Service Decision Caching, Cisco Nexus 1000V Series remembers network service policy from prior traffic, reducing traffic steering, and the performance of virtual network services can be accelerated through enforcement in the hypervisor kernel.

Cisco virtualized network services with Cisco vPath is beyond the scope of this guide.

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 (UCS) provides enhanced flexibility and integration for VMware environments.

Figure 2 - Cisco SBA data center architecture



Cisco 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—Cisco UCS 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-Gigabit Ethernet, Fibre Channel, and Fibre Channel over Ethernet (FCoE) capabilities—to the system. Cisco UCS 6200 fabric interconnects provide 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 Cisco UCS Blade Server Chassis.
- Cisco UCS fabric extenders—Cisco UCS 2200 Series fabric extenders (FEX), 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 Series FEX, which can connect to the data center foundation Nexus 5500 Series switch, Cisco UCS 2200 Series fabric extenders logically extend the fabric from the Cisco UCS fabric interconnects into each of the enclosures for Ethernet, Fibre Channel over Ethernet (FCoE), and management purposes.
- 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. Cisco UCS B-Series Blade Servers are 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 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 eight ports of 10-Gigabit Ethernet and 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 Cisco 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 Cisco 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 Cisco UCS B-Series servers, the Cisco UCS C-Series servers offer a wide array of processor, memory, network adapter, and disk options.

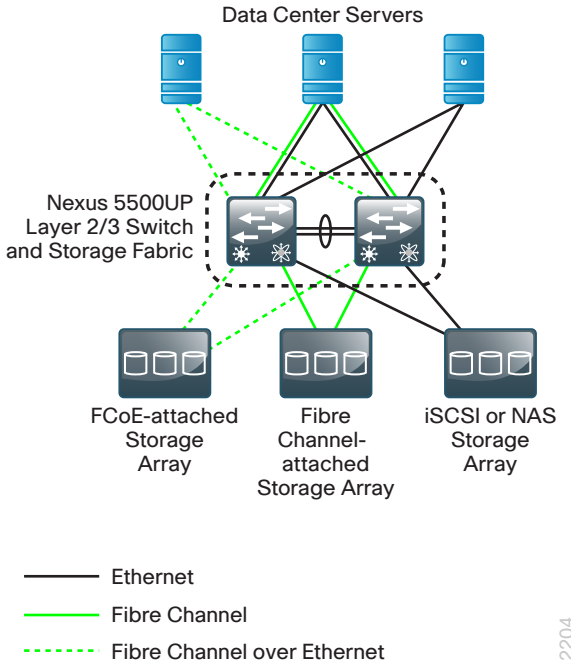
The Cisco Integrated Management Controller (Cisco IMC) is the management service for Cisco UCS C-Series servers. Cisco IMC runs within the server. Cisco IMC allows you to use a web-based GUI or Secure Shell (SSH) Protocol–based CLI to remotely access, configure, administer, and monitor the server. Almost 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.

Cisco UCS Manager can manage the Cisco 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-mount 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



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. 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.

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 switches in a VMware environment.
- Deploying Cisco VM-FEX on a Cisco UCS B-Series server 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.

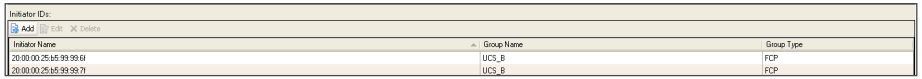
Step 1: Log in to the NetApp System Manager using the username **root** and the password you configured on the NetApp.

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.



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 5500UP-A	4	304	SAN-A
Nexus 5500UP-B	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.

```
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*.

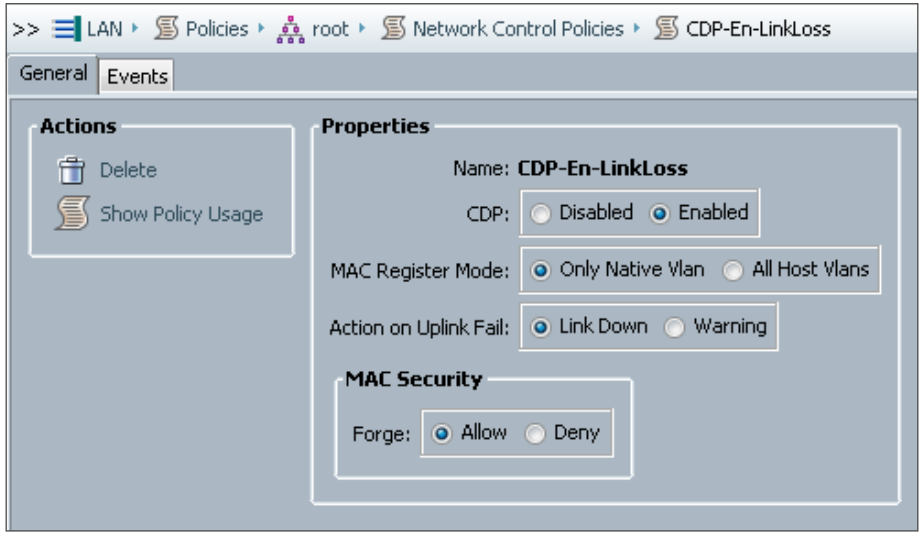
The VMware setup for the Cisco UCS B-Series blade servers includes two virtual Ethernet NICs (vNICs) and two virtual Fibre Channel host bus adapters (vHBAs) defined in a Cisco UCS service profile. These are presented to the vSphere ESXi operating system as VMNICs and VMHBAs.

The Cisco UCS M81KR, VIC 1240, or VIC 1280 virtual interface cards 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 midplane. 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. A link-down network control policy has been defined in the *Cisco SBA—Data Center Unified Computing System Deployment Guide* to push a notification to the 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 issues 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.

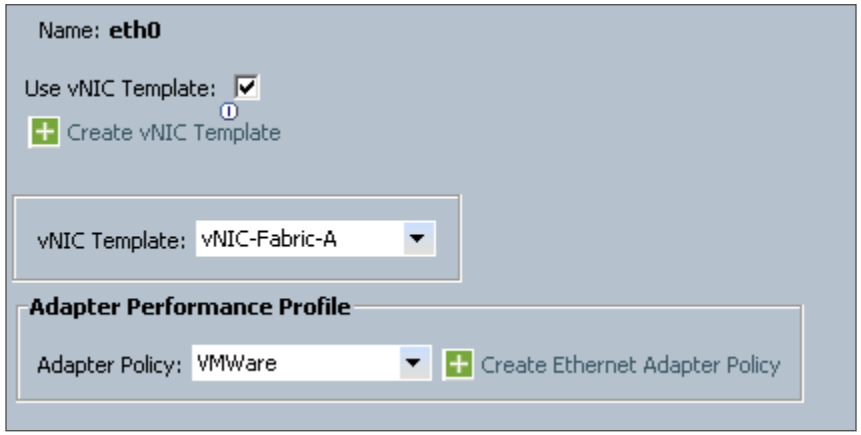
Step 1: In the Cisco UCS Manager navigation pane, click the **LAN** tab, and expand **LAN** > **Policies** > **root** > **Network Control Policies**. Ensure that you have a network control policy created with CDP option enabled and with Action on Uplink Fail as Link Down.



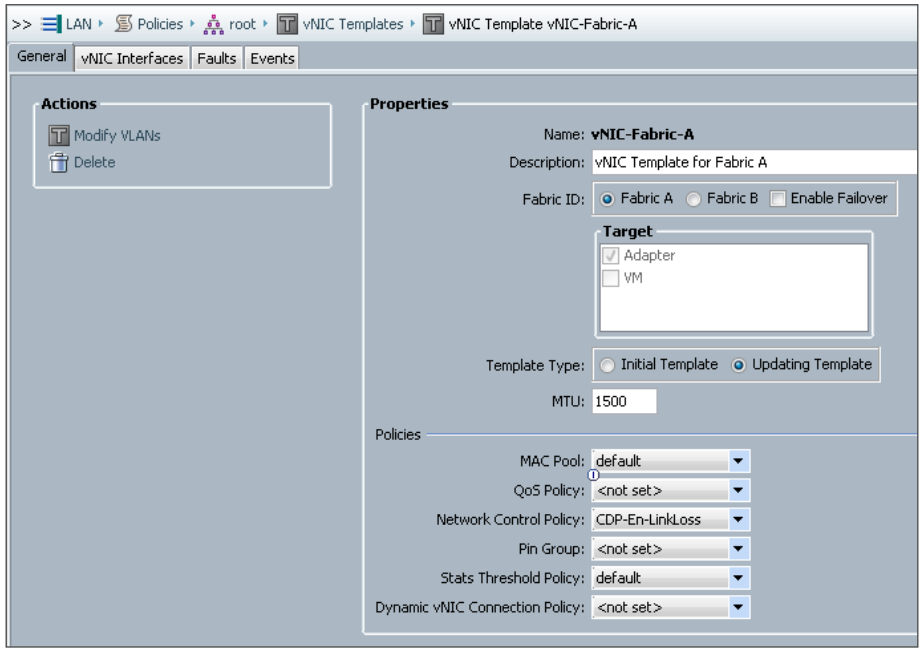
Step 2: In the navigation pane, click the **Servers** tab, select the service profile that you plan to assign to the server, and then in the work pane, click the **Network** tab.

Step 3: 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 4: If you have created the vNIC using a vNIC template (vNIC-Fabric-A for the first NIC eth0 or vNIC-Fabric-B for the second NIC eth1), as directed in the *Data Center Unified Computing System Deployment Guide*, you will notice the vNIC template name used. You must modify the template in order to verify settings.



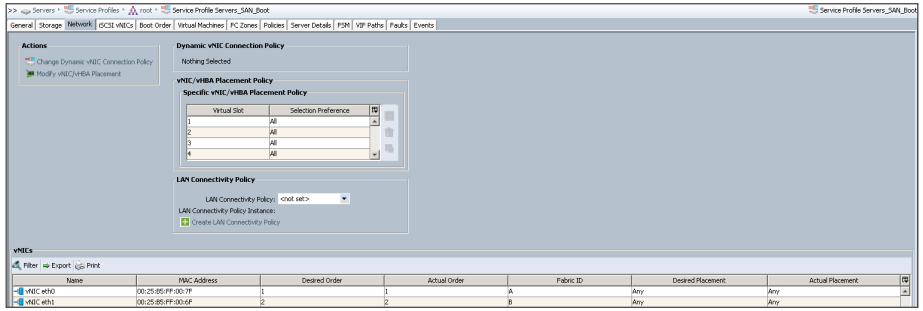
Step 5: In the navigation pane, click the **LAN** tab, navigate to **LAN > Policies > root > vNIC Templates**, and then click the vNIC template used to create the vNICs.



Step 6: Ensure **Enable Failover** is cleared, and then in the Policies section, in the **Network Control Policy** list, choose the control policy as shown in Step 1, and then click **OK**.

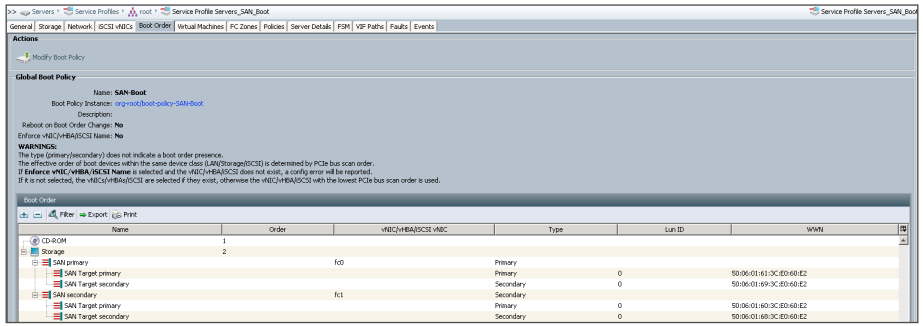
It is recommended that you do not enable fabric failover for the virtual switch uplinks.

Step 7: Verify that vNIC eth0 is connected to Fabric A and that vNIC eth1 is connected to Fabric B. The vNICs eth0 and eth1 will carry management traffic and data traffic, such as virtual machine and storage traffic. You have created a total of two vNICs, with failover disabled.

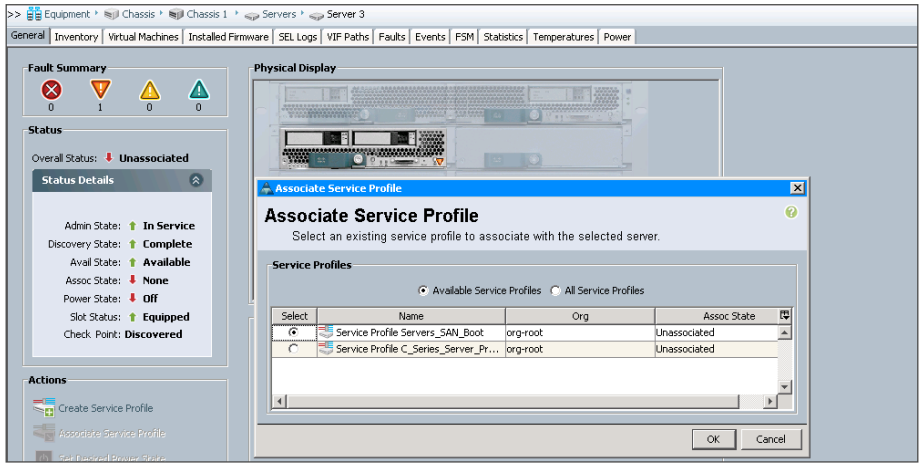


Step 8: Select a service profile to associate to a Cisco UCS B-Series blade server.

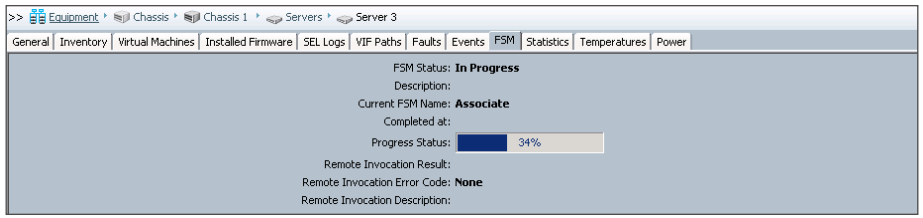
Step 9: On the Boot Order tab, ensure that you have configured the correct boot policy (either SAN boot policy or Local Disk boot policy). If you are using SAN boot policy, ensure that the SAN boot target configurations are correct.



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.



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



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 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 Cisco UCS C-Series server. Where appropriate, the differences are noted.

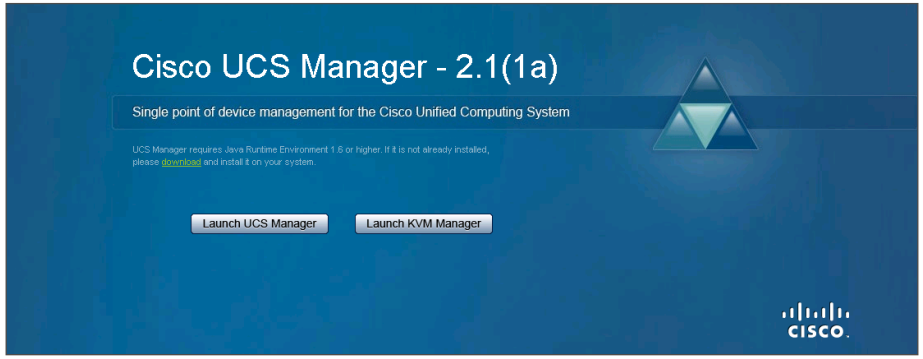
Procedure 1 Mapping the ESXi ISO file using virtual KVM

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: In a browser, connect to Cisco UCS Manager by using the Cisco UCS virtual management IP address.

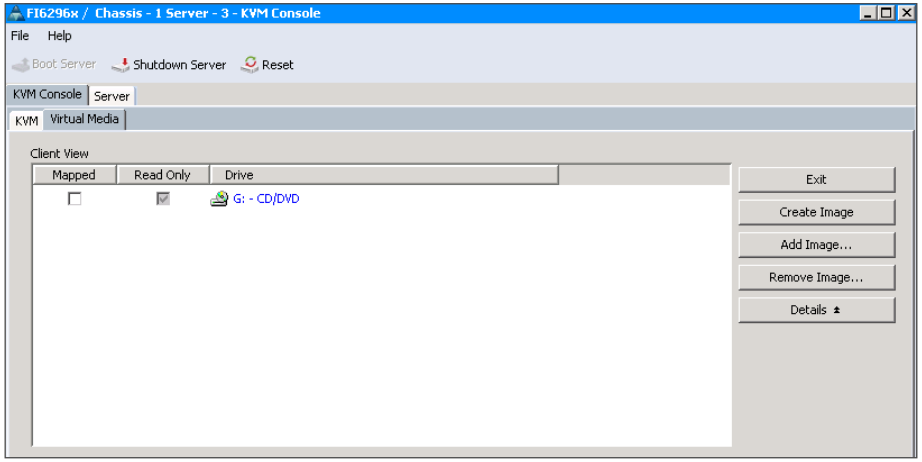
Step 2: Click **Launch UCS Manager**, and then log in to Cisco UCS Manager by using your administrator username and password.



Step 3: 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 4: In the work pane, on the General tab, in the Actions area, click **KVM Console**. The KVM console opens in a separate window.

Step 5: In the KVM console window, on the KVM Console tab, click the **Virtual Media** tab.

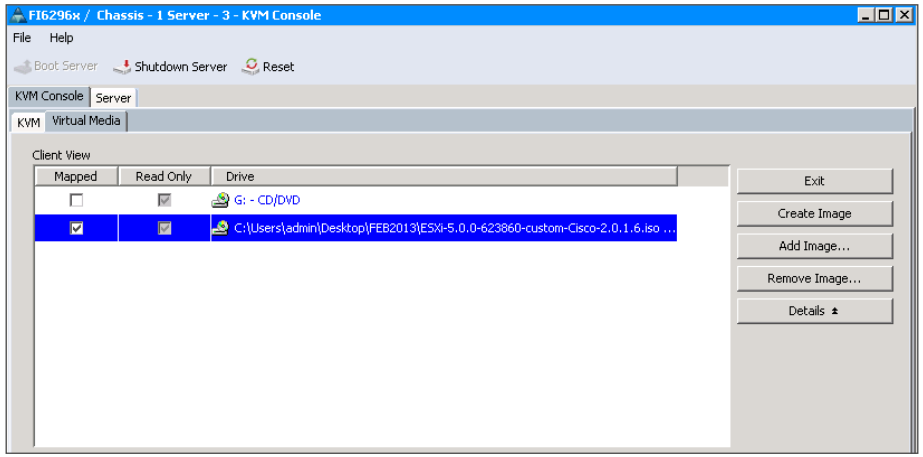


Step 6: Click **Add Image**, navigate to the VMware-VMvisor ISO file, and then select it. The ISO image is displayed as a device in the Client View pane.

Step 7: 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.

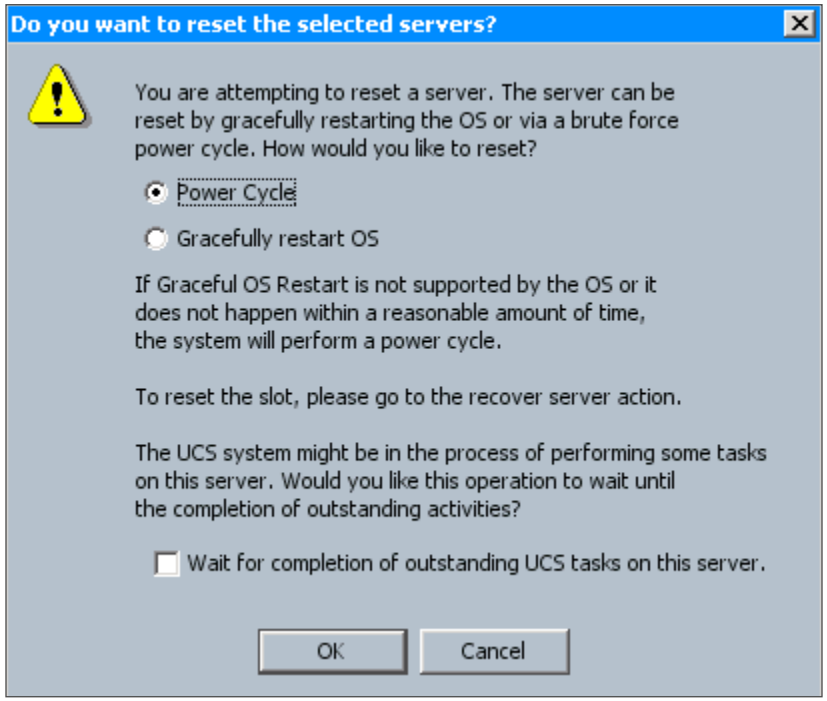
Tech Tip

Leave the KVM Virtual Media window open, and do not press exit until you are told to in Step 7 of the next procedure, "Install vSphere Hypervisor (ESXi)".

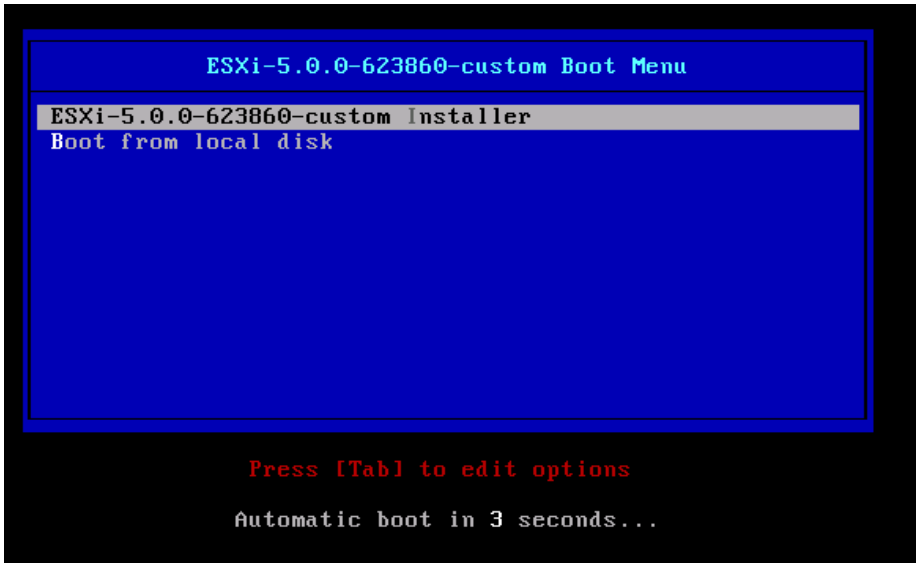


Step 8: When mapping is complete, at the top of the screen, click **Reset**.

Step 9: 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.



Step 10: Click the **KVM** tab to watch the server boot, and when the VMware VMvisor Boot Menu appears, select **ESXi Installer**. In the next procedure, you continue configuration in the ESXi Installer.



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.

If you are deploying a Cisco UCS C-Series C220 M3, C240 M3, and C260 M2 server, these servers have an onboard Secure Digital (SD) card, called Cisco FlexFlash, installed in them.

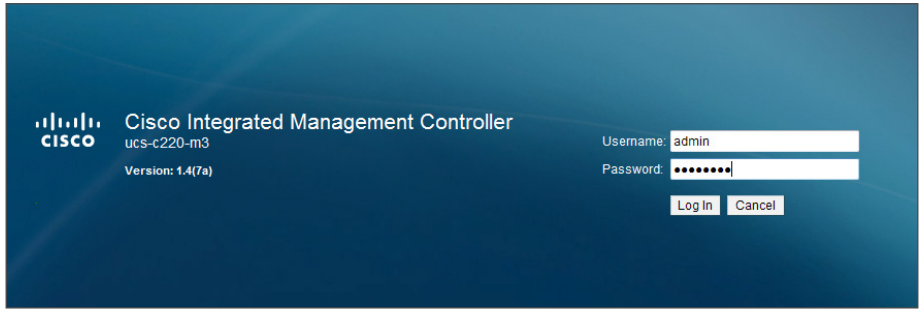
The Cisco FlexFlash SD card has four partitions, and each partition is presented as a USB drive to the BIOS and to any installed OS. The four partitions are:

- **Hardware Upgrade Utility (HUU)**—Contains a bootable upgrade ISO installed.
- **Server Configuration Utility (SCU)**—Contains a bootable configuration ISO installed.
- **Drivers**—Contains the Cisco Drivers ISO.
- **Hypervisor (HV)**—Is used to install Hypervisor OS, and it can also be used to store files that can be accessed by the OS.

The images in the partition can be installed or updated by using SCU Release 3.0 or later. If you have a Cisco FlexFlash card, the following Step 3 through Step 5 will be used to activate the partition through Cisco IMC and enable the HV partition for installation of the VMware ESXi ISO file.

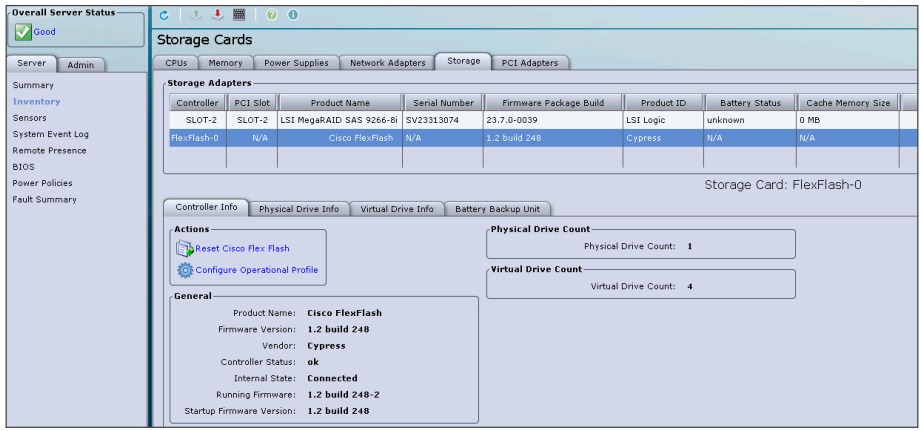
Step 1: In a browser, enter the Cisco IMC IP address.

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



Step 3: If you are not deploying a Cisco UCS C-Series server utilizing Cisco FlexFlash, skip to Step 6.

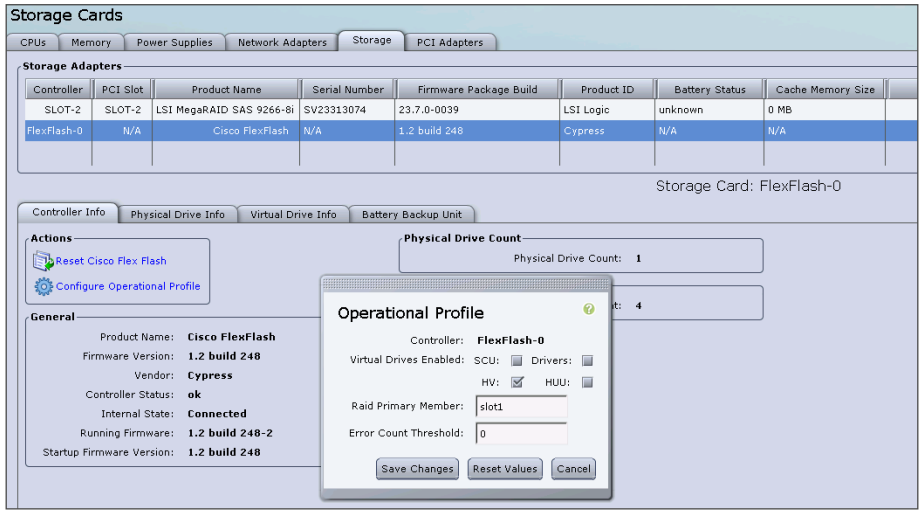
If you are deploying a Cisco UCS C220 M3, C240 M3, or C260 M2 server with Cisco FlexFlash installed, on the Server tab, click **Inventory**, and in the work pane, click the **Storage** tab, and then in the Storage Adapter section, select the **FlexFlash-0** controller.



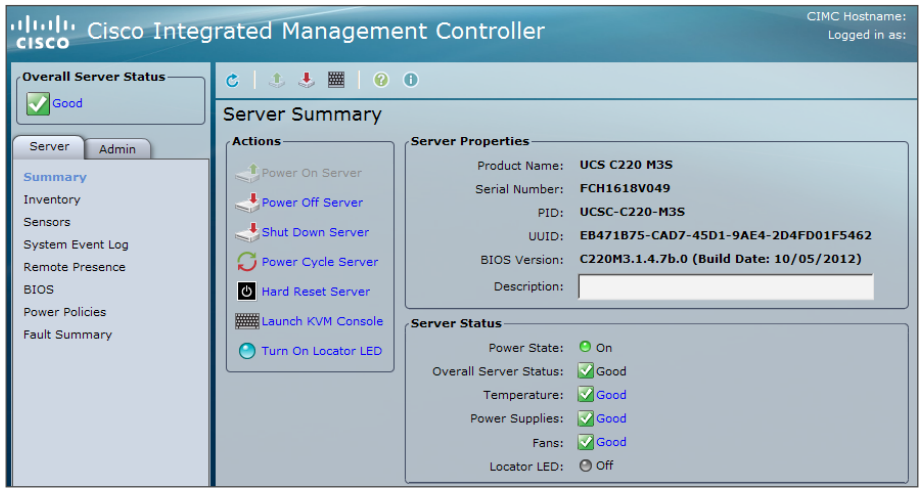
Next, you activate the HV partition.

Step 4: Click the **Controller Info** tab, and then under the Actions pane, click **Configure Operational Profile**.

Step 5: On the Operational Profile dialog box, click **Save Changes**. The HV partition is now available to install a VMware ESXi ISO file on it.

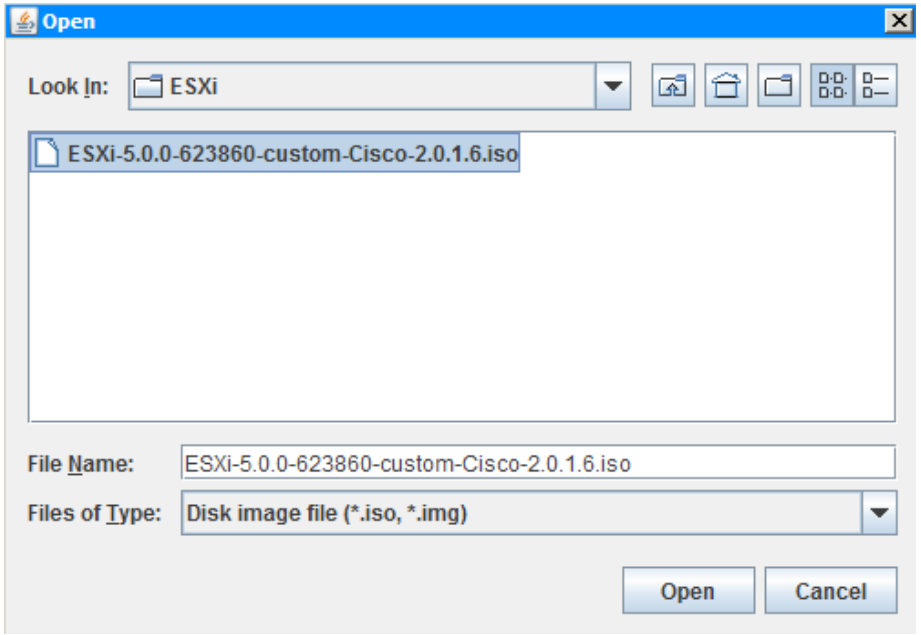


Step 6: On the Server tab, click **Summary**, and then in the work pane, click **Launch KVM Console**.

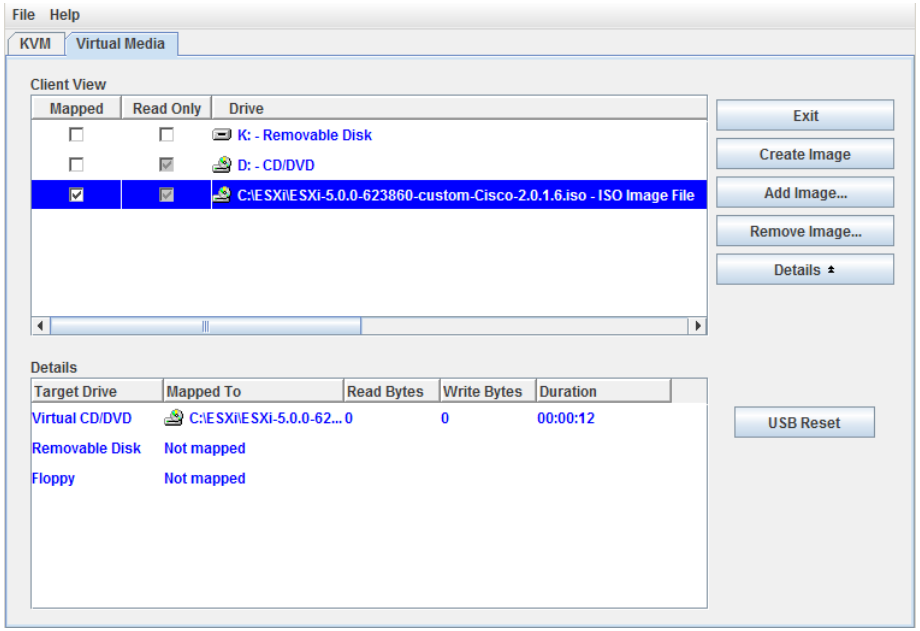


Step 7: In the KVM console, click the **Virtual Media** tab.

Step 8: On the Open dialog box, click **Add Image**, select your ISO file, and then click **Open**.



Step 9: For the image you selected in the preceding step, select the **Mapped** check box. Do not click **Exit**.

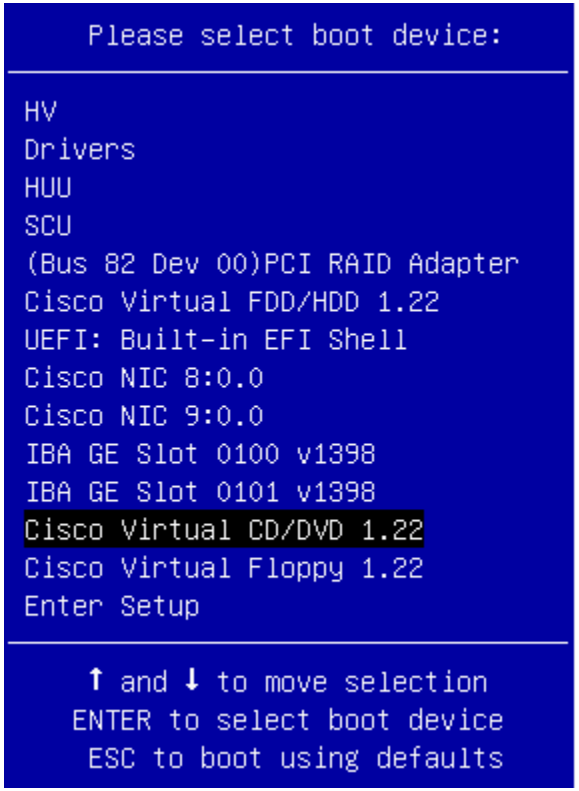


Tech Tip

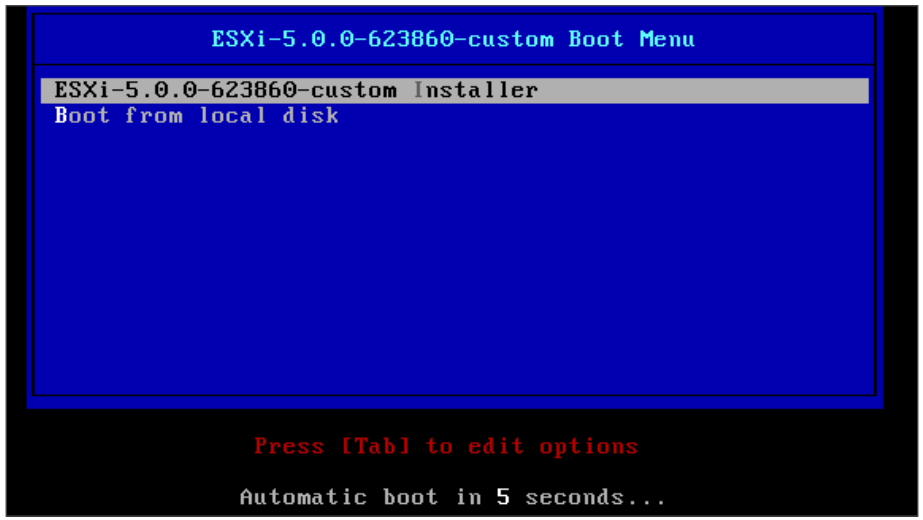
Leave the KVM Virtual Media window open, and do not press exit until you are told to in Step 7 of the next procedure, "Install vSphere Hypervisor (ESXi)".

Step 10: On the KVM tab, in the menu bar, choose **Macros**, and then press **Ctrl-Alt-Del**. This reboots the server.

Step 11: When the server reboots, press **F6** to enter the boot menu, select **Cisco Virtual CD/DVD**, and then press **Enter**. Selecting the correct boot device enables files from the ISO file to be read and the ESXi installation to begin.



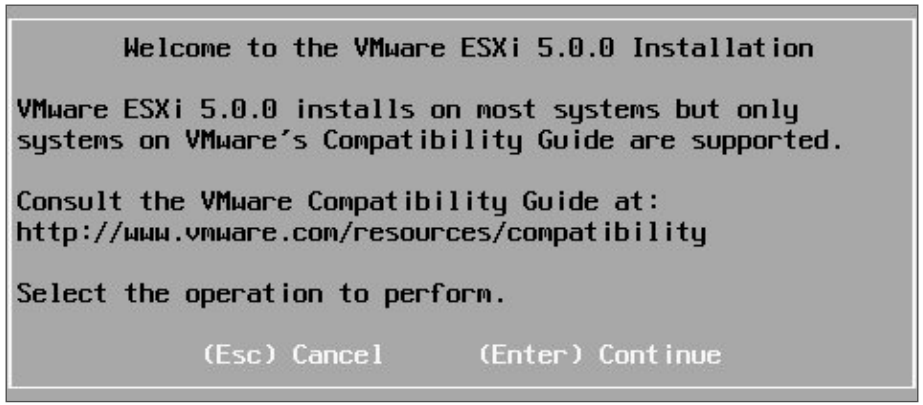
Step 12: When the VMware VMvisor Boot Menu appears, select **ESXi Installer**.



Procedure 2 Install vSphere Hypervisor (ESXi)

After your Cisco UCS B-Series or C-Series server boots with the VMware ESXi installer from the previous procedure, continue with this procedure.

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



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

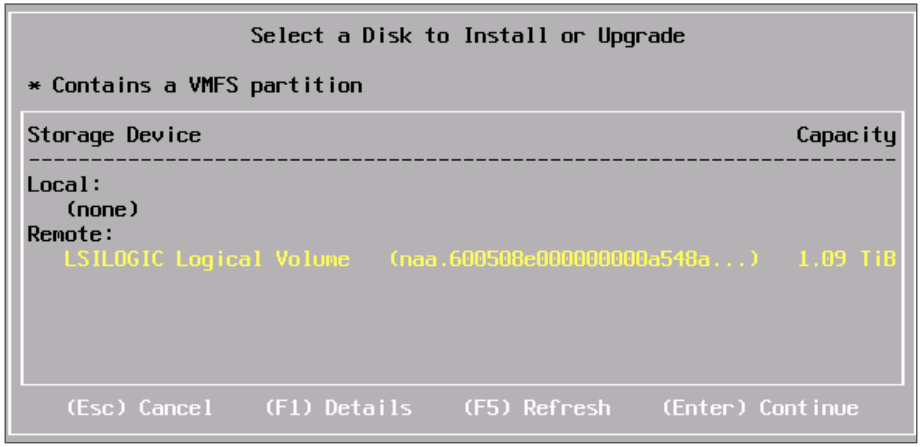
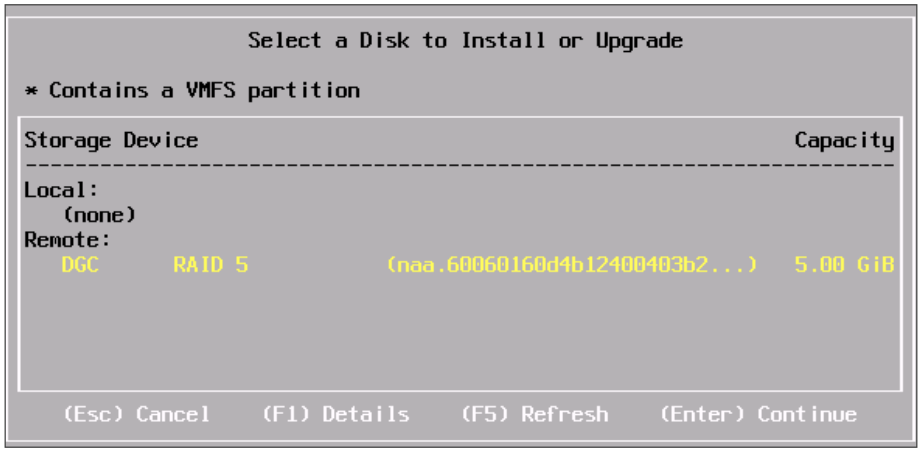


Figure 5 - Cisco UCS B-Series storage array–based LUN



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

Reader Tip

When the Cisco UCS C-Series server is provisioned with suitable NICs and drivers, it can also boot from a SAN disk, similar to the Cisco UCS B-Series procedure. For more details see: http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/gui/config/guide/1.4.1/b_Cisco_UCS_C-Series_GUI_Configuration_Guide_141_chapter_01001.html#d31886e1041a1635

Figure 6 - Cisco UCS C-Series local disk drive

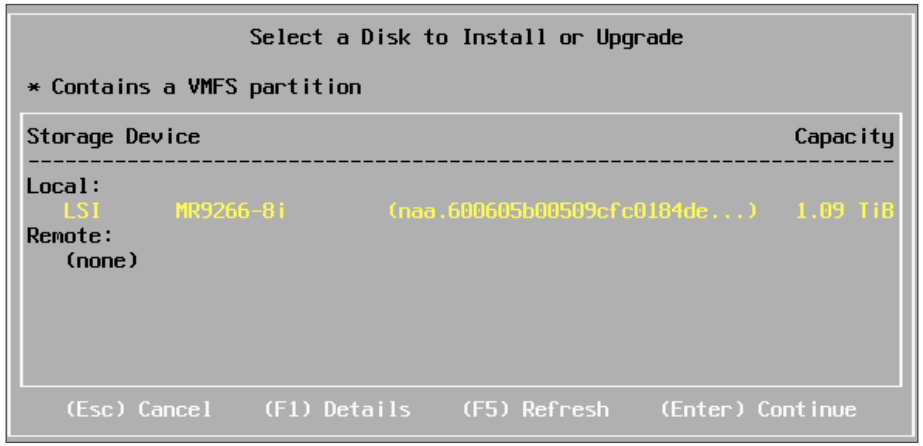


Figure 7 - Cisco UCS C-Series USB thumb drive

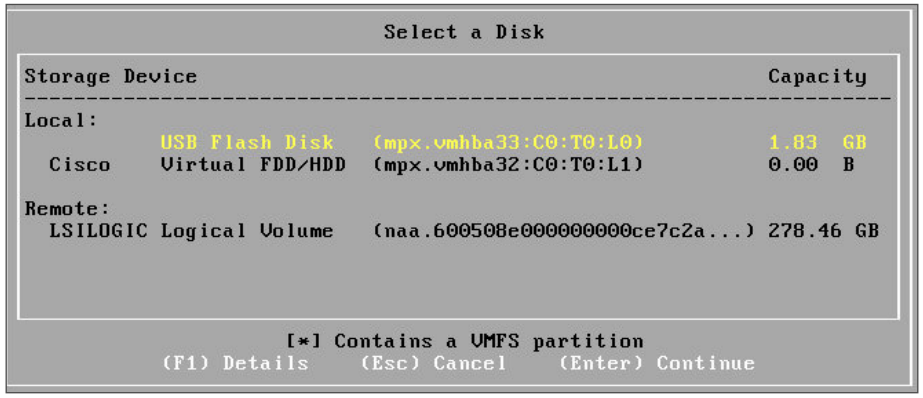
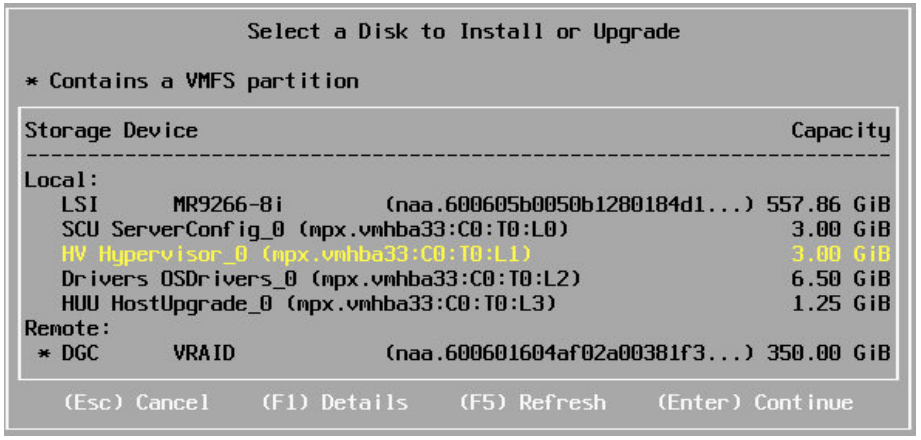
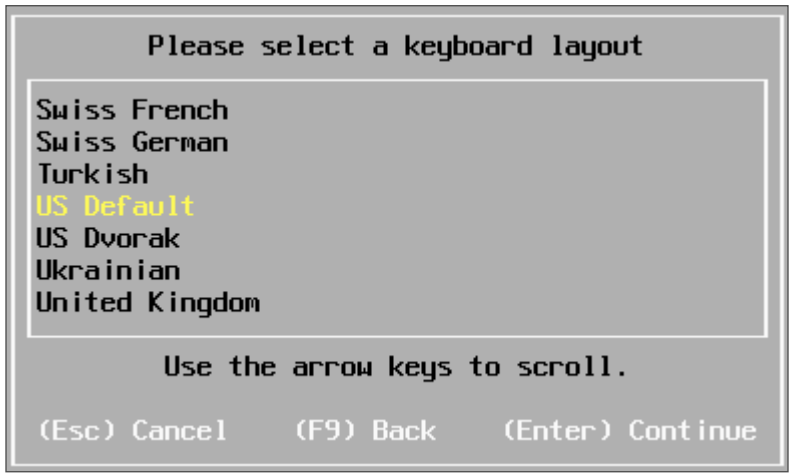


Figure 8 - Cisco UCS C-Series FlexFlash HV partition

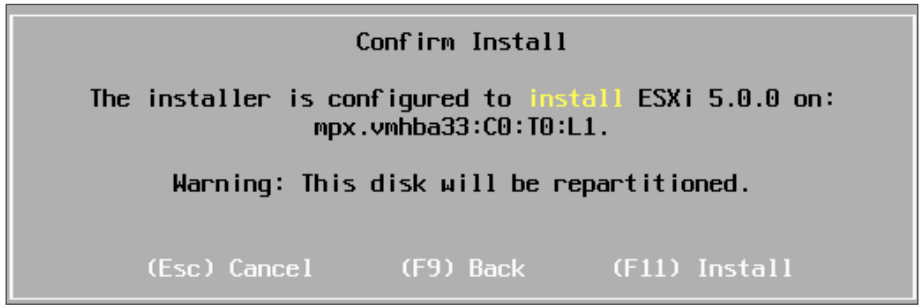


Step 4: Select the desired keyboard layout, and then press Enter.



Step 5: Enter a password for the root account, confirm the password by entering it again, and then press **Enter**.

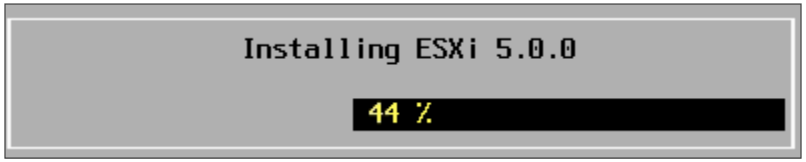
Step 6: Review the Confirm Install screen, and then press **F11**.



Tech Tip

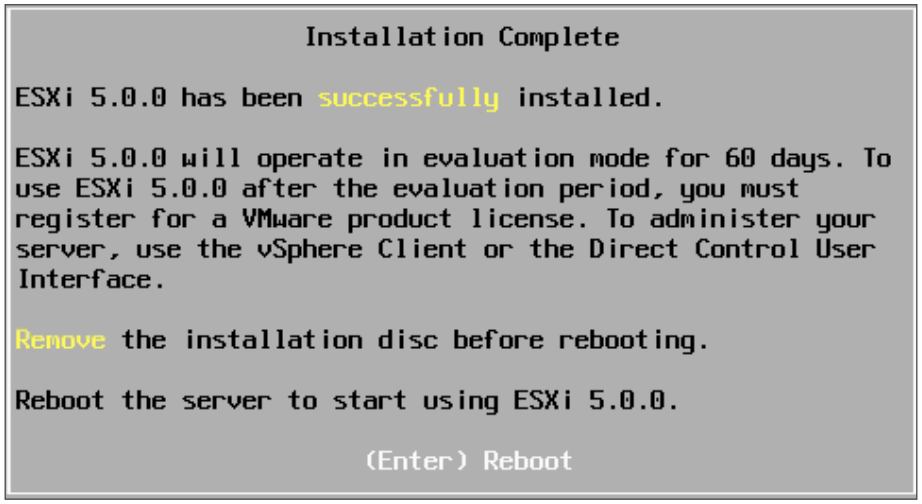
The system alerts you that any existing data on the target drive will be overwritten.

VMware ESXi installation begins and displays a status window.



Step 7: 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 8: On the Installation Complete screen, press **Enter**. The server reboots.



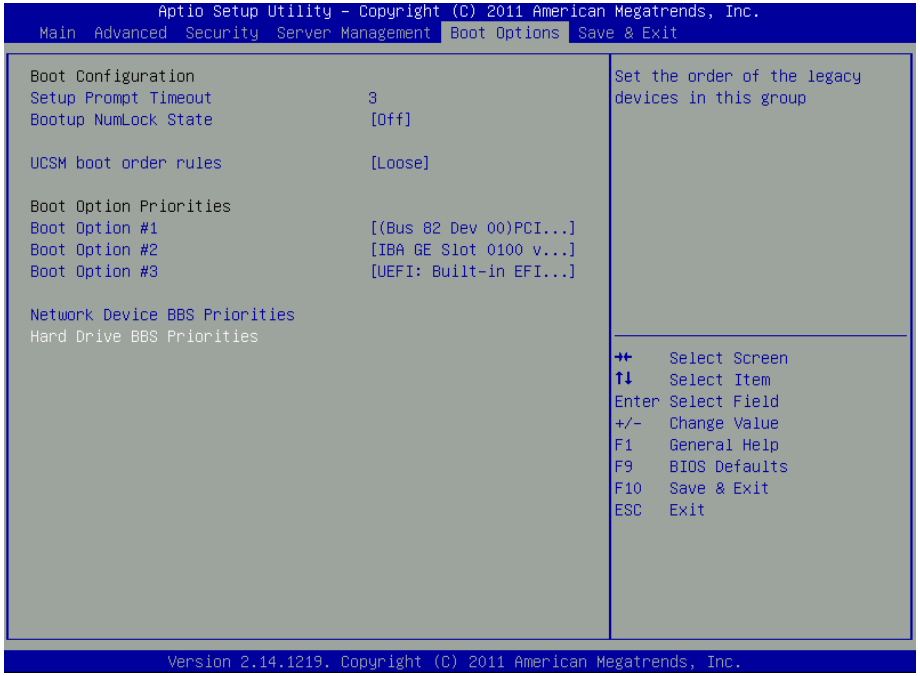
Step 9: If you are using the Cisco UCS B-Series Server or the UCS C-Series server with the boot-from-local-drive option, proceed to the next process "Configuring the ESXi Console."

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

Step 10: When the server boots, press **F2**. BIOS setup opens, where you can modify the BIOS boot order.

Step 11: Use the arrow keys to choose the Boot Options tab.

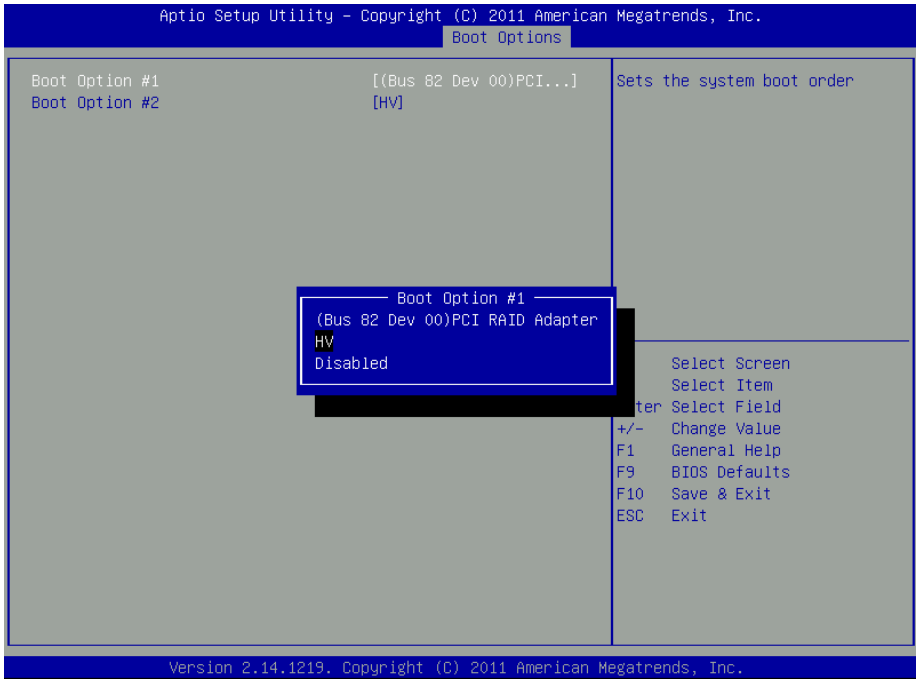
Step 12: In the Boot Options menu, select **Hard Drive BIOS Boot Specifications (BBS) Priorities**, and then press **Enter**.



Step 13: Select **Boot Option #1**, and then press **Enter**.

Step 14: If you are using a Cisco FlexFlash HV partition, select **HV**.

If you are using a USB thumb drive, select **USB** (not shown).



Step 15: Press **F10**. This saves your changes and reboots the server.

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

Process

Configuring the ESXi Console

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

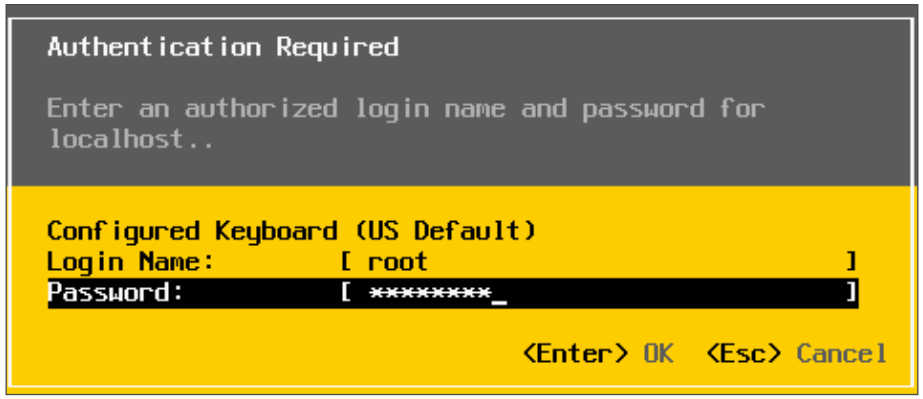
Procedure 1 Configure the management network

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. In this procedure, you configure management access to VMware ESXi on the server by assigning a static IP address to the ESXi management console.

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 when possible.

Step 1: On the ESXi home screen, press **F2**. This allows you to customize the system.

Step 2: On the Authentication Required screen, enter the root password set in Step 5 of the previous procedure, and then press **Enter**.

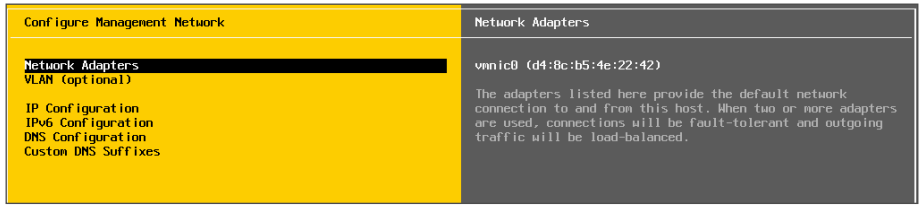


Reader Tip

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

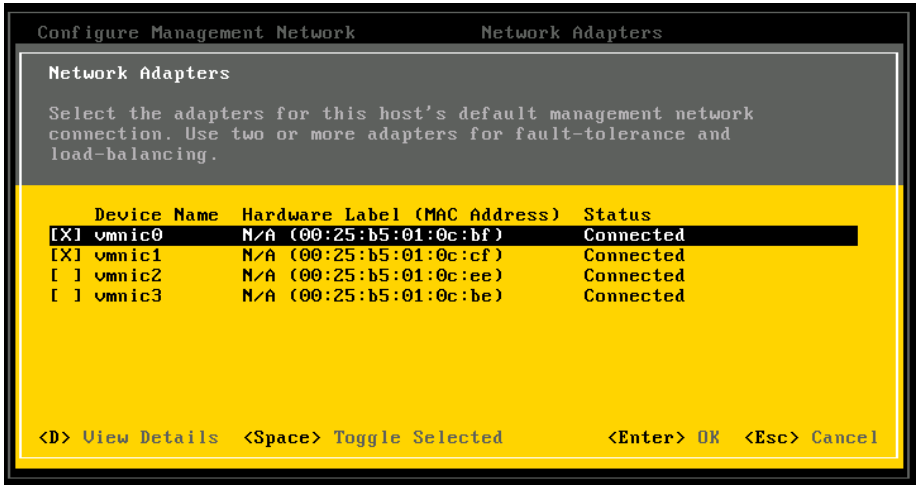
Step 3: On the System Customization screen, choose **Configure Management Network**.

Step 4: On the Configure Management Network screen, choose **Network Adapters**, and then press **Enter**.



Step 5: Press the **Space bar** to select **vmnics**, and then press **Enter**.

Step 6: 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.

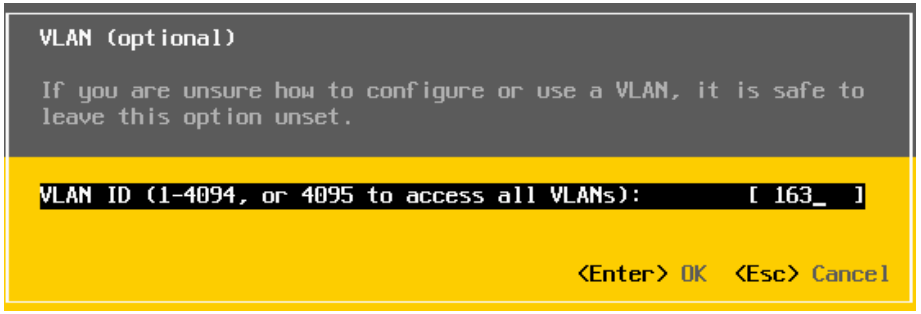


If you are using the Cisco UCS B-Series server, complete Step 7 and Step 8. These steps configure a trunk port and specify the management VLAN.

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 9.

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

Step 8: Enter the management VLAN number **163**, and then press **Enter**. The Cisco SBA data center foundation design uses VLAN 163.



Step 9: On the Configuration Management Network screen, choose **IP Configuration**, and then press **Enter**.

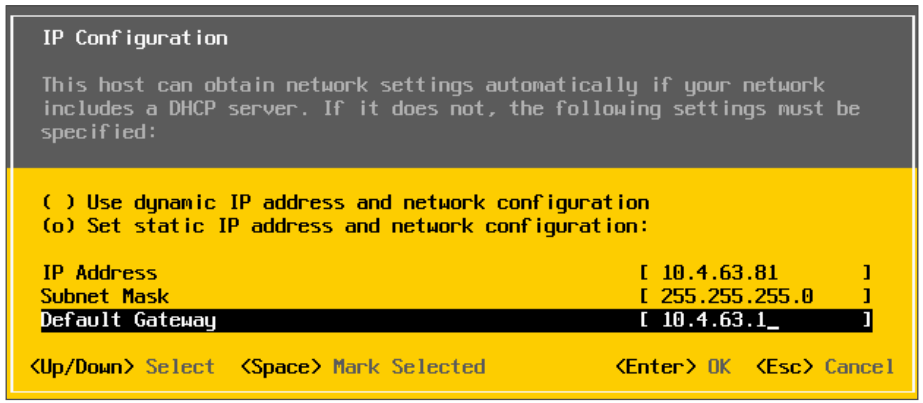
Step 10: On the IP Configuration screen, choose **Set static IP address and network configuration**.

Step 11: 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—10.4.63.81
- 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.



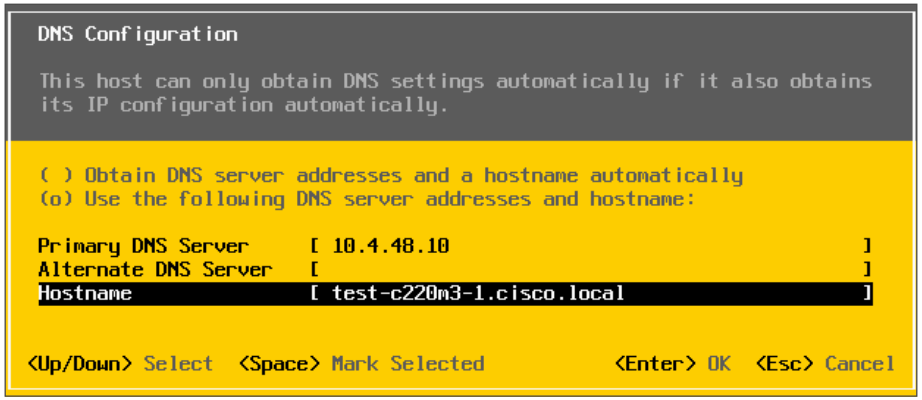
Procedure 2 Configure DNS address

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**:

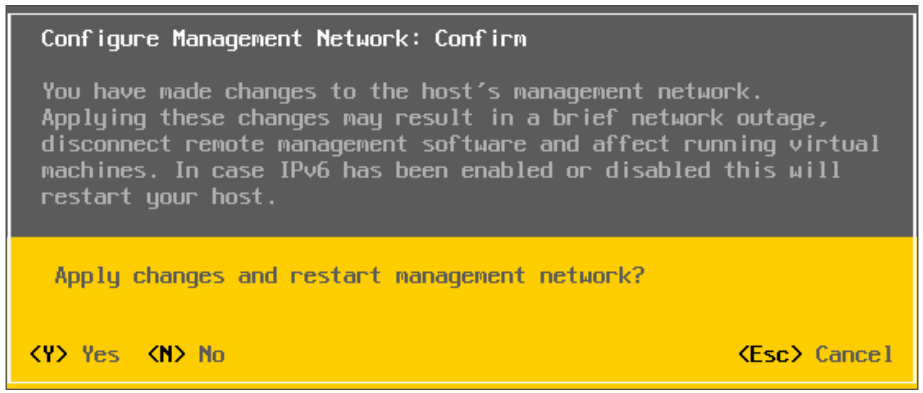
- Primary DNS server
- Backup (or alternate) DNS server
- A fully qualified host name for this node



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.

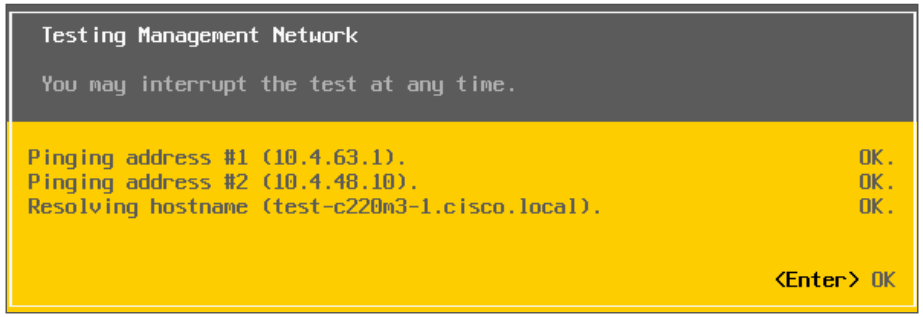


Procedure 3 Test the configuration

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**.



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

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 enable high availability by using VMware High Availability. 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 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 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, this procedure will show the details on how to install vSphere Client from the vCenter Server installation media.

Step 1: Obtain the VMware vCenter Server release 5.0U1 image (from a disc, ISO, download, etc.) and make the installation media available via CD/DVD to the system where you want to install the vSphere Client.

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.

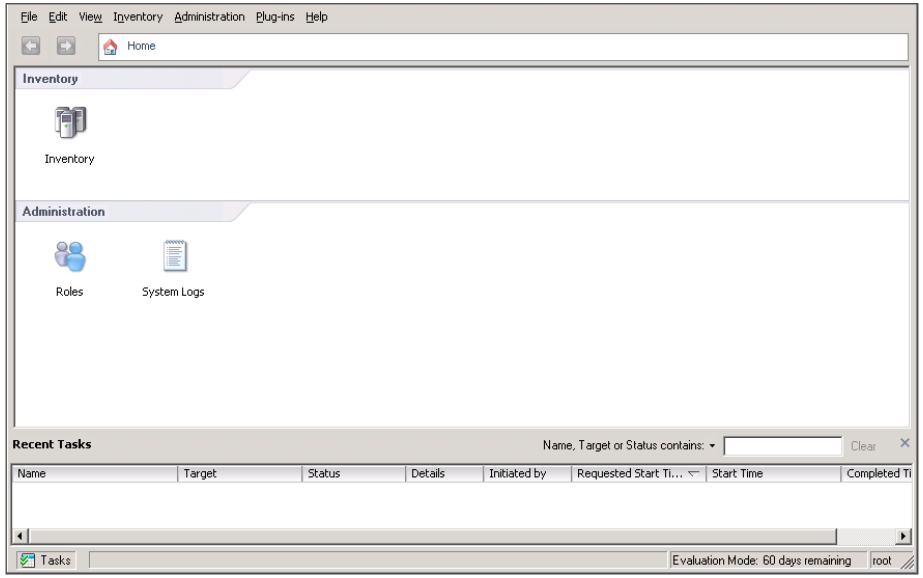
Step 2: Double-click Autorun.exe. This starts the VMware vCenter Installer.

Step 3: In the VMware vCenter Installer main screen, select **vSphere Client**, and then click **Install**.

Step 4: Once the installation completes, 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**.

Step 5: 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.



Tech Tip

If you are installing the vSphere client on a server with USB storage for ESXi, you may receive a warning "System logging not Configured on host <hostname>" indicating that you do not have a location to store log files for ESXi on this host. In this case, you can store log files on a syslog server. More information can be found at:
http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2003322

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 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.

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 vSphere Hypervisor. VSwitch 0 was created during the ESXi setup process when the vSphere Hypervisor management interface 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

In this procedure you will configure Virtual Machine physical interfaces (VMNICs) as uplinks in order to carry production traffic from the VMs to the data center network.

Table 2 - Example production traffic VLANs used in the Cisco SBA data center design

VLAN number	VLAN name	Description
148	Servers_1	Virtual Machine Network Data
149	Servers_2	Virtual Machine Network Data
150	Servers_3	Virtual Machine Network Data
154	FW_Inside_1	Firewall-protected servers
155	FW_Inside_2	Firewall and IPS protected servers
157	VDI_Clients	VDI Client secured servers

To avoid a single point of failure, in this deployment, each uplink adapter connects to two different physical switches in NIC teams. The teams can then either share the load of traffic between physical and virtual networks among some or all of its members, or they can provide passive failover in the event of a hardware failure or a network outage. By default, the NIC teaming is set to use the vSwitch port-based load-balancing policy.

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

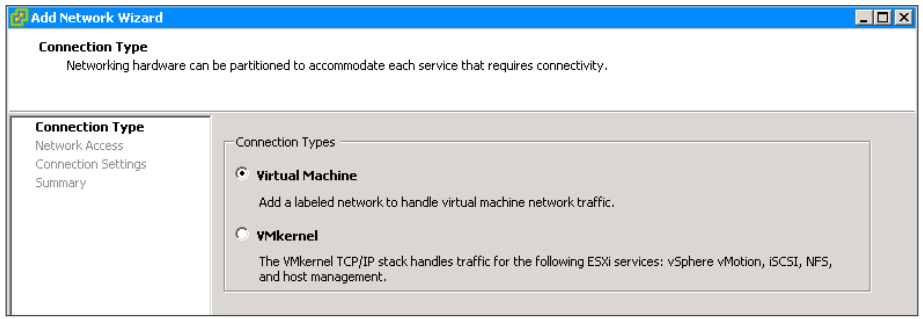
Step 2: Ignore the License warning. Licensing is covered in its own process in this guide.

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

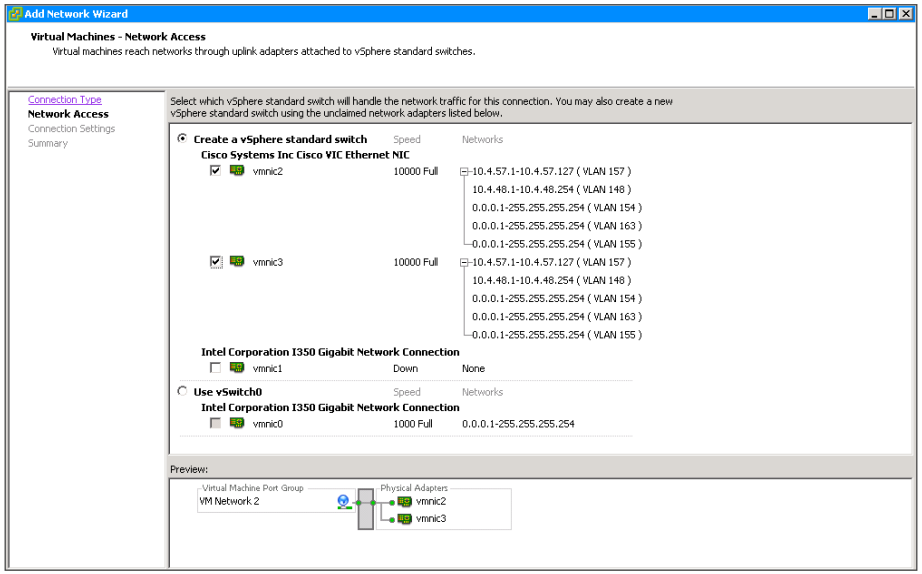
Step 4: In the left column, select the ESXi host, click the **Configuration** tab, and then select **Networking**.

Step 5: Click **Add Networking**.

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



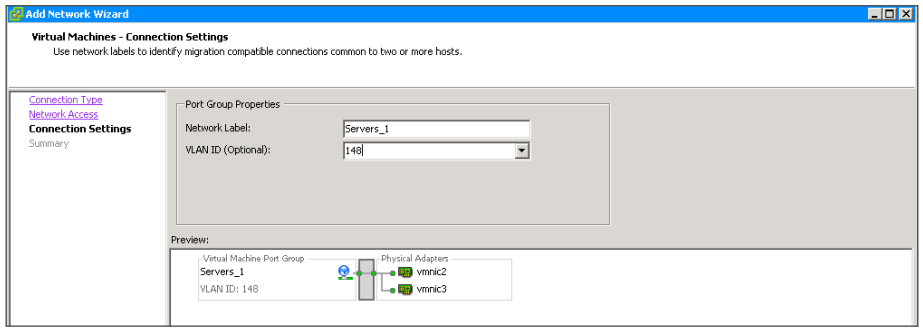
Step 7: Select the desired VMNIC physical interfaces to use on the new vSwitch, and then click **Next**. These interfaces are the uplinks that will carry production traffic from the server to the data center network.



Tech Tip

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

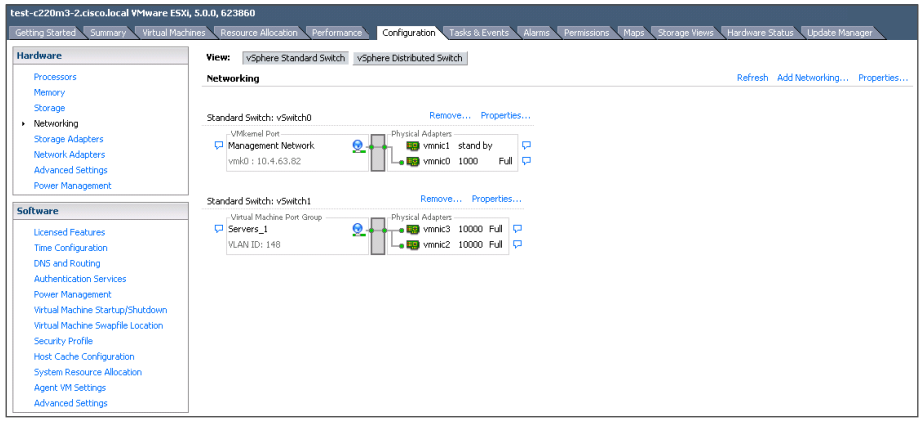
Step 8: Name the VLAN, enter the VLAN ID (Example: 148), and then click **Next**.



Tech Tip

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

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



Step 10: Repeat Step 5 through Step 9 to add additional VM production traffic VLANs, and reuse the new vSwitch that you created in Step 7.

Process

Configuring Data Storage for the ESXi Host

1. Set up shared storage
2. 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.

Tech Tip

If you are installing the vSphere client on a server with USB storage for ESXi, you may receive a warning "System logging not Configured on host <hostname>" indicating that you do not have a location to store log files for ESXi on this host. In this case, you can store log files on a syslog server. More information can be found at:
http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2003322

This process will guide you through the following procedures:

- Setting up shared storage with iSCSI, Fibre Channel, or FCoE transport.
- Adding VMware data stores or "persistent storage" for your virtual machines.

This guide uses the Cisco custom image for ESXi 5.0 U1 GA Install CD, which includes VMware operating system, as well as current drivers for Ethernet, Fiber Channel, and FCoE for VMware operation. This CD is available under the "OEM Customized Installer CDs" selection at:
https://my.vmware.com/web/vmware/info/slug/datacenter_cloud_infrastructure/vmware_vsphere/5_0#drivers_tools

If you do not use the customized image, you will need to make sure that the Ethernet (eNIC) and Fiber Channel (fNIC) drivers are updated on your system for compatibility between the virtual interface cards (VIC) and the VMware release.

Procedure 1 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 Cisco 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.

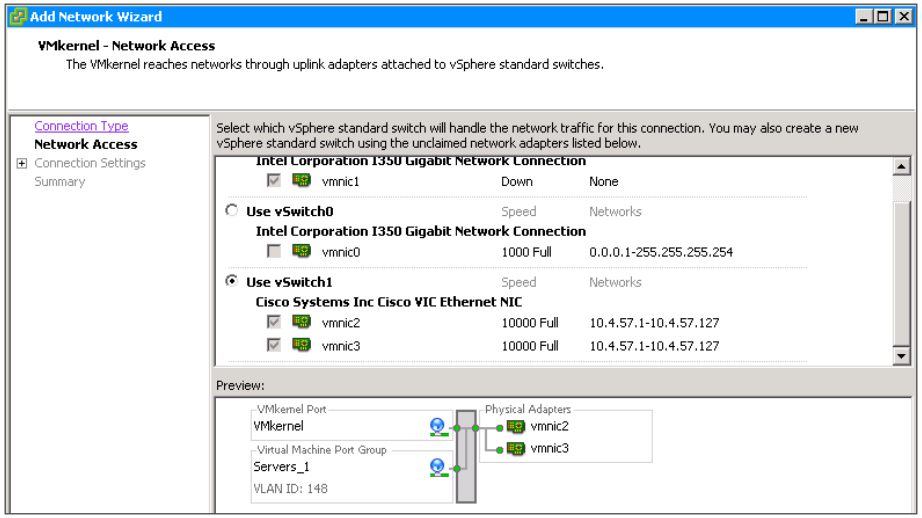
Step 1: Using vSphere Client, establish a connection to the ESXi host.

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

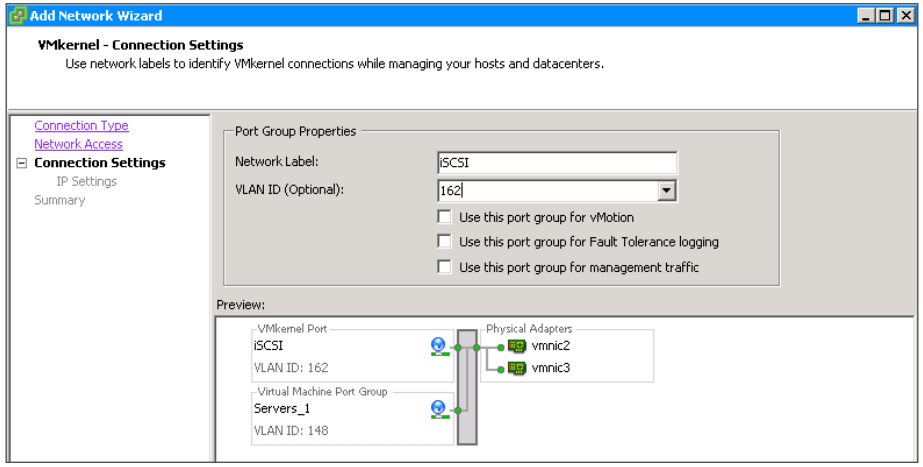
Step 3: Click **Add Networking**. This starts the Add Network Wizard.

Step 4: On the Connection Type page, select **VMkernel**.

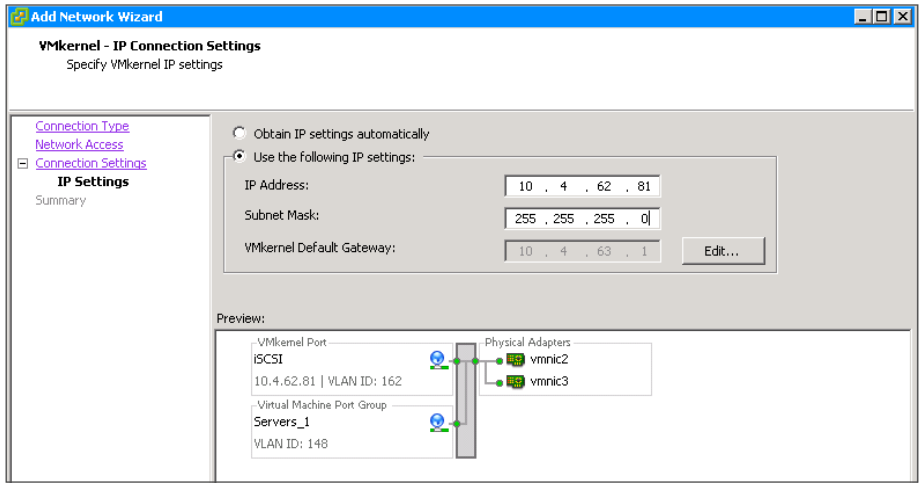
Step 5: On the Network Access page, select the appropriate vSwitch that will carry iSCSI traffic, and then click **Next**. This procedure uses the vSwitch that was created in the previous Procedure 1 "Run the Add Network Wizard."



Step 6: On the Connection Settings page, enter a name 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**.



Step 7: On the IP Settings page, enter an IP address (Example: 10.4.62.81) 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.



Step 8: On the Summary page, click **Next**, and then click **Finish**.

Step 9: Select **Configuration** > **Storage Adapter** > **Add**, and then in the Add Storage Adapter window, select Add **Software iSCSI Adapter**. In the Software iSCSI Adapter window, select **OK**.

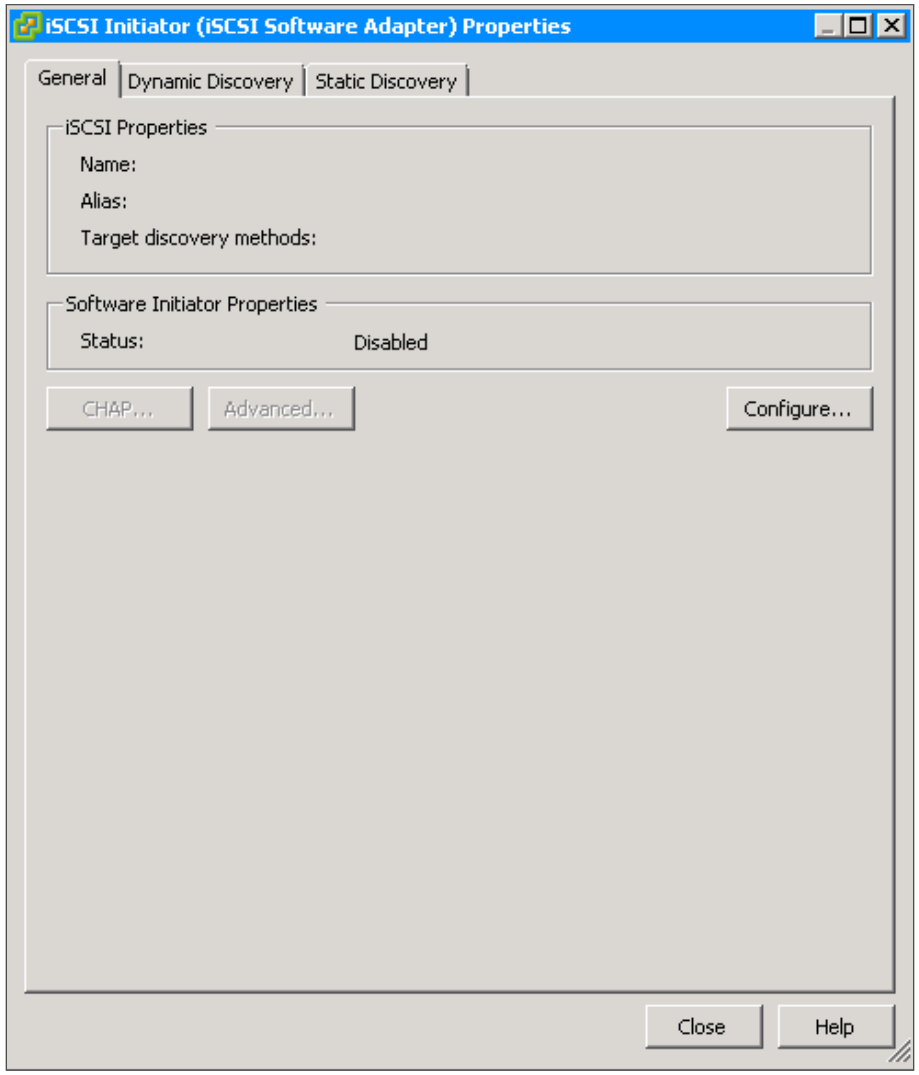
Tech Tip

If you use hardware-accelerated iSCSI adapters, the iSCSI adapter will appear on the list of storage adapters available for configuration. The remaining steps are the same for both software and hardware iSCSI adapters.

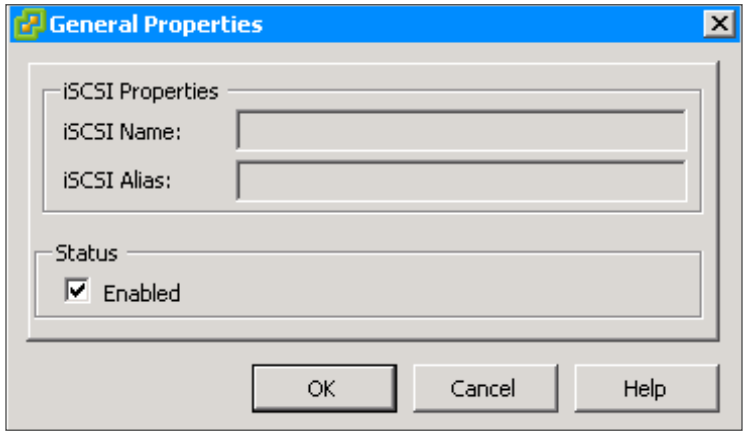
Step 10: Select the iSCSI Adapter, and then click **Properties**.

The iSCSI Initiator Properties dialog box appears.

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

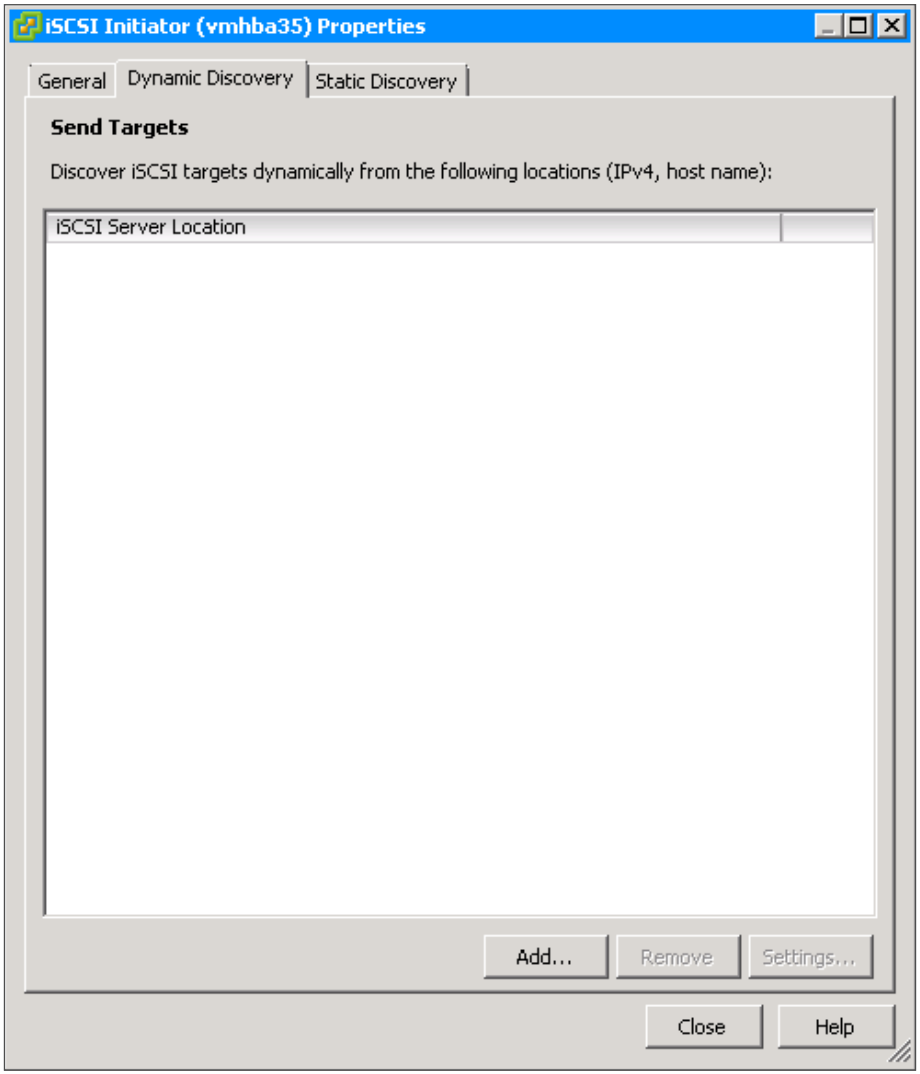


Step 12: Select the **Enabled** check box, and then click **OK**.

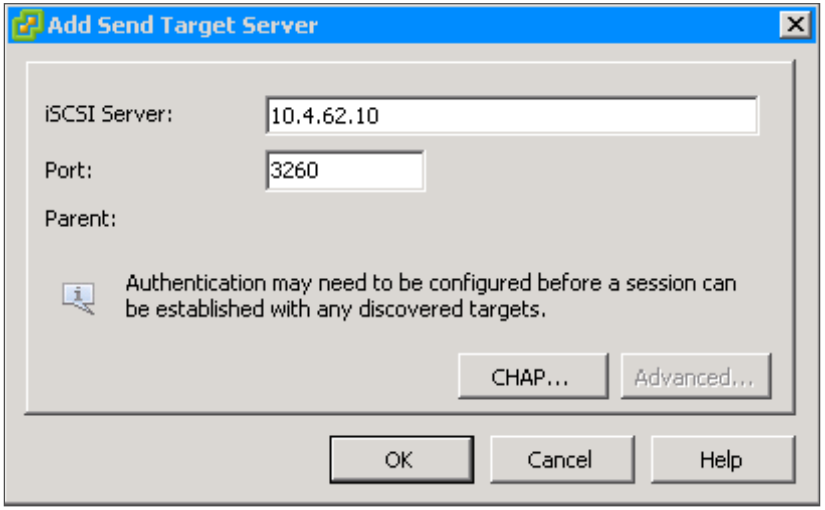


The iSCSI name self-creates. If you need to change the name for your setup, click **Configure** again and edit the name.

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



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



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, Procedure 2, "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 diskless servers, 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."

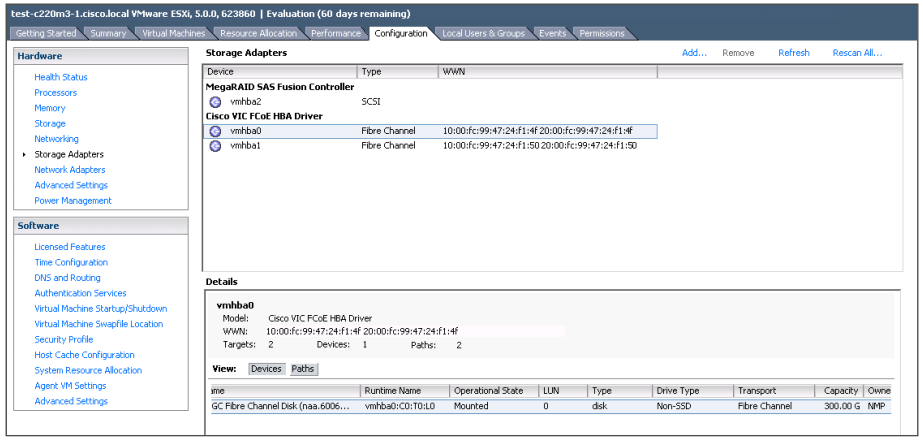
Also, FCoE vHBA and storage connectivity must have been deployed on the server as detailed in the *Cisco SBA—Data Center Unified Computing System Deployment Guide.*

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

Step 2: In the Hardware pane, click **Storage Adapters**, and then note the World Wide Node Name and World Wide Port Name of the HBAs. You must properly zone and mask the ports and their corresponding World Wide Names to your particular array by following Procedure 2 "Configure SAN zones" of the Process "Preparing the Environment for Server Access to SAN."

Reader Tip

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



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, Procedure 2, "Add a datastore to ESXi hosts."

Procedure 2 Add a datastore to ESXi hosts

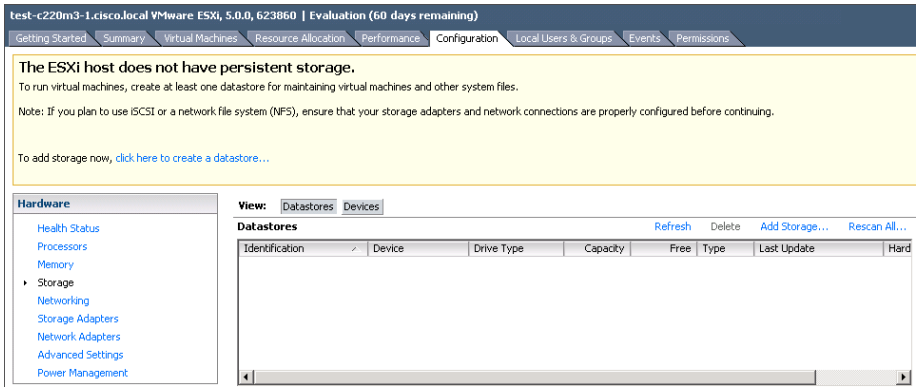
In this procedure, you will add storage for the virtual machines and other system files to use. The storage can be a disk drive physically located on the server, or it can be a disk or LUN located on a shared storage array.

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

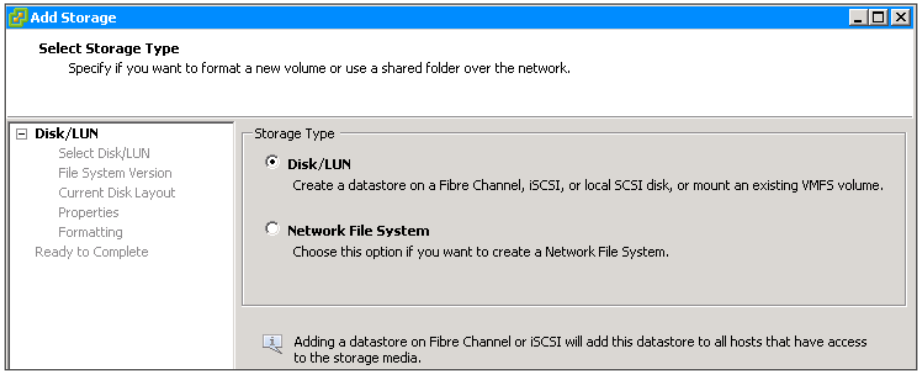
Step 2: On the Configuration tab, in the Hardware pane, click **Storage**.

Step 3: If your ESXi host does not have a provisioned virtual machine file system (VMFS), in main window, in the "The VMware ESX Server does not have persistent storage" message, click **Click here to create a datastore**.

If your system already has persistent storage configured, you can use this procedure to add additional storage to the ESXi datastore.



Step 4: In the Add Storage wizard, select **Disk/LUN**, and then click **Next**.



Step 5: 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 Figure 10.

Figure 9 - Local disk drive

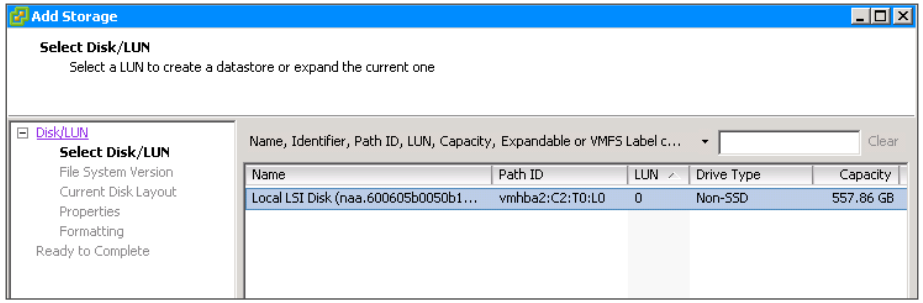
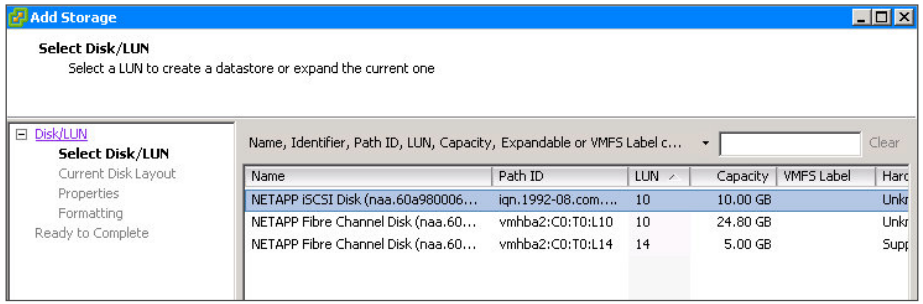


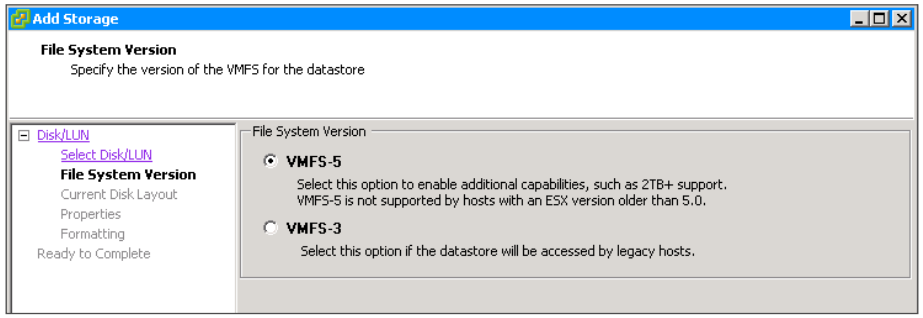
Figure 10 - Shared iSCSI and Fibre Channel LUNs



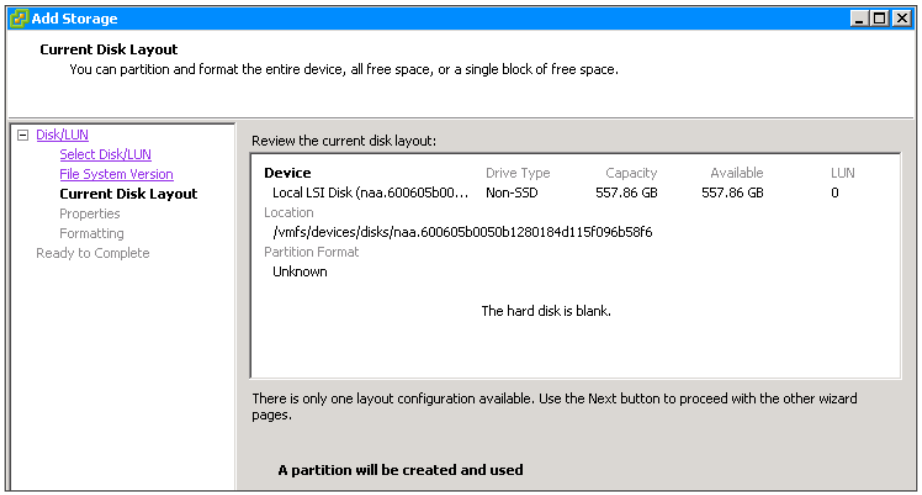
Step 6: On the File System Version page, select **VMFS-5** or **VMFS-3**. Hosts running ESXi 4.x will not be able to access VMFS-5 datastores. Unlike VMFS-3, VMFS-5 uses standard 1 MB file system block size with support of 2 TB+ virtual disks.

Reader Tip

For more information on vSphere 5 VMFS datastores see: http://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.vsphere.storage.doc_50%2FGUID-3CC7078E-9C30-402C-B2E1-2542BEE67E8F.html



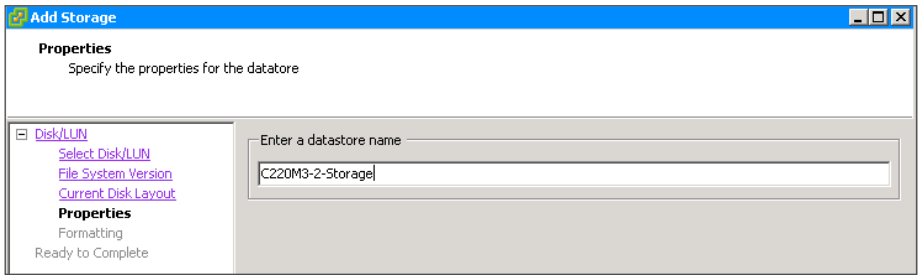
Step 7: Review the disk capacity and partition information, and then click **Next**.



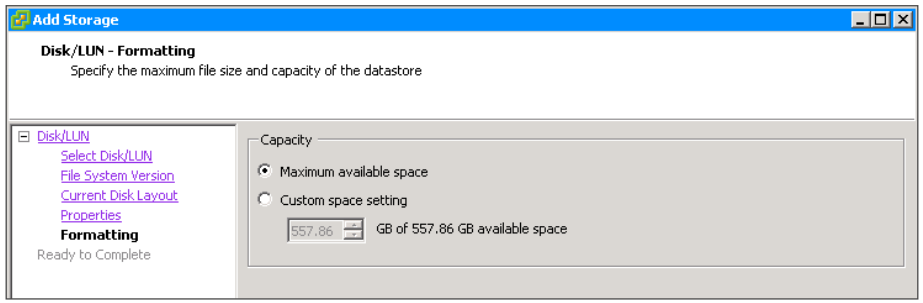
Step 8: Enter a datastore name, and then click **Next**.

Tech Tip

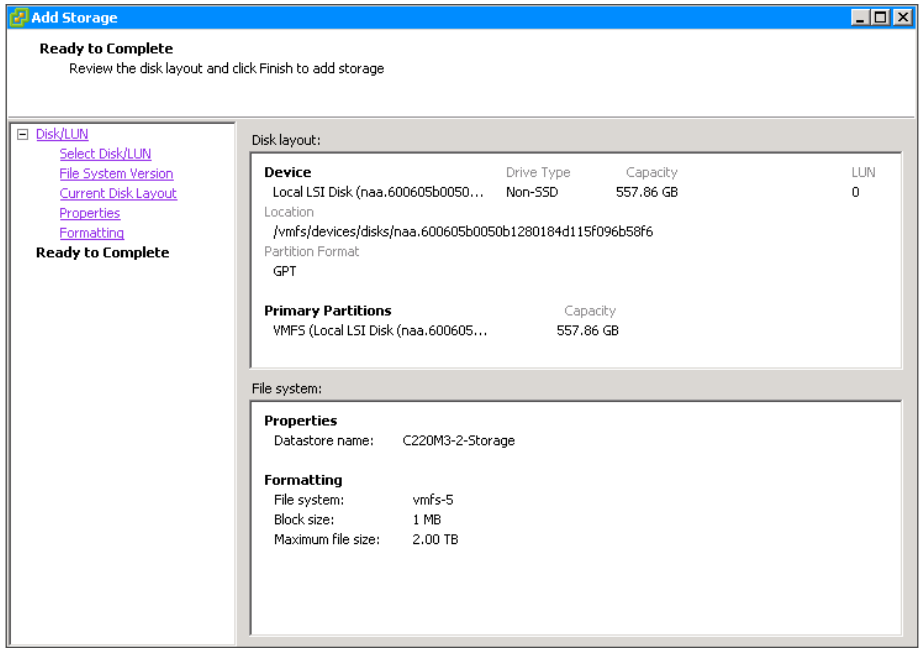
Use a descriptive name for the datastore, to help you identify which datastore is which when you add more of them.



Step 9: On the Disk/LUN Formatting page, accept the defaults by clicking **Next**. This formats the maximum available space in the disk.



Step 10: Click **Finish**. The Add Storage wizard is completed.



Process

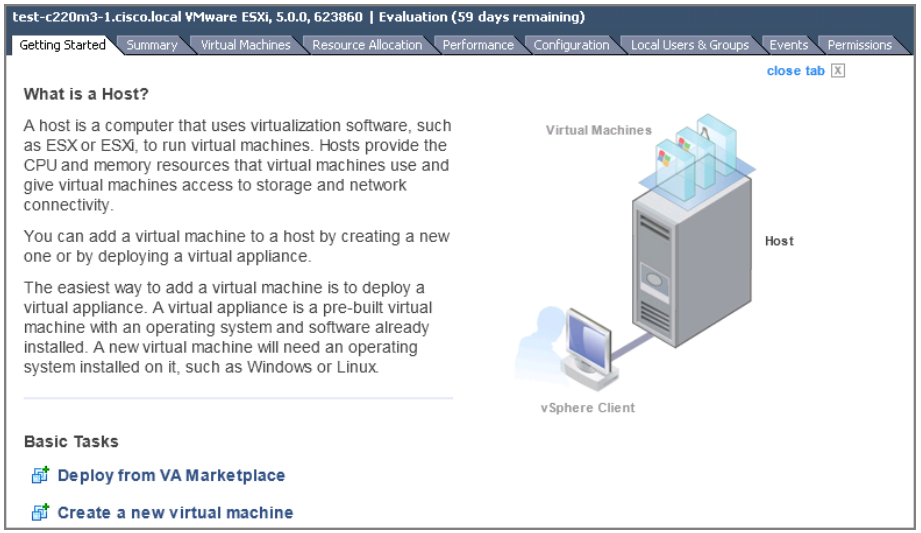
Creating a Virtual Machine

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

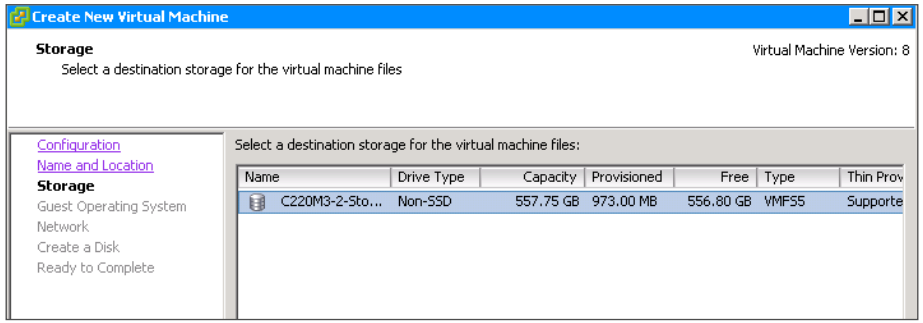
Step 1: In vSphere Client, on the Getting Started tab, click **Create a new virtual machine**.



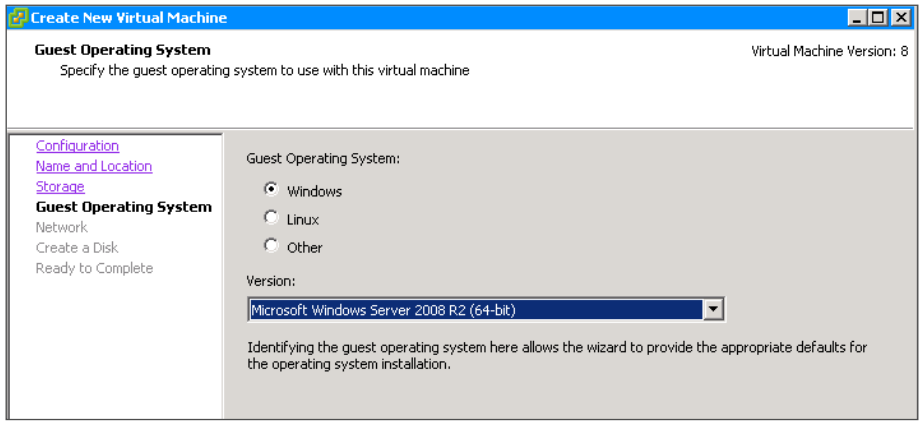
Step 2: On the Configuration page, select **Typical**, and then click **Next**.

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

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



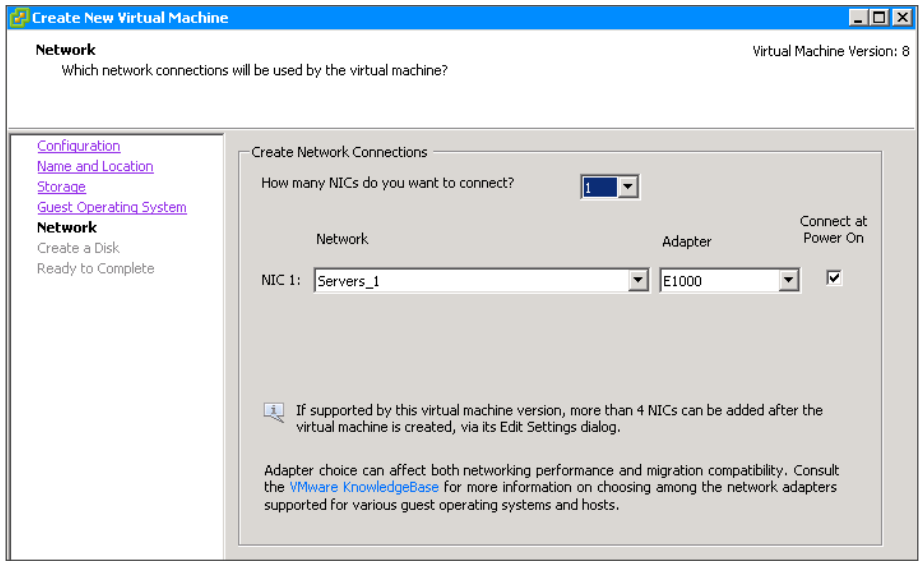
Step 5: Select the guest operating system for the virtual machine, and then click **Next**.



Step 6: On the Network page, enter the following, and then click **Next**:

- How many NICs do you want to connect?—1
- NIC 1—Servers_1
- Adapter—E1000

Depending on the guest operating system that is being installed, a choice of adapter types for each virtual NIC might not be available. If more than one type of adapter is supported, the recommended type for the guest operating system is selected by default.



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.

Reader Tip

For more information regarding adapter type selection see: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1001805

Step 7: On the Create a Disk page, enter a virtual disk size, select a disk format option, and then click **Next**.

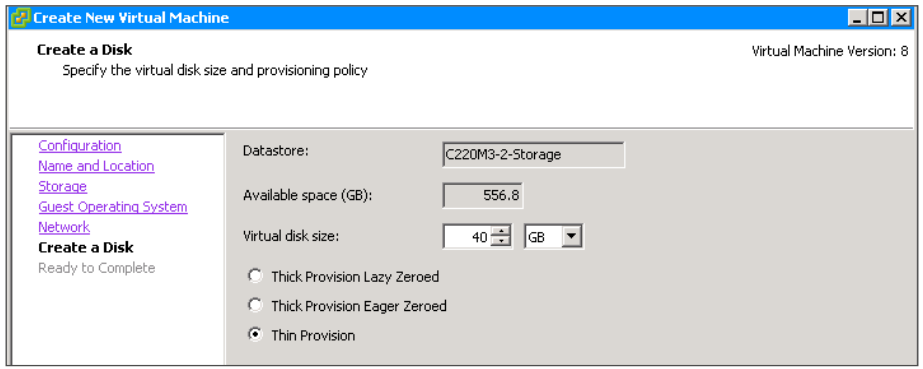
In the following figure, the default disk size of 40 Gb is used. The example uses thin provisioning in order to conserve actual datastore used versus what is provisioned

Select the disk format according to your requirement

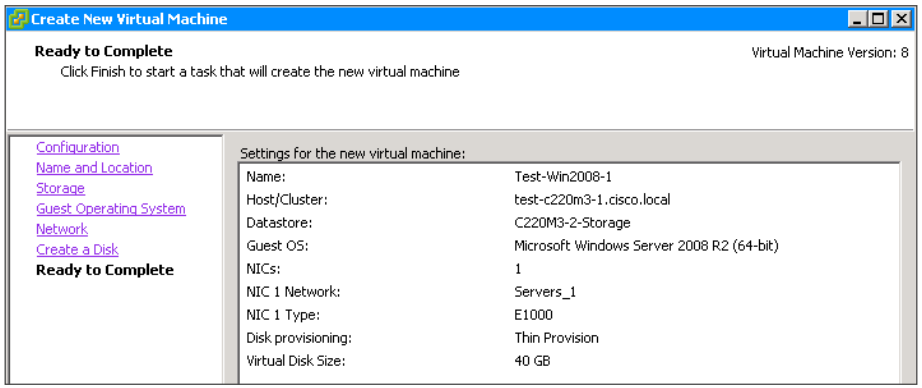
- **Thick Provision Lazy Zeroed**—Space required for the virtual disk is allocated during virtual machine creation. Any data remaining on the physical device is not erased during creation, but it is zeroed out on demand at a later time on first write from the virtual machine.
- **Thick Provision Eager Zeroed**—Space required for the virtual disk is allocated at creation time. Any data remaining on the physical device is zeroed out during virtual machine creation. It might take much longer to create disks in this format than to create other types of disks.
- **Thin Provision**—VMware VMFS starts with a small provisioned disk space on the storage system and then increases the disk space as the system requires more storage.

Tech Tip

Ensure that the disk size matches your operating system requirements and does not exceed the available datastore.



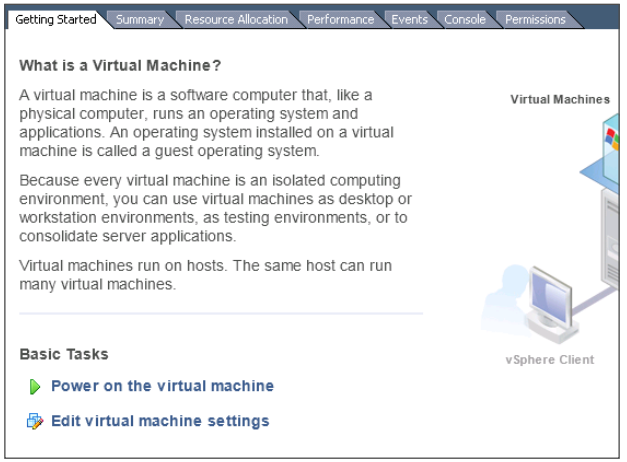
Step 8: On the Ready to Complete page, review the information, and then click **Finish**. The virtual machine is created.



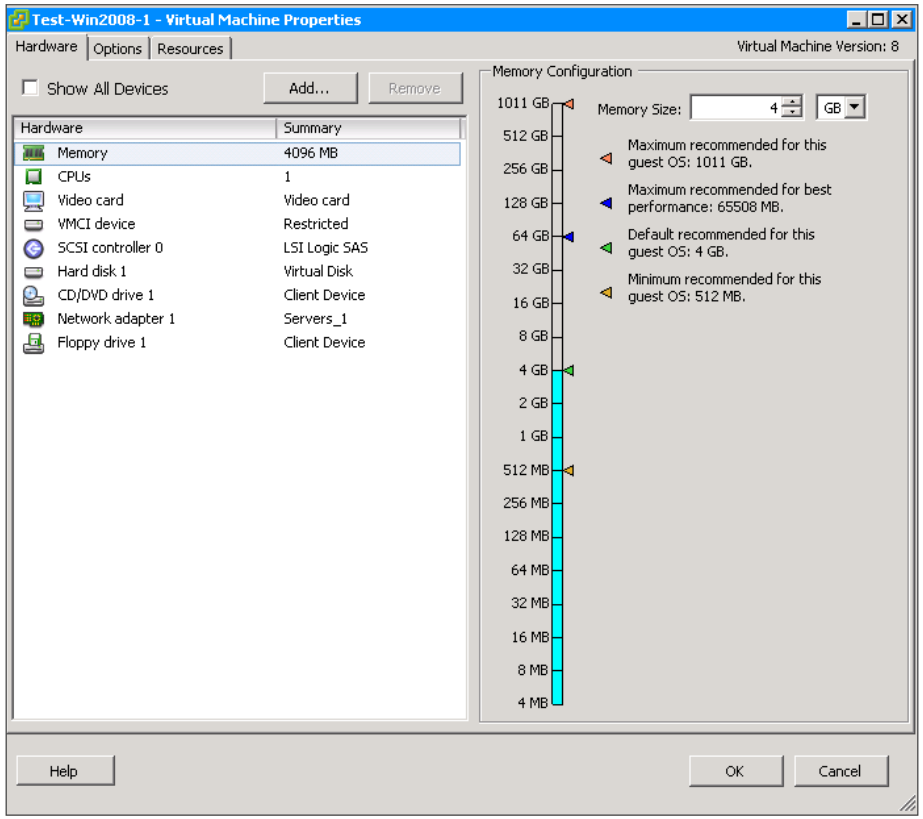
Procedure 2 Edit virtual machine settings

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

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**.



Step 2: On the Virtual Machine Properties dialog box, click the **Hardware** tab, and then make any necessary modifications to the hardware parameters listed.



Step 3: When you are finished editing the parameters, click **OK**.

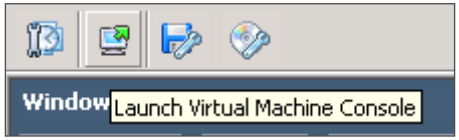
Procedure 3 Install a guest operating system

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.

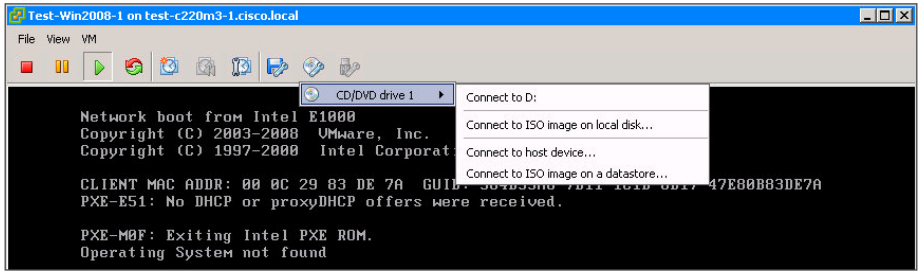


Tech Tip

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.

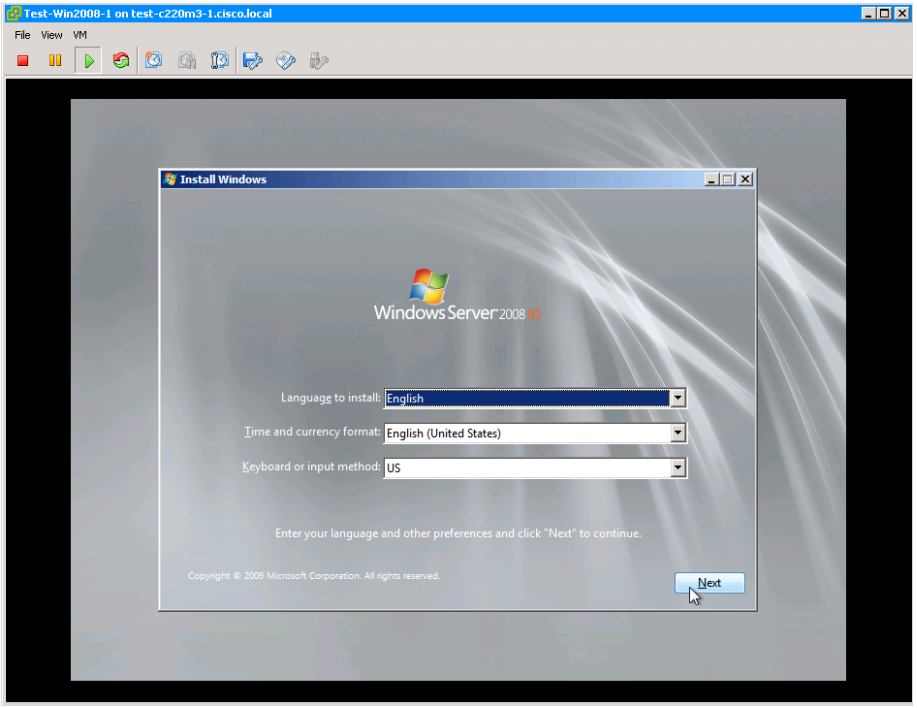


Tech Tip

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, navigate to **Guest**, and then click **Send Ctrl+Alt+Del**. The virtual machine reboots to the attached ISO file.

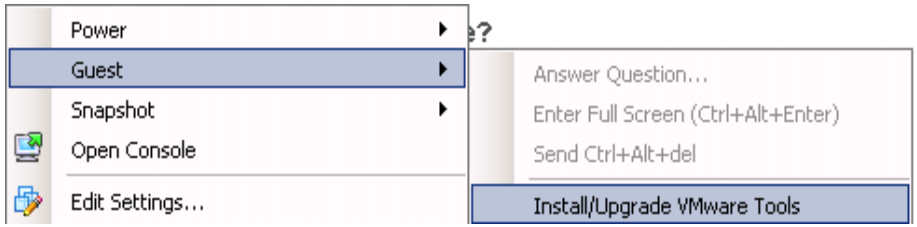
The Install Windows dialog box for Windows 2008 is shown in the following figure. Other operating system installations work similarly; Windows Server 2008 was chosen arbitrarily.



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.

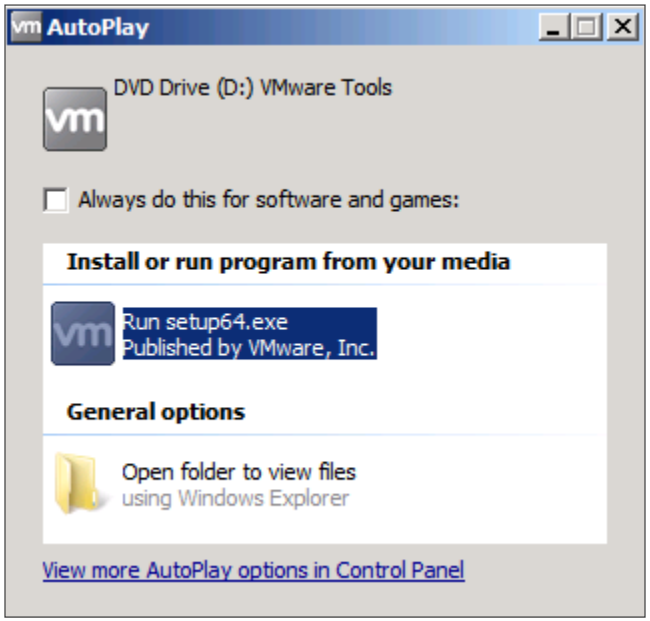
Step 1: In vSphere Client, in the tree, right-click the virtual machine, and then choose **Guest > Install/Upgrade VMware Tools**.



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 11 - Tools install prompt in Windows Server 2008



Tech Tip

Make sure to update VMware tools after each ESXi upgrade.

Process

Installing and Configuring VMware vCenter Server

1. Install VMware vCenter Server
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, high availability, vSphere distributed switches, vSphere Update Manager, or VMware Fault Tolerance, you must set up vCenter Server and configure it accordingly.

In order to install vCenter Server, on the target system, you must do the following:

- Use a 64-bit operating system
- Assign a static IP address
- Configure a computer hostname of no more than 15 characters
- Register the host in DNS as a fully qualified domain name that matches the computer hostname
- Ensure that the host is resolvable with a name server lookup
- Join the vCenter Server to a domain controller
- Make sure that the domain user account has the following permissions:
  - Is a member of the Administrators group
  - Acts as part of the operating system
  - Logs on as a service

Reader Tip

For more information on vCenter Server prerequisites, see the following:
http://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.vsphere.install.doc_50%2FGUID-C6AF2766-1AD0-41FD-B591-75D37DDB281F.html

vCenter Server offers core services in the following areas:

- Host and VM configuration
- Virtual machine provisioning
- Virtual machine inventory management
- Resource management of ESXi hosts and VMs
- Scheduling tasks
- Statistics and logging
- Alarms and event management

Procedure 1 Install VMware vCenter Server

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.

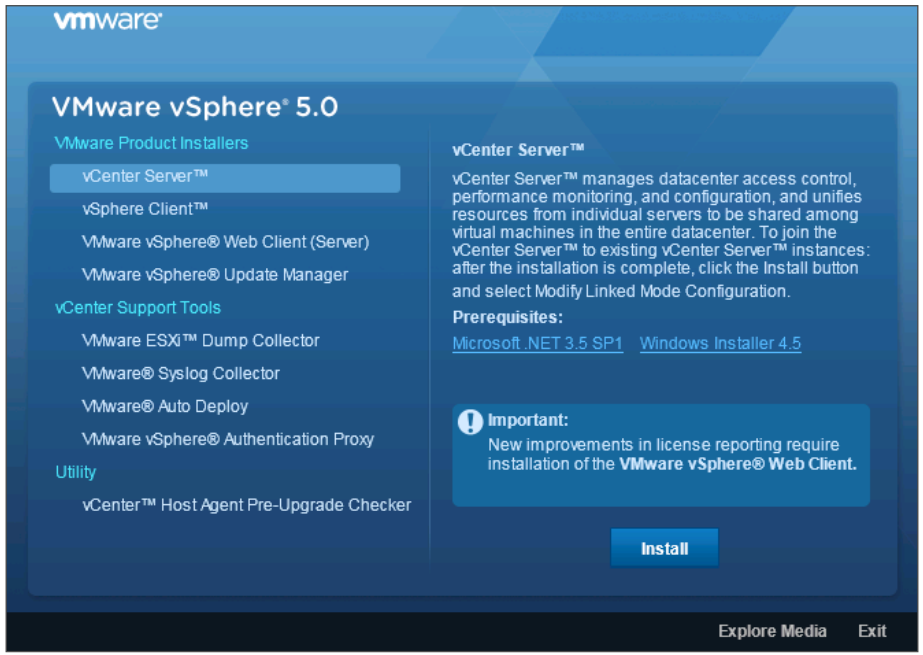
Tech Tip

To function properly, vCenter Server 4.1 and later 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."

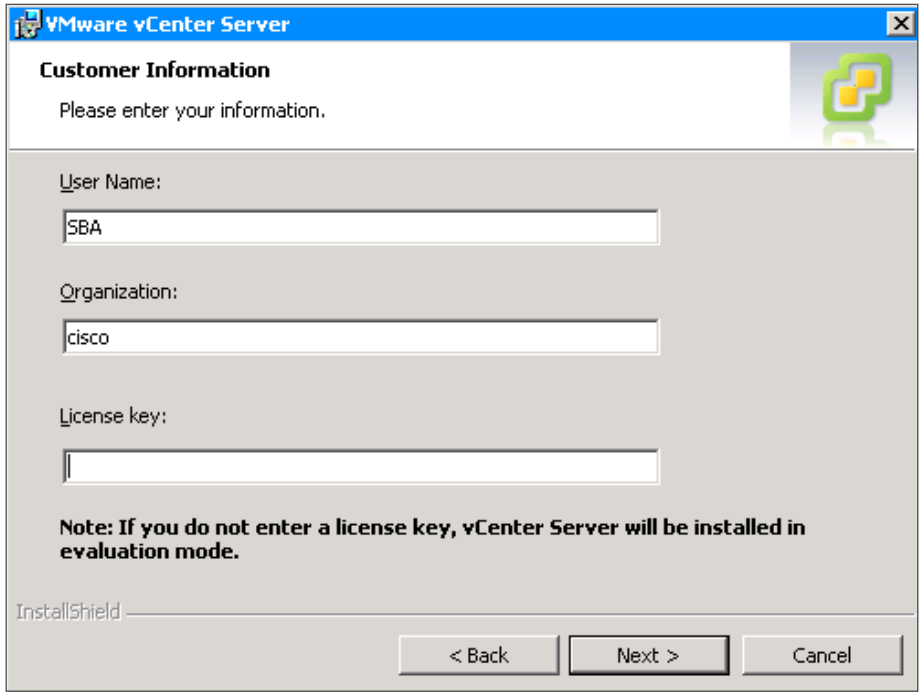
Step 4: Run the VMware vCenter Installer. The following screen appears.



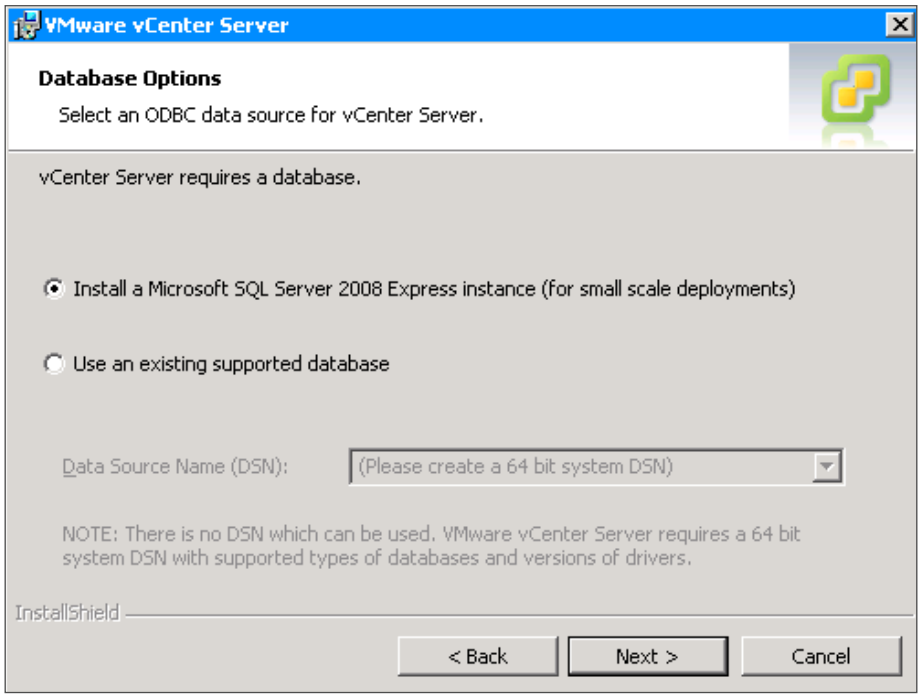
Step 5: Click **vCenter Server**. The VMware vCenter Server wizard starts.

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.



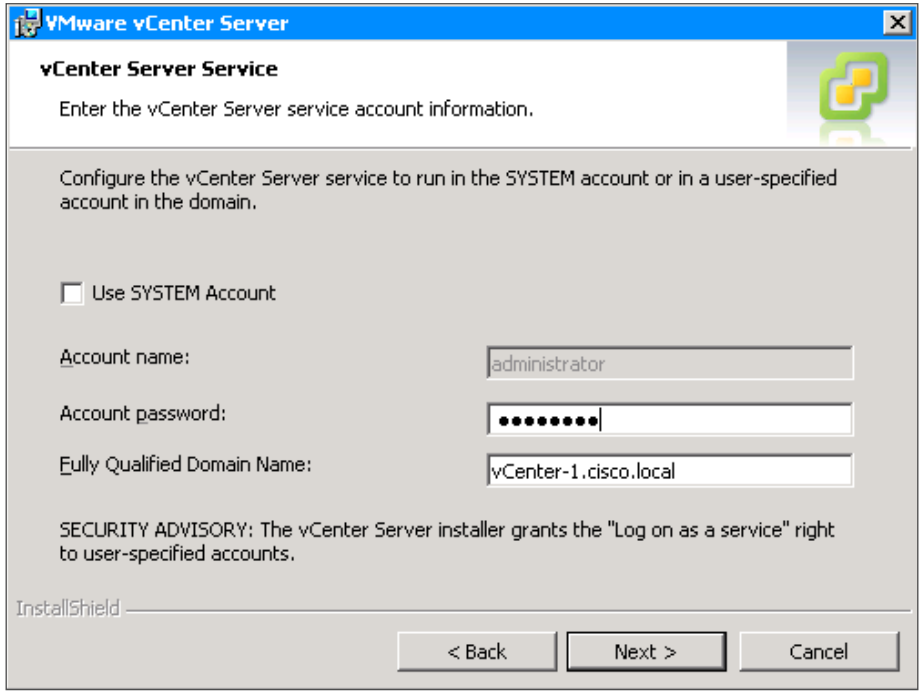
- On the Database Options page, choose an ODBC data source for vCenter Server, and then click **Next**.



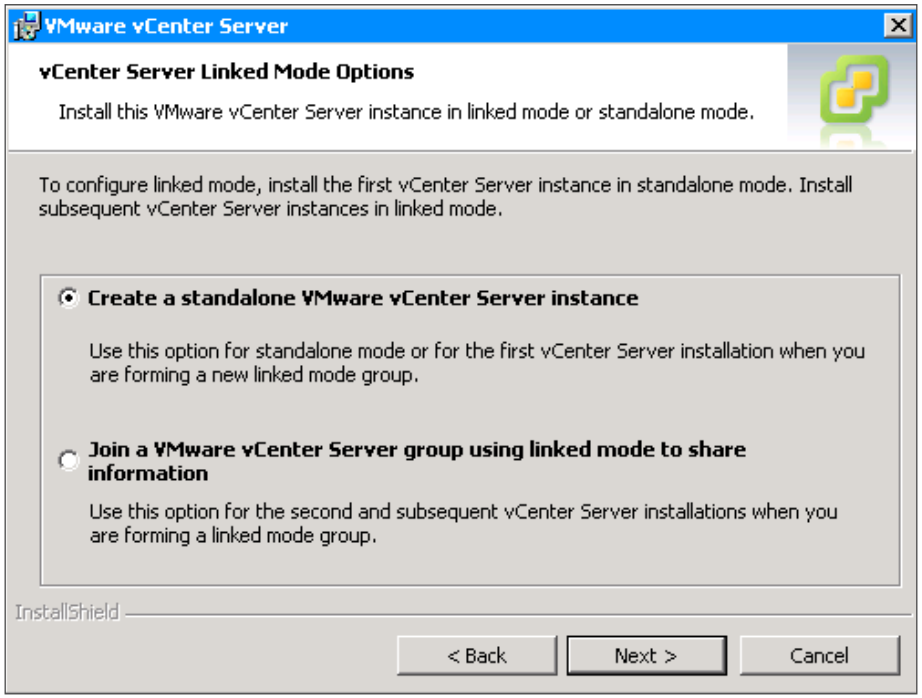
Tech Tip

Many customers purchase their own SQL database for this use. This example uses Microsoft SQL Server 2008 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. Click **Next**.

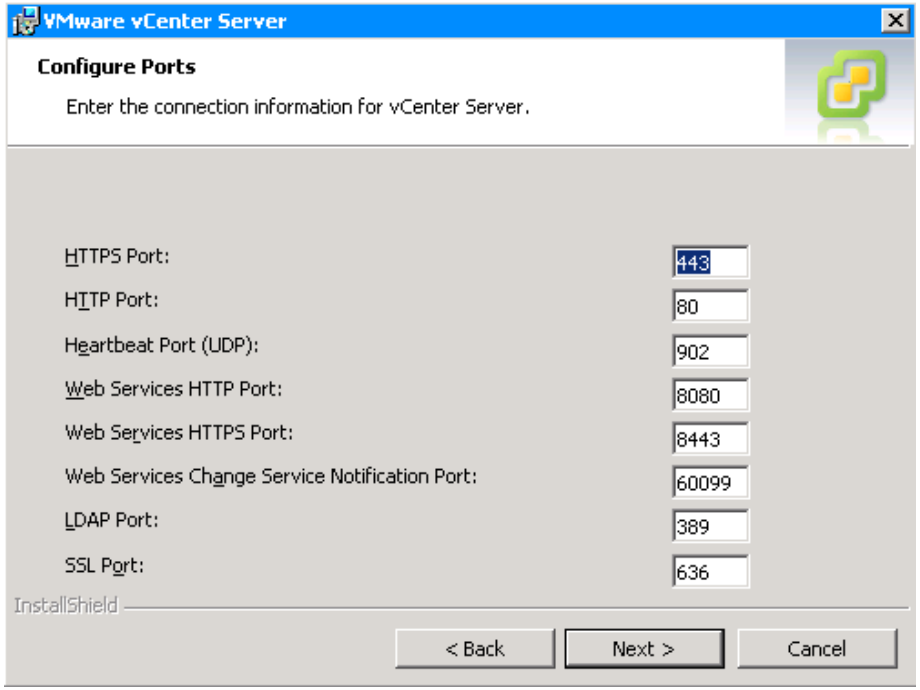


- On the vCenter Server Linked Mode Options page, for this example, select **Create a standalone VMware vCenter Server instance**, and then click **Next**.



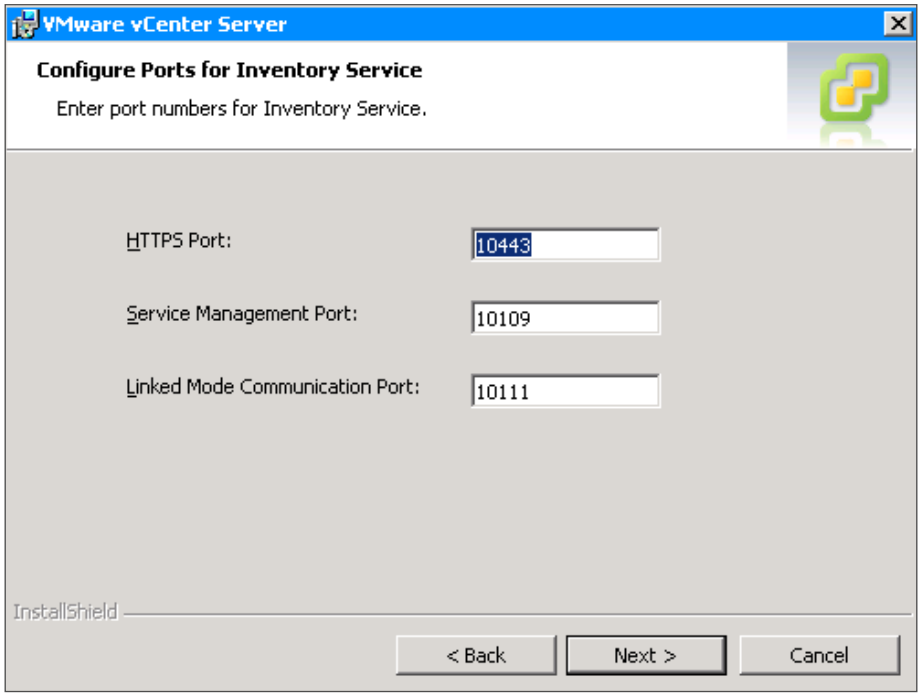
- If vCenter services need to run on different ports for security or policy reasons, on the Configure Ports page, enter the appropriate ports, and then click **Next**.

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

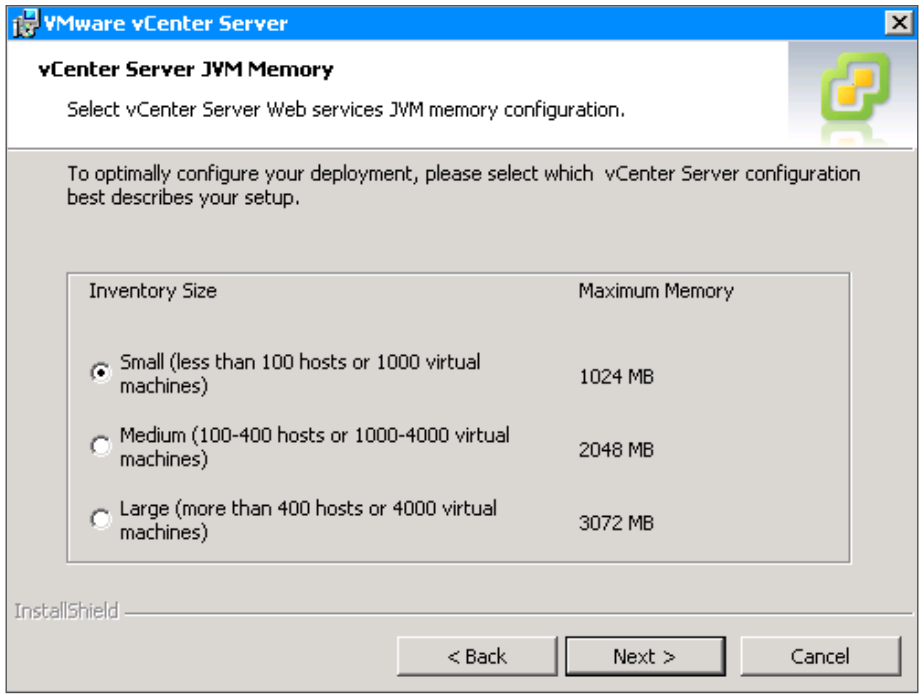


- If you want to use the default inventory service ports, on the Configure Ports for Inventory Service page, accept the defaults, and then click **Next**.

  If you want to select the inventory service ports, enter the port numbers, and then click **Next**.



- Select the size of your deployment. In this example, the Inventory Size is **Small**, because the deployment has less than 100 hosts. Click **Next**.



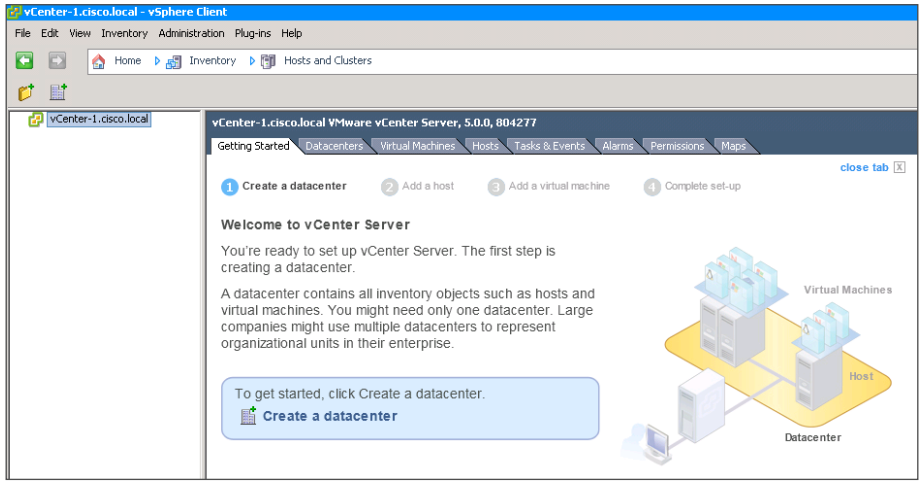
- Continue following the instructions in the wizard, accepting default values, until it finishes.

Procedure 2 Create a data center

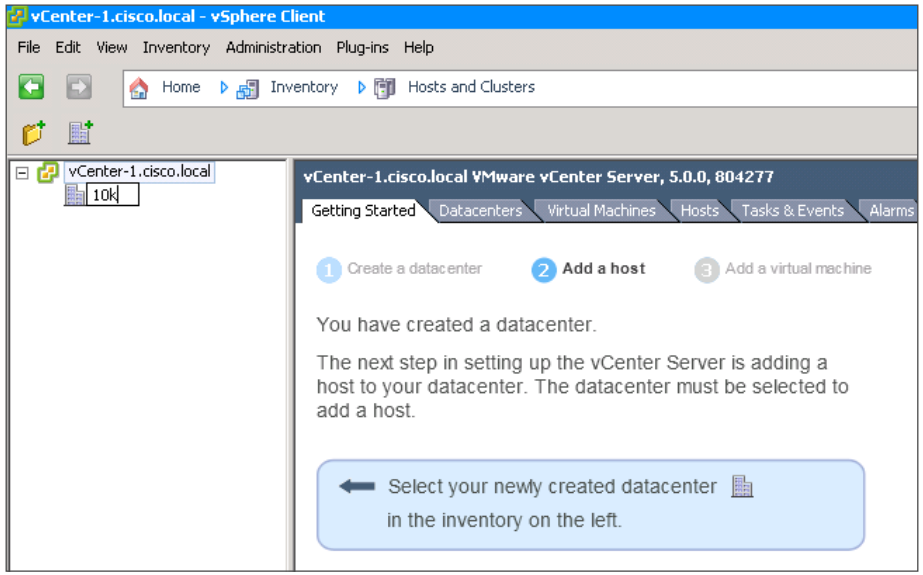
Now that vCenter is installed, you must configure it to manage the previously installed ESXi hosts. To do so, you must first create the data center to which you will add the ESXi hosts.

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

Step 2: On the Getting Started tab, click **Create a datacenter**.



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



Procedure 3 Create a cluster

(Optional)

A *cluster* is a collection of multiple ESX or ESXi hosts and associated virtual machines with shared resources and a shared management interface. When you add an ESX or 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 vSphere high availability (HA) and Distributed Resource Scheduler (DRS). vSphere 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.

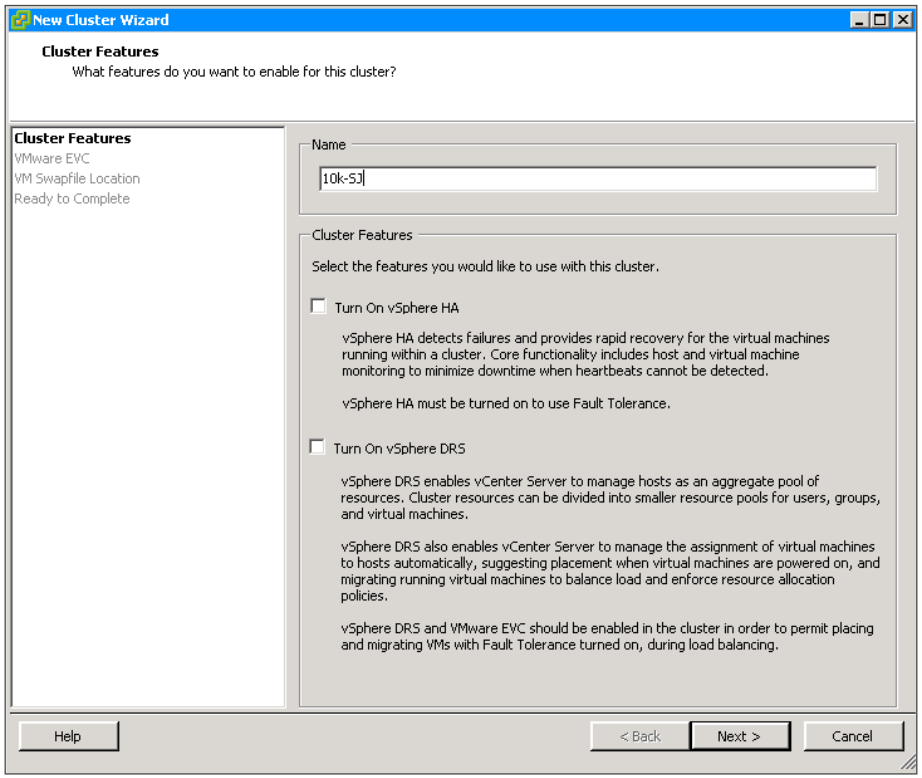
Step 1: In the Inventory tree, right-click **Datacenter**, and then click **New Cluster**.

Step 2: In the New Cluster Wizard, on the Cluster Features page, enter an appropriate name for the cluster, and then click **Next**.

Tech Tip

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

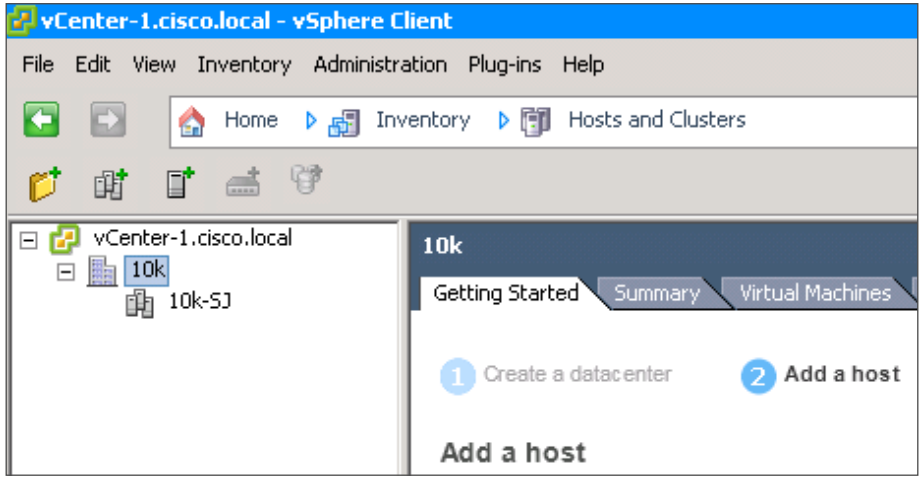
For more information about high availability, please see the following:
http://www.vmware.com/pdf/vmware_ha_wp.pdf



Step 3: On the VMware EVC page, accept the defaults, and then click **Next**.

Step 4: On the VM Swapfile Location page, accept the defaults, and then click **Next**.

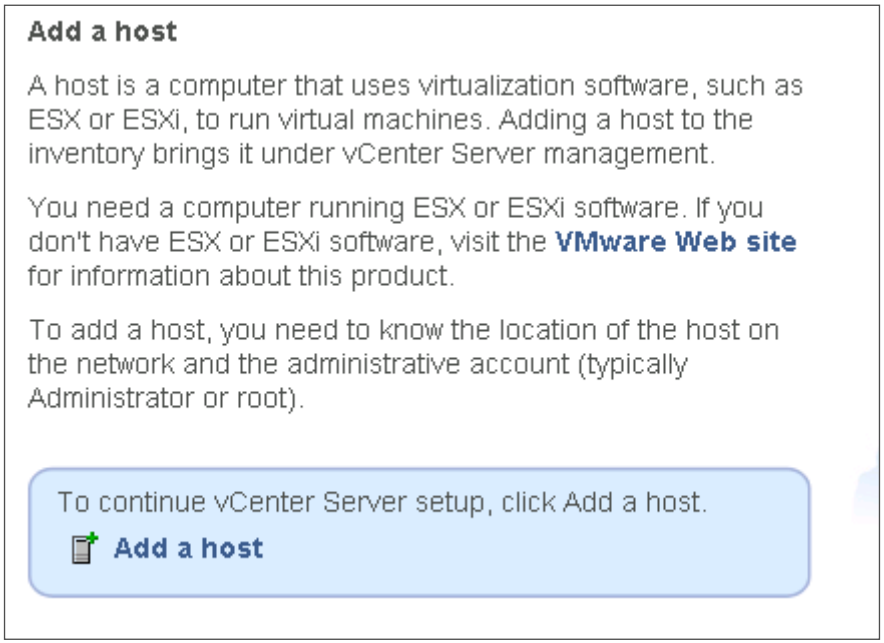
Step 5: On the Ready to Complete page, click **Finish**. This completes the creation of a cluster. When a cluster has been created, you can add ESXi hosts to the cluster by dragging the host into the cluster in the navigation pane.



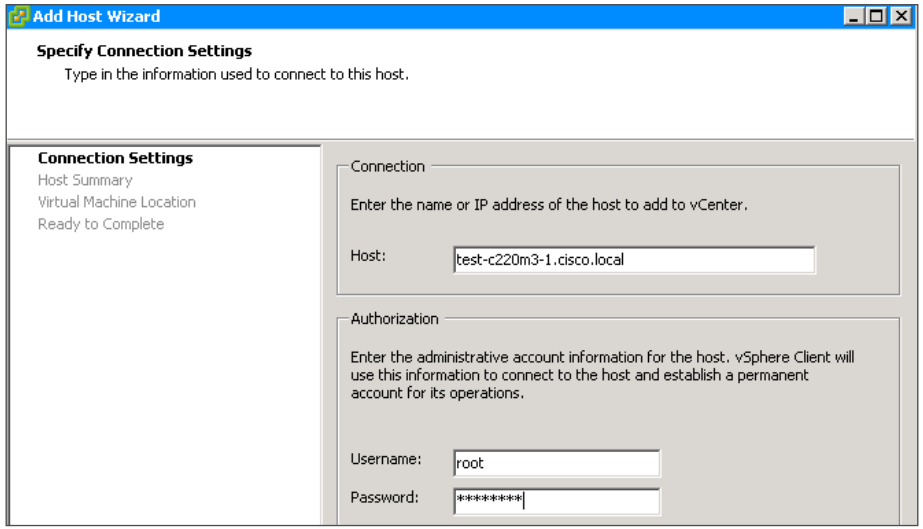
Procedure 4 Add an ESXi server to the data center

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

Step 1: On the Getting Started tab, click **Add a Host**.



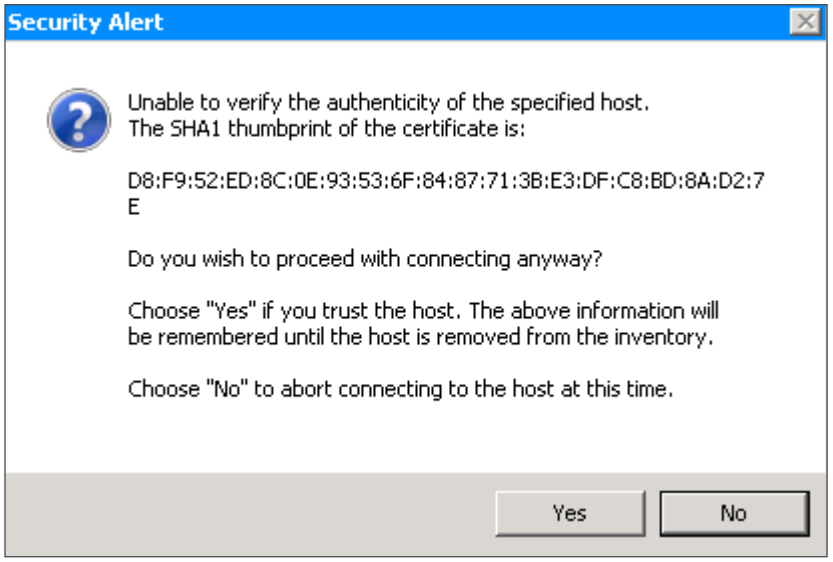
Step 2: In the Add Host Wizard, enter the name or IP address, username, and password you configured in Procedure 1"Configure the management network," and then click **Next**.



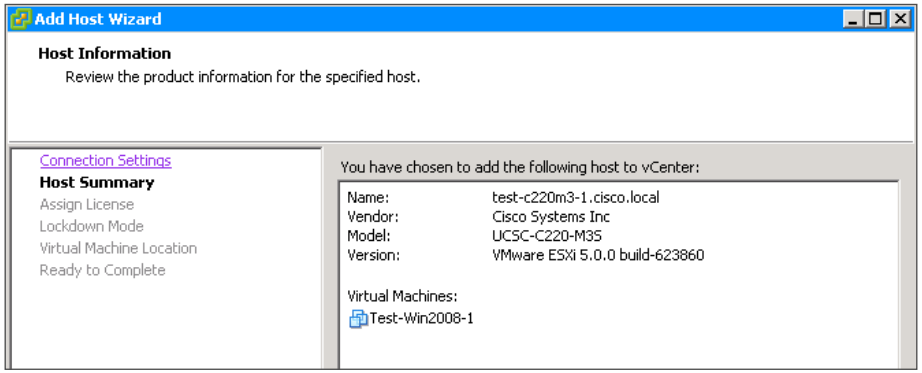
Tech Tip

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 Alert message that appears, click **Yes**. The message appears because this is the first time this host has been seen by the vCenter.

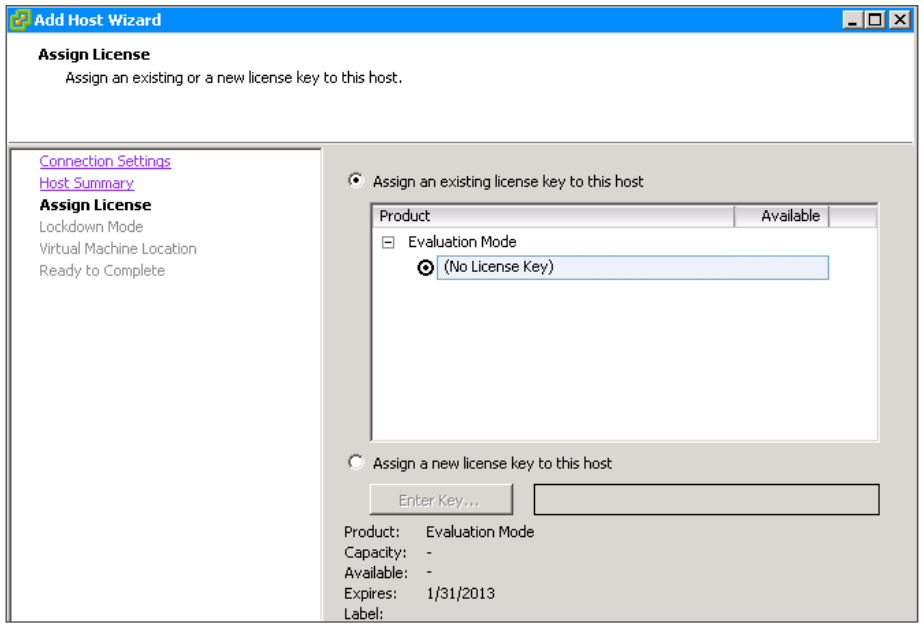


Step 4: Verify that this is the correct host, and then click **Next**.



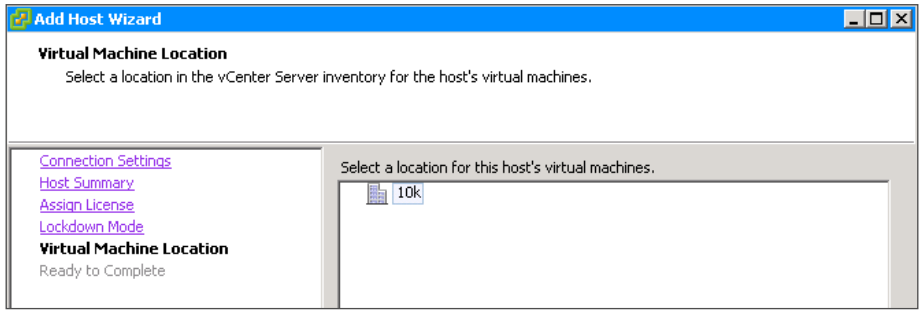
Step 5: If you have a license to assign to this host, select **Assign a new license key to this host**, enter the key, and then click **Next**.

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

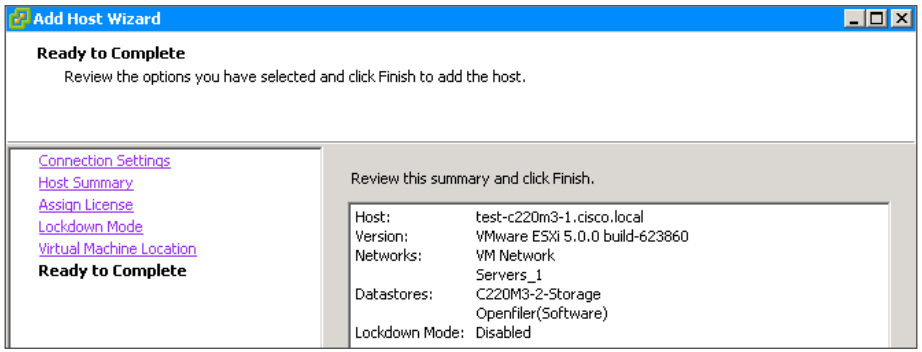


Step 6: On the Configure Lockdown Mode page, click **Next**. For this example, lockdown mode is not used.

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: On the Ready to Complete page, review the information, and then click **Finish**. vCenter is ready to add the ESXi host into its inventory.

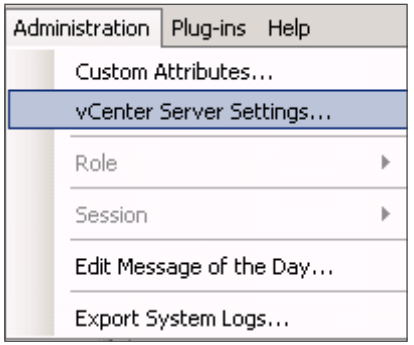


The wizard is finished. In the vCenter tree, a new host appears under the data center you created earlier.

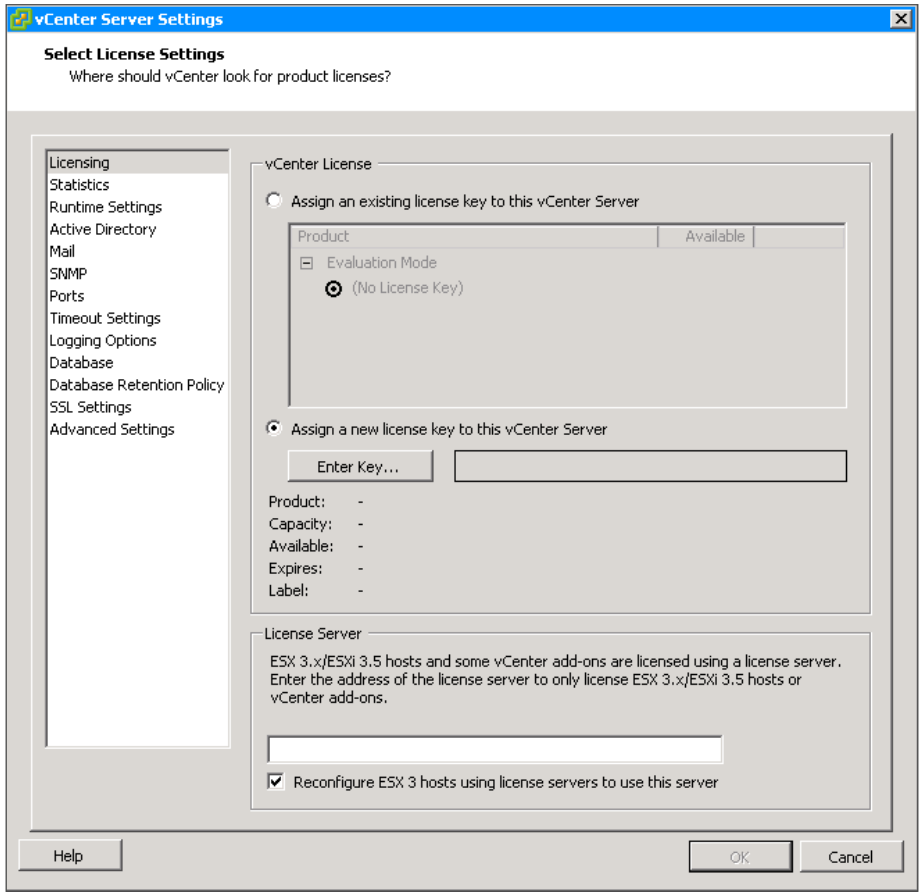
Procedure 5 License vCenter

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.

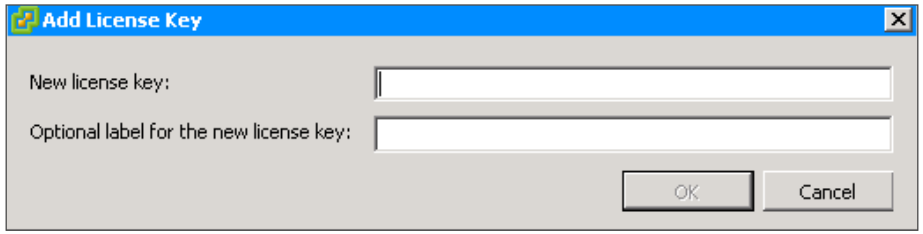
Step 1: On the top menu bar in vCenter, navigate to **Administration > vCenter Server Settings**.



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**.



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



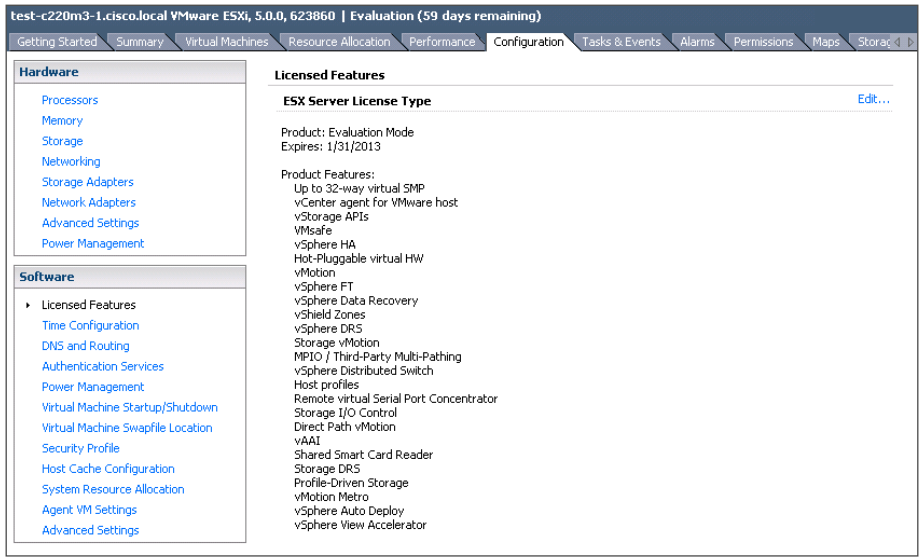
Step 4: On the vCenter Server Settings dialog box, click **OK**.

Procedure 6 License ESXi hosts

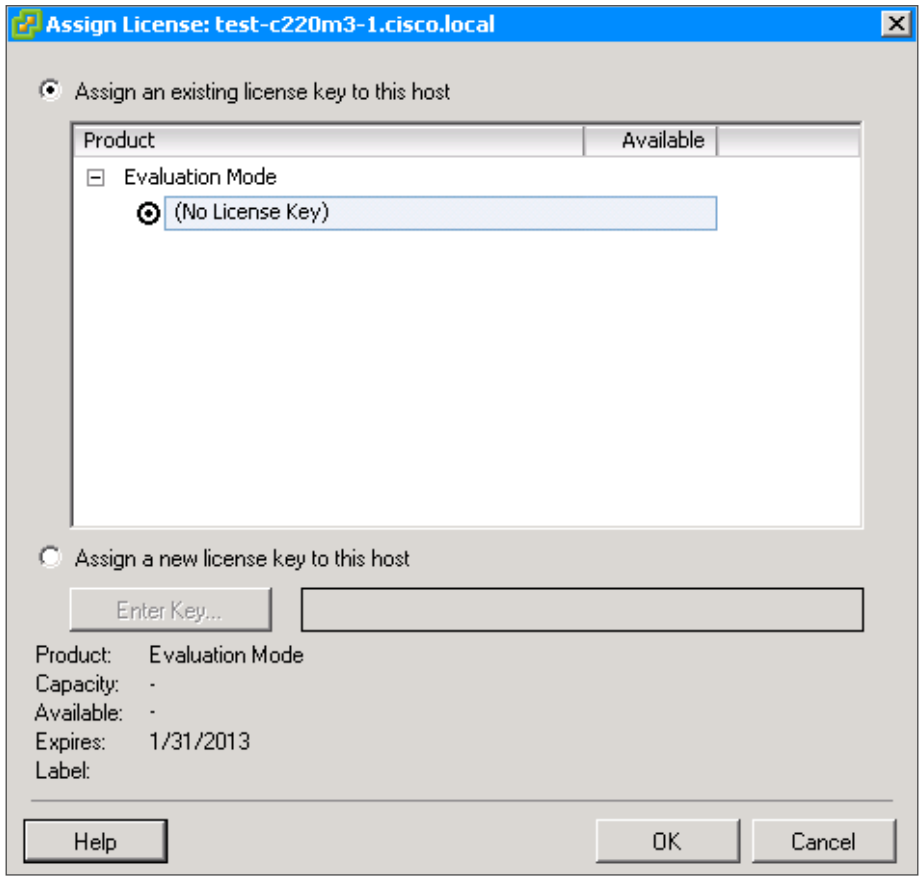
If you have already licensed the ESXi hosts, skip this procedure. VMware allows ESXi hosts to run for 60 days on an evaluation license. To run your host longer, you must acquire and provide a new license key. For more information, see the VMware documentation. Be sure you are using a license for ESXi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

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

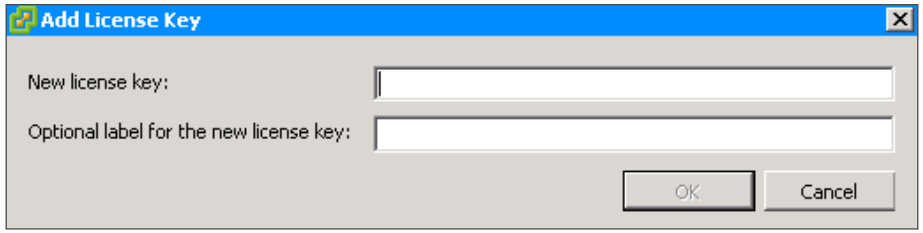
Step 2: On the Configuration tab, in the Software list, select **Licensed Features**, and then in the upper right corner, click **Edit**.



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

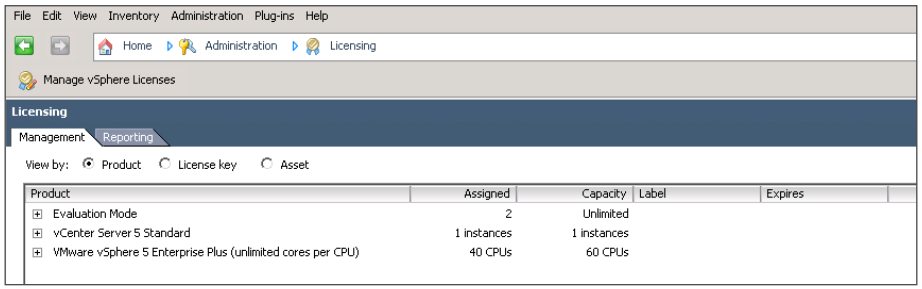


Step 4: Enter the license key (including dashes), and then click **OK**.



Step 5: On the Assign License dialog box, click **OK**.

Step 6: If you want to view the license keys available in the vCenter Server license inventory, in the vSphere client, select **Home** > **Licensing**.



Process

Installing VMware vSphere Update Manager

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

VMware vSphere Update Manager (VUM) is a tool that streamlines the process of scanning and applying patches or upgrades to VMware ESX or 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 or ESXi hosts, virtual machines, and templates. Updating your virtual machines, appliances, and ESX or 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.

In order to install VMware vSphere Update Manager Server, on the target system, on the target system, you must do the following:

- Use a 64-bit operating system
- Assign a static IP address
- Configure a computer hostname of no more than 15 characters
- Register the host in DNS as a fully qualified domain name that matches the computer hostname
- Ensure that the host is resolvable with a name server lookup
- Join the vCenter Server to a domain controller
- Make sure that the domain user account has the following permissions:
  - Is a member of the Administrators group
  - Acts as part of the operating system
  - Logs on as a service

Before proceeding with this procedure, please visit the VMware website 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 2008 Express Edition, which is included in the VMware vCenter media, or 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.

Reader Tip

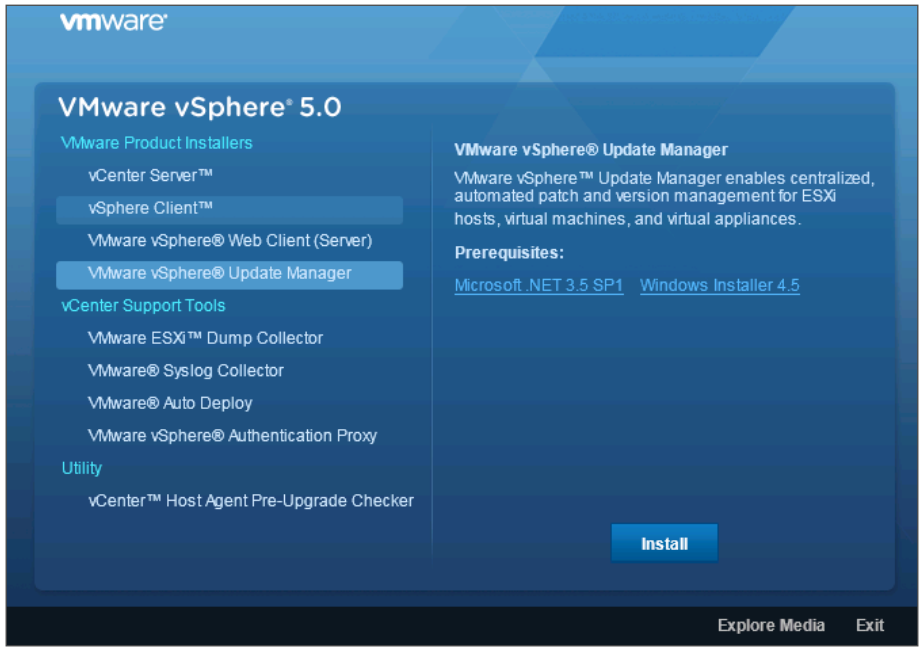
For hardware and software requirements, refer to the VMware vSphere Update Manager documentation for more information: http://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.update_manager.doc_50%2FGUID-B5FB88E4-5341-45D4-ADC3-173922247466.html

Procedure 1 Install VUM

In this procedure, you install VUM on a new VM and use an instance of SQL Server 2008 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 VMware Product Installers, select **VMware vSphere Update Manager**.



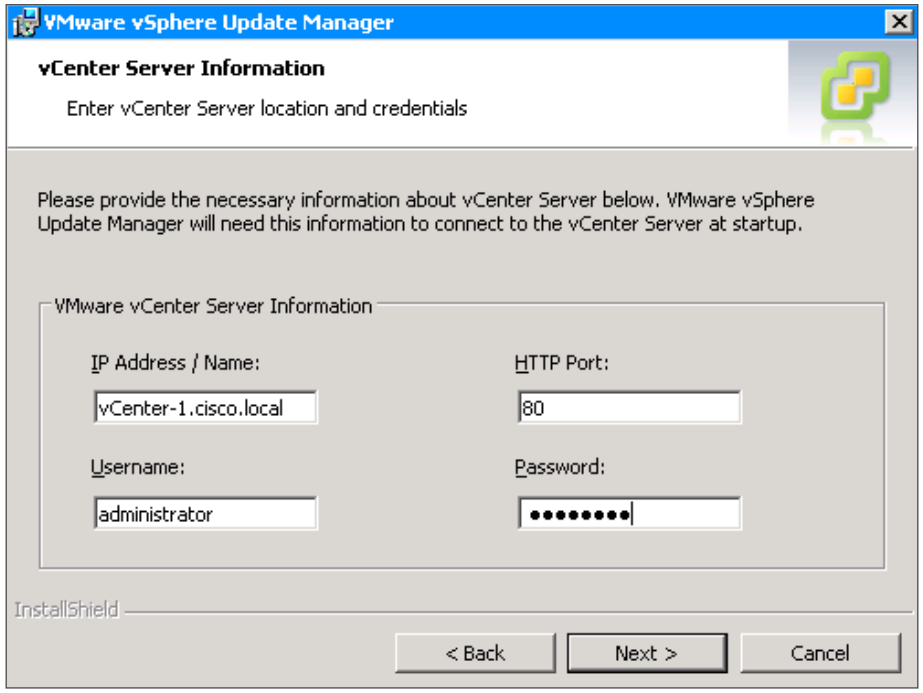
Step 3: Choose the correct language for the installation, and then click **OK**.

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

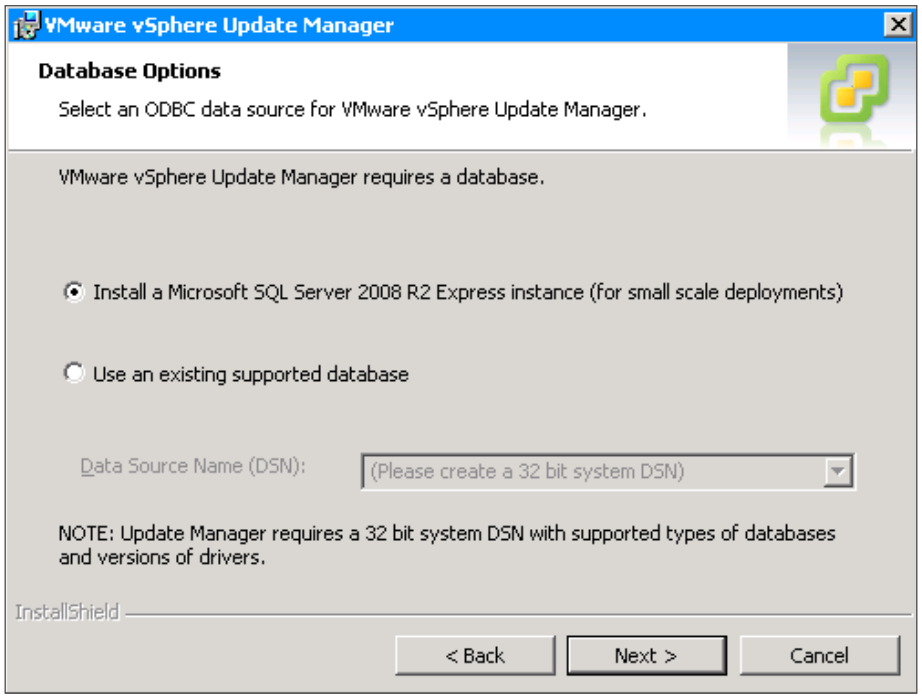
Step 5: Read and accept the VMware End User License Agreement, and then click **Next**.

Step 6: On the Support Information page, leave the default settings, and then click **Next**.

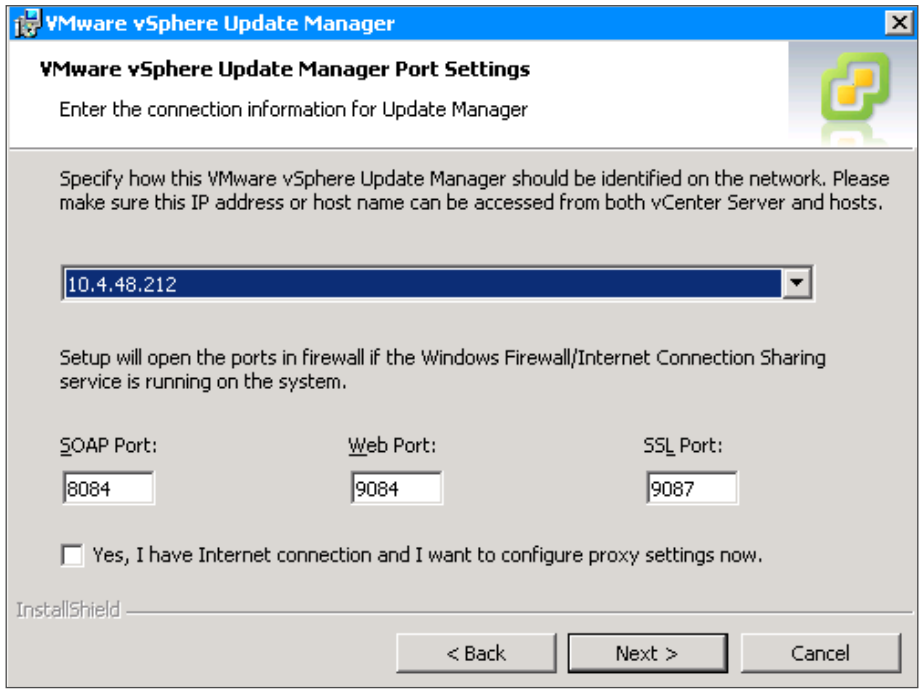
Step 7: Enter the IP address, username, password, and HTTP port of the vCenter Server instance to which you want to associate this VUM, and then click **Next**.



Step 8: Select **Install a Microsoft SQL Server 2008 R2 Express instance (for small scale deployments)**, and then click **Next**.

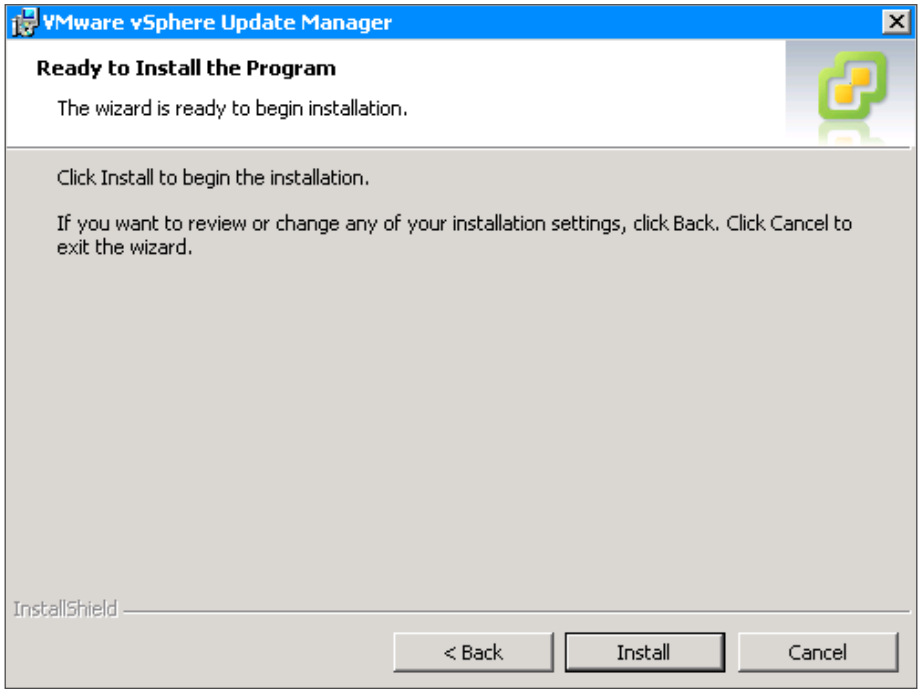


Step 9: On the VMware vSphere Update Manager Port Settings page, leave the default settings, and then click **Next**.



Step 10: On the Destination Folder page, 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.

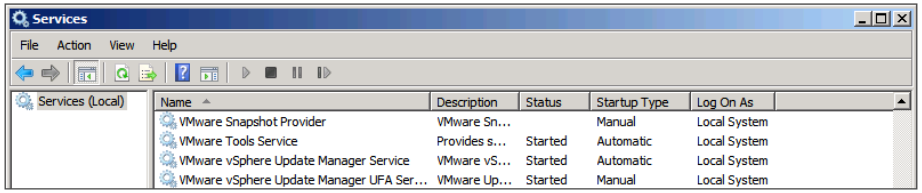
Step 11: Click **Install**.



Step 12: When the installation is complete, click **Finish**.

Step 13: From the computer where VUM was installed, run **services.msc** from a command prompt, and then click **OK**. This launches the Services console.

Step 14: Scroll down to the VMware vSphere Update Manager Service, and make sure the service is started. If it is not, right-click the VMware vSphere Update Manager Service, and then click **Start**.



Procedure 2 Install vSphere Update Manager plug-in

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

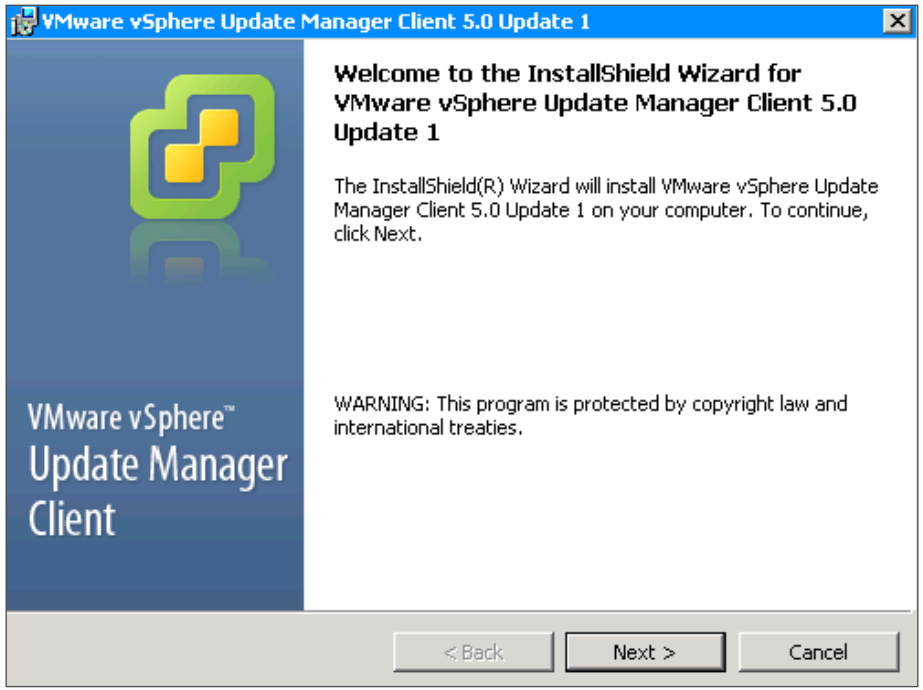
Step 1: Launch vSphere Client, and then connect to your vCenter Server instance.

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

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

Step 4: Select a language for the installer, and then click **OK**.

Step 5: In the InstallShield Wizard for VMware vSphere Update Manager Client, click **Next**.

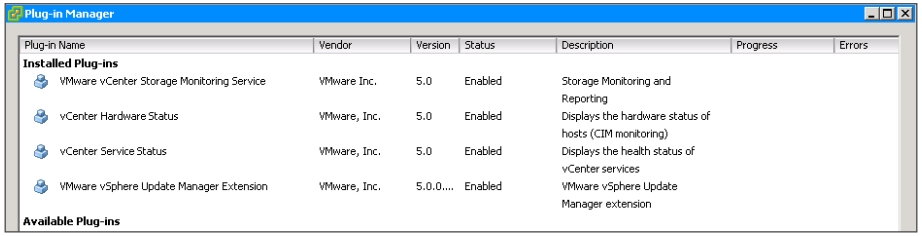


Step 6: On the License Agreement page, accept the license, and then click **Next**.

Step 7: Click **Install**.

Step 8: After installation is complete, click **Finish**.

Step 9: In the Plug-in Manager window, under Installed Plug-ins, make sure the VMware vSphere Update Manager Extension is displayed as **Enabled**, and then click **Close**.



Procedure 3 Configure VUM

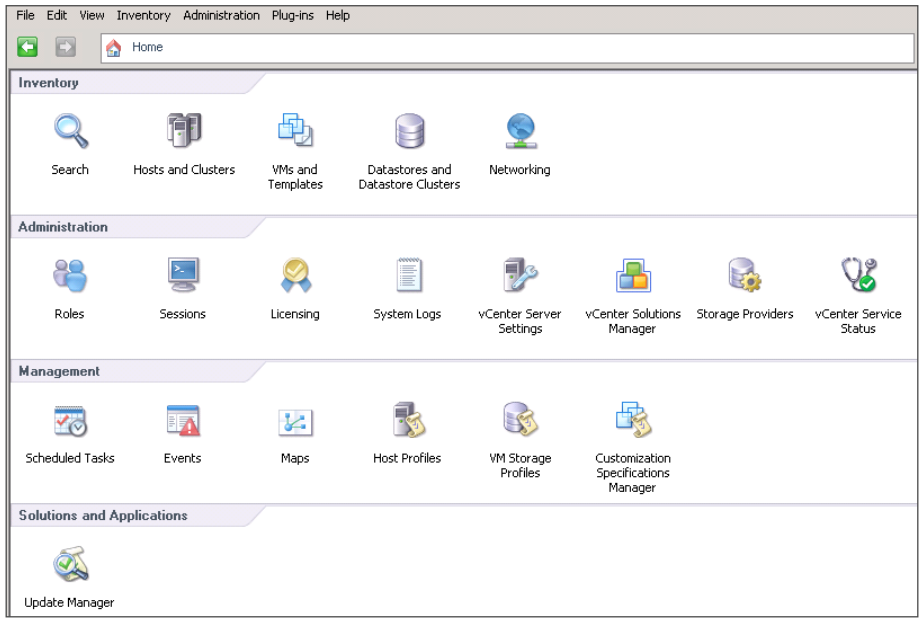
vSphere Update Manager includes many default baselines that can be used to scan any virtual machine, virtual appliance or host in order to determine if they have all patches applied or if they need to be upgraded to latest version.

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

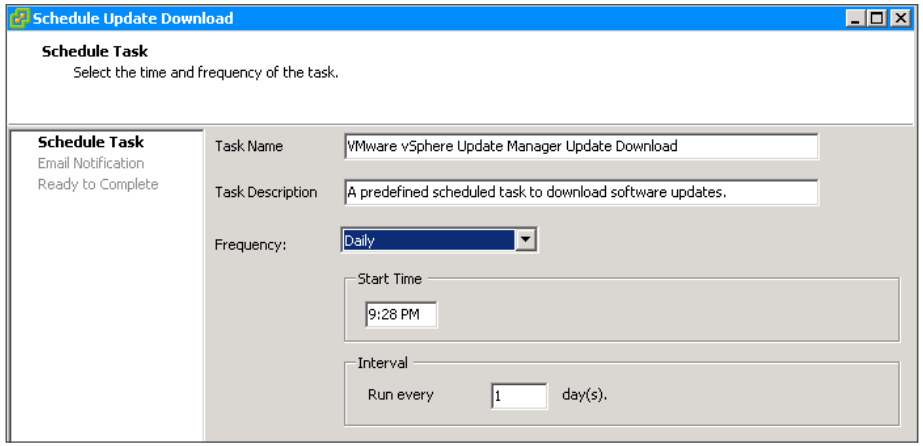
In this procedure, you check whether ESX or ESXi hosts are compliant with all critical and optional patches. Also, you apply patches for non-complying hosts.

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

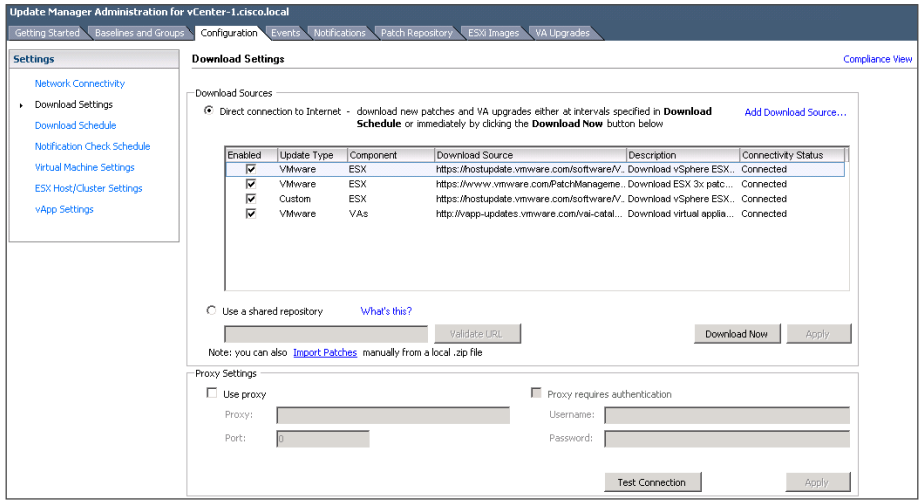


Step 2: Navigate to the Configuration tab, select **Download schedule**, and then make sure the **State** check box is selected.

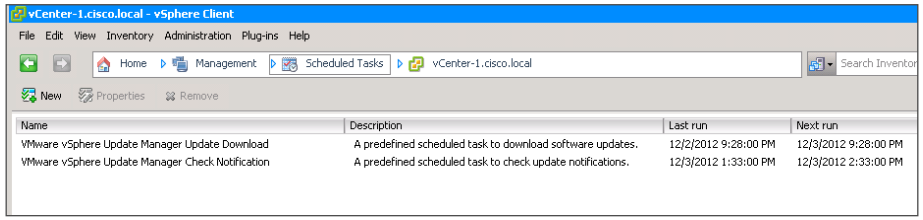
Step 3: If you want to modify how frequently the patch definitions are downloaded, click **Edit Download Schedule**. The Schedule Update Download wizard opens. On the Schedule Task page, in the **Frequency** list, choose the frequency with which the patch definitions are downloaded, and then complete the wizard.



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

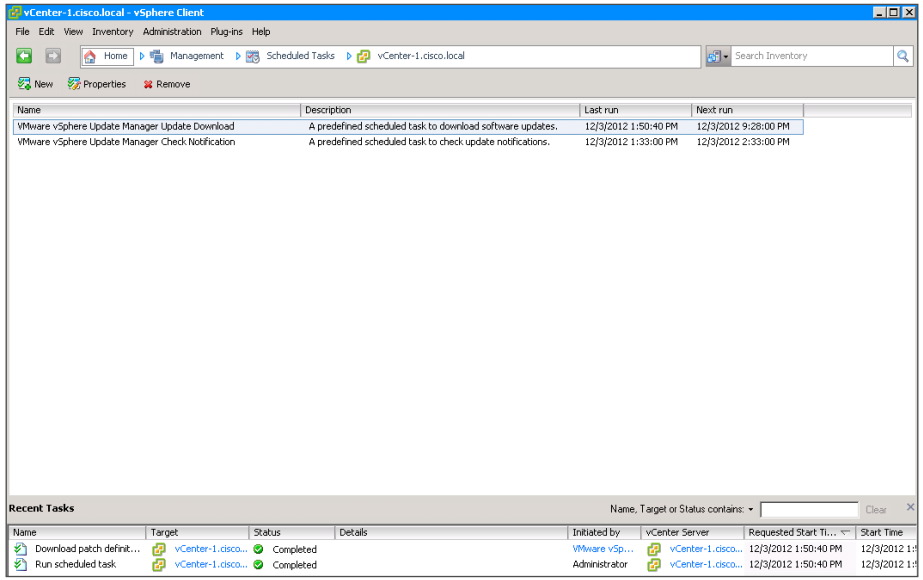


Step 5: Navigate to **Home > Management**, and then click **Schedule Task**. This shows when you are scheduled to download patch definitions. In the next step, you manually run this task.

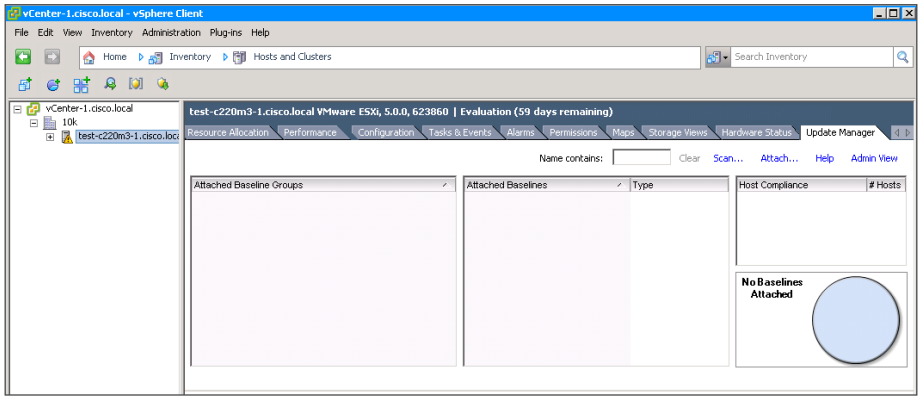


Step 6: Right-click **VMware vSphere Update Manager Update Download**, and then click **Run**. This downloads the patch definitions from the VMware site.

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



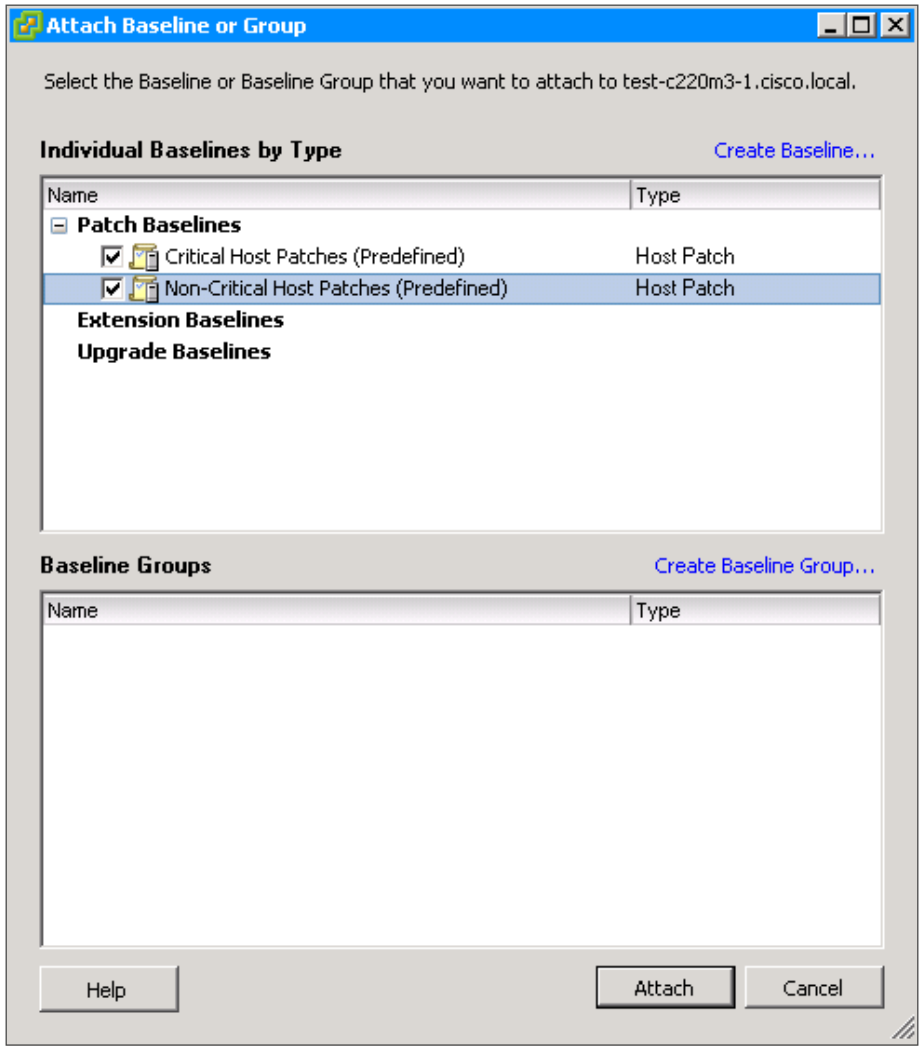
Step 8: Navigate to **Home > Inventory > Hosts and Clusters**, select the host on which you want to install the patches, navigate to the **Update Manager** tab, and then click **Attach**.



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

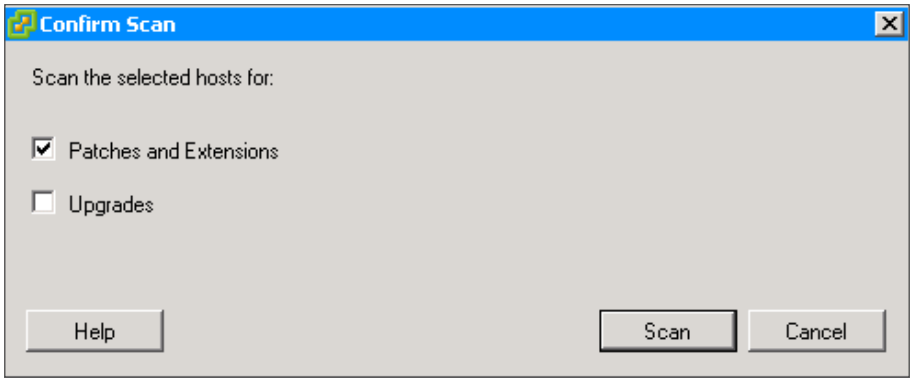
Reader Tip

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

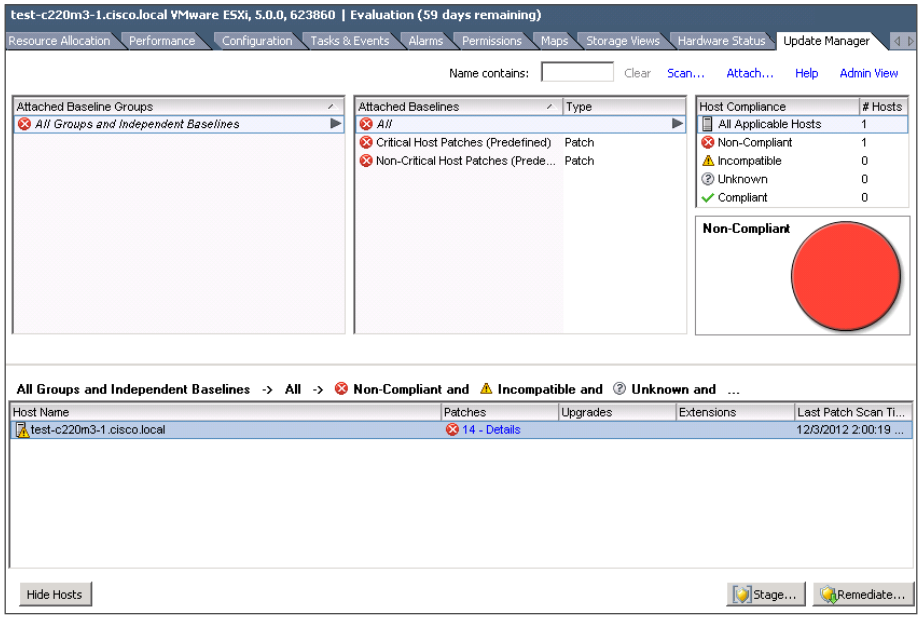


Step 10: Right-click the host to which you attached the default patch baselines, and then choose **Scan for Updates**.

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



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

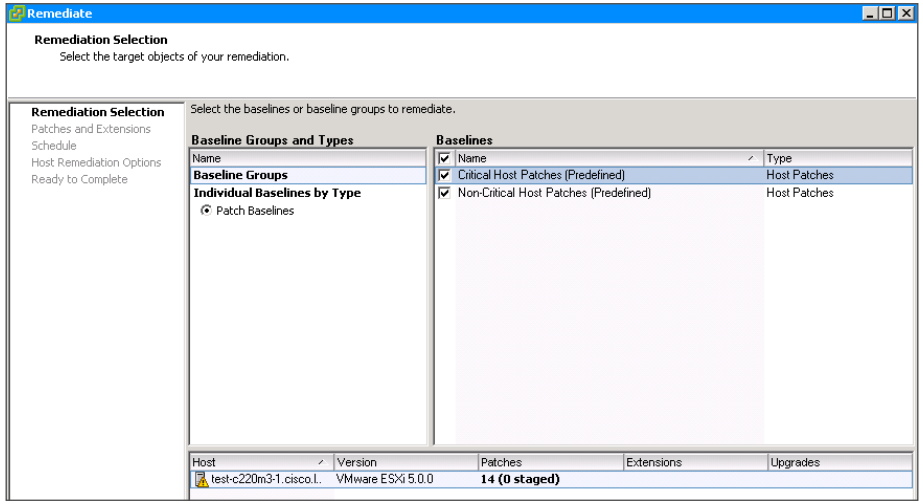


Next, you remediate the patches onto the host. Patches are installed on a host by putting the host in maintenance mode, which disrupts any active VMs on the host.

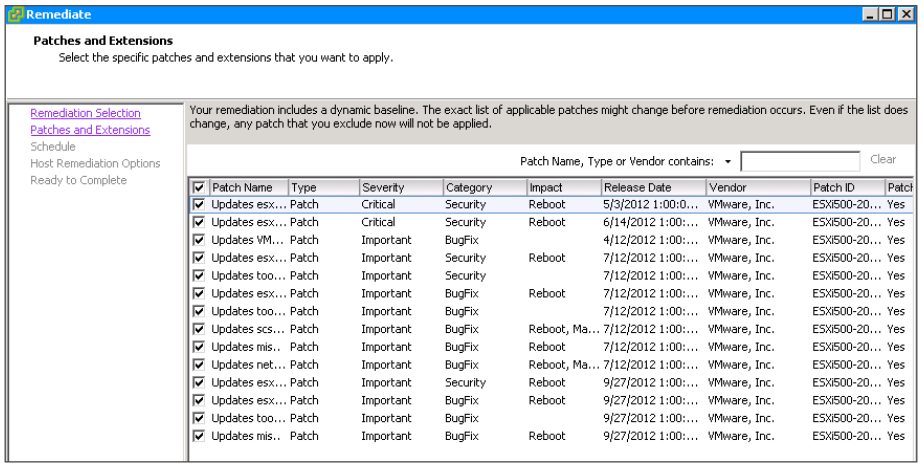
Step 12: Power off the virtual machines on the host. It is recommended to first move the virtual machines to a different host by using VMware vMotion, as described in Procedure 2 "Migrate VM to another ESXi host."

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

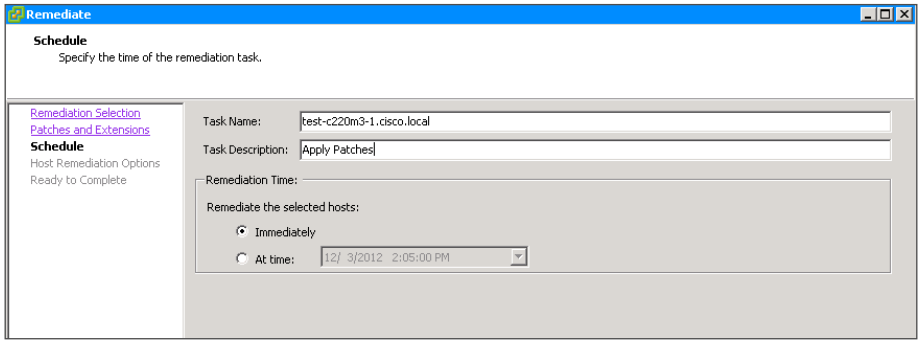
Step 14: In the Remediate wizard, on the Remediation Selection page, select **Critical Host Patches** and **Non-Critical Host Patches**, and then click **Next**.



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



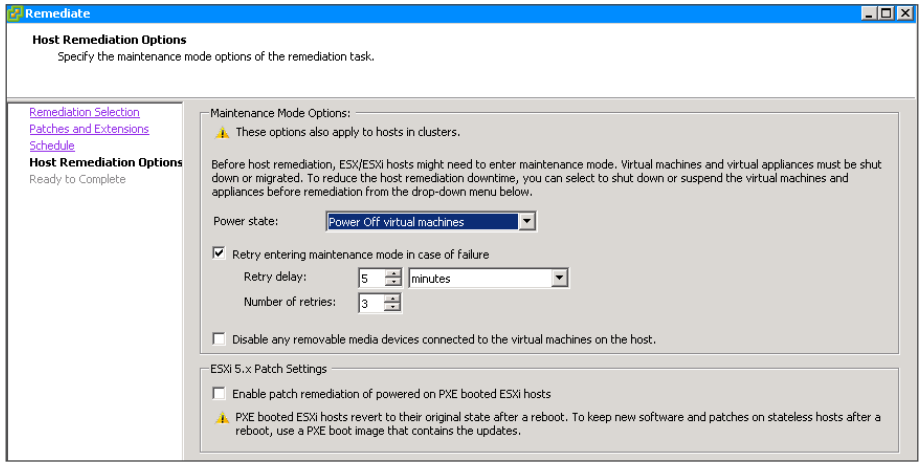
Step 16: Enter a description for the task, select **Immediately**, and then click **Next**.



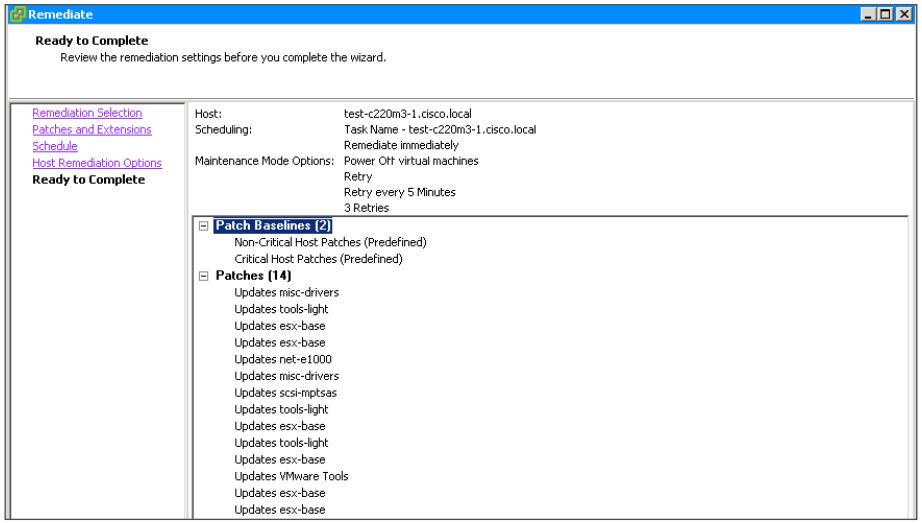
Step 17: On the Host Remediation Options page, in the **Power state** list, choose **Power Off virtual machines**, and then click **Next**.

Tech Tip

To avoid disruption you should have migrated your VMs on this server to another server prior to remediation, as described in Procedure 2 “Migrate VM to another ESXi host.”



Step 18: Review your remediation request, and then click **Finish**.



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

At some point in virtual machine management, you may need to migrate a virtual machine or its storage. If you find it necessary to do so, complete this process.

If you have an Enterprise or Enterprise Plus license for your VMware environment, you can use VMware vMotion in order 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 for storage requires an Enterprise or Enterprise Plus license. If you have a Standard license, skip Procedure 1, "Migrate virtual machine storage."

Procedure 1 Migrate virtual machine storage

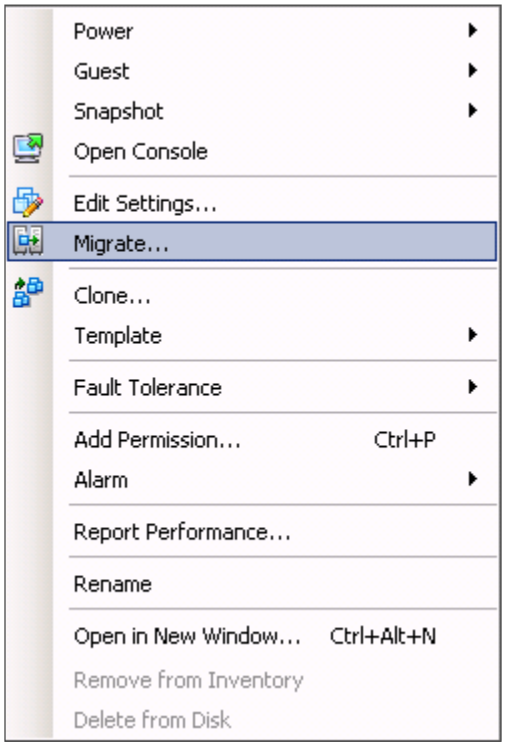
You can move storage from local ESXi server datastores to Fibre Channel or iSCSI datastores. If you installed your new VM as described earlier in this guide, it is located on a local datastore on the ESXi host. To maximize flexibility and enable the ability to use vMotion to move the VM, the storage 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 by 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) by using Storage vMotion. In the thick format, the size of the virtual machine disk (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.

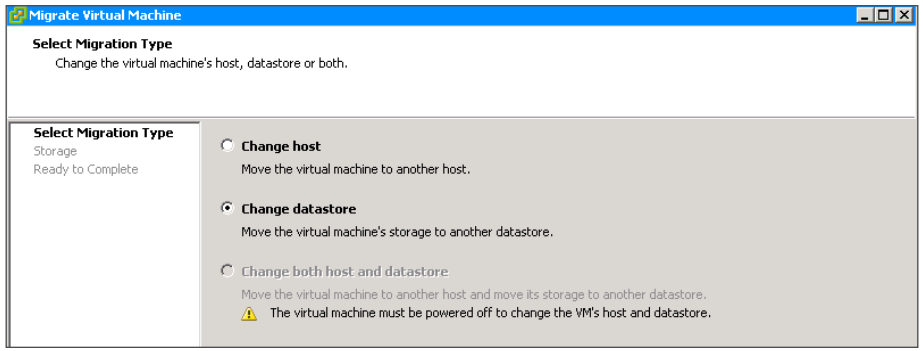
Tech Tip

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 being 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**.



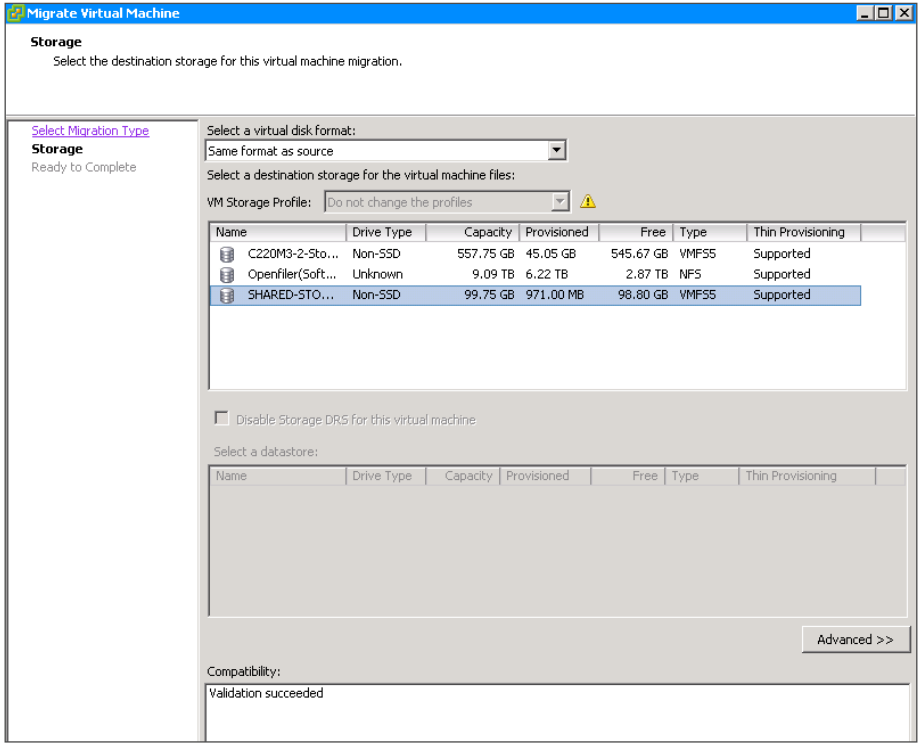
Step 2: In the Migrate Virtual Machine wizard, on the Select Migration Type page, select **Change Datastore**, and then click **Next**.



Step 3: On the Storage page, select a disk format, and then select the destination datastore. Click **Next**.

There are four choices for disk format:

- Same format as source (this is the default setting)
- Thin provision
- Thick provision Lazy Zeroed
- Thick provision Eager Zeroed



Step 4: Click **Finish**. The status of the migration is displayed in the Recent Tasks pane at the bottom of the vSphere Client window.

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 across Layer 3 boundaries without careful consideration and configuration customization. Migration with vMotion to move virtual machines between data centers requires low-latency (below 10 ms) and high-bandwidth links. More information on vMotion can be found at:
http://www.vmware.com/files/pdf/vmotion-perf-vsphere5.pdf

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 configuration, with the exception of the check box for vMotion.

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

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

Step 3: Click the **Configuration** tab, and then in the **Hardware** pane, choose **Networking**.

Step 4: Click **Add Networking**.

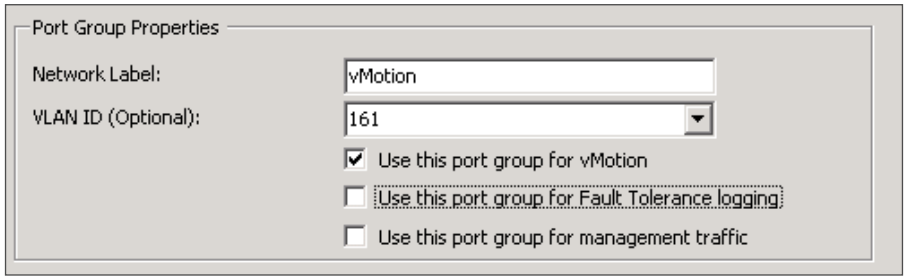
Step 5: Select Connection Type **VMkernel**.

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: In the **Network Label** box, enter a value, and in the **VLAN ID** box, enter the VMkernel port that will be used to service vMotion traffic (Example: 161).

Step 8: Ensure that **Use this port group for vMotion** is selected, and then click **Next**.



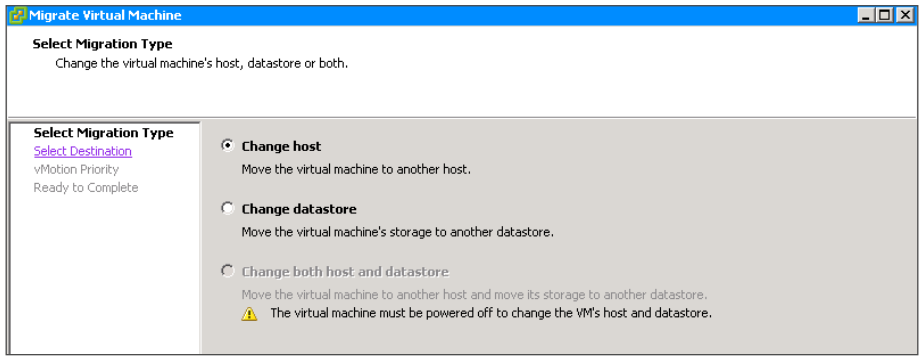
Step 9: Specify an IP address and subnet mask for this VMkernel interface, and then click **Next**.

Step 10: On the Summary page, review the configuration, and then click **Finish**.

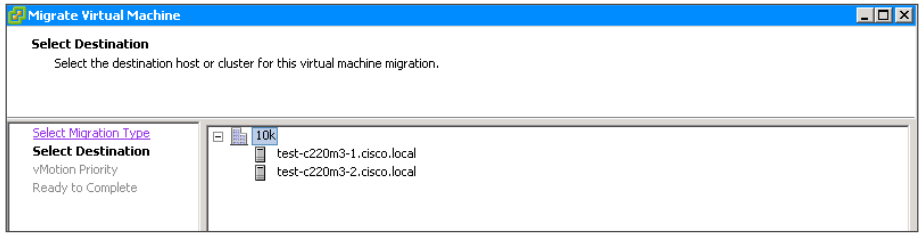
Step 11: Repeat Step 2 through Step 10 for all of the ESXi hosts on which you plan to enable vMotion.

Step 12: In vSphere Client, in the tree, right-click the virtual machine you want to migrate, and then click **Migrate**.

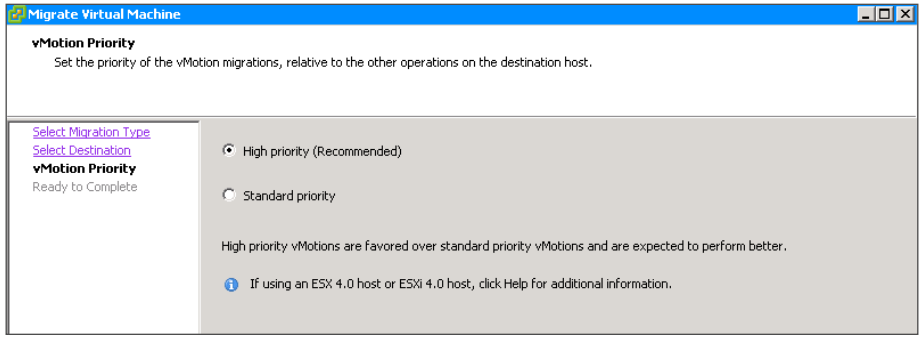
Step 13: In the Migrate Virtual Machine wizard, on the Select Migration Type page, select **Change host**. You are prompted for a destination.



Step 14: Choose the correct destination host, and then click **Next**.



Step 15: Choose the reservation priority for the ESXi host CPU, and then click **Next**.



Step 16: 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 Nexus Operating System (NX-OS) 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 1100 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 or ESXi host. This requirement helps ensure high availability even if one of the VMware ESX or ESXi servers fails. It is recommended that you disable Distributed Resource Scheduler (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 heart-beats, 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 3 - VLANs used for Cisco Nexus 1000V VSM installation

VLAN	Description
160	Cisco Nexus 1000V control
163	Data center management traffic

Table 4 - Additional VLANs defined in the Cisco 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 contains VSM files with an .ova extension and an OVF folder with the .ovf extension file. This procedure uses the file with the .ova extension.

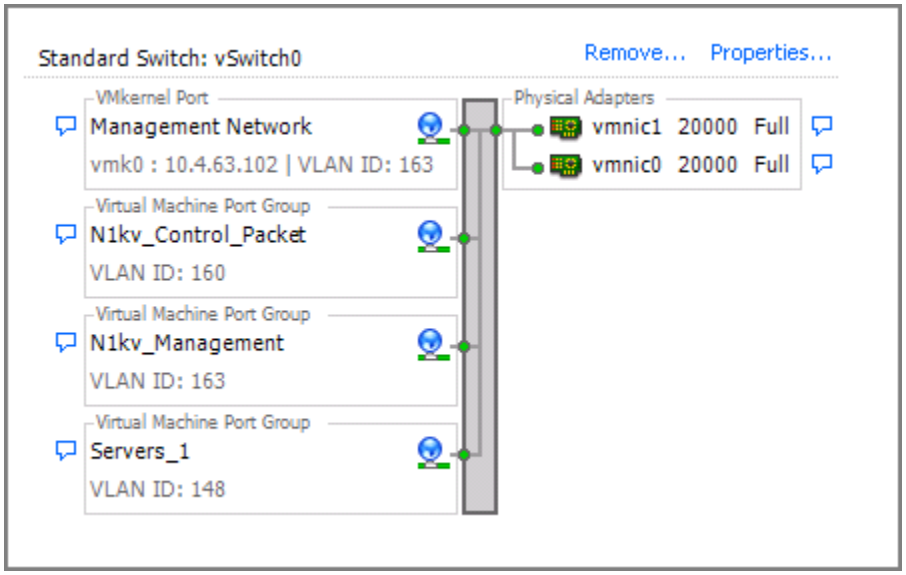
Tech Tip

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.

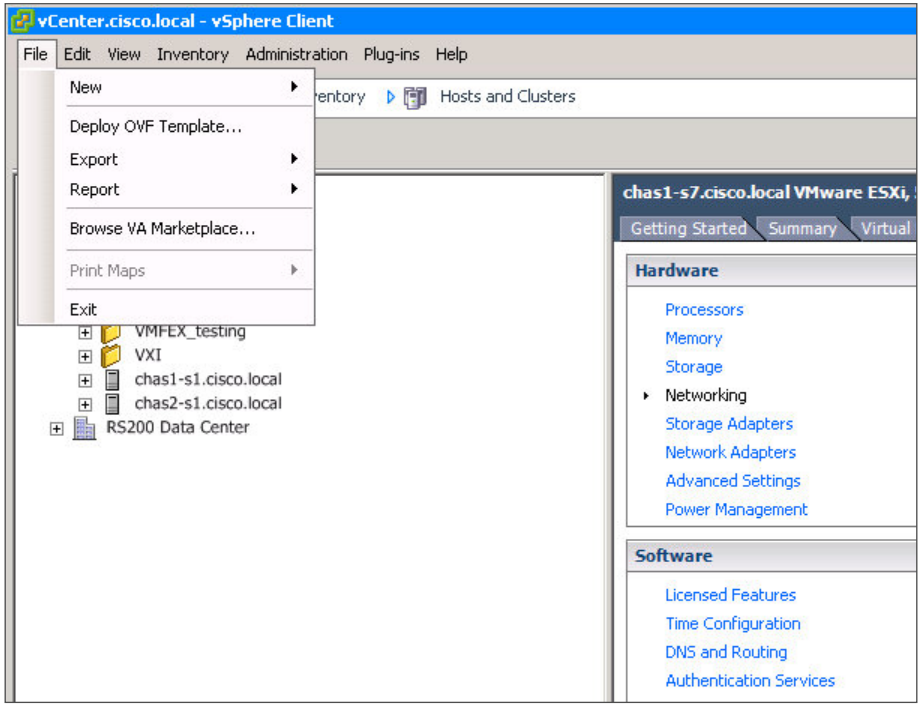
Step 2: Log in to your vCenter Server via the VMware vSphere Client, with the domain administrator username and password.

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

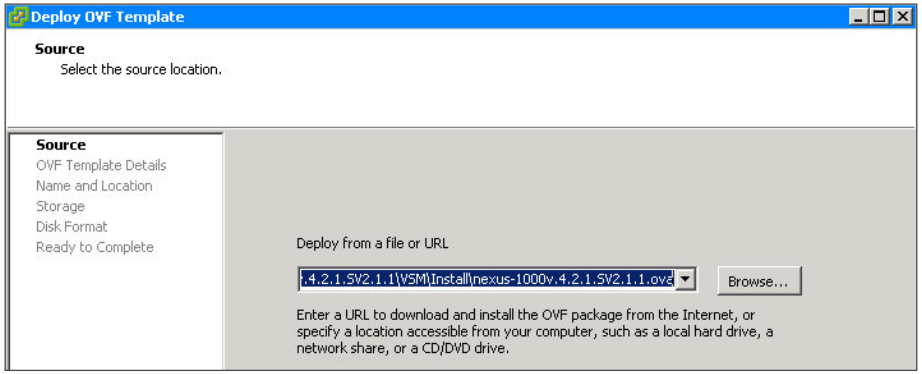
Step 4: Navigate to **Configuration > Networking > Virtual Switch**, and then ensure that the control and management port groups are configured with correct VLANs, as shown in Table 3.



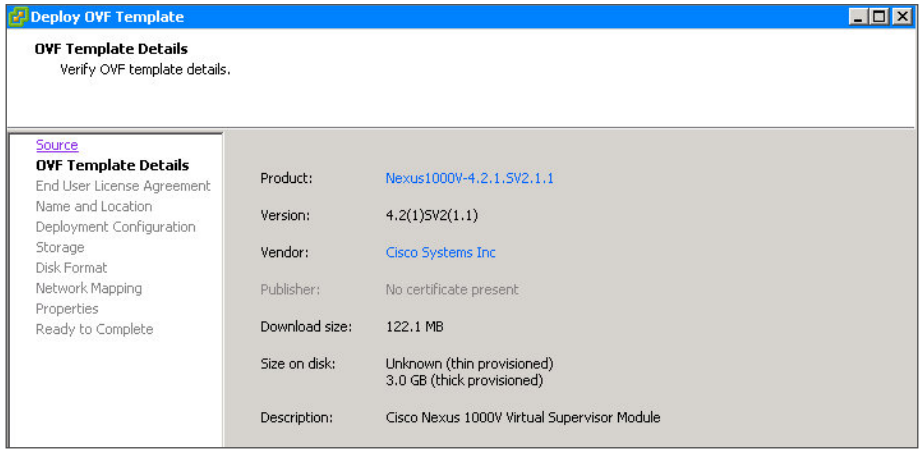
Step 5: In the vSphere Client, from the File menu, choose **Deploy OVF Template**.



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

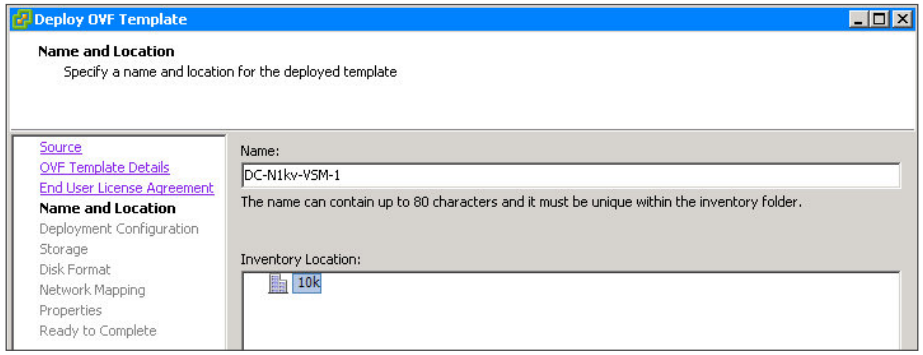


Step 7: You are presented with product information, size of the file, and the size of VM disk. Verify that you have selected the correct version and product, and then click **Next**.

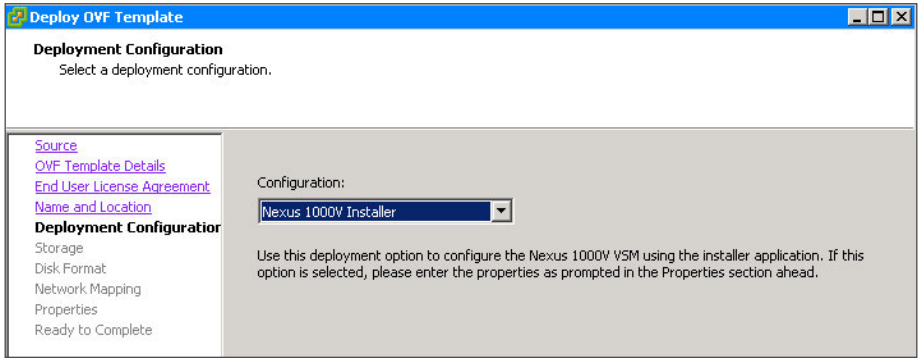


Step 8: Accept the Cisco Nexus 1000V License Agreement, and then click **Next**.

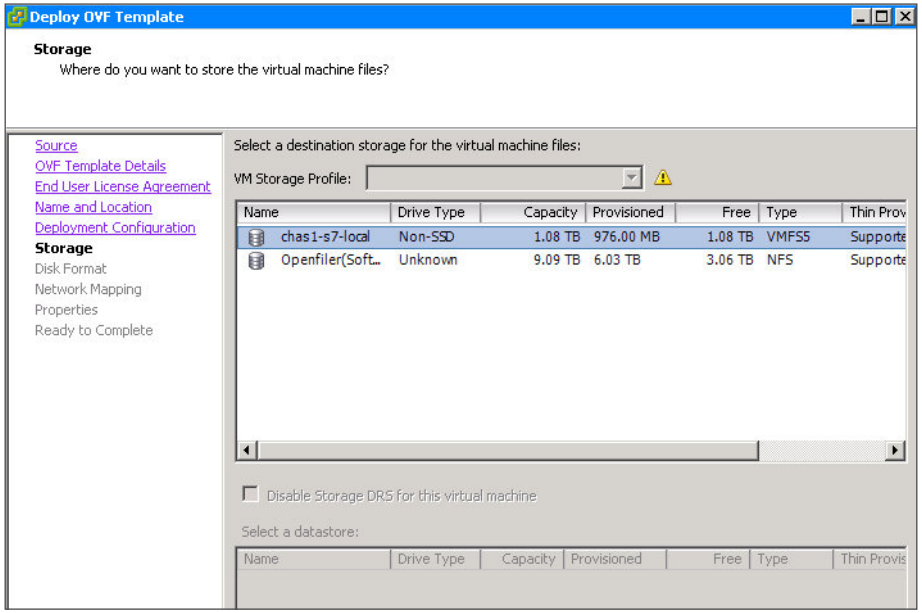
Step 9: Specify the name of your VSM, choose the location, and then click **Next**.



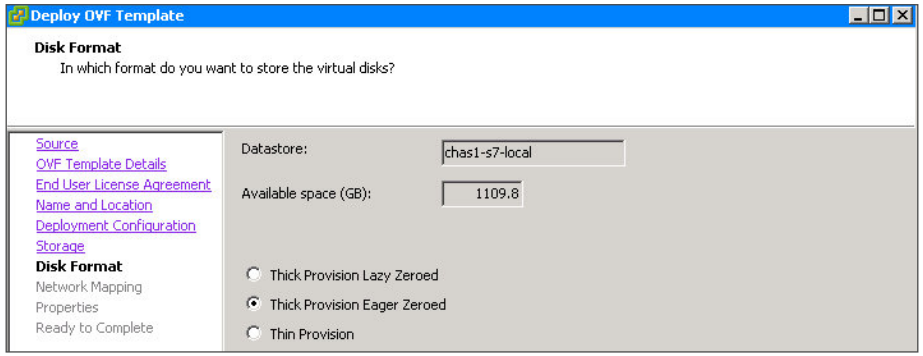
Step 10: In the Configuration list, choose **Nexus 1000V Installer**, and then click **Next**.



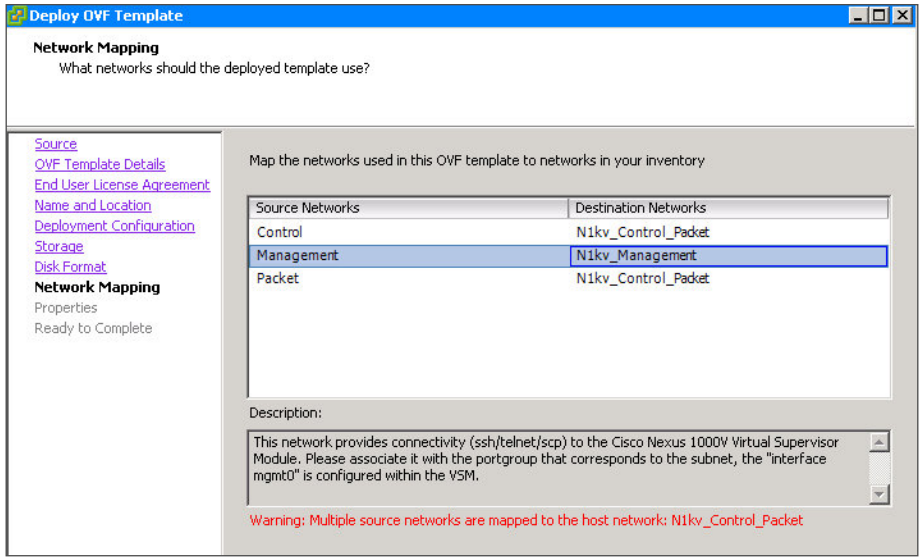
Step 11: Choose the storage you want the VSM to use, and then click **Next**.



Step 12: Select **Thick provision Eager Zeroed**, and then click **Next**. This allocates all storage needed to store the virtual machine virtual disks at the time of creation. The size of the VSM will be approximately 3 GB.

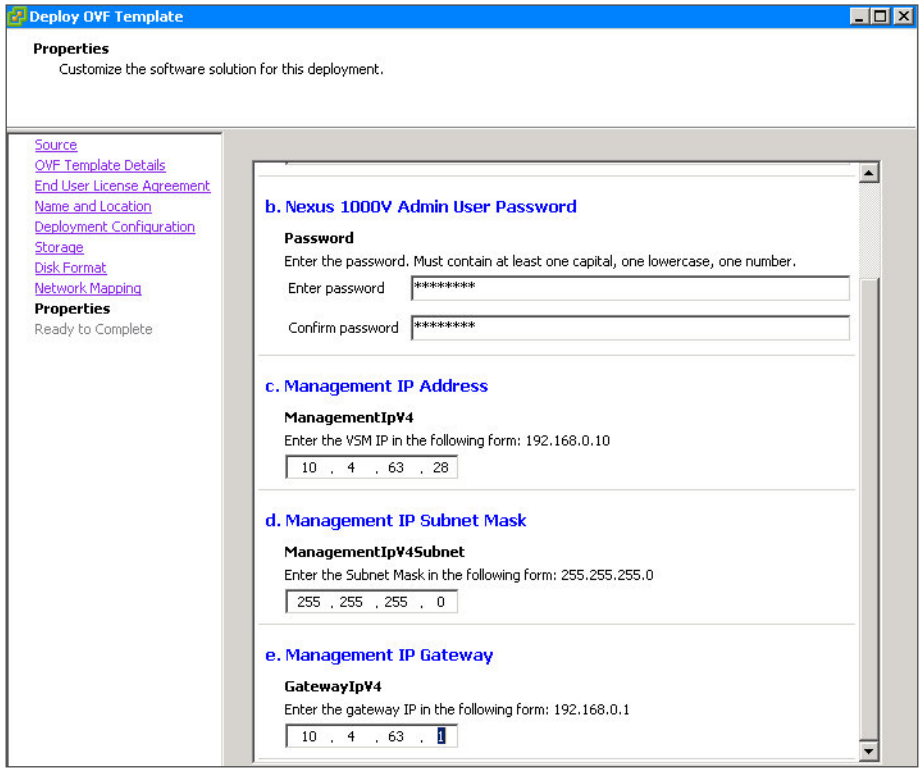


Step 13: In the Layer 3 control mode, the packet NIC does not get used on the VM. The VM still expects the packet NIC to be present. On the Network Mapping page, in the **Destination Network** list, map the Control port-group for the Control Source network and the Packet Source network, and the Management port-group for the Management Source network. Click **Next**.

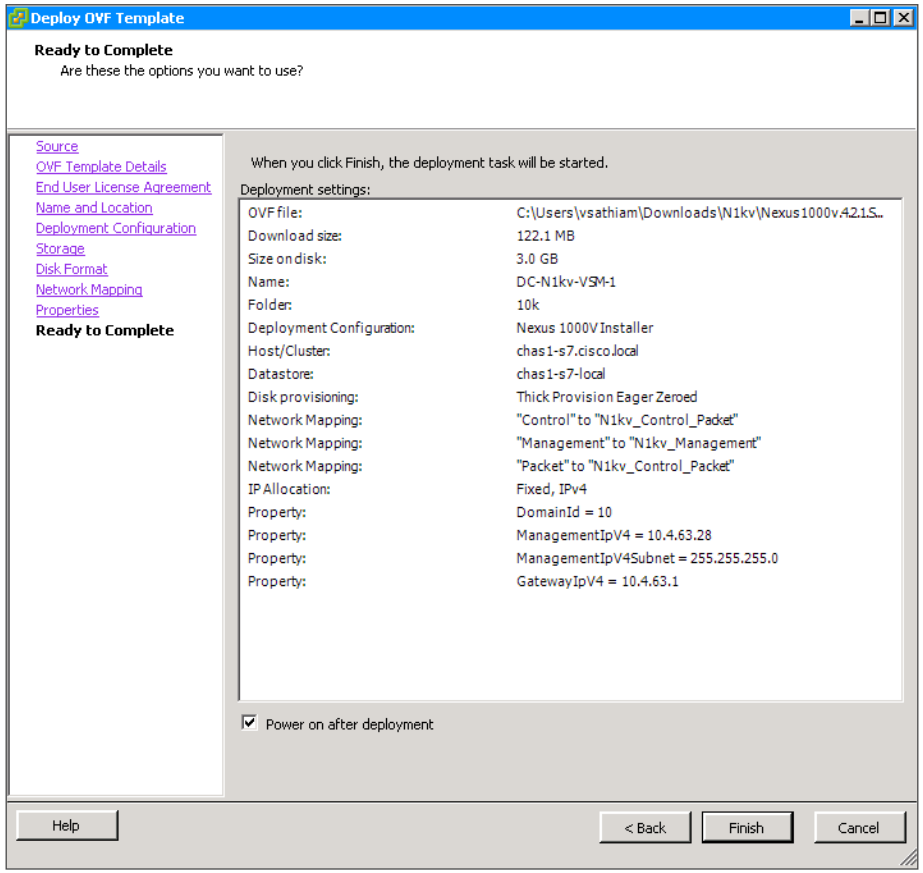


Step 14: Specify the following properties for your primary VSM, and then click **Next**:

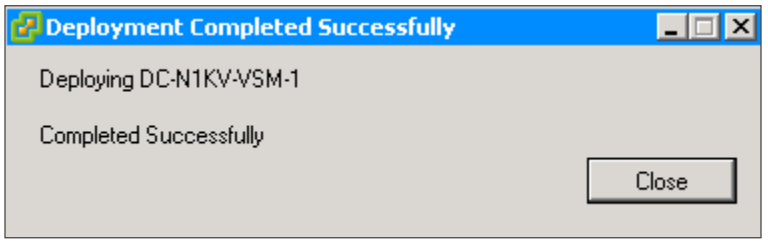
- VSM Domain ID
- Nexus 1000V Admin User Password
- Management IP Address
- Management IP Subnet mask
- Management IP Gateway



Step 15: Verify that your configuration settings are correct. Select **Power on after deployment**, and then click **Finish**. VMware starts to deploy your VSM.

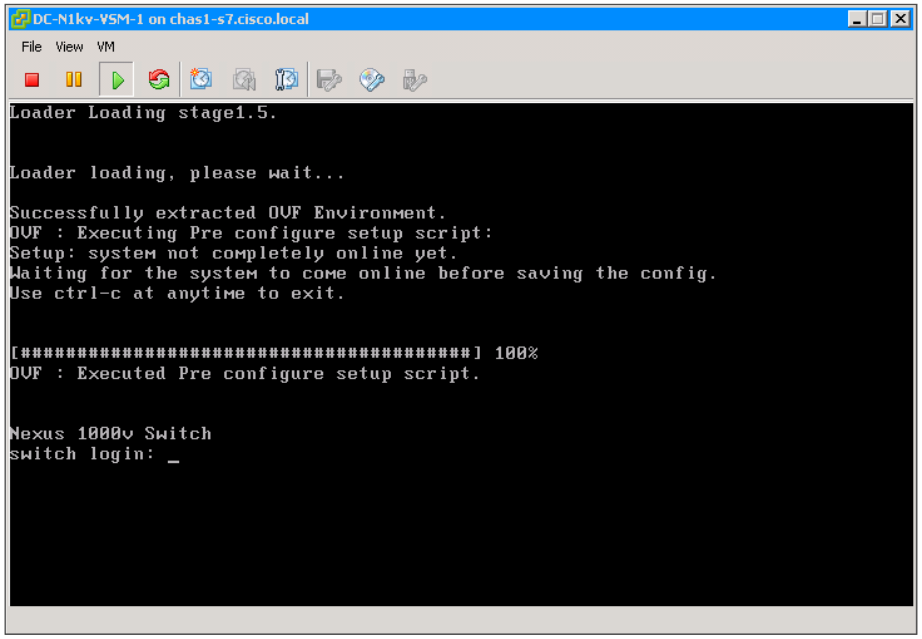


Step 16: On the "Deployment Completed Successfully" message that appears, click **Close**.



You can find the VSM in the inventory window under the machine it was installed on.

Step 17: Right-click the VSM, choose **Open Console**, and then wait for the VSM to finish the boot process and display the login prompt.

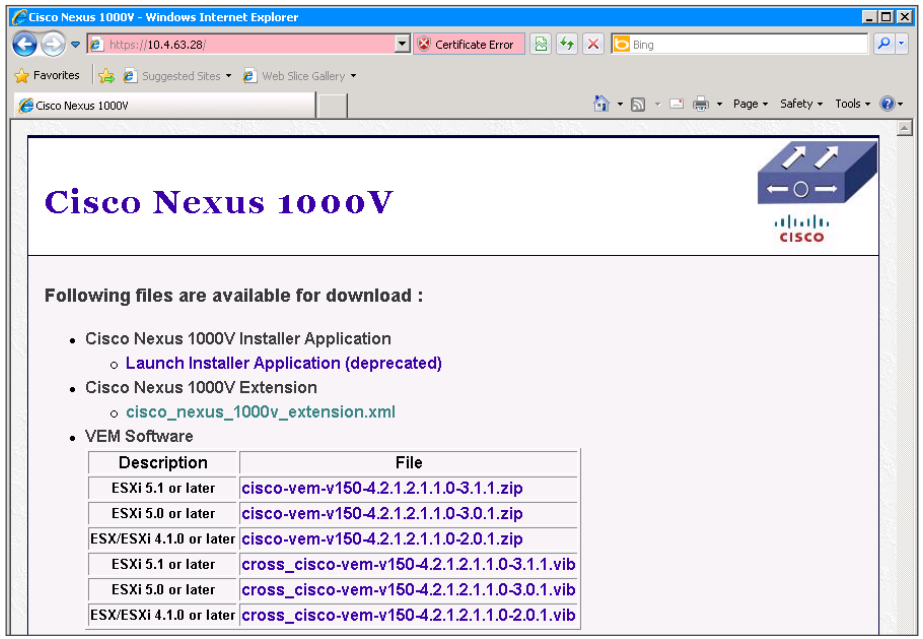


Procedure 2 Configure the primary VSM

In this procedure, you perform the following:

- Install the Cisco Nexus 1000V extension in VMware vCenter
- Set the transport mode of VSM to Layer 3
- Connect the VSM to vCenter Server
- Verify the connectivity from the VSM to vCenter Server
- Configure the VSM as primary VSM

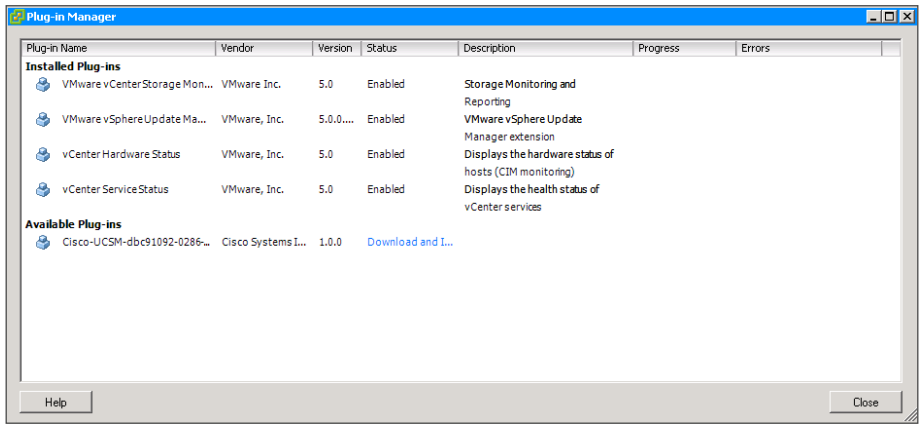
Step 1: Launch a web browser, and then browse to the IP address of the VSM (Example: https://10.4.63.28).



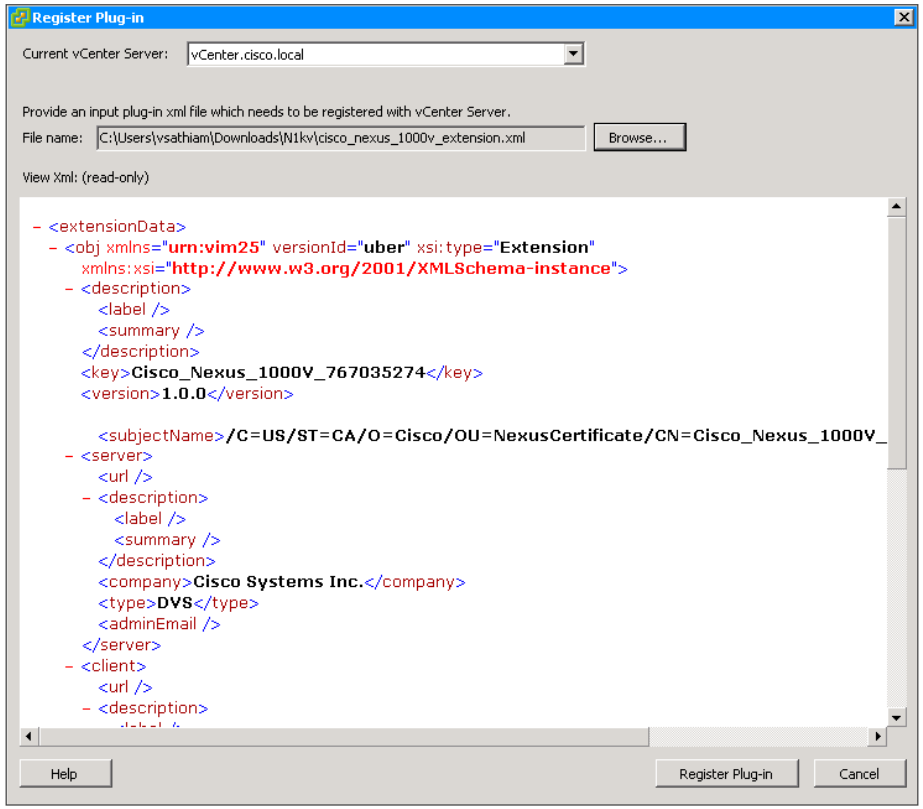
Step 2: Under the Cisco Nexus 1000V Extension, right-click on the **cisco_nexus_1000v_extension.xml** file, select the **Save target as** option, and then save the xml file to the local directory of the machine from where you launch vSphere Client.

Step 3: In the vSphere Client, from the **Plug-ins** menu, choose **Manage Plug-ins**. The Plug-in Manager screen pops up.

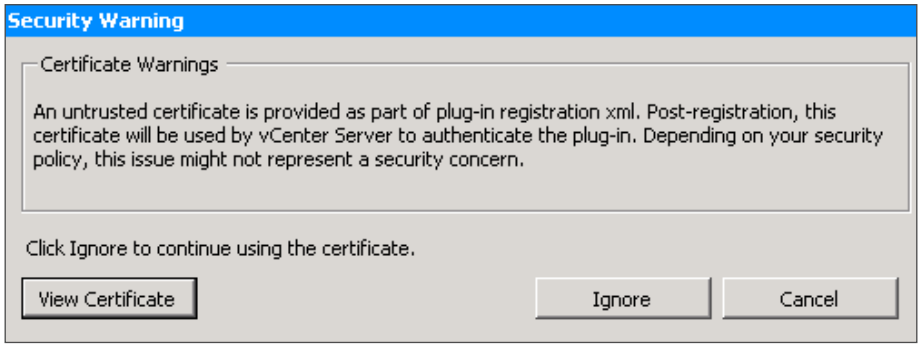
Step 4: On the Plug-in Manager screen, under the Available Plug-ins section, right-click, and then select **New Plug-in**.



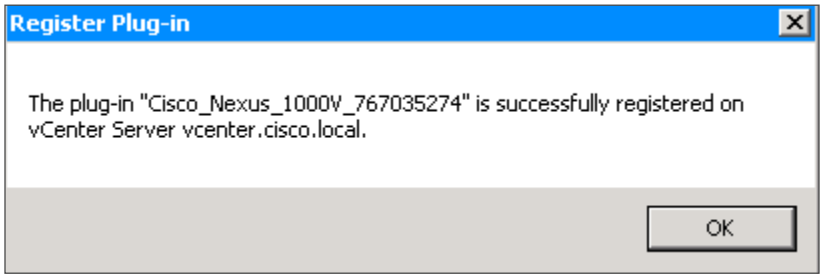
Step 5: In the Register Plug-in screen, browse to the location where you have stored the Cisco Nexus 1000V extension xml file that was downloaded in Step 2, and then click **Register Plug-in**.



Step 6: In the Security Warning message, click **Ignore**.



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.



Step 7: 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 8: Configure the device hostname.

```
hostname [hostname]
```

Step 9: In this step, you set the transport mode of the VSM Layer 3.

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 10: Configure the **ip name-server** command with the IP address of the DNS server for the network. At the command line of a Cisco NX-OS device, it is helpful to be able to type a domain name instead of the IP address.

```
vrf context management
  ip name-server 10.4.48.10
```

Step 11: Set the NTP server address and local time zone for the device location. Network Time Protocol (NTP) is designed to synchronize time across all devices in a network, for troubleshooting.

```
ntp server 10.4.48.17
clock timezone PST -8 0
clock summer-time PDT 2 Sunday march 02:00 1 Sunday nov 02:00
60
```

Step 12: Define a read-only SNMP community (Example: cisco) and a read-write SNMP community for network management (Example: cisco123).

```
snmp-server community cisco group network-operator
snmp-server community cisco123 group network-admin
```

Step 13: If you are using an authentication, authorization, and accounting (AAA) server, set TACACS+ to be the primary protocol used to authenticate management logins.

```
feature tacacs+
tacacs-server host 10.4.48.15 key SecretKey
aaa group server tacacs+ tacacs
    server 10.4.48.15
    use-vrf management
    source-interface mgmt0
aaa authentication login default group tacacs
```

Tech Tip

A local AAA user database was defined during the setup of the Cisco Nexus 1000V switch in order to provide a fallback authentication source in the event that the centralized TACACS+ server is unavailable.

Step 14: 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 15: Verify that communication with vCenter Server is working.

```
N1kvVSM# show svs connections

connection vcenter:
    ip address: 10.4.48.11
    remote port: 80
    protocol: vmware-vim https
    certificate: default
    datacenter name: 10k
    admin:
    max-ports: 8192
    DVS uuid: ca 56 22 50 f1 c5 fc 25-75 6f 4f d6 ad 66 5b 88
    config status: Enabled
    operational status: Connected
    sync status: Complete
    version: VMware vCenter Server 5.0.0 build-804277
    vc-uuid: E589E160-BD5A-488A-89D7-E8B5BF732C0C
```

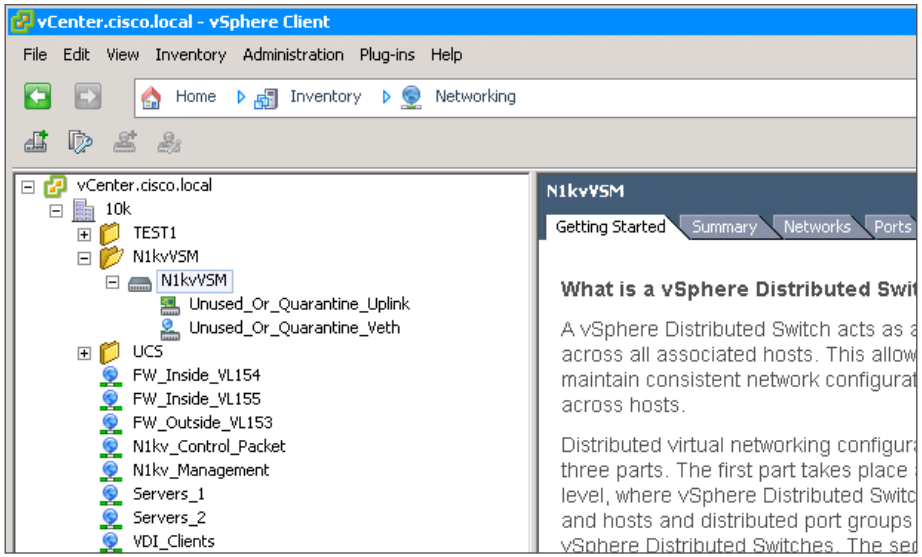
Step 16: After the installation of VSM, it is left in a standalone mode. The best practice for deployment of VSM is in a high availability pair. Convert the VSM standalone role to primary role.

```
N1kvVSM# system redundancy role primary
```

Step 17: Save the running configuration to the startup configuration.

```
copy running-config startup-config
```

Step 18: In your vSphere Client, navigate to **Home** > **Inventory** > **Networking**, and then verify that your Cisco Nexus 1000V switch has been created.



Procedure 3 Install and setup the secondary VSM

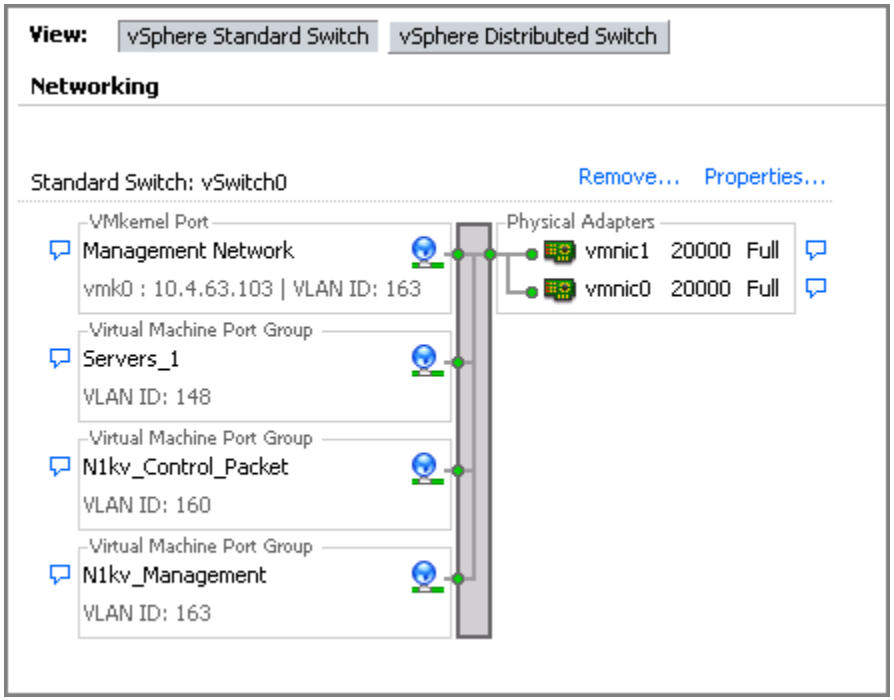
Step 1: Select the host on which you plan to run the secondary VSM VM.

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 Table 3.

For consistency, give the same port-group names you gave for the primary VSM's control, management and packet interfaces.

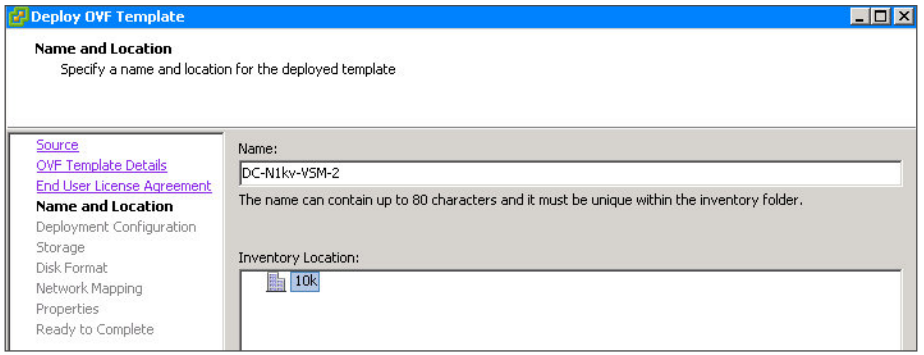


Step 3: In the vSphere Client, from the **File** menu, choose **Deploy OVF Template**, browse to the location where you have downloaded the Cisco Nexus 1000V installation files, choose the OVA file, and then click **Next**.

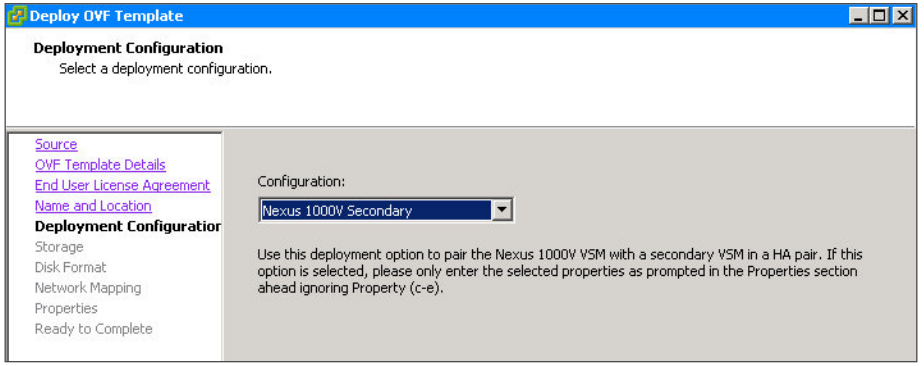
Step 4: On the OVF Template Details page, you are presented with product information, size of the file, and the size of VM disk. Verify that you have selected the same version and product as the primary VSM, and then click **Next**.

Step 5: Accept the Cisco Nexus 1000V License Agreement, and then click **Next**.

Step 6: On the Name and Location page, give a unique name to your secondary VSM, choose the inventory location, and then click **Next**.



Step 7: On the Deployment Configuration page, in the **Configuration** list, choose **Nexus 1000V Secondary**, and then click **Next**.



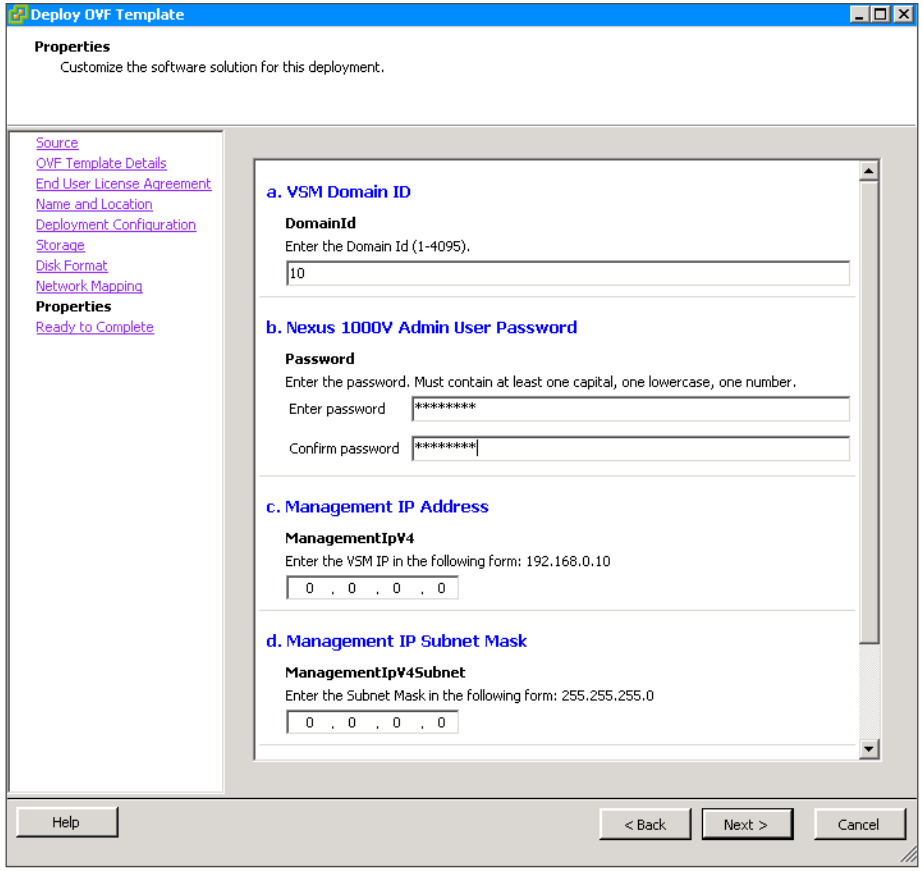
Notice that you are told to ignore section (c-e) in the Properties section.

Step 8: On the Storage page, choose the datastore you want the VSM to use, and then click **Next**.

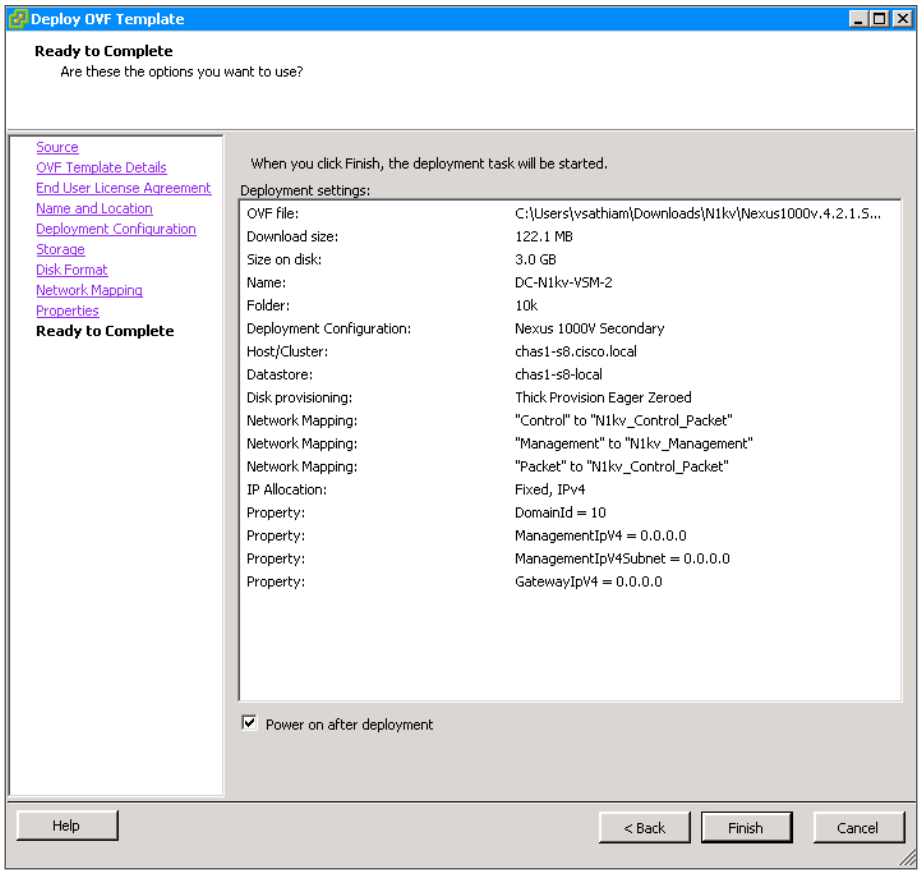
Step 9: On the Disk Format page, select **Thick provision Eager Zeroed**, and then click **Next**.

Step 10: On the Network Mapping page, 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 11: On the Properties page, 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 "Install the first VSM" procedure earlier in this process), skip sections c through e, and then click **Next**.



Step 12: Review your settings, select **Power on after deployment**, and then click **Finish**.



Step 13: Right-click the secondary 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.

Next, you verify that the secondary VSM has joined the high-availability cluster along with the primary VSM.

Step 14: 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 (Example: 10.4.63.28).

Step 15: Verify that the system is in high availability mode, and then verify that Sup-1 and Sup-2 have been detected and are in active or standby state.

```
N1kvVSM# 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
N1kvVSM# 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)SV2(1.1)      0.0
2    4.2(1)SV2(1.1)      0.0

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

Mod  Server-IP        Server-UUID            Server-Name
---  ---------------  ---------------------  ------------
1    10.4.63.28       NA                     NA
2    10.4.63.28       NA                     NA

* this terminal session
```

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 vSphere 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 virtual ethernet 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.

Table 5 lists the VLANs you create for the Cisco Nexus 1000V Series switch and provides a description of each VLAN.

Table 5 - VLANs for Cisco Nexus 1000V Series switch

VLANs	VLAN name	Description
148	Servers_1	Virtual Machine Network Data
149	Servers_2	Virtual Machine Network Data
150	Servers_3	Virtual Machine Network Data
154	FW_Inside_1	Firewall-protected servers
155	FW_Inside_2	Firewall and IPS protected servers
157	VDI_Clients	VDI Client secured servers
160	1kv-Control	Cisco Nexus 1000V Control
161	vMotion	VMware vMotion
162	iSCSI	iSCSI transport traffic
163	DC-Management	Data Center Management Traffic

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 "Install the first VSM" procedure (Example: 10.4.63.28).

Step 2: Create the VLANs required for your setup. Refer to Table 5 for a list of VLANs and their descriptions.

```
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 149-157
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) in 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 interconnects are set up in end-host mode; therefore, MAC-pinning is used for Cisco UCS B-Series servers as well.

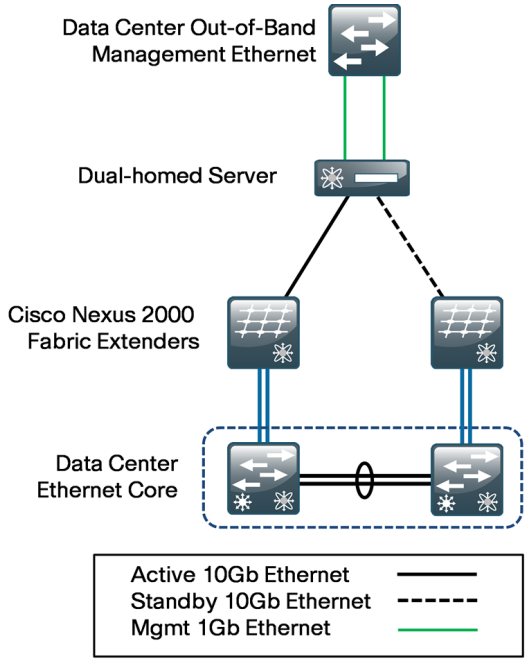
Step 3: Create an uplink port profile named System-Uplink.

```
port-profile type ethernet System-Uplink
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 148-157,160-163
  channel-group auto mode on mac-pinning
  no shutdown
  system vlan 160,162-163
  description B-Series Uplink all traffic
  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 12, 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 12 - 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 148-157,160-162
  channel-group auto mode on mac-pinning
  no shutdown
  description Uplink for C-Series
  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, you 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.

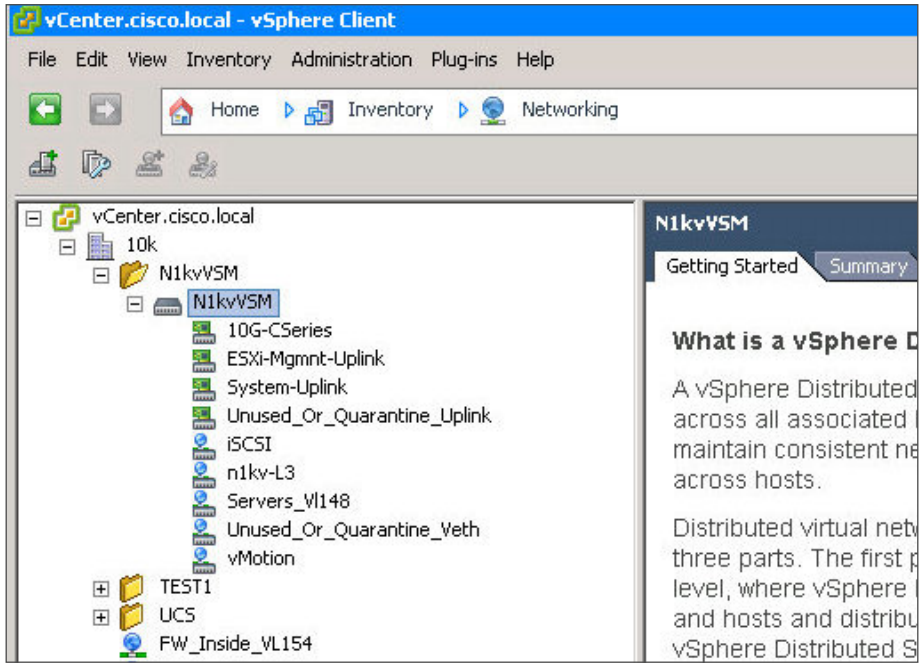
```
port-profile type vethernet iSCSI
  vmware port-group
  switchport mode access
  switchport access vlan 162
  no shutdown
  system vlan 162
  state enabled
```

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, configure additional port profiles according to Step 5 through Step 7 based on the type of port profile needed.

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. In the figure below, the ethernet Uplink profiles appear with the green adapter icon, and the vethernet profiles appear with the blue circle icon.



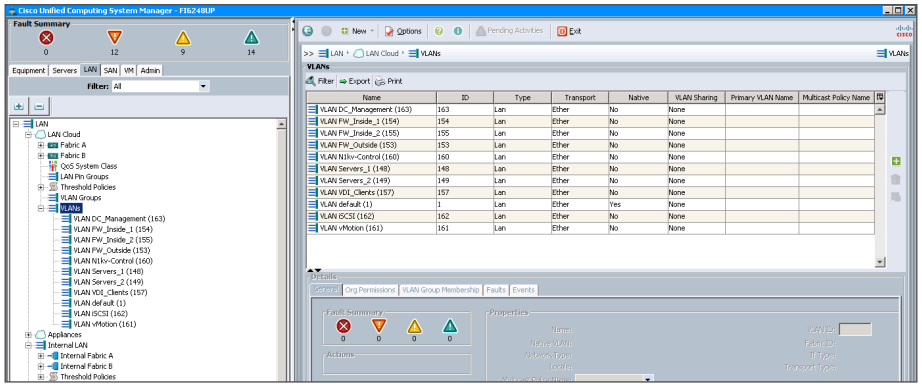
Procedure 2 Prepare Cisco UCS B-Series server for VEM

If you are installing a Cisco Nexus 1000V Series 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, 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 5 (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.



For each vNIC mapped to the Cisco Nexus 1000V switch, ensure that the **Enable Failover** check box is cleared, as recommended for VMware installations in the *Cisco SBA—Data Center Unified Computing System Deployment Guide*.

Procedure 3 Install VEM using vSphere 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 vSphere 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.

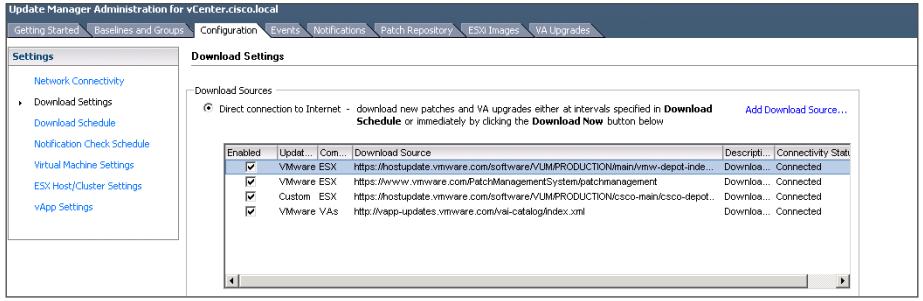
VMware vCenter Server sends opaque data containing the switch domain ID, switch name, control and packet VLAN IDs, and system port profiles to the VEM, which the VEM uses to establish communication with the VSM and download appropriate configuration data.

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.

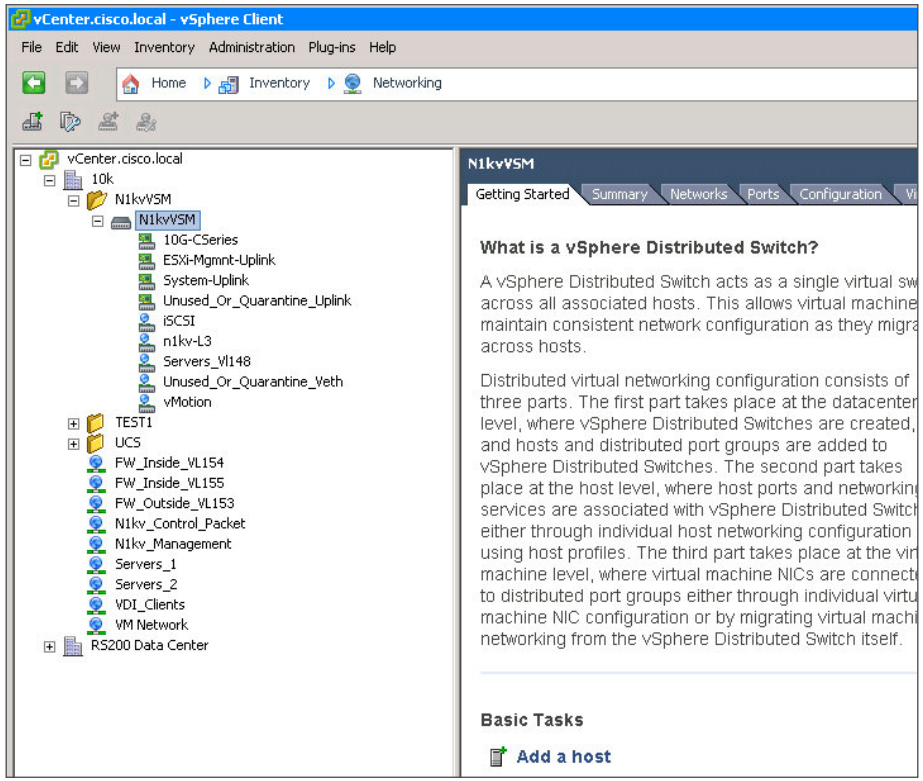
Step 1: In the vSphere Client, navigate to **Home**, and then under Solutions and Applications, choose **Update Manager**.

Step 2: Navigate to the Configuration tab, click **Download Settings**, and then ensure that for the **Custom** Patch Type, **Enabled** is selected and the Connectivity status is **Connected**.

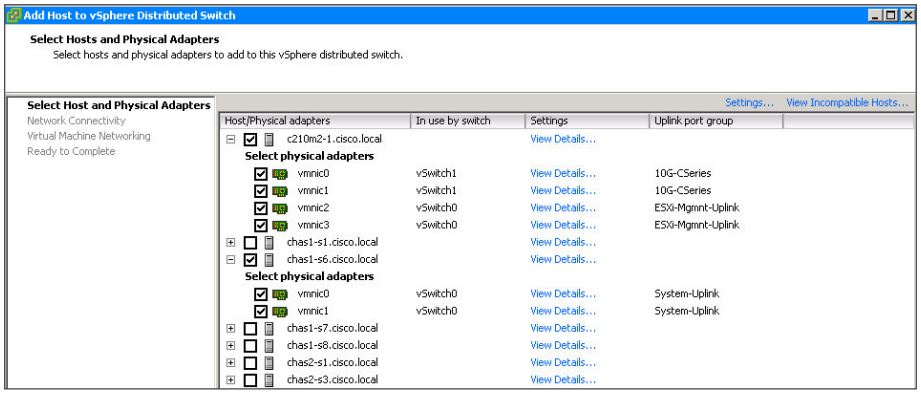


At this point, you are ready to install a VEM.

Step 3: Navigate to **Home > Inventory > Networking**, select the Cisco Nexus 1000V Series switch you created, and then in the work pane, on the Getting Started tab, click **Add a host**.



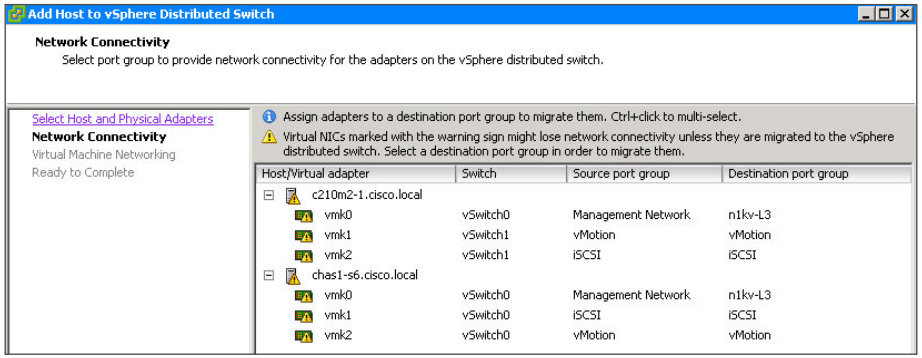
Step 4: In the Add Host to vSphere Distributed Switch wizard, select the host on which you want to install VEM, select the check boxes next to the physical adapters to provide connectivity between the vDS and the host, and then in the **Uplink port group** column, in the list, choose the uplink port profile you created in Step 3 of Procedure 1 "Configure port profiles". Click **Next**.



Step 5: On the Network connectivity page, for each source port group, in the **Destination port group** list, choose the following values, and then click **Next**:

- Management Network—**n1kv-L3**
- vMotion—**vMotion**
- iSCSI—**iSCSI**

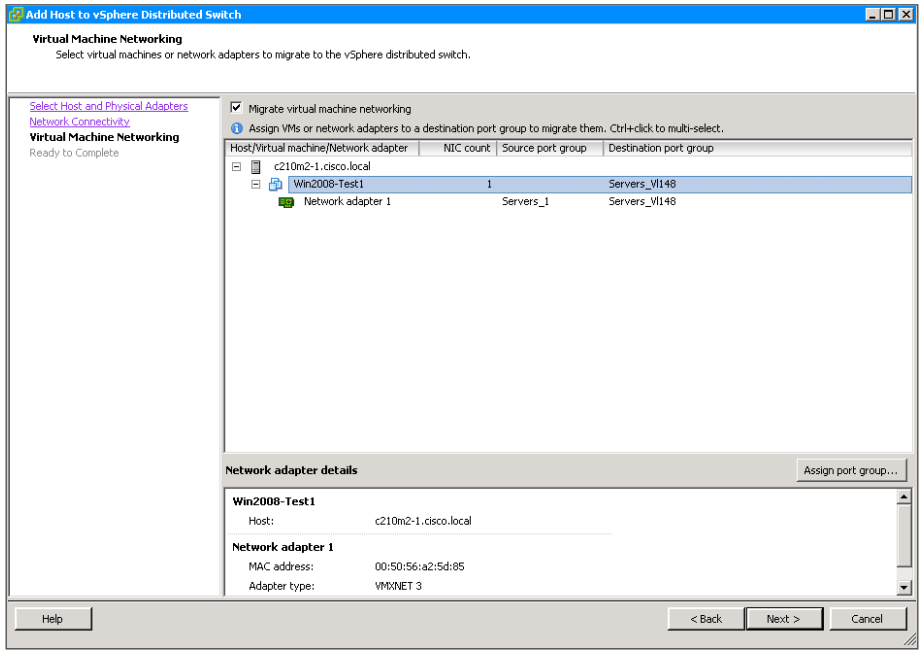
This step assigns virtual adapters to an appropriate port group for the traffic that they are carrying. Vmk0, Vmk1 and vmk2 are going to be migrated from VMware vSwitch to the Cisco Nexus 1000V vDS.



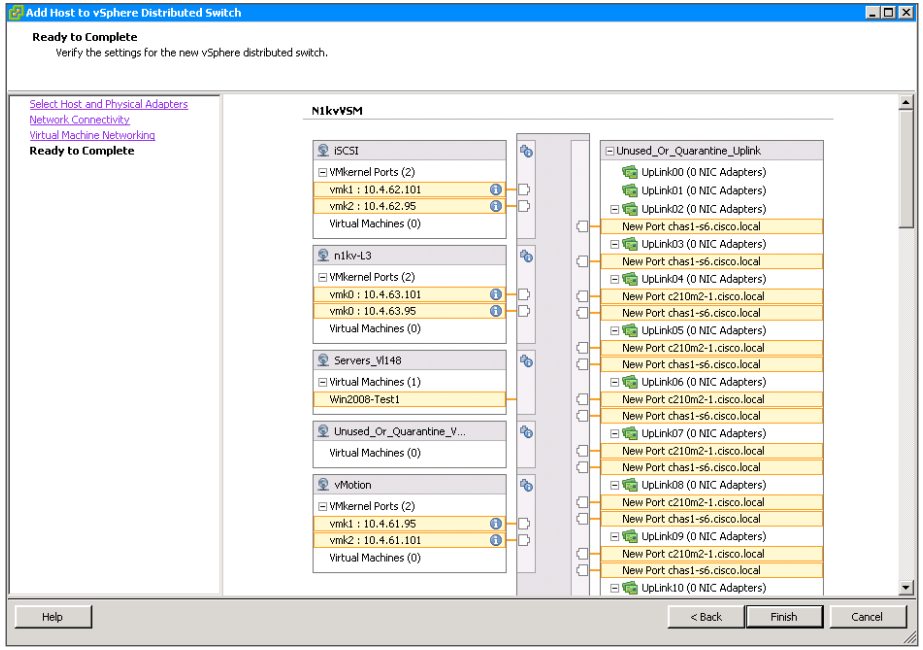
Step 6: If you have virtual machines already assigned to the host, select **Migrate virtual machine networking**, and in the **Destination port group** list for each virtual machine, choose the appropriate destination port group, and then click **Next**.

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 switch 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.

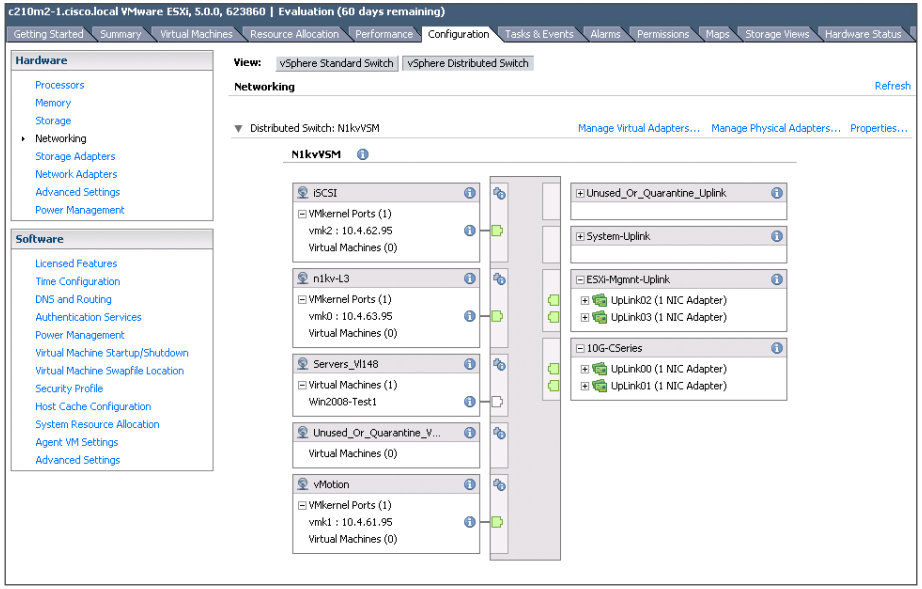


Step 7: On the Ready to Complete page, verify that the settings for the new vSphere distributed switch are correct, and then click **Finish**. Existing interfaces from other hosts are included in the display, because it represents a switch that is distributed across multiple hosts.



Step 8: In the vSphere Client, in the Recent Tasks pane, monitor the remediation of the host.

Step 9: When the host has completed the Update Network Configuration task, navigate to **Inventory > Hosts and Clusters**, select the host name, navigate to the Configuration tab, choose **Networking**, and then click **vSphere Distributed Switch**. View the results of the configuration.



Cisco Virtual Machine Fabric Extender Configuration and Deployment

A VMware virtualized server implementation consists of one or more VMs that run as guests on a single physical server. The guest VMs are hosted and managed by a software layer called the *hypervisor* or *virtual machine manager* (VMM). Typically, the hypervisor presents a virtual network interface to each VM and performs Layer 2 switching of traffic from a VM to other local VMs or to another interface to the external network.

Working with a Cisco virtual interface card (VIC) adapter, the Cisco Virtual Machine Fabric Extender (VM-FEX) bypasses software-based switching of VM traffic by the hypervisor for external hardware-based switching in the fabric interconnect. This method reduces the load on the server CPU, provides faster switching, and enables you to apply a rich set of network management features to local and remote traffic.

Cisco VM-FEX extends the IEEE 802.1Qbh port extender architecture to the VMs by providing each VM interface with a virtual Peripheral Component Interconnect Express (PCIe) device and a virtual port on a switch. This solution allows precise rate limiting and quality of service (QoS) guarantees on the VM interface.

This deployment will guide you through deploying Cisco VM-FEX on a Cisco UCS B-Series Blade Server system running Cisco UCS Manager version 2.1 software and a VMware ESXi version 5.0U1 virtual machine.

Virtualization with a Virtual Interface Card Adapter

A Cisco VIC adapter, such as the Cisco UCS VIC 1240, VIC 1280, or M81KR Virtual Interface Card, is a *converged network adapter* that is designed for both single-OS and VM-based deployments. The VIC adapter supports static or dynamic virtualized interfaces, which include up to 256 virtual network interface cards (vNICs) depending on the VIC model in use. VIC adapters support Cisco VM-FEX in order to provide hardware-based switching of traffic to and from virtual machine interfaces.

In a VMware environment, Cisco VM-FEX supports the standard VMware integration with VMware ESX hypervisors installed on the server and all virtual machine management performed through the VMware vCenter.

Cisco VM-FEX Modes of Operation

Cisco VM-FEX ports can operate in standard mode or high-performance mode:

- **Standard mode**—Traffic to and from a virtual machine passes through the distributed virtual switch (DVS) and the hypervisor.
- **High-performance mode**—Traffic to and from a virtual machine (VM) bypasses the DVS and hypervisor. Traffic travels directly between VMs and the virtual interface card (VIC) adapter.

The benefits of high-performance mode are as follows:

- Increases I/O performance and throughput
- Decreases I/O latency
- Improves CPU utilization for virtualized I/O-intensive applications

With VMware, high-performance mode also supports vMotion. During vMotion, the hypervisor reconfigures links in high-performance mode to be in standard mode, transitions the link to the new hypervisor, and then reconfigures the link to be in high-performance mode.

Reader Tip

For more information about Cisco VM-FEX please see: http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/vm_fex/vmware/gui/config_guide/2.1/b_GUI_VMware_VM-FEX_UCSM_Configuration_Guide_2_1_chapter_01.html

The Cisco VM-FEX deployment assumes that you have followed the "VMware vSphere Installation and Setup" section of this document, and that the following is true:

- A server exists and is running vSphere Client
- A vCenter Server exists and manages the ESXi hosts
- A Cisco UCS Manager service profile has been created (either with local disk or SAN boot policy) and has been associated to a Cisco UCS B-Series blade server with a Cisco UCS VIC
- VMware ESXi has been installed and is operation on the target Cisco UCS B-Series blade server

Process

Configuring a Service Profile with Cisco VM-FEX

1. Configure dynamic vNIC connection policy
2. Configure a high-performance BIOS policy
3. Modify service profile

This deployment will guide you through deploying Cisco VM-FEX on a Cisco UCS B-Series Blade Server system running Cisco UCS Manager version 2.1 software and a VMware ESXi version 5.0U1 virtual machine.

To configure Cisco VM-FEX in this deployment, you will require access to Cisco UCS Manager for the Cisco UCS B-Series blade servers deployed in the *Cisco SBA—Data Center Unified Computing System Deployment Guide* and used previously in this guide, and you need access to the VMware vCenter server deployed earlier in this guide.

Procedure 1 Configure dynamic vNIC connection policy

The maximum number of dynamic vNICs available to configure per Cisco UCS B-Series blade server for Cisco VM-FEX is dependent on many factors. For more information please consult: http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns224/ns944/vm_fex_best_practices_deployment_guide_ns1124_Networking_Solutions_White_Paper.html

This guide uses the default setting for the number of dynamic vNICs to assign in Step 3.

This procedure modifies an existing service profile deployed in the *Data Center Unified Computing System Deployment Guide*.

Step 1: In a browser, connect to Cisco UCS Manager by using your Cisco UCS virtual management IP address.

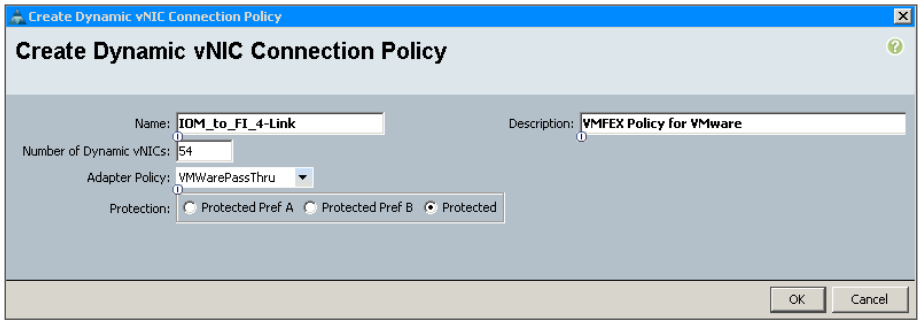
Step 2: Click **Launch UCS Manager**, and then log in to Cisco UCS Manager by using your administrator username and password.

Step 3: In the navigation pane, click the **LAN** tab, and then expand **LAN** > **Policies** > **root** > **Dynamic vNIC Connection Policies**.

Step 4: Right-click **Dynamic vNIC Connection Policies**, and then click **Create Dynamic vNIC Connection Policy**.

Step 5: On the Create Dynamic vNIC Connection Policy dialog box, enter the following, and then click **OK**:

- Name—IOM_to_FI_4-Link
- Description—VMFEX Policy for VMware
- Number of dynamic vNICs—54 (or your configuration-specific value)
- Adapter Policy—VMWarePassThru
- Protection—Protected (allows Cisco UCS to choose whichever fabric is available)



Step 6: On the confirmation dialog box, click **Yes**.

Procedure 2 Configure a high-performance BIOS policy

In order for Cisco VM-FEX to operate in high-performance mode, you must enable the following settings in the BIOS policy:

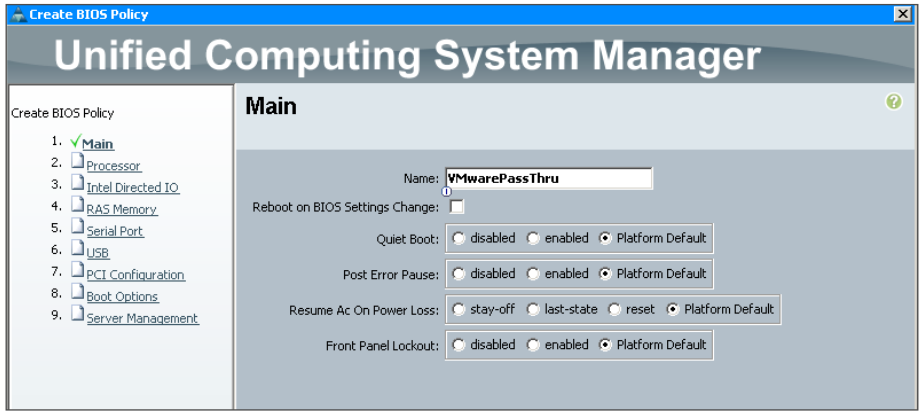
- Processor—Virtualization Technology (VT) and Direct Cache Access
- Intel Directed IO
  - VT for Directed IO
  - Interrupt Remap
  - Coherency Support
  - ATS Support
  - Pass Through DMA Support

Step 1: In the Cisco UCS Manager navigation pane, click the **Servers** tab, and then expand **Servers** > **Policies** > **root** > **BIOS Policies**.

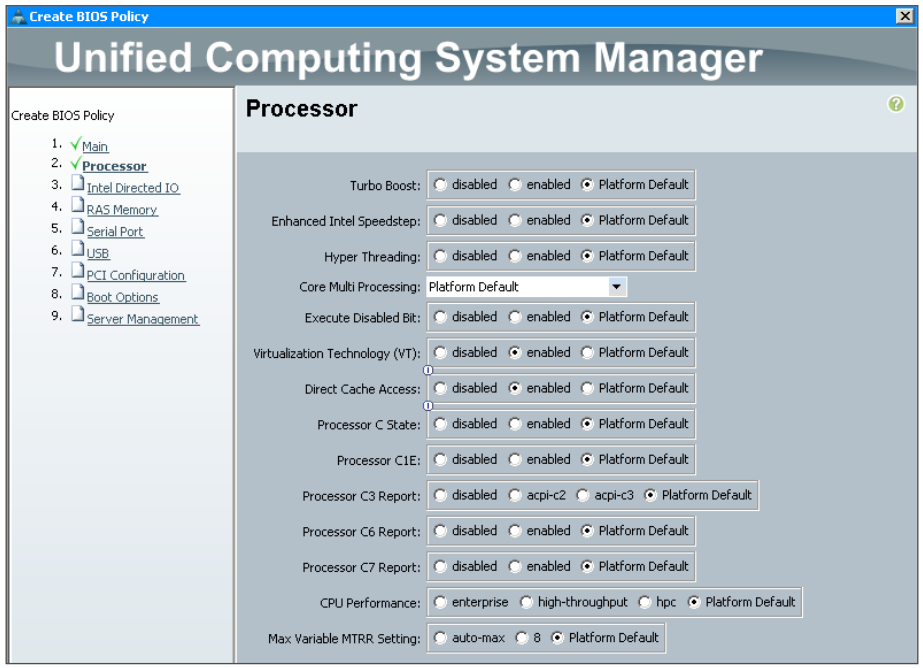
Step 2: Right-click **BIOS Policies**, and then click **Create BIOS Policy**.

Step 3: Follow the instructions in the Create BIOS Policy wizard and note the following:

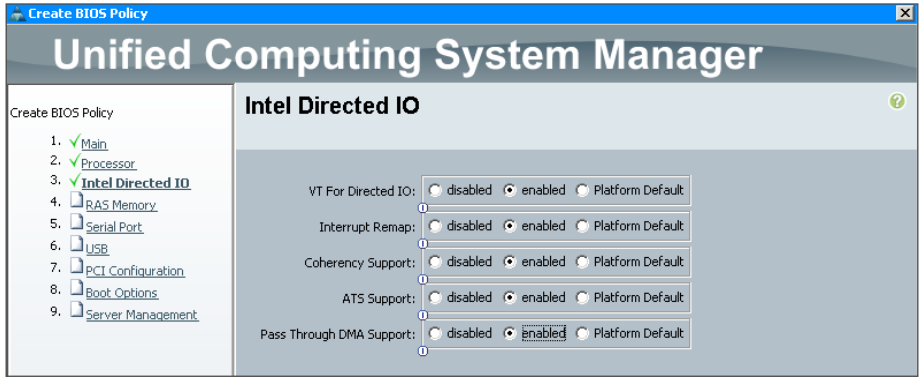
- On the Main page, enter the name of the BIOS policy, and then click **Next**.



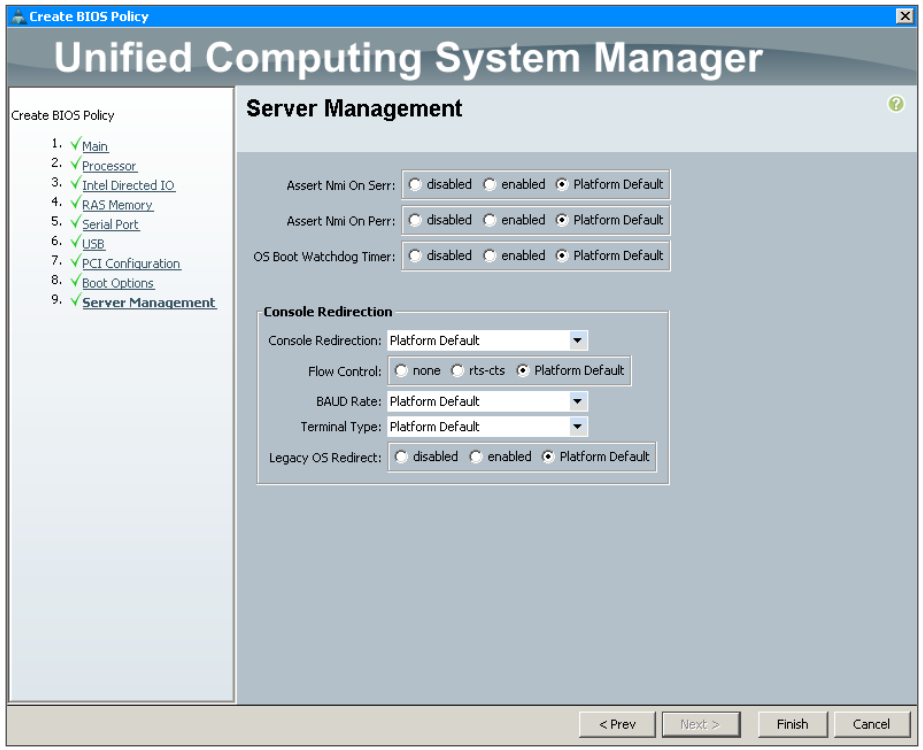
- On the Processor page, for Virtualization Technology (VT) and Direct Cache Access, select **enabled**, and then click **Next**.



- On the Intel Directed IO page, for all options, select **enabled**, and then click **Next**.



- On all remaining pages, accept the defaults by clicking **Next**.
- On the Server Management page, click **Finish**. This completes the creation of BIOS policy.

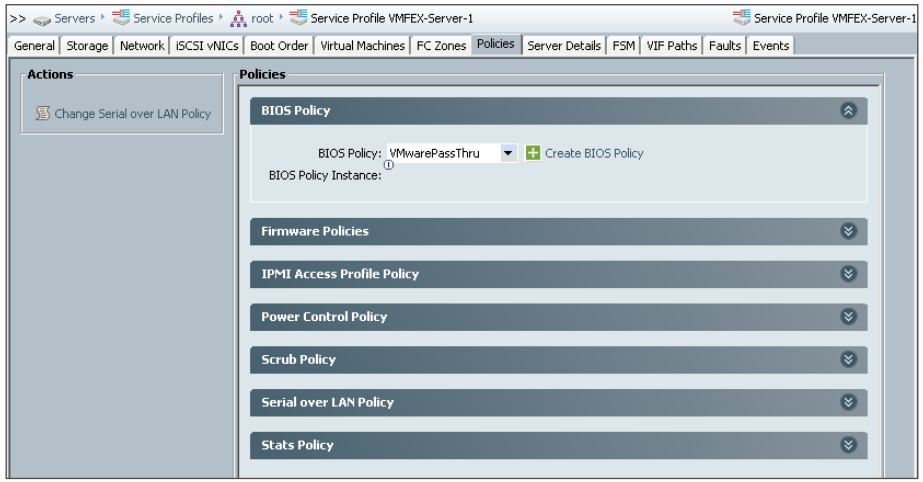


Procedure 3 Modify service profile

In this procedure, you edit an existing service profile in order to add the dynamic vNIC connection policy and BIOS policy created in Procedure 1 and Procedure 2. This allows Cisco VM-FEX for VMware to function optimally.

Step 1: In the Cisco UCS Manager navigation pane, click the **Servers** tab, select the service profile that you want to modify for Cisco VM-FEX operation, and then in the work pane, click the **Policies** tab.

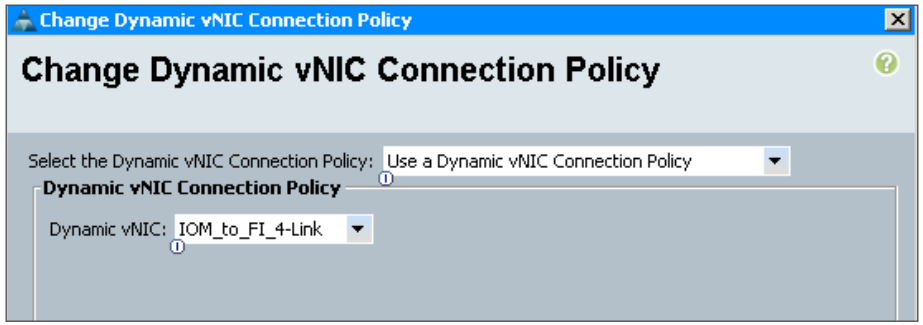
Step 2: On the Policies tab, expand the **BIOS Policy** section, and in the **BIOS Policy** list, choose the BIOS policy created in Procedure 2 (Example: VMwarePassThru), and then click **Save Changes**.



Step 3: Click the **Network** tab, and then in the Actions pane, click **Change Dynamic vNIC Connection Policy**.

Step 4: On the Change Dynamic vNIC Connection Policy dialog box, in the **Select the Dynamic vNIC Connection Policy** list, choose **Use a Dynamic vNIC Connection Policy**.

Step 5: In the **Dynamic vNIC** list, select the policy created in Procedure 1, (Example: IOM_to_FI_4-Link), and then click **OK**. The server reboots after the policy has been applied.



Process

Configuring Distributed Virtual Switches

1. Install Cisco VEM software bundle
2. Configure VMware integration
3. Add a host to the Cisco VM-FEX DVS
4. Configure VM to use DirectPath I/O

Procedure 1 Install Cisco VEM software bundle

Cisco VM-FEX uses the same VEM software functionality as the Cisco Nexus 1000V Series switch for creating and using port profiles.

Step 1: In a web browser, navigate to the Cisco website, and then navigate to **Downloads Home > Products > Servers - Unified Computing > Cisco UCS B-Series Blade Server Software > Unified Computing System (UCS) Drivers**.

Step 2: Select the driver ISO image corresponding to the Cisco UCS release you are working on.

Step 3: Download the driver package ISO image file, and then save it on your local disk drive (Example: ucs-bxxx-drivers.2.1.1a.iso).

Step 4: Use an ISO extraction tool in order to extract the contents of the ISO image.

Step 5: Navigate to **VMware > VM-FEX > Cisco > 1280 > ESXi_5.0U1**, and then extract the .vib file labeled **cross_cisco-vem-v132-...vib** (Example: cross_cisco-vem-v132-4.2.1.1.4.1.0-3.0.4.vib) to your local disk drive.

Step 6: Launch VMware vSphere Client, and then log into the VMware vCenter server that you created in Procedure 1 "Install VMware vCenter Server."

Next, you upload the locally saved .vib file to the storage system of the Cisco UCS B-Series server that will be used for Cisco VM-FEX operation.

Step 7: In vSphere Client, select the host.

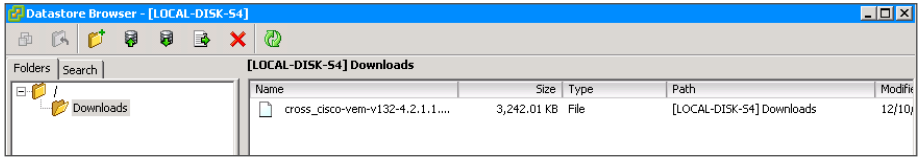
Step 8: Navigate to **Configuration > Storage**.

Step 9: Right-click the datastore, and then click **Browse Datastore**.

Step 10: In the Datastore Browser window, on the Folders tab, create a folder named Downloads.

Step 11: Double-click the **Downloads** folder, click the **Upload Files** to this datastore icon, and then browse to the folder where you have stored the VEM .vib file.

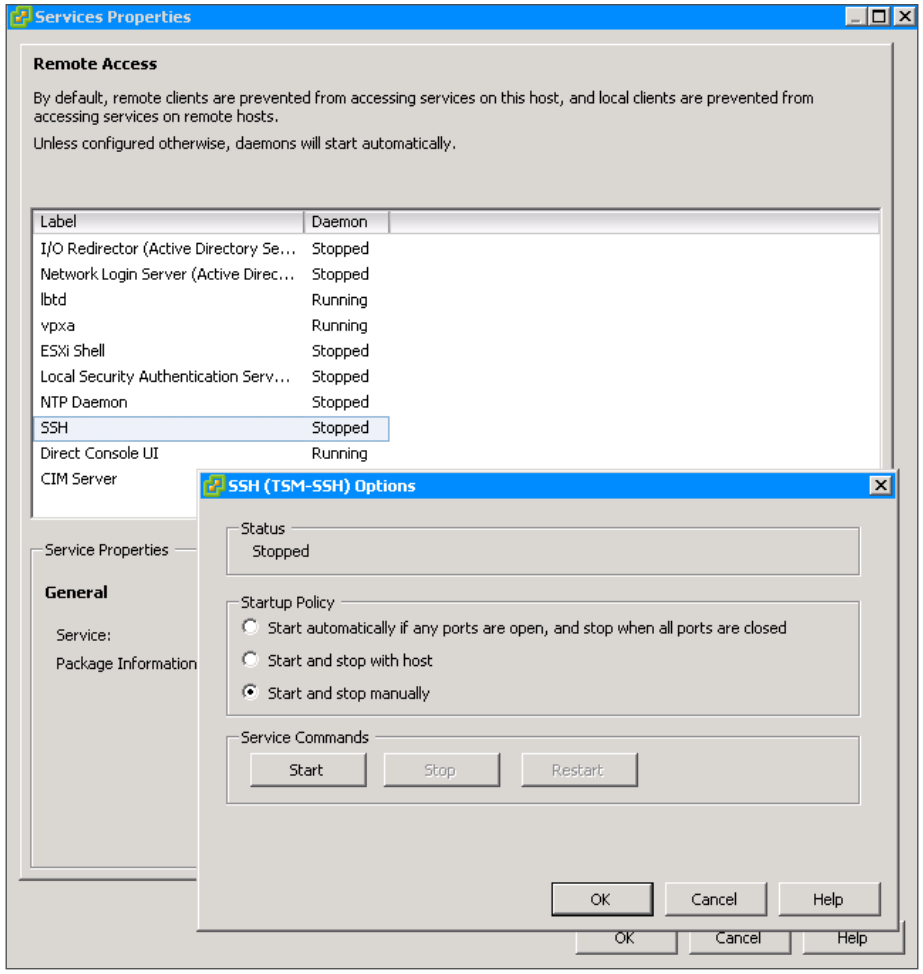
Step 12: Once complete, browse to the folder, and make sure the file has been uploaded.



Step 13: On the Configuration tab, from the Software list, choose **Security Profile**, and then on the Security Profile screen, in the Services section, click **Properties**.

Step 14: If the status of SSH is Running, skip to the next step.

If the status of SSH is Stopped, select **SSH**, click **Options**, and under Startup Policy, select **Start and Stop manually**, and then click **OK**.



Step 15: Open an SSH client, and then log in to the management IP address of the ESXi server. This server is the same target Cisco UCS B-Series server for the Cisco VM-FEX operation.

Step 16: Copy the .vib file to the /var/log/vmware/ directory.

```
# cp /vmfs/volumes/LOCAL-DISK-S4/Downloads/cross_cisco-vem-v132-4.2.1.1.4.1.0-3.0.4.vib /var/log/vmware/
```

Step 17: Install the Cisco VEM software bundle.

```
/var/log/vmware # esxcli software vib install -v cross_cisco-vem-v132-4.2.1.1.4.1.0-3.0.4.vib
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: Cisco_bootbank_cisco-vem-v132-esx_4.2.1.1.4.1.0-3.0.4
   VIBs Removed:
   VIBs Skipped:
```

Step 18: Verify the installation of the Cisco VEM software bundle was successful.

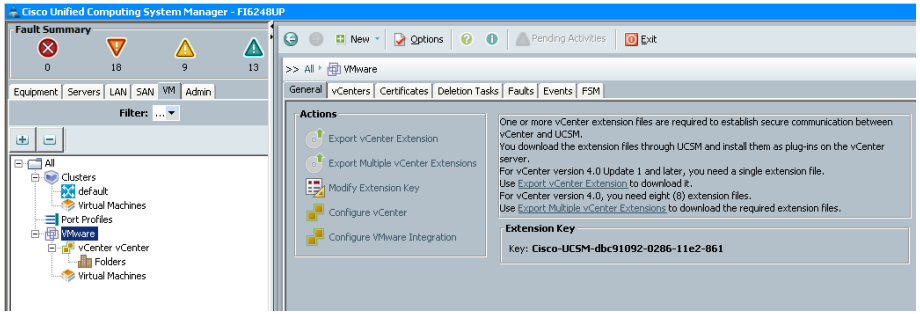
```
/var/log/vmware # vem status -v
Package vssnet-esxmn-ga-release
Version 4.2.1.1.4.1.0-3.0.4
Build 4
Date Thu Aug 25 10:47:10 PDT 2011

Number of PassThru NICs are 54
VEM modules are loaded

Switch Name Num Ports Used Ports Configured Ports MTU   Uplinks
vSwitch0    128       4          128              1500  vmnic0,vmnic1

Number of PassThru NICs are 54
VEM Agent (vemdpa) is running
```

Procedure 2 Configure VMware integration

In this procedure, you integrate VMware vCenter with Cisco UCS Manager in order to provide a communications path for the Cisco VM-FEX port profiles created on Cisco UCS Manager to be learned by vCenter. A port profile in Cisco UCS Manager is represented as a port group in vCenter.

Step 1: In the Cisco UCS Manager navigation pane, click the **VM** tab, and then expand **All** > **VMware**.

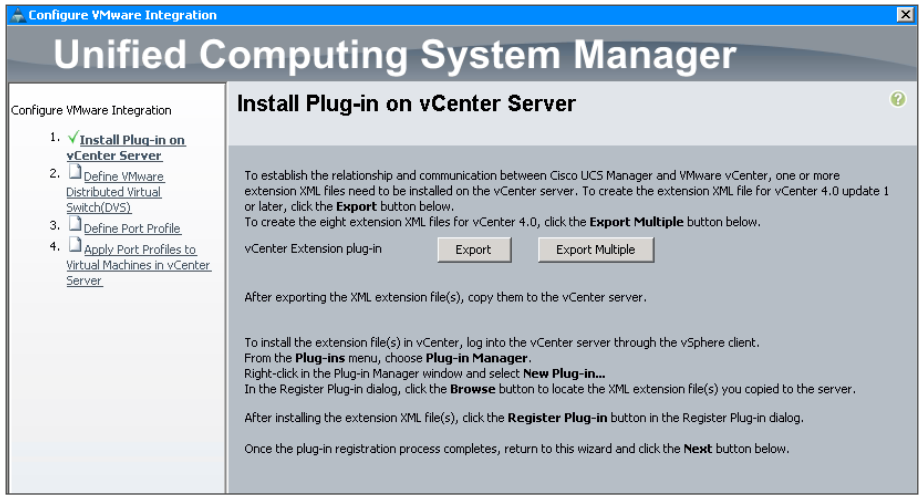
Step 2: In the work pane, click the **General** tab, and then in the Actions pane, click **Configure VMware Integration**.



Step 3: In the Configure VMware Integration wizard, on the Install Plug-in on vCenter Server page, click **Export**. Do not click **Next** until you complete Step 4 through Step 11.

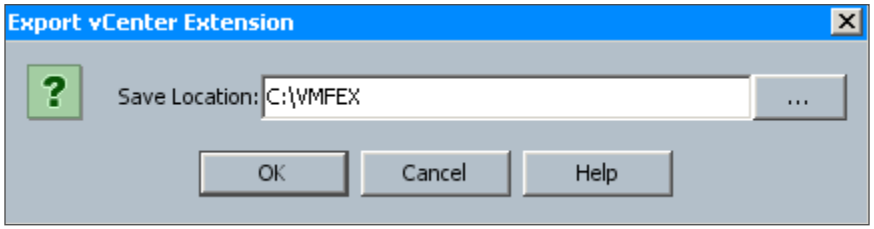
Caution

If you click **Next** on the Install Plug-in on vCenter Server page before completing Step 4 through Step 11, the vCenter server will be unable to establish communications with Cisco UCS Manager.



The Extension plug-in requires that you store the file on the local machine on which you are running Cisco UCS Manager.

Step 4: On the Export vCenter Extension dialog box, click the **...** button, browse to the location where you want the exported XML extension files to be saved, and then click **OK**.

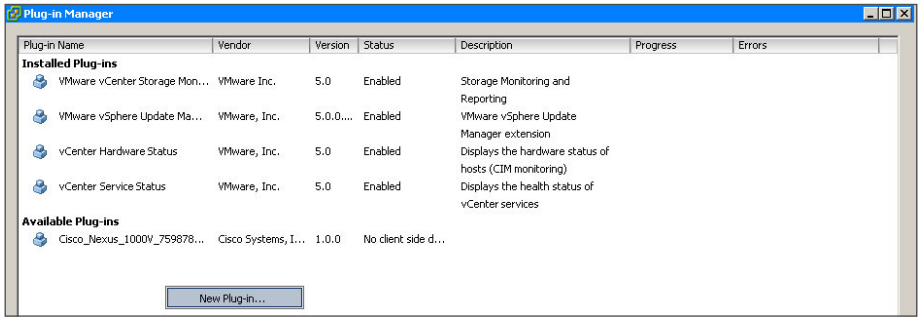


Step 5: Copy the exported XML extension files from your local machine to the server on which you are running vSphere Client, configured in Procedure 1 “Install vSphere Client”.

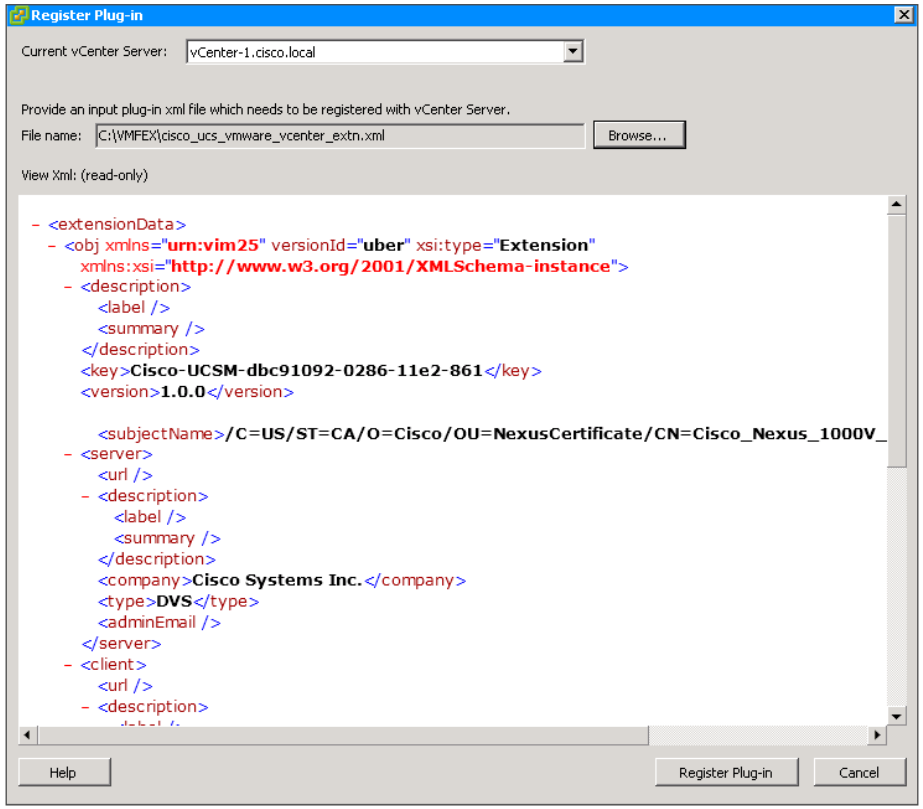
Step 6: Launch vSphere Client, and then enter the IP address and login credentials of the vCenter server.

Step 7: In vCenter, navigate to **Plug-ins** > **Manage Plug-ins**.

Step 8: On the Plug-in Manager window, under the Available Plug-ins section, right-click, and then click **New Plug-in**.



Step 9: On the Register Plug-in dialog box, browse to the location where you have stored the extension XML file that was copied in Step 5, and then click **Register Plug-in**.



Step 10: In the Security warning message, click **Ignore**.

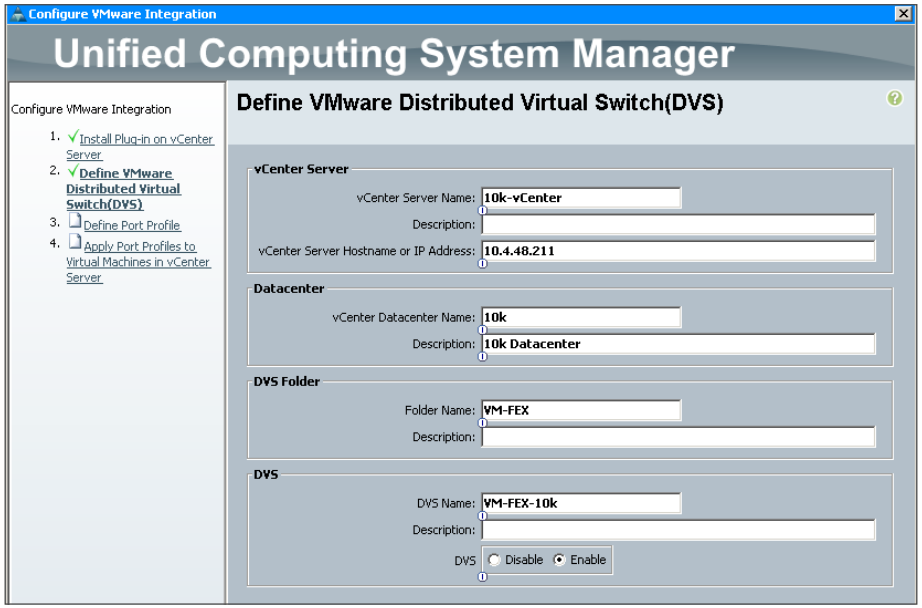
Step 11: On the message confirming that the plug-in has registered successfully with the vCenter server, click **OK**.

Step 12: Return to the Cisco UCS Manager Configure VMware Integration wizard, and then on the Install Plug-in on vCenter Server page, click **Next**.

Step 13: On the Defining a VMware vCenter Distributed Virtual Switch (DVS) page, enter the following, and then click **Next**:

- vCenter Server Name—10k-vCenter
- vCenter Server Hostname or IP Address—10.4.48.211
- vCenter Datacenter Name—10k
- DVS Folder Name—VM-FEX
- DVS Name—VM-FEX-10k
- DVS—Enable

Any configuration changes related to DVS will now be pushed to VMware vCenter.



Port profiles contain the properties and settings used to configure virtual interfaces in Cisco UCS. In VMware vCenter, a port profile is represented as *port group*. At least one port profile client for a port profile has to be configured, if you want Cisco UCS Manager to push the port profile to VMware vCenter. The port profile client determines the DVS to which a port profile is applied. In the following step you define the initial port profile to be added to the DVS, then in a later step, you can add more port profiles (VLANs) to the DVS.

Step 14: On the Define Port Profile page, in the Port Profile group box, enter the following:

- Name—DC_Management
- Network Control Policy—CDP-En-LinkLoss
- Max Ports—64 (the default number of ports that can be associated with a single DVS)

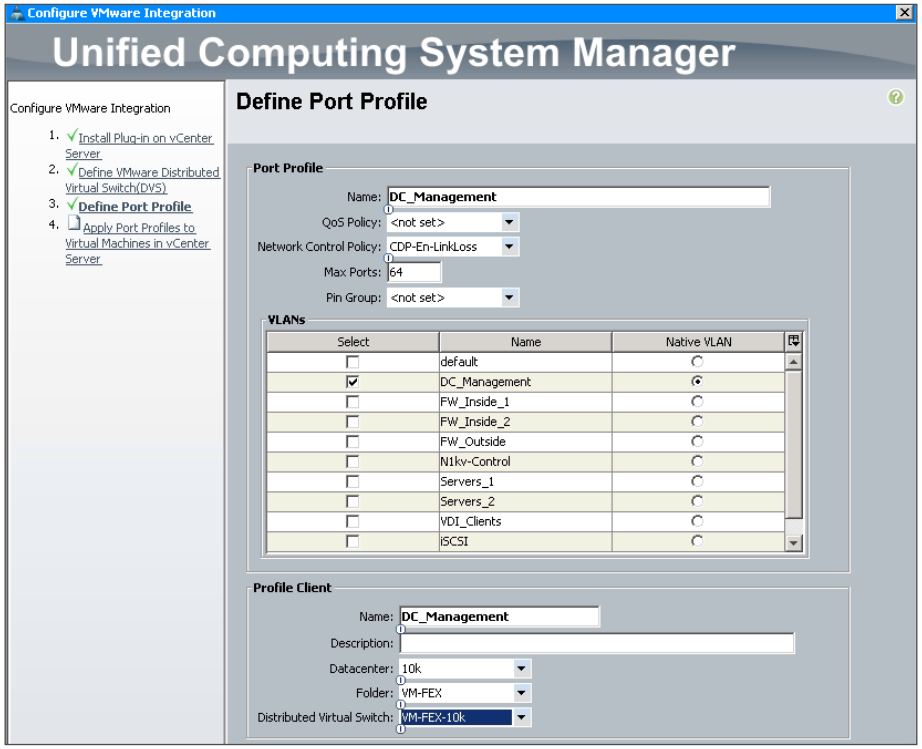
Step 15: In the VLANs list, for the VLAN that you want to associate to your first port profile (Example: DC_Management), select **Select**, and then select **Native VLAN**.

Tech Tip

If the virtual machine can tag the traffic, it is not necessary to select **Native VLAN**.

Step 16: In the Profile Client group box, enter the following, and then click **Next**:

- Name—DC_Management
- Datacenter—10k
- Folder—VM-FEX
- Distributed Virtual Switch—VM-FEX-10k

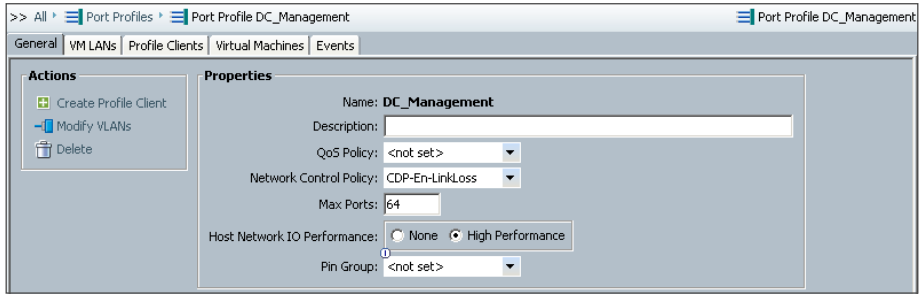


Step 17: On the Apply Port Profiles to Virtual Machines in vCenter Server page, click **Finish**. Cisco UCS Manager connects to the vCenter Server, creates the specified DVS, and applies the port profile.

Step 18: In Cisco UCS Manager, click the **VM** tab, expand **All** > **Port Profiles**, and then select the port profile you created in Step 14. (Example: DC_Management)

Step 19: In the General tab, in the Properties section, for Host Network IO Performance, select **High Performance**, and then click **OK**.

High-performance mode allows traffic to and from a VM to bypass the software DVS and hypervisor.



Step 20: If you want to create additional port profiles, in Cisco UCS Manager, click the **VM** tab, expand **All** > **Port Profiles**, right-click, and then click **Create Port Profile**.

If you do not want to create any additional port profiles, skip to Step 23.

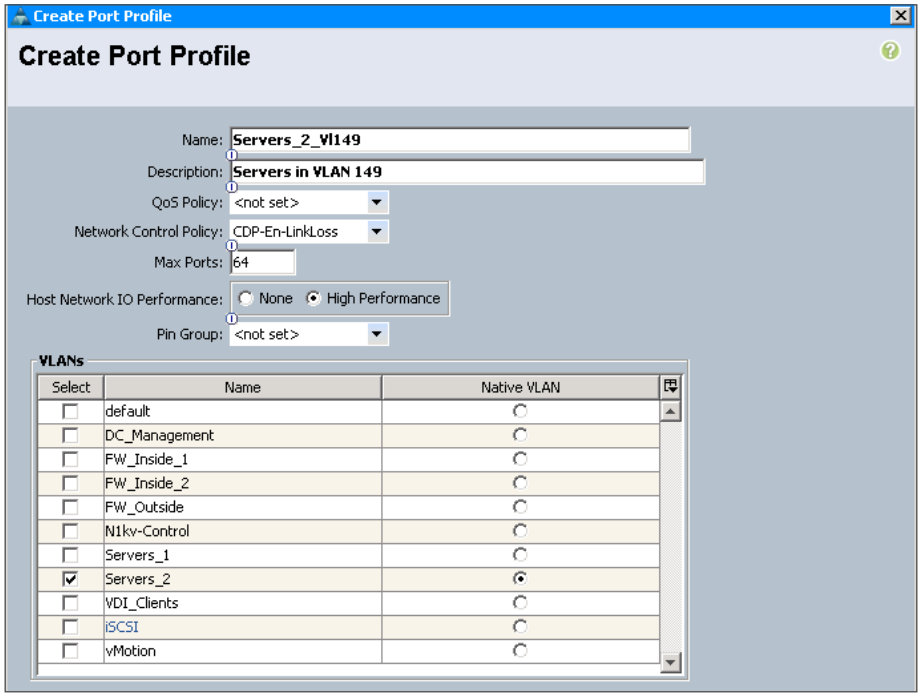
Step 21: On the Create Port Profile dialog box, enter the following information:

- Name—**Servers_2_VI149**
- Network Control Policy—**CDP-En-LinkLoss**
- Max Ports—**64** (the default number of ports that can be associated with a single DVS)
- Host Network IO Performance—**High Performance**

Step 22: In the VLANs list, for the VLAN that you want to associate to your port profile (Example: Servers_2), select **Select**, select **Native VLAN**, and then click **OK**.

Tech Tip

If the virtual machine can tag the traffic, it is not necessary to select **Native VLAN**.

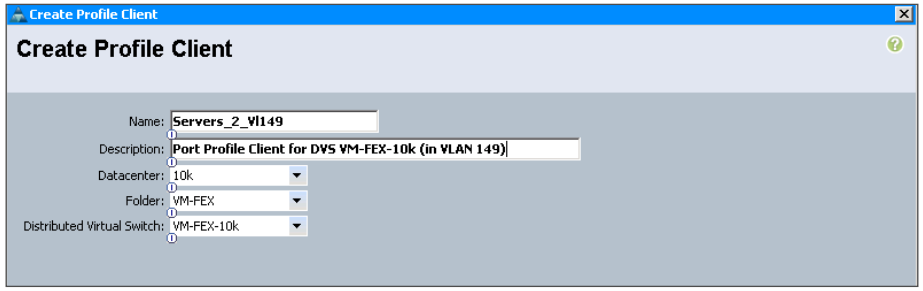


Next, you create the associated additional port profile client.

Step 23: Right-click on the port profile for which you want to create a profile client, and then click **Create Profile Client**.

Step 24: On the Create Profile Client dialog box, enter the following information, and then click **OK**:

- Profile Client Name—Servers_2_VI149
- Profile Client Datacenter—10k
- Profile Client Folder—VM-FEX
- Profile Client Distributed Virtual Switch—VM-FEX-10k



The following figures illustrate the successful creation of port profiles in Cisco UCS Manager and the successful communication of the port profiles in vCenter.

Figure 13 - Port profiles in Cisco UCS Manager

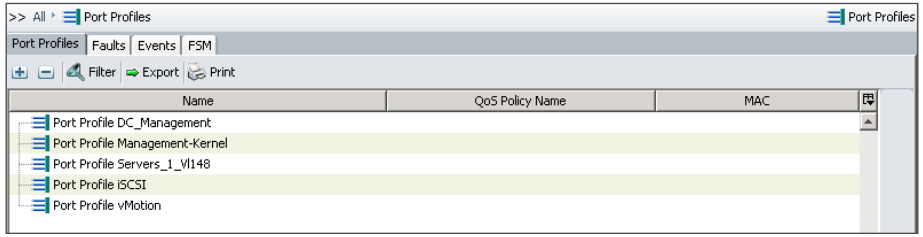
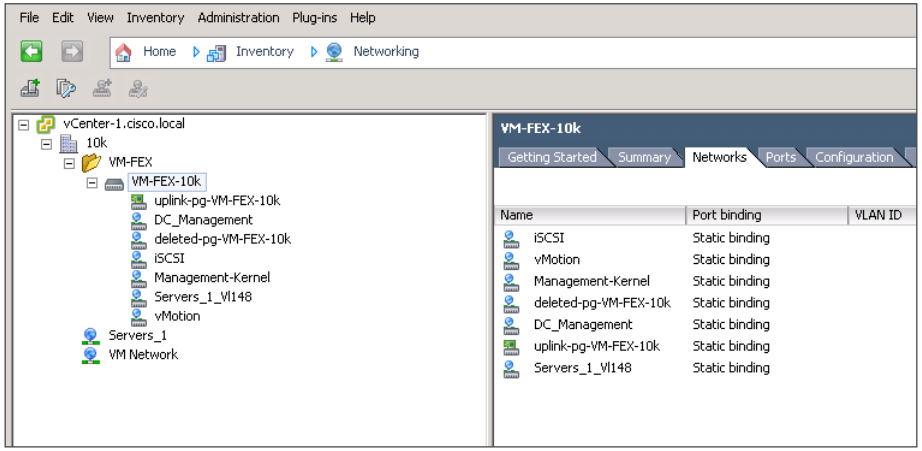


Figure 14 - DVS created in VMware vCenter



Procedure 3 Add a host to the Cisco VM-FEX DVS

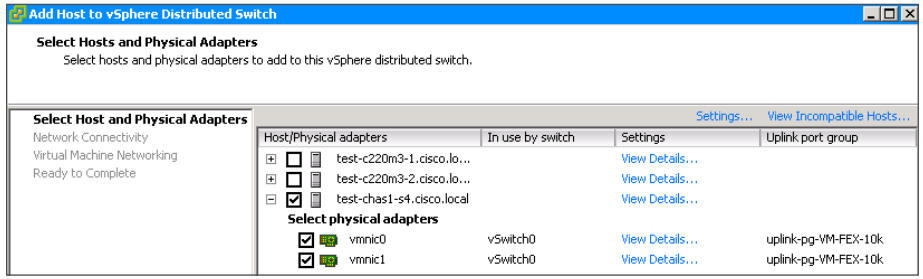
At this point, you are ready to connect the target Cisco UCS B-Series server for the Cisco VM-FEX operation to the created DVS (Example: VM-FEX-10k).

Step 1: In vCenter, navigate to **Home > Inventory > Networking**, select the distributed virtual switch you created, right-click on the DVS, and then click **Add a Host**.

Step 2: Complete the Add Host to vSphere Distributed Switch wizard and note the following:

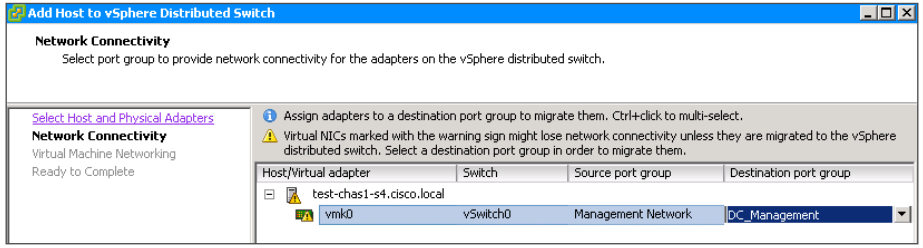
- On the Select Host and Physical Adapters page, select the ESXi host you want to add to the DVS (Example: test-chas1-s4.cisco.local), select the host's physical adapters that you want to use, and then click **Next**.

  The physical adapters are placed in the uplink port group that was automatically created during the creation of the DVS.



- On the Network Connectivity page, assign the virtual adapters to an appropriate port group for the traffic that they are carrying, and then click **Next**.

  In this example, the vmKernel management network port group is being assigned to the DC_Management port group.

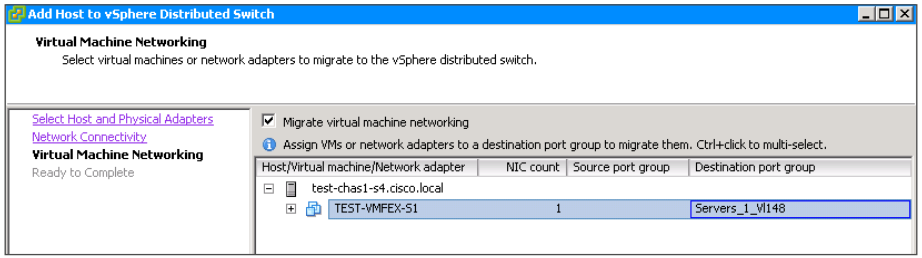


- If you have virtual machines already assigned to this ESXi host, on the Virtual Machine Networking page, select **Migrate virtual machine networking**, and in the **Destination port group** list for each virtual machine, choose the appropriate destination port group, and then click **Next**.

  In this example, the vmNIC for the VM is being assigned to the Servers_1_VI148 port group.

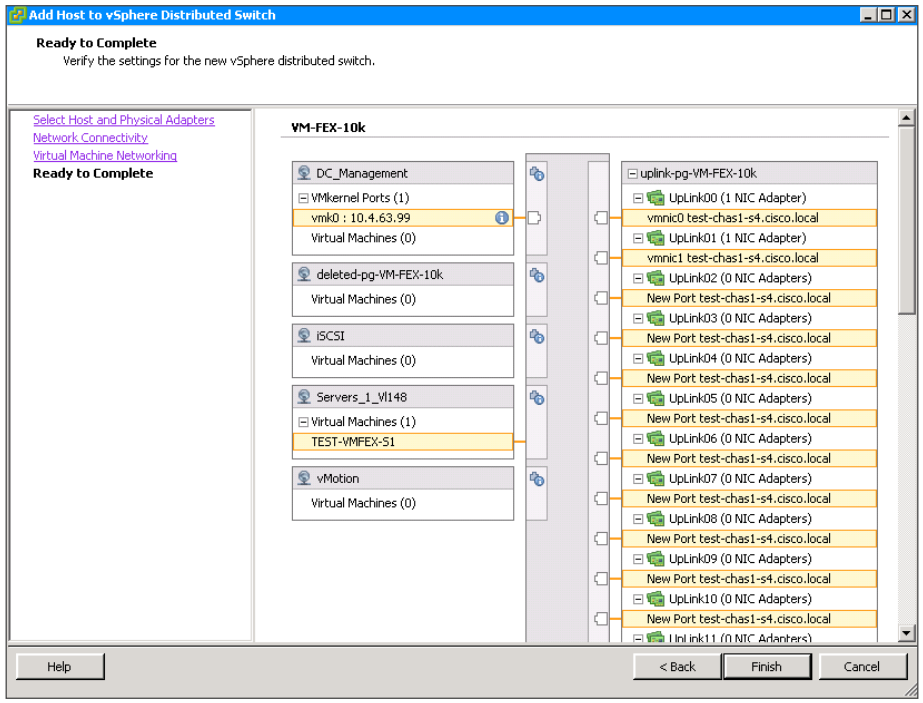
Tech Tip

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 VM-FEX DVS for the new VMs. When a new virtual machine is provisioned, the server administrator selects the appropriate port profile. The server administrator can reuse the port profile to provision similar virtual machines as needed.

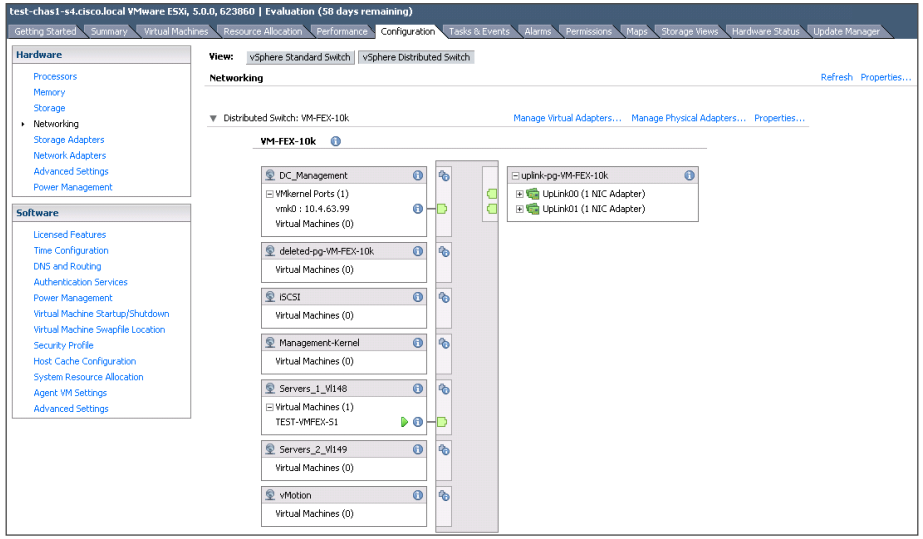


- On the Ready to Complete page, verify that the settings for the new vSphere distributed switch are correct, and then click **Finish**.

  Existing interfaces from other hosts are included in the display, because it represents a switch that is distributed across multiple hosts.



Step 3: When the host has completed the Update Network Configuration task, navigate to **Inventory > Hosts and Clusters**, select the host name, navigate to the Configuration tab, choose **Networking**, and then click **vSphere Distributed Switch**. View the results of the configuration.



At this point, your host is connected to the DVS, and traffic is flowing through the DVS in standard mode. The next procedure will allow the virtual machine to operate in high-performance mode, using DirectPath I/O.

Procedure 4 Configure VM to use DirectPath I/O

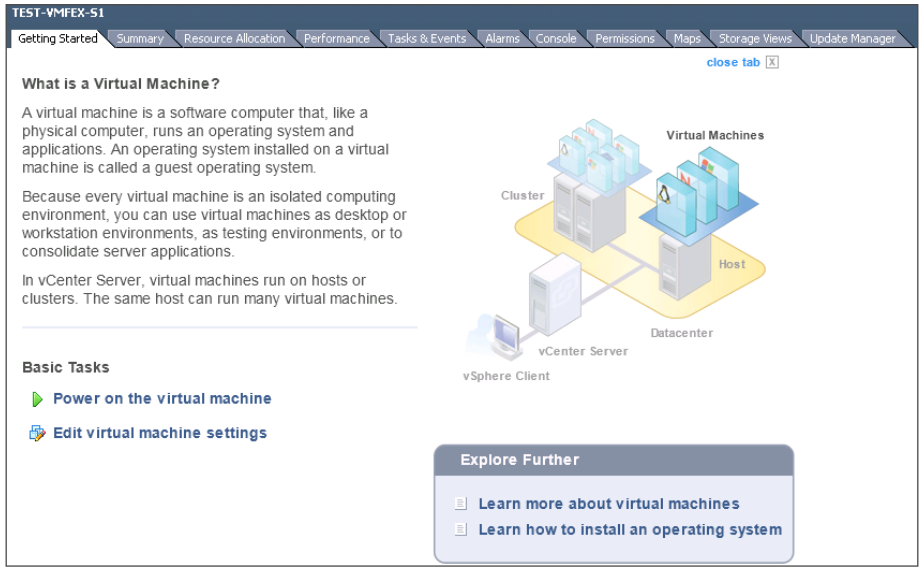
VM DirectPath I/O with VMware vMotion supported in ESXi 5.0 is the high-performance mode in Cisco VM-FEX. The virtual machines using the VM DirectPath I/O dynamic vNICs should have a reservation for all of the provisioned memory for that VM. If you are configuring for high-performance mode, and memory resources are over-provisioned, the VM cannot operate in high-performance mode. The memory reserved for all VMs must not exceed the physical available memory on the ESXi host.

In this procedure, you reserve memory for high-performance mode. The network adapter type will be VMXNET3, which is the required adapter type for a Windows OS virtual machine that uses DirectPath I/O.

Step 1: In vCenter Server, navigate to **Home > Inventory > Hosts and Clusters**, and then select the host that you have added to the DVS (Example: VM-FEX-10k).

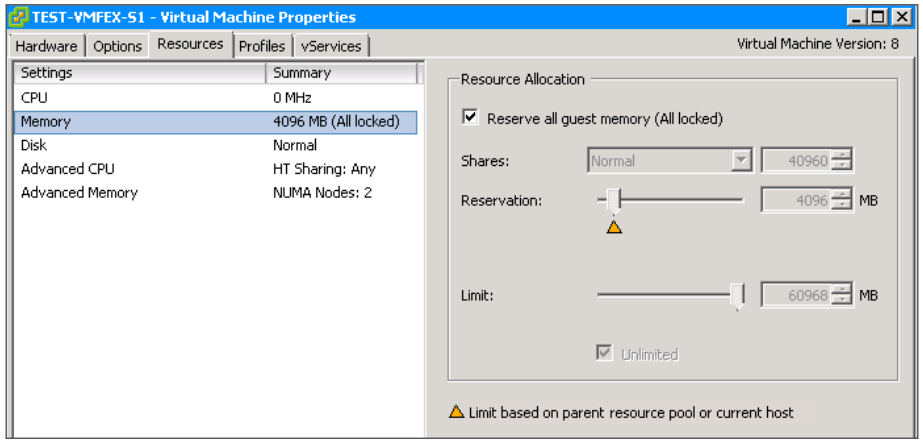
Step 2: Select the virtual machine for which you want to reserve memory (Example: test-chas1-s4.cisco.local).

Step 3: In the Getting Started tab, under the Basic Tasks section, select **Edit virtual machine settings**.



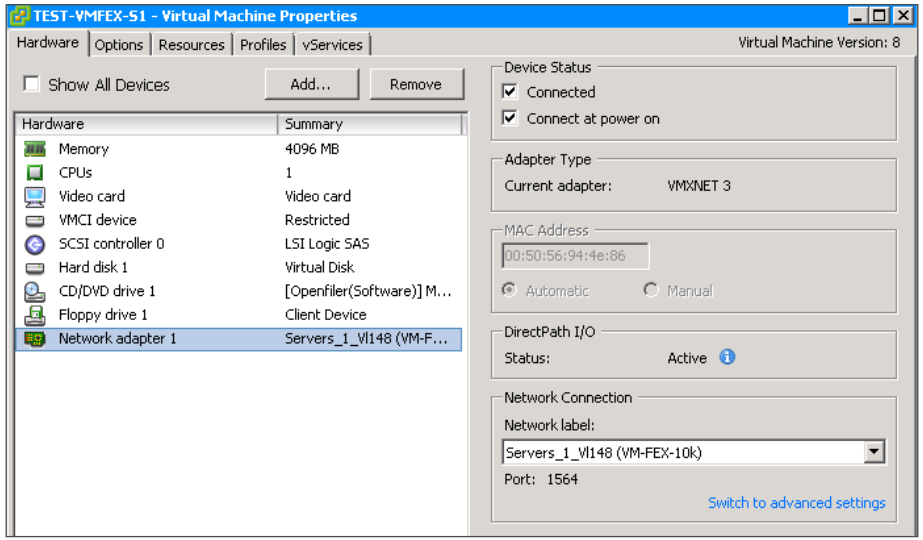
Step 4: On the Virtual Machine Properties dialog box, click the **Resources** tab, and then under Settings, select **Memory**.

Step 5: In the Resource Allocation section, select **Reserve all guest memory (All locked)**, and then click **OK**.



Step 6: For the same virtual machine, click **Edit virtual machine settings**. The Virtual Machine Properties dialog box reopens.

Step 7: Click the **Hardware** tab, and then under Hardware, select **Network adapter 1**. Under DirectPath I/O, the Status is Active. This confirms that VM DirectPath I/O feature is active.



This concludes the "Cisco Virtual Machine Fabric Extender (VM-FEX) Configuration and Deployment" section.

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 high-performance, virtual machine environments, you can increase throughput and reduce latency with Cisco VM-FEX, while retaining the resilience and manageability of your VMware environment.

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)SV2(1.1)
	Nexus 1000V VSM on Physical Media	N1K-VSMK9-404S12=	
VMWare	ESXi	ESXi	5.0U1

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 5.2(1)N1(1b) 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 (enhanced) Fabric Extender	N2K-C2248TP-E	—
	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T Fabric Extender	N2K-C2248TP-1GE	
	Cisco Nexus 2000 Series 32 1/10 GbE SFP+, FCoE capable Fabric Extender	N2K-C2232PP-10GE	

Data Center Services

Functional Area	Product Description	Part Numbers	Software
Firewall	Cisco ASA 5585-X Security Plus IPS Edition SSP-40 and IPS SSP-40 bundle	ASA5585-S40P40-K9	ASA 9.0(1) IPS 7.1(6) E4
	Cisco ASA 5585-X Security Plus IPS Edition SSP-20 and IPS SSP-20 bundle	ASA5585-S20P20X-K9	
	Cisco ASA 5585-X Security Plus IPS Edition SSP-10 and IPS SSP-10 bundle	ASA5585-S10P10XK9	

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(8)
	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	2.1(1a) Cisco UCS Release
	Cisco UCS up to 96-port Fabric Interconnect	UCS-FI-6296UP	
UCS B-Series Blade Servers	Cisco UCS Blade Server Chassis	N20-C6508	2.1(1a) Cisco UCS Release
	Cisco UCS 8-port 10GbE Fabric Extender	UCS-IOM2208XP	
	Cisco UCS 4-port 10GbE Fabric Extender	UCS-IOM2204XP	
	Cisco UCS B200 M3 Blade Server	UCSB-B200-M3	
	Cisco UCS B200 M2 Blade Server	N20-B6625-1	
	Cisco UCS B250 M2 Blade Server	N20-B6625-2	
	Cisco UCS 1280 Virtual Interface Card	UCS-VIC-M82-8P	
	Cisco UCS M81KR Virtual Interface Card	N20-AC0002	
UCS C-Series Rack-mount Servers	Cisco UCS C220 M3 Rack Mount Server	UCSC-C220-M3S	1.4.6 Cisco UCS CIMC Release
	Cisco UCS C240 M3 Rack Mount Server	UCSC-C240-M3S	
	Cisco UCS C200 M2 Rack Mount Server	R200-1120402W	
	Cisco UCS C210 M2 Rack Mount Server	R210-2121605W	
	Cisco UCS C250 M2 Rack Mount Server	R250-2480805W	
	Cisco UCS 1225 Virtual Interface Card Dual Port 10Gb SFP+	UCSC-PCIE-CSC-02	
	Cisco UCS P81E Virtual Interface Card Dual Port 10Gb SFP+	N2XX-ACPCI01	

Appendix B: Configuration Files

The following is the configuration from the deployed Cisco Nexus 1000V Virtual Supervisor Module.

```
N1kvVSM# show run
version 4.2(1)SV2(1.1)
no feature telnet
feature tacacs+
feature dhcp
feature cts
feature vtracker

username admin password 5 *****  role network-admin

banner motd #Nexus 1000v Switch#

ssh key rsa 2048
ip domain-lookup
ip host N1kvVSM 10.4.63.28
tacacs-server host 10.4.48.15 key 7 "VagwwtFjq"
aaa group server tacacs+ tacacs
    server 10.4.48.15
    use-vrf management
    source-interface mgmt0
aaa group server radius aaa-private-sg
hostname N1kvVSM
errdisable recovery cause failed-port-state
vem 3
  host vmware id 6a41e931-fca6-11e0-bd1d-70ca9bce3498
vem 4
  host vmware id dbc91092-0286-11e2-00ff-0000000000ff
vem 5
  host vmware id dbc91092-0286-11e2-00ff-00000000002f
vem 6
  host vmware id dbc91092-0286-11e2-00ff-0000000001bf
snmp-server user admin network-admin auth md5 ***** priv *****
localizedkey
snmp-server community cisco group network-operator
snmp-server community cisco123 group network-admin
ntp server 10.4.48.17
aaa authentication login default group tacacs

vrf context management
  ip name-server 10.4.48.10
  ip route 0.0.0.0/0 10.4.63.1
vlan 1,148-157,160-163
vlan 148
  name Servers_1
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 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 148-157,160-162
  channel-group auto mode on mac-pinning
  no shutdown
  system vlan 160,162
  description Uplink for C-Series
  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 vMotion
  vmware port-group
  switchport mode access
  switchport access vlan 161
  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 ethernet System-Uplink
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 148-157,160-163
  channel-group auto mode on mac-pinning
  no shutdown
  system vlan 160,162-163
  description Uplink for B-Series
  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 VDI_Servers
  vmware port-group
  switchport mode access
  switchport access vlan 157
  no shutdown
  state enabled

vdc N1kvVSM 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
```

```
interface port-channel1
  inherit port-profile ESXi-Mgmnt-Uplink
  vem 3

interface port-channel2
  inherit port-profile 10G-CSeries
  vem 3

interface port-channel3
  inherit port-profile System-Uplink
  vem 4

interface port-channel4
  inherit port-profile System-Uplink
  vem 5

interface port-channel5
  inherit port-profile System-Uplink
  vem 6

interface mgmt0
  ip address 10.4.63.28/24

interface Vethernet1
  inherit port-profile n1kv-L3
  description VMware VMkernel, vmk0
  vmware dvport 128 dvswitch uuid "ca 56 ... 5b 88"
  vmware vm mac 70CA.9BCE.349C

interface Vethernet2
  inherit port-profile vMotion
  description VMware VMkernel, vmk1
  vmware dvport 64 dvswitch uuid "ca 56 ... 5b 88"
  vmware vm mac 0050.567E.A8E0

interface Vethernet3
  inherit port-profile iSCSI
  description VMware VMkernel, vmk2
  vmware dvport 101 dvswitch uuid "ca 56 ... 5b 88"
  vmware vm mac 0050.5671.F767

interface Vethernet4
  inherit port-profile n1kv-L3
  description VMware VMkernel, vmk0
  vmware dvport 129 dvswitch uuid "ca 56 ... 5b 88"
  vmware vm mac 0025.B5FF.009E

interface Vethernet5
  inherit port-profile iSCSI
  description VMware VMkernel, vmk1
  vmware dvport 100 dvswitch uuid "ca 56 ... 5b 88"
  vmware vm mac 0050.567E.562C

interface Vethernet6
  inherit port-profile vMotion
  description VMware VMkernel, vmk2
  vmware dvport 65 dvswitch uuid "ca 56 ... 5b 88"
  vmware vm mac 0050.5675.7342

interface Vethernet7
  inherit port-profile Servers_Vl148
  description Win2008-Test1, Network Adapter 1
  vmware dvport 32 dvswitch uuid "ca 56 ... 5b 88"
  vmware vm mac 0050.56A2.5D85

interface Vethernet8
  inherit port-profile IT_VDI_users
  description IT-VDI-Users, Network Adapter 1
  vmware dvport 224 dvswitch uuid "ca 56 ... 5b 88"
  vmware vm mac 0050.56A2.5D94
```

```
interface Vethernet10
  inherit port-profile n1kv-L3
  description VMware VMkernel, vmk0
  vmware dvport 131 dvswitch uuid "ca 56 ... 5b 88"
  vmware vm mac 0025.B5FF.003F

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 Ethernet4/1
  inherit port-profile System-Uplink

interface Ethernet4/2
  inherit port-profile System-Uplink

interface Ethernet6/1
  inherit port-profile System-Uplink

interface Ethernet6/2
  inherit port-profile System-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.4.2.1.SV2.1.1.bin
sup-1
boot system bootflash:/nexus-1000v.4.2.1.SV2.1.1.bin sup-1
boot kickstart bootflash:/nexus-1000v-kickstart.4.2.1.SV2.1.1.bin
sup-2
boot system bootflash:/nexus-1000v.4.2.1.SV2.1.1.bin sup-2
ip dhcp snooping vlan 157
svs-domain
  domain id 10
  control vlan 1
  packet vlan 1
  svs mode L3 interface mgmt0
svs connection vcenter
  protocol vmware-vim
  remote ip address 10.4.48.11 port 80
  vmware dvs uuid "ca 56 22 50 f1 c5 fc 25-75 6f 4f d6 ad 66 5b
88" datacenter-name 10k
  max-ports 8192
  connect
vservice global type vsg
  tcp state-checks invalid-ack
  tcp state-checks seq-past-window
  no tcp state-checks window-variation
  no bypass asa-traffic
vnm-policy-agent
  registration-ip 0.0.0.0
  shared-secret **********
  log-level
```

Appendix C: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series:

- We upgraded the VMware environment to version 5.0U1 and updated processes to match the new procedures and steps required for deployment.
- We added Cisco UCS C-Series servers with Cisco FlexFlash as an option for VMware ESXi image boot.
- We updated the Cisco Nexus 1000V software to the 2.1 release and updated procedures and steps required for deployment.
- We added the "Cisco Virtual Machine Fabric Extender Configuration and Deployment" section, targeted at environments using Cisco UCS B-Series servers with Cisco virtual interface cards and VMware ESXi release 5.0U1.

Notes

Feedback

Please use the feedback form to send comments and suggestions about this guide.

SMART BUSINESS ARCHITECTURE

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.

B-0000555-1 2/13