## cisco.



# Virtualization with Cisco UCS, Nexus 1000V, and VMware

TECHNOLOGY DESIGN GUIDE

August 2013



## Table of Contents

Preface	.1
CVD Navigator	.2
Use Cases	2
Scope	2
Proficiency	3
Introduction	.4
Technology Use Cases	4
Use Case: Reduce Application Deployment Time	5
Use Case: Simplify Network Management in the Data Center	5
Use Case: Increase Network Performance in the Hypervisor Environment	5
Design Overview	6
VMware Scalable Solutions	6
Virtual Switching with Cisco Nexus 1000V	7
Cisco Unified Computing System Server Hardware 1	10
Network and Storage Connectivity1	12

Deployment Details	
Preparing the Environment for VMware	13
Preparing the Environment for Server Access to SAN	13
VMware vSphere Installation and Setup	19
Installing VMware ESXi on Cisco UCS Servers	19
Configuring the ESXi Console	
Installing vSphere Client	
Adding Networking for Virtual Machines	
Configuring Data Storage for the ESXi Host	
Creating a Virtual Machine	54
Installing and Configuring VMware vCenter Server	
Installing VMware vSphere Update Manager	
Migrating Virtual Machine Storage and Virtual Machines	
Cisco Nexus 1000V Series Switch Installation and Deployment	
Deploying Cisco Nexus 1000V VSM as a VM on an ESXi Host	
Configuring Virtualized Hosts to use the Cisco Nexus 1000V switch	110
Cisco Virtual Machine Fabric Extender Configuration and Deployment	
Virtualization with a Virtual Interface Card Adapter	
Cisco VM-FEX Modes of Operation	
Configuring a Service Profile with Cisco VM-FEX	
Configuring Distributed Virtual Switches	
Summary	
Appendix A: Product List	140
Appendix B: Configuration Files	

## Preface

Cisco Validated Designs (CVDs) provide the framework for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Cisco engineers have comprehensively tested and documented each CVD in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested and validated design and deployment details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.
- Solution design guides integrate or reference existing CVDs, but also include product features and functionality across Cisco products and may include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems using their own setup and configuration.

### **How to Read Commands**

Many CVD guides tell you how to use a command-line interface (CLI) to configure network devices. 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 at a CLI or script prompt appear as follows:

Router# enable

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

police rate 10000 pps burst 10000 packets conform-action set-discard-classtransmit 48 exceed-action transmit

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 feedback form.

For the most recent CVD guides, see the following site:

http://www.cisco.com/go/cvd

## CVD Navigator

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

### **Use Cases**

This guide addresses the following technology use cases:

- Reduce Application Deployment Time—Quickly deploy a new application on a portion of a server (or virtual machine) by using the VMware hypervisor. Optimize server deployment by virtualizing the physical server and network connectivity components.
- Simplify Network Management in the Data Center– Virtualization of the data center provides flexibility for server and network components, but can lead to increased operational complexity. Reduce complexity by using a single CLI and common feature set for the data center core switching and the hypervisor-based virtual switches.
- Increase Network Performance in the Hypervisor Environment—Bypass software-based virtual switches and connect directly to the data center switch fabric for high performance applications.

For more information, see the "Use Cases" section in this guide.

## Scope

This guide covers the following areas of technology and products:

- VMware ESXi version 5.0 installation on Cisco UCS B-Series Blade Servers and C-Series Rack-Mount Servers
- VMware ESXi for Ethernet and storage connectivity including boot from local storage and boot from SAN
- VMware management tools for deploying and managing virtual servers
- Cisco Nexus 1000V Series distributed virtual switch
- Cisco Virtual Machine Fabric Extender (VM-FEX) on a Cisco UCS B-Series Server for high performance network connectivity

For more information, see the "Design Overview" section in this guide.

### **Related CVD Guides**



Unified Computing System Technology Design Guide



Data Center Technology Design Guide



To view the related CVD guides, click the titles or visit the following site: http://www.cisco.com/go/cvd

## **Proficiency**

This guide is for people with the following technical proficiencies-or equivalent experience:

- CCNP Data Center-3 to 5 years designing, implementing, and troubleshooting data centers in all their components
- VCP VMware—At least 6 months installing, deploying, scaling, and managing VMware vSphere environments

## Introduction

The *Virtualization with Cisco UCS, Nexus 1000V, and VMware Design Guide* is designed to build upon the Cisco Unified Computing System (UCS) B-Series and C-Series server foundation deployment detailed in the Unified Computing System Design 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 5.0 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. VMware vSphere Update Manager installation is included and can be used to update the virtualized servers to the latest patches recommended for your deployment.
- 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.

## **Technology Use Cases**

Virtualization technology simplifies IT so that organizations can more effectively use their storage, network, and computing resources to control costs and respond faster to application deployment requests. 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.

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. 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 reduces the time needed to deploy these new solutions and applications.

#### **Use Case: Reduce Application Deployment Time**

Utilize the VMware hypervisor to quickly deploy a new application on a portion of a server (or virtual machine). Virtualize the physical server and network connectivity components in order to optimize server deployment for hypervisor or single operating system requirements.

This design guide enables the following data center capabilities:

- Combine hypervisor and server hardware virtualization—The combination of pools of physical server hardware, the ability to quickly assign a service profile to the hardware, and the use of hypervisor technology reduces the time needed to deploy a new application on a standalone server or a virtual machine of an existing server.
- **Replicate existing servers**—Use templates to quickly replicate physical servers with the optimal setup for VMware hypervisor installation.
- **Connect the application to the database**—By using centralized storage and multiprotocol SAN transport, applications can connect to shared data regardless of their location in the data center.
- Quickly satisfy application resource demands—As an application's requirements for processing power or storage changes, IT administrators can quickly add or reclaim virtual server resources across the data center.
- Boot from SAN for stateless computing—By moving operating system and data files to the SAN combined with the hardware independence of provisioning servers through service profiles, you can achieve the ideal of stateless computing.

#### Use Case: Simplify Network Management in the Data Center

The challenge in the virtualized data center is to reduce complexity while enabling the flexibility that virtualization provides. Deploy a single Cisco Nexus-based switch fabric on physical and virtual switches.

This design guide enables the following data center network capabilities:

- Single CLI for network switches—Use the same set of CLI commands and monitoring for physical Ethernet and virtual machine Ethernet switch ports.
- **Consistent network services**—Apply network host port features like Dynamic Host Configuration Protocol (DHCP) snooping and IP source guard to physical and virtual machine switch ports.
- Policy application-Recognize protocols and applications at the edge of the network and apply policy.

#### **Use Case: Increase Network Performance in the Hypervisor Environment**

Optimize network throughput in VMware hypervisor environments by bypassing software-based switches and allowing virtual machines to connect directly to the data center fabric by using virtual machine fabric extension (VM-FEX).

This design guide enables the following data center network capabilities:

- Flexible network connectivity–Use the standard mode of hypervisor switching for typical virtual machine requirements and when moving virtual machines between servers.
- High performance—Switch to direct path I/O to bypass the virtual switch and connect the virtual interface card directly to the virtual machine for lower latency, higher performance and throughput, and less processor impact.
- Virtual network interfaces—Use the Cisco virtual network interface card (NIC) to create multiple standard or high performance network interfaces for virtual machines with a single hardware adapter.

## **Design 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 CVD 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 CVD 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(1.1a) and VMware ESXi version 5.0U1 patched to 5.0U2.

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.





#### 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.

#### **Cisco Unified Computing System Server Hardware**

The primary computing platforms deployed in the CVD 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 CVD. When deployed in conjunction with the CVD 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 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 halfwidth 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 halfwidth 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 (CIMC) is the management service for Cisco UCS C-Series servers. CIMC runs within the server and 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 CIMC 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 Unified Computing System Design 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 *Virtualization with Cisco UCS, Nexus 1000V, and VMware Design Guide* is designed as an extension of the Data Center Design Guide. The basis of this architecture is an Ethernet switch fabric consisting of two Cisco Nexus 5500UP switches, as shown in the following figure.





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.

### Preparing the Environment for Server Access to SAN

- 1. Configure a storage array
- 2. Configure SAN zones

PROCESS

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 Unified Computing System Design Guide.

Procedure 1 and Procedure 2 of this process are also necessary if your server will be using Fibre Channel SANbased 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, VIC 1240, and VIC1280 in the Cisco UCS B-Series server are 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

This installation procedure provides a summary for configuring storage when you are using a NetApp FAS3200 storage array, which was used in the CVD data center validation. If you are using another manufacturer's storage array, the requirements are similar, but the exact steps may differ.

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

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

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

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

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

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

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

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

Initiator IDs:		
Add R Edit X Delete		
Initiator Name	Group Name	Group Type
20:00:00:25:65:99:99:67	UCS_8	FCP
20:00:00:25:65:99:99:71	UCS_8	FCP

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

#### Procedure 2 Configure SAN zones

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

しハ	Doodor Lir	٦.
-		,

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 Data Center Design 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 Unified Computing System Design 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 Unified Computing System Design 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.

>> 🚍 LAN + 💈 Policies + 🎄 root + 写 Network Control Policies + 写 CDP-En-LinkLoss			
General Events			
Actions	Properties		
📅 Delete	Name: CDP-En-LinkLoss		
Show Policy Usage	CDP: O Disabled O Enabled		
	MAC Register Mode: Only Native Vlan O All Host Vlans		
	Action on Uplink Fail: 💿 Link Down 🕓 Warning		
	MAC Security		
	Forge: O Allow O Deny		
	·		

**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 Unified Computing System Design Guide, and then at the bottom of the screen, click **Modify**.

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 Unified Computing System Design Guide, you will notice the vNIC template name used. You must modify the template in order to verify settings.

Name: eth0		
Use vNIC Templa Treate vNIC	te: 🔽 O Template	
vNIC Template:	vNIC-Fabric-A	-
Adapter Perfo	rmance Profile	
Adapter Policy:	VMWare	Create Ethernet Adapter Policy

Step 4: 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.

>> 📑 LAN + 🔊 Policies + 🚑 root + 🛐 vNIC Ter	nplates 🕨 📅 vNIC Template vNIC-F	Fabric-A
General VNIC Interfaces Faults Events		
Actions	Properties	
Modify VLANs	Name:	vNIC-Fabric-A
🗂 Delete	Description:	vNIC Template for Fabric A
	Fabric ID:	Fabric A      Fabric B      Enable Failover
		Target ✓ Adapter VM
	Template Type:	<ul> <li>Initial Template</li> <li>Updating Template</li> </ul>
	MTU:	1500
	Policies	
	MAC Pool:	default 🔹
	QoS Policy:	<not set=""></not>
	Network Control Policy:	CDP-En-LinkLoss
	Pin Group:	<not set=""></not>
	Stats Threshold Policy:	default
	Dynamic vNIC Connection Policy:	<not set=""></not>

Step 5: 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 6:** 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.

>> 🧔 Servers 🕴 🍮 Service Profiles 👌 🛕	root * 🖫 Service Profile Servers_SAU, Boot							
amenal Storage Methodik ISCSI MICS Boot Order Virtual Machines IPC Zones Policies Server Details IPSM VIIP Paths Pauls Events								
Action Change Dynamic Hill Convertion I Proofly MIC/Hills Flagment	Pyramic VIII: Connection VIII: Valid Science Specific VIII: Vital Sta Specific VIII: Vital Sta S	Policy sky Solition Policy Solition Policy Al Al Al Al Al Al Al Al Al Al	8					
VNICs								
💐 Filter 👄 Export 👸 Print								
Name	MAC Address	Desired Order	Actual Order	Fabric ID	Desired Placement	Actual Placement	172	
-II vNIC eth0	00:25:85:FF:00:7F	1	1	A	Any	Any		
-II vNIC eth1	00:25:85:FF:00:6F	2	2	6	Arry	Any		

Step 7: Select a service profile to associate to a Cisco UCS B-Series blade server.

**Step 8:** 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.

>> _ Servers 🖲 Service Profiles 👌 📩 root 👌 🐯 Service Profile Servers_SAN_Boot				💙 Service Profile Servers_SAN_Bo
General Storage Network ISCSI vNICs Boot Order Virtual Machines FC Zones Policies Se	arver Details FSM VIF Paths Faults Events			
Actions				
Modify Boot Policy				
Global Boot Policy				
Name: SAN-Boot				
Boot Policy Instance: org-root/boot-policy-SAN-Boot				
Description:				
Reboot on Boot Order Change: No				
Enforce vHIC/VHBA/(SCSI Name: No				
WARNINGS:				
The type (primary/secondary) does not indicate a boot order presence.				
The effective order of boot devices within the same device class (LAN(Storage(SCS)) is determine If Enforce white (within (SEEST Name is calented and the with Listen bits of a con-	ad by PCIe bus scan order.			
If it is not selected, the vHICs/vHBAs/ISCSI are selected if they exist, otherwise the vHIC/vHBA/	SCSI with the lowest PCIe bus scan order is used.			
Book Ovder				
🗶 🖃 🖧 Filter 👄 Export 读 Print				
Name Order	VNEC/VHBA//SCSI VNIC	Туре	Lun ID	www (R)
-@ CD-ROM 1				×
E Storage 2				
SAN primary	fc0	Primary		
- E SAN Target primary		Primary	0	50:06:01:61:3C:E0:60:E2
SAN Target secondary		Secondary	0	50:06:01:69:3C:E0:60:E2
E = SAN secondary	fci	Secondary		
SAN Target primary		Primary	0	50:06:01:60:3C:E0:60:E2
54N Target secondary		Secondary	0	50:06:01:68:3C:E0:60:E2

**Step 9:** 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.

>> 🛱 Equipment : 🥡 Chassis : 🔊 Chassis 1 · 🦏 General Inventory Virtual Machines Installed Firmw	Servers ' 🧠	» Server 3   VIF Paths   Faults   Events   FSM   Stati	stics Temperatures Power		
Fault Summary Solution Status Overal Status: 4 Unassociated Status Details	Physical Disp				_1
Admin State: 1 In Service Discovery State: 1 Complete Avail State: 1 Available Assoc State: 3 None Power State: 4 Off	Associate Associate Selec	e Service Profile iate Service Profile t an existing service profile to asso rofiles • Available Service	ciate with the selected serve	и.	
Slot Status: <b>† Equipped</b>	Select	Name	Org	Assoc State	
Crieck Point: Discovered	0	Service Profile C_Series_Server_Pr	org-root	Unassociated	
Actions Create Service Profile				▼ ▲	
Associate Service Profile				OK Cancel	

Step 10: In the work pane, on the FSM tab, check the progress of the service profile that is being applied on the server.

>> 🛱 Equipment ' 🔊 Chassis ' 🗊 Chassis 1 ' 🥪 Servers ' 🥪 Server 3
General Inventory Virtual Machines Installed Firmware SEL Logs VIF Paths Faults Events FSM Statistics Temperatures Power
FSM Status: In Progress
Description:
Current FSM Name: Associate
Completed at:
Progress Status: 34%
Remote Invocation Result:
Remote Invocation Error Code: None
Remote Invocation Description:

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

## VMware vSphere Installation and Setup

### 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

PROCESS

- · 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 (CIMC). 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.

Cisc	co UCS Manager - 2.1(1b)	
Single poi	nt of device management for the Cisco Unified Computing System	
UCS Manager please <u>downlo</u>	requires Java Runtime Environment 1.6 or higher. If it is not already installed, ad and install it on your system.	

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.

🚔 FI6296x / Chassis - 1 Server - 3 - KVM Console					
File Help					
🚙 Boot Server 🛛 🔩 Shutdown Server 🤐 Reset					
KVM Console Server					
KYM Virtual Media					
Client View					
Mapped Read Only Drive	Exit				
🗖 🖉 🗟 G: - CD/DVD	Create Image				
	Add Image				
	Remove Image				
	Details ±				

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.



K۷	y Virtual Media	•		
	Client View			
	Mapped	Read Only	Drive	Exit
		1	A G: - CD/DVD	
			C:\Users\admin\Desktop\FEB2013\E5Xi-5.0.0-623860-custom-Cisco-2.0.1.6.iso	Create Image
				Add Image
				Remove Image
				Details ±

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.

Do you wa	ant to reset the selected servers?	×
	You are attempting to reset a server. The server can be reset by gracefully restarting the OS or via a brute force power cycle. How would you like to reset?	
	Power Cycle	
	C Gracefully restart OS	
	If Graceful OS Restart is not supported by the OS or it does not happen within a reasonable amount of time, the system will perform a power cycle.	
	To reset the slot, please go to the recover server action.	
	The UCS system might be in the process of performing some tasks on this server. Would you like this operation to wait until the completion of outstanding activities?	
	Wait for completion of outstanding UCS tasks on this server.	
	OK Cancel	

**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.

ESXi-5.0.0-623860-custom Boot Menu
ESXi-5.0.0-623860-custom Installer
Boot from local disk
Press [Tab] to edit options
Automatic boot in 3 seconds

#### **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 (CIMC), is provided in the Unified Computing System Design Guide. It is assumed that you have completed the UCS C-Series preparation before beginning this procedure.

This guide is based on deploying a Cisco UCS C-Series server, which, like the Cisco UCS C-Series C220 M3 or C240 M3 servers, has an onboard Secure Digital (SD) card called Cisco FlexFlash installed in it.

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. You use Step 3 through Step 5 to activate the partition on the Cisco FlexFlash through CIMC and enable the HV partition for installation of the VMware ESXi ISO file.

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

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

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 Storage tab, click **Cisco FlexFlash**.

cisco Cisco Integra	ated Management Controller					
Overall Server Status	C   1 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2					
Good	Cisco FlexFlash (FlexFlash-0)					
Server Admin Storage	Controller Info Physical Drive Info Virtual Drive Info	Battery Backup Unit Storage Log				
<ul> <li>LSI MegaRAID SAS 9266-8i</li> <li>(SI OT-2)</li> </ul>	Actions	Physical Drive Count				
Cisco FlexFlash	Reset FlexFlash Controller	Physical Drive Count: 1				
	Reset Configuration	Virtual Drive Count				
	Retain Configuration	Virtual Drive Count: 4				
	Configure Operational Profile					
	Health/Status					
	Health: 🛆 Degraded RAID					
	Status: ok					
	General					
	Product Name: Cisco FlexFlash					
	Firmware Version: 1.2 build 253					
	Controller Status: ok					
	Internal State: Connected					
	Running Firmware: 1.2 build 253-2					
	Startup Firmware Version: 1.2 build 253					
	Cards Manageable: Yes					

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, from the list of Virtual Drives Enabled options, choose **HV**, and then click **Save Changes**. The HV partition is now available to install a VMware ESXi ISO file on it.

Operational Profile	0
Controller: FlexFlash-0	
Virtual Drives Enabled: SCU: 🗹 Drivers:	
HV: 🗹 HUU:	$\leq$
Raid Primary Member: SLOT1	
Raid Secondary Role: N/A	
I/O Read Error Threshold: 0	
I/O Write Error Threshold: 0	
Clear Errors: 🔲	
Save Changes Reset Values Car	ncel

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

cisco Cisco Integrated Management Controller							
CISCO Critegie Verall Server Status Good Server Admin Storage Summary Inventory Sensors Remote Presence BIOS Power Policies Faults and Logs	C C C C C C C C C C C C C C C C C C C	Server Properties Product Name: Serial Number: PID: UUID: BIOS Version: Description: Server Status Overall Server Status: Temperature: Power Supplies: Fans:	UCS C220 M35 FCH1612V033 UCSC-C220-M35 21671984-2828-4899-87D9-98B06FB24D0B C220M3.1.5.1g.0 (Build Date: 03/15/2013)				
		Overall Storage Status:	Good				

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.

🕌 Open	×
Look <u>i</u> n:	SXi 💌 🖬 🖨 🖽 🗄
ESXi-5.0.0	623860-custom-Cisco-2.0.1.6.iso
File <u>N</u> ame:	ESXi-5.0.0-623860-custom-Cisco-2.0.1.6.iso
Files of <u>Type</u> :	Disk image file (*.iso, *.img)
	Open Cancel

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

File	e Help								
۲	🕻 күм 📑	Virtual Media							
	Client View								
	Mapped	Read Only	Drive						Exit
		$\checkmark$	🔊 E: - CD/DVD						
		$\checkmark$	🖃 D: - Removabl	e Disk					Create Image
			🔺 C:\Users\admi	n\Desktop\Au	g2013\ESXi-5.(	).0-6238			Add Image
									Remove Image
									Details ±
	Details								
	Target Drive	Mapped	То	Read Bytes	Write Bytes	Duration			
	Virtual CD/DV	D 🎒 C:\U	sers\admin\Desk	20480	0	00:00:48		-	USB Reset
	Removable D	isk Not map	ped					=	
	Floppy	Not map	ped					-	



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

Step 11: When the server reboots, press F6 to enter the boot menu, select Cisco vKVM-Mapped vDVD1.22, and then press Enter. Selecting the correct boot device enables files from the ISO file to be read and the ESXi installation to begin.

Please select boot device:
UEFI: Built-in EFI Shell IBA GE Slot 0100 v1398 IBA GE Slot 0101 v1398 Cisco NIC 8:0.0 Cisco NIC 9:0.0 HV (Bus 82 Dev 00)PCI RAID Adapter SCU Drivers HUU Cisco vKVM-Mapped vHDD1.22
Cisco CIMC-Mapped vHDD1.22
Cisco vKVM-Mapped vDVD1.22
Cisco CIMC-Mapped vDVD1.22
Cisco vKVM-Mapped vFDD1.22
Enter Setup
↑ and ↓ to move selection ENTER to select boot device ESC to boot using defaults

**Deployment Details** 

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 3 - Cisco UCS B-Series local disk

Select a Disk to Install or Upgrade	
* Contains a VMFS partition	
Storage Device  Local: (none) Remote:	Capacity
LSILOGIC Logical Volume (naa.600508e0000000000a548a	) 1.09 TiB
(Esc) Cancel (F1) Details (F5) Refresh (Enter)	Continue

Figure 4 - Cisco UCS B-Series storage array-based LUN

Select a Disk to Install or Upgrade	
* Contains a VMFS partition	
Storage Device	Capacity
Local: (none) Remote: DGC RAID 5 (naa.60060160d4b12400403b2)	5.00 GiB
(Esc) Cancel (F1) Details (F5) Refresh (Enter)	Continue

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 driver can also boot from a SAN disk, similar to the Cisco UCS B-Series procedure. For 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.htn #d31886e1041a1635	rs, it more nl

	Selec	t a Disk to	Install or Up	grade	
* Contains	a VMFS parti	tion			
Storage Dev Local: S1 Remote: (none)	ice MR9266-81	(naa ,i	600605b00509cf	c0184de)	Capacity
(Esc) Ca	ncel (F1)	Details	(F5) Refresh	(Enter) Co	ontinue

Figure 6 - Cisco UCS C-Series USB thumb drive

		Select a Disk	
Storage De	vice		Capacity
Local:			
	USB Flash Disk	(mpx.umhba33:CO:TO:LO)	1.83 GB
Cisco	Virtual FDD/HDD	(mpx.vmhba32:C0:T0:L1)	0.00 B
Remote:			
LSILOGIC	Logical Volume	(naa.600508e000000000ce7c2a)	278.46 GB
	[*] Co (F1) Details	ntains a UMFS partition (Esc) Cancel (Enter) Continue	

Figure 7 - Cisco UCS C-Series FlexFlash HV partition

	Select	a Disk t	o Install or Up <u>o</u>	grade
* Contain	ns a VMFS partit	ion		
Storage D	)evice			Capacity
Local:				
LSI	MR9266-8 i	(naa	.600605b0050b128	30184d1) 557.86 GiB
SCU Se	erverConfig 0 (r	ipx.vmhba3	3:CO:TO:LO)	3.00 GiB
HV Hup	ervisor 0 (mpx)	vmhba33:C	0:T0:L1)	3.00 GiB
Driver	s OSDrivers 0	mpx.vmhba	33:CO:TO:L2)	6.50 GiB
HUU Ho Remote:	ostUpgrade_0 (mp	ix.vmhba33	:CO:TO:L3)	1.25 GiB
* DGC	VRAID	(naa	.600601604af02a0	00381f3) 350.00 GiB
(Esc)	Cancel (F1)	Details	(F5) Refresh	(Enter) Continue

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

Please select a keyboard layout
Swiss French Swiss German Turkish US Default US Dvorak Ukrainian United Kingdom
Use the arrow keys to scroll.
(Esc) Cancel (F9) Back (Enter) Continue

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

Please	enter a roo	t password	l (recom	ended)
Root pa firm pa	ssword: **** ssword: ****			
	Passu	ords match	۱.	
(Esc) C	ancel (F9	) Back	(Enter)	Cont inue

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

C	Confirm Install	
The installer is configured to install ESXi 5.0.0 on: mpx.vmhba33:CO:TO:L1.		
Warning: This disk will be repartitioned.		
(Esc) Cancel	(F9) Back	(F11) Install

i	Tech Tip
The sys	stem 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.

#### Installation Complete

ESXi 5.0.0 has been successfully installed.

ESXi 5.0.0 will operate in evaluation mode for 60 days. To use ESXi 5.0.0 after the evaluation period, you must register for a VMware product license. To administer your server, use the vSphere Client or the Direct Control User Interface.

Remove the installation disc before rebooting.

Reboot the server to start using ESXi 5.0.0.

(Enter) Reboot

**Step 9:** If you are using the Cisco UCS B-Series Server or the UCS C-Series server with the boot-from-localdrive 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.

Aptio Setup Utility Main Advanced Security Server	– Copyright (C) 2011 Americar Management Boot Options Sav	∣Megatrends, Inc. /e & Exit
Boot Configuration Setup Prompt Timeout Bootup NumLock State UCSM boot order rules Boot Option Priorities Boot Option #1 Boot Option #2 Boot Option #3	3 [Off] [Loose] [(Bus 82 Dev 00)PCI] [IBA GE Slot 0100 v] [UEFI: Built-in EFI]	Set the order of the legacy devices in this group
Network Device BBS Priorities Hard Drive BBS Priorities		Select Screen 11 Select Item Enter Select Field +/- Change Value F1 General Help F9 BIOS Defaults F10 Save & Exit ESC Exit
Version 2.14.1219.	Copyright (C) 2011 American M	legatrends, Inc.

#### 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).

Aptio Setup U	tility – Copyright (C) 2011 America Boot Options	n Megatrends, Inc.
Boot Option #1 Boot Option #2	[(Bus 82 Dev 00)PCI] [HV] Boot Option #1 (Bus 82 Dev 00)PCI RAID Adapter HV Disabled	Sets the system boot order Select Screen Select Item ter Select Field +/- Change Value F1 General Help F9 BIOS Defaults F10 Save & Exit ESC Exit
Version 2.14	.1219. Copyright (C) 2011 American	Megatrends, Inc.

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

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



### 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**.



10-0	Reader Tip
You ca	an modify the Troubleshooting Options field to allow configuration of remote
trouble	eshooting via SSH or directly from the console. Please refer to VMware KB
Article	: 1017910 for more information:
http://I	kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=display
KC&ex	tternalld=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.

Configure Management Network	Network Adapters	
Network Adapters VLAN (optional) IP Configuration IPv6 Configuration DNS Configuration Custon DNS Suffixes	vnnic0 (d4:8c:b5:4e:22:42) The adapters listed here provide the default network connection to and from this host. When two or more adapters are used, connections will be fault-tolerant and outgoing traffic will be load-balanced.	

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.

Configure Managem	nent Network	Network Adapters	
Network Adapters Select the adapters for this host's default management network connection. Use two or more adapters for fault-tolerance and load-balancing.			
Device Name [X] vmnic0 [X] vmnic1 [] vmnic2 [] vmnic3	Hardware Label (MAC N/A (00:25:b5:01:0c N/A (00:25:b5:01:0c N/A (00:25:b5:01:0c N/A (00:25:b5:01:0c	Address)Status:bf)Connected:cf)Connected:ee)Connected:be)Connected	
<d>&gt; View Details</d>	<space> Toggle Sele</space>	cted <enter> OK</enter>	<esc> Cancel</esc>
If you are using the Cisco UCS B-Series server, or a UCS C-Series Server that is using a single pair of NIC cards for management and production traffic, 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. This 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

i

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

DNS Configuration				
This host can only obtain DNS settings automatically if it also obtains its IP configuration automatically.				
( ) Obtain DNS server addresses and a hostname automatically (o) Use the following DNS server addresses and hostname:				
Primary DNS Server [ 10.4.48.10 ] Alternate DNS Server [ ]				
Hostname L test-c22UM3-1.c1sco.local J				
<pre><up down=""> Select <space> Mark Selected <enter> OK <esc> Cancel</esc></enter></space></up></pre>				

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 nondisruptive 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. In a later procedure you can update to the latest patches for VMware vCenter Server release 5.0.

i	Tech Tip
VSphe	ere Client is adaptive, and it only shows what the ESXi host knows how to do.
VSphe	ere Client is also used for access to vCenter (which will be covered later), allowing
for vM	lotion and other functions. Be aware of what destination you are connecting to.
ESXi h	nosts 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**.

🕜 VMware vSphere Client	×					
vmware <sup>.</sup> ‱are vSphere <sup>™</sup> Client	e e e e e e e e e e e e e e e e e e e					
To directly manage a single host, enter the IP address or host name. To manage multiple hosts, enter the IP address or name of a vCenter Server.						
IP address / Name:	test-c220m3-1.cisco.local					
User name:	root					
Password:	*****					
	Use Windows session credentials					

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.

<u>File E</u> dit Vie <u>w</u> I <u>n</u>	ventory <u>A</u> dministration <u>P</u> lu	ug-ins <u>H</u> elp					
🕞 🗈 🛕	Home						
Inventory							
<u>p</u>							
Inventory							
Administration							
8							
Roles	System Logs						
Decent Tacks				N			×
Name	Target	Status	Details	Initiated by	Requested Start Ti	*   Start Time	Completed Ti
- Hamo	, argee	Jacus	Docais	And the by	Requested State Int. V	Start Mile	Completed II
Tasks					Evalua	tion Mode: 60 day	vs remaining root //

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



# 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.

## CO 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.

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

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

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.

🛃 Add Network Wizard		_ 🗆 🗡
Connection Type Networking hardware can	be partitioned to accommodate each service that requires connectivity.	
Connection Type Network Access Connection Settings Summary	Connection Types Virtual Machine Add a labeled network to handle virtual machine network traffic. VMkernel The VMkernel TCP/IP stack handles traffic for the following ESXI services: vSphere vMotion, iSCSI, NFS, and host management.	

**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.

ction Type ork Access	Select which vSphere standard switch will handle vSphere standard switch using the unclaimed ne	e the network tr twork adapters	affic for this connection. You may also create a new listed below.
ry	Create a vSphere standard switch Cisco Systems Inc Cisco VIC Ethern	Speed et NIC	Networks
	Vmnic2	10000 Full	⊡-10.4.57.1-10.4.57.127 ( VLAN 157 )
			10.4.48.1-10.4.48.254 ( VLAN 148 )
			0.0.0.1-255.255.255.254 (VLAN 154)
			0.0.0.1-255.255.255.254 (VLAN 163)
			-0.0.0.1-255.255.255.254 ( VLAN 155 )
	Vmnic3	10000 Full	E-10.4.57.1-10.4.57.127 ( VLAN 157 )
			10.4.48.1-10.4.48.254 ( VLAN 148 )
			0.0.0.1-255.255.255.254 ( VLAN 154 )
			0.0.0.1-255.255.255.254 (VLAN 163)
			-0.0.0.1-255.255.255.254 ( VLAN 155 )
	Intel Corporation 1350 Gigabit Netw	vork Connecti	on
	vmnic1	Down	None
	O Use vSwitch0	Speed	Networks
	Intel Corporation I350 Gigabit Netw	vork Connecti	on
	mic0	1000 Full	0.0.0.1-255.255.255.254
	Preview:		
	-Virtual Machine Port Group	Physical Adapters	· · · · · · · · · · · · · · · · · · ·
	VM Network 2 😌 🛶	🛶 🔛 vmnic2	



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

🛃 Add Network Wizard			
Virtual Machines - Conne Use network labels to id	ction Settings entify migration compatible connections com	mon to two or more hosts.	
Connection Tupe Network Access Connection Settings Summary	─Part Group Properties Network Label: 5 VLAN ID (Optional): 1	iervers_1 48j <b>v</b>	
	Preview:		
	Virtual Machine Port Group Servers_1 VLAN ID: 148	Physical Adapters	

i	Tech Tip
The vS future t	Switches in this example are set up for trunking, which allows for expansion in the 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.

Getting Started Summary Virtual Machines	Kesource Allocation Verrormance Configuration Last's & Events Alarms Vermissions Maps Storage Views 1	Haroware status Upda	e manager
Li sudar sun			
naruware	View: vSphere Standard Switch vSphere Distributed Switch		
Processors     Memory     Storage     Networking     Storage     Networking     Storage     Networking     Storage     Networking     Storage     Networking     Storage     Software     Licensed Features     Time Configuration     Otils and Routing     Authentication Services     Power Minagement     Vitual Machine Startup/Stutdown     Vitual Machine     Startup/Stutdown     Vitual Machine     Startup/Stutdown     Vitual Machine     Startup/Stutdown     Vitual Machine     Startup/Stutdown     Vitual Machine     Startup/Stutdown     Vitual Machine     Startup/Stutdown     Vitual Machine     Startup/Stutdown     Vitual Machine     Startup/Stutdown     Vitual Machine     Startup/Stutdown     Vitual Machine     Startup/Stutdown     Vitual Machine     Startup/Stutdown     Vitual Machine     Startup/Stutdown     Vitual Machine     Startup/Stutdown     Vitual Machine     Startup/Stutdown     Vitual     Startup/Stut	View: Vsphere Standard Switch Vsphere Distributed Switch Remove Propeties Vsphere Standard Switch Vswitch Remove Propeties Physicial Adquire Physicial Adquire Vsmido 110.4.63.82 Standard Switch VSwitch1 Remove Propeties Vswitch Itol. Remove Propeties Vswitch Itol. Itol. Remove Propeties	Refresh Add Network	ng Propertes

**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.



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

1

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. In a later procedure you can update to the latest patches for VMware ESXi release 5.0.

#### 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.



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."

🛃 Add Network Wizard		
VMkernel - Network Ad The VMkernel reache	Access es networks through uplink adapters attached to vSphere standard switches.	
Connection Type Network Access	Select which vSphere standard switch will handle the network traffic for this connection. You may also or vSphere standard switch using the unclaimed network adapters listed below.	reate a new
	Intel Lorporation 1350 Ligabit Network Lonnection	<b>_</b>
Summary	🔽 🖼 vmnic1 Down None	
	C Use vSwitch0 Speed Networks	
	Intel Corporation I350 Gigabit Network Connection	
	🔲 📟 vmnic0 1000 Full 0.0.0.1-255.255.255	
	Use vSwitch1 Speed Networks	
	Cisco Systems Inc Cisco VIC Ethernet NIC	
	🕅 📟 vmnic2 10000 Full 10.4.57.1-10.4.57.127	
	🕅 🖼 vmnic3 10000 Full 10.4.57.1-10.4.57.127	-
	, Preview:	
	VMkernel Port Physical Adapters	
	VMkernel 👱 🔶 🚥 vmnic2	
	-Virtual Machine Port Group	
	bervers_1	
	VLAN ID: 148	

**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**.

🛃 Add Network Wizard		_ 🗆 ×
VMkernel - Connection Use network labels to i	Settings identify VMkernel connections while managing your hosts and datacenters.	
Connection Type Network Access Connection Settings IP Settings Summary	Port Group Properties         Network Label:       ISCSI         VLAN ID (Optional):       162         Use this port group for vMotion       Use this port group for Fault Tolerance logging         Use this port group for roup for management traffic	
	Preview: VMIkemel Port ISCSI VLAN ID: 162 VItual Machine Port Group Servers_1 VLAN ID: 148	

**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 design guide uses VLAN **162** and IP subnet **10.4.62.X** for iSCSI connectivity.

🚰 Add Network Wizard		
VMkernel - IP Connectio Specify VMkernel IP set	n Settings tings	
Connection Type Network Access Connection Settings IP Settings Summary	C Obtain IP settings automatically Use the following IP settings: IP Address: ID . 4 . 62 . 81 Subnet Mask: Z55 . 255 . 255 . 0 VMkernel Default Gateway: ID . 4 . 63 . 1 Edit Preview:	
	VMkemel Port ISCSI I0.4.62.81   VLAN ID: 162 Virtual Machine Port Group Servers_1 VLAN ID: 148	

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.

i	Tech Tip
lf you u list of s for bot	use hardware-accelerated iSCSI adapters, the iSCSI adapter will appear on the torage adapters available for configuration. The remaining steps are the same in software and hardware iSCSI adapters.

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

iSCS	I Software Adapter			
$\bigcirc$	iSCSI Software Adapter	iSCSI		
Deta	ils			
				Properties
M	odel:			
iS	CSI Name:			
iS	CSI Alias:			
G	onnected Targets:	Devices:	Paths:	

The iSCSI Initiator Properties dialog box appears.

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

🛃 iSCSI Initiator (iSC	SI Software Adapter) Properties	
General Dynamic Dis	covery Static Discovery	
-iSCSI Properties -		
Name:		
Alias:		
Target discovery	methods:	
Software Initiator I Status:	Properties	
CHAP	Advanced,	Configure

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

🛃 General Propert	ties		×
iSCSI Properties iSCSI Name: iSCSI Alias:			
Status Enabled	,		
	ОК	Cancel	Help

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

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

🗿 iSCSI I	nitiator (vmhba35	Properties	_ 🗆 🗡
General	Dynamic Discovery	Static Discovery	
Send 1	argets		
Discove	r iSCSI targets dynar	ically from the following locations (IPv4, host name	):
iSCSI S	erver Location		
I			
		Add Remove	Settings
		Close	Help
			/

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

Ċ	Add Send Target 9	5erver	X
	iSCSI Server:	10.4.62.10	
	Parent:	13260	
	Authentication be establishe	on may need to be configured before a session can ad with any discovered targets.	
		CHAP Advanced	
		OK Cancel Help	

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

http://www.vinware.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 Unified Computing System Design 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."

CO Re	ader Tip							
or more inf	ormation on c	configuring	a a SAN or	storade	arrav	soo the	Data	a Center
		Johngunn	g a OAN OI	Storage	Junuy	300 110	Date	
esign Guid	e.							
0m3-1.cisco.local VMware E Carted Summary Virtual M	SXi, 5.0.0, 623860   Evaluation (6)	D days remaining)	Local Users & Groups Events	Permissions				
re	Storage Adapters			, , ,	Add	Remove Refresh	Rescan A	Al
th Status	Device	Туре	WWN					
essors	MegaRAID SAS Fusion Cont	roller						
orv	O vmhba2	SCSI						
	Cisco VIC FCoE HBA Driver							
ogo unking	🕥 vmhba0	Fibre Channel	10:00:fc:99:47:24:f1:4f 20:00:	fc:99:47:24:f1:4f				
winning	🕥 vmhba1	Fibre Channel	10:00:fc:99:47:24:f1:50 20:00	fc:99:47:24:f1:50				
age Adapters								
vork Adapters								
anced Settings								
er Management								
e								
sed Features								
and Routing								
entication Services	Details							
al Machina Startun/Shutdown	vmhba0							
al Machine Swaefile Location	Model: Cisco VIC FCoE	HBA Driver						
iai machine owaptile cooddorf	WWN: 10:00:fc:99:47:	24:f1:4f 20:00:fc:99:47:24:	f1:4f					
anty Prome	Targets: 2 Der	vices: 1 Paths:	2					
em Resource Allocation	View: Devices Paths							
t VM Settings	ime	Runtime Name	Operational State IIIN	Type	Drive Type	Transport	Capacity	Owne
		i i a como negitio				the second provide the		and the second sec
anced Settings	GC Eibre Channel Disk (naa. 60	06 vmbba0:C0:T0:L0	Mounted 0	disk	Non-SSD	Eibre Channel	300.00.6	NMP

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.

test-c220m3-1.cisco.local ¥Mware E	SXI, 5.0.0, 623860   Eva	aluation (60 days ren	naining)						
Getting Started Summary Virtual M	lachines 🔍 Resource Alloca	ation Performance	Configuration Local User	rs & Groups 🔪 E	vents Perr	nissions			
The ESXi host does not ha	ve persistent stor	age.							
To run virtual machines, create at least	To run virtual machines, create at least one datastore for maintaining virtual machines and other system files.								
Note: If you plan to use iSCSI or a netw	ork file system (NFS), ensu	e that your storage ada	pters and network connect	ions are properly	configured b	efore conti	nuing.		
To add storage now, click here to create	a datastore								
Hardware	View: Datastore	es Devices							
Health Status	Datastores				Refresh	Delete	Add Storage	Rescan All	
Processors	Identification	<ul> <li>Device</li> </ul>	Drive Type	Capacity	Free	Туре	Last Update	Hard	
Memory									
<ul> <li>Storage</li> </ul>									
Networking									
Storage Adapters									
Network Adapters									
Advanced Settings									
Power Management	4							F	

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

🛃 Add Storage	
Select Storage Type Specify if you want to fo	rmat a new volume or use a shared folder over the network.
Disk/LUN     Select Disk/LUN     File System Version     Current Disk Layout     Properties     Formatting     Ready to Complete	Storage Type  Disk/LUN  Create a datastore on a Fibre Channel, iSCSI, or local SCSI disk, or mount an existing VMFS volume.  Network File System  Choose this option if you want to create a Network File System.
	Adding a datastore of Hore Chainer of 15C51 will add this datastore to an hosts that have access to the storage media.

**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.



Figure 8 – Local disk drive

🚰 Add Storage					_ 🗆 🗵
Select Disk/LUN Select a LUN to create a	a datastore or expand the current one				
Disk/LUN     Select Disk/LUN     File System Version	Name, Identifier, Path ID, LUN, Capaci	ty, Expandable or VMF:	5 Label c	• Drive Type	Clear
Current Disk Layout Properties Formatting Ready to Complete	Local LSI Disk (naa.600605b0050b1	vmhba2:C2:T0:L0	0	Non-SSD	557.86 GB

Figure 9 - Shared iSCSI and Fibre Channel LUNs

or expand the current one					
e, Identifier, Path ID, LUN, Capacity	y, Expandable or VMFS	Label c	•		Clear
ie	Path ID	LUN 🔼	Capacity	VMFS Label	Har
APP iSCSI Disk (naa.60a980006	ign.1992-08.com	10	10.00 GB		Unk
APP Fibre Channel Disk (naa.60	vmhba2:C0:T0:L10	10	24.80 GB		Unk
APP Fibre Channel Disk (naa.60	vmhba2:C0:T0:L14	14	5.00 GB		Sup
e 1 7	s, Identifier, Path ID, LUN, Capacit e APP ISCSI Disk (naa.60a980006 APP Fibre Channel Disk (naa.60 APP Fibre Channel Disk (naa.60	e, Identifier, Path ID, LUN, Capacity, Expandable or VMFS e Path ID APP ISCSI Disk (naa.60a980006 iqn.1992-08.com APP Fibre Channel Disk (naa.60 vmhba2:C0:T0:L10 APP Fibre Channel Disk (naa.60 vmhba2:C0:T0:L14	e, Identifier, Path ID, LUN, Capacity, Expandable or VMFS Label c e Path ID LUN > 1 APP ISCSI Disk (naa.60a980006 ign.1992-08.com 10 APP Fibre Channel Disk (naa.60 vmhba2:C0:T0:L10 10 APP Fibre Channel Disk (naa.60 vmhba2:C0:T0:L14 14	e, Identifier, Path ID, LUN, Capacity, Expandable or VMFS Label c  e Path ID LUN × Capacity PP ISCSI Disk (naa.60a980006 ign.1992-08.com 10 10.00 GB APP Fibre Channel Disk (naa.60 vmhba2:C0:T0:L10 10 24.80 GB APP Fibre Channel Disk (naa.60 vmhba2:C0:T0:L14 14 5.00 GB	e         Path ID         LUN >         Capacity, Expandable or VMFS Label c         •           e         Path ID         LUN >         Capacity         VMFS Label           APP Fibre Channel Disk (naa.60         vmhba2:C0:T0:L10         10         24.80 G8           APP Fibre Channel Disk (naa.60         vmhba2:C0:T0:L14         14         5.00 G8

**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.

CO Reade	r 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				
Add Storage File System Version Specify the version of the V	MFS for the datastore			
Disk/LUN     Select Disk/LUN     File System Version     Current Disk Layout     Properties     Formatting     Ready to Complete	File System Version         Image: WFFS-5         Select this option to enable additional capabilities, such as 2TB+ support.         VMFS-5 is not supported by hosts with an ESX version older than 5.0.         Image: VMFS-3         Select this option if the datastore will be accessed by legacy hosts.			

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

🛃 Add Storage					_ 🗆 🗙
Current Disk Layout You can partition and forma	t the entire device, all free space, or a si	ngle block of fre	e space.		
Select Disk/LUN File System Version Current Disk Layout Properties Formatting Ready to Complete	Pevice Local LSI Disk (naa.600605b00 Location /vmfs/devices/disks/naa.600605b Partition Format Unknown	Drive Type Non-SSD 0050b1280184d The hard disk is	Capacity 557.86 GB 115f096b58f6 : blank.	Available 557.86 GB	LUN O
	There is only one layout configuration pages.	i available. Use t <b>nd used</b>	he Next button to	proceed with the ot	her wizard

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

Tech T	īp	
Use a descriptive when you add m	e name for the datastore, to help you identify which datastore ore of them.	e is which
Add Storage Properties Specify the properties for t	he datatore	
Disk/LUN     Select Disk/LUN     File System Version     Current Disk Layout     Properties     Formatting     Ready to Complete	Enter a datastore name C220M3-2-Storage	

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

🛃 Add Storage		
Disk/LUN - Formatting Specify the maximum file size	e and capacity of the datastore	
Disk/LUN     Select Disk/LUN     File System Version     Current Disk Layout     Properties     Formatting     Ready to Complete	Capacity Capaci	

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

🛃 Add Storage		
Ready to Complete Review the disk layout and	click Finish to add storage	
E Disk/LUN	Disk layout:	
File System Version Current Disk Layout Properties Formatting Ready to Complete	Device         Drive Type         Capacity           Local LSI Disk (naa.600605b0050         Non-SSD         557.86 GB           Location         /vmfs/devices/disks/naa.600605b0050b1280184d115f096b58f6           Partition Format         GPT           Primary Partitions         Capacity           VMFS (Local LSI Disk (naa.600605         557.86 GB	LUN O
	File system:  Properties Datastore name: C220M3-2-Storage  Formatting  File system: vmfs-5 Block size: 1 MB Maximum file size: 2.00 TB	



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.

🖉 Create New Virtual Machin	e			_ 🗆 >
Storage Virtual Machine Versic Select a destination storage for the virtual machine files				
Configuration Name and Location	Select a destination stor	age for the virtua	al machine files: Capacity   Provisione	d Free Type Thin Prov
Storage Guest Operating System Network Create a Disk Ready to Complete	2220M3-2-Sto	Non-SSD	557.75 GB 973.00 MB	556.80 GB VMFS5 Supporte

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

🛃 Create New Virtual Machine	
Guest Operating System Specify the guest operatin	9 System to use with this virtual machine Version: 8
Configuration Name and Location Storage Guest Operating System Network Create a Disk Ready to Complete	Guest Operating System:



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

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

- How many NICs do you want to connect?-1
- NIC 1-Servers\_1
- · Adapter-VMXNET 3

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.

Network       Virtual Machine Version: 8         Which network connections will be used by the virtual machine?       Configuration         Name and Location       Storage         Guest Operating System       How many NICs do you want to connect?         Network       Adapter         Ornect at Power On       Power On         NIC 1:       Servers_1         VITUAL Machine Version: 8       VMXNET 3         VITUAL Machine Version: 9       VMXNET 3	伊 Create New Virtual Machine	e	
Configuration         Name and Location         Storage         Guest Operating System         Network         Create a Disk         Ready to Complete         NIC 1:         Servers_1         VMXNET 3         If supported by this virtual machine version, more than 4 NICs can be added after the virtual machine is created, via its Edit Settings dialog.         Adapter choice can affect both networking performance and migration compatibility. Consult the VMware KnowledgeBase for more information on choosing among the network adapters supported for various guest operating systems and hosts.	Network Which network connection	s will be used by the virtual machine?	al Machine Version: 8
	Configuration Name and Location Storage Guest Operating System Network Create a Disk Ready to Complete	Create Network Connections How many NICs do you want to connect? Network NIC 1: Servers_1  If supported by this virtual machine version, more than 4 NICs can be added af virtual machine is created, via its Edit Settings dialog. Adapter choice can affect both networking performance and migration compatibil the VMware KnowledgeBasefor more information on choosing among the netwo supported for various guest operating systems and hosts.	Connect at Power On ter the lity. Consult rk adapters



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

i

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

🚰 Create New Virtual Machin	e		
Create a Disk Specify the virtual disk siz	e and provisioning policy		Virtual Machine Version: 8
Configuration Name and Location	- Datastore:	C220M3-2-Storage	
<u>Storage</u> Guest Operating System	Available space (GB):	556.8	
<u>Network</u> Create a Disk	Virtual disk size:	40 😴 GB 💌	
Ready to Complete	C Thick Provision Lazy 2	Zeroed	
	C Thick Provision Eager	Zeroed	
	Thin Provision		

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

🚰 Create New Virtual Machi	ne	
Ready to Complete Click Finish to start a task	that will create the new virtual machine	Virtual Machine Version: 8
Configuration Name and Location Storage Guest Operating System Network Create a Disk Ready to Complete	Settings for the new virtual machine Name: Folder: Host/Cluster: Datastore: Guest OS: NICs:	: Test-Win2008-1 10k test-c220m3-1.cisco.local C220M3-2-Storage Microsoft Windows Server 2008 R2 (64-bit) 1
	NIC 1 Network: NIC 1 Type: Disk provisioning: Virtual Disk Size:	Servers_1 VMXNET 3 Thin Provision 40 GB

#### 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.





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.



To regain control of the mouse from a console window, press <b>Ctrl-Alt</b> , and the mouse will be released.	i	Tech Tip
	To rega will be	ain control of the mouse from a console window, press <b>Ctrl-Alt</b> , and the mouse 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.

Test-Win2008-1	on test-c220m3	-1.cisco.local	_
e View VM			
	<b>S</b> 🖸 🕅		
			sicastality states in
	S Inst	all Windows	
334	iles in the second		
-41			
÷			
- Andrews		Windows Server 2008 P2	
Sec. 10			
1. A.			
Server -		Language to Sector II. Constant	
		Time and currency format: English (United States)	
		Keyboard or input method: US	122 Mar 1
and the		A REAL PROPERTY OF THE REAL PR	
		Enter your language and other preferences and click "Next" to continue.	and the second second
		nyright © 2009 Microsoft Corporation. All rights reserved.	
		C. TICKI	
			The appropriate of the second se
Start 1			

#### 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**.

	Power >	?
	Guest 🔸	Answer Question
	Snapshot •	Enter Full Screen (Ctrl+Alt+Enter)
2	Open Console	Send Ctrl+Alt+del
₿	Edit Settings	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 10 - Tools install prompt in Windows Server 2008





# Installing and Configuring VMware vCenter Server

- 1. Install VMware vCenter Server
- 2. Create a data center
- 3. Create a cluster

PROCESS

- 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

#### CO 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

**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.

li	Tech Tip
To fund	I ction 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.

<b>vm</b> ware <sup>.</sup>	
VMware vSphere <sup>®</sup> 5.0	
VMware Product Installers	vCenter Server™
vCenter Server™	vCenter Server™ manages datacenter access control,
vSphere Client™	performance monitoring, and configuration, and unifies resources from individual servers to be shared among
VMware vSphere® Web Client (Server)	virtual machines in the entire datacenter. To join the vCenter Server™ to existing vCenter Server™ instances:
VMware vSphere® Update Manager	after the installation is complete, click the Install button
vCenter Support Tools	and select Modify Linked Mode Configuration.
Mware ESXi™ Dump Collector	Microsoft .NET 3.5 SP1 Windows Installer 4.5
VMware® Syslog Collector	
VMware® Auto Deploy	
Mware vSphere® Authentication Proxy	Wew improvements in license reporting require
Jtility	installation of the VMware vSphere® Web Client.
vCenter™ Host Agent Pre-Upgrade Checker	
	Install
	Explore Media E

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

- Step 6: Follow the instructions in the wizard. Note the following:
  - On the Customer Information page, enter your username and organization, and then click **Next**. This installation uses an evaluation mode license, which is valid for 60 days. If a valid license came with a purchase of vCenter, it can be entered now or after the installation.

🔂 VMware vCenter Server		×
Customer Information Please enter your information.		
User Name:		
Organization: Cisco		
License key:		
Note: If you do not enter a licens evaluation mode.	se key, vCenter Server wi	ll be installed in
InstallShield	< Back Ne:	kt > Cancel

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

VMware vCenter Server			×
Database Options Select an ODBC data source for vCen	ter Server.		2
vCenter Server requires a database.			
Install a Microsoft SQL Server 2008	Express instance (f	or small scale deploy	/ments)
Use an existing supported database			
Data Source Name (DSN):	ase create a 64 bit	system DSN)	<b>v</b>
NOTE: There is no DSN which can be used. VMware vCenter Server requires a 64 bit system DSN with supported types of databases and versions of drivers.			
InstallShield			
	< Back	Next >	Cancel

#### Tech Tip

1

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**.

Howare vCenter Server		x
<b>vCenter Server Service</b> Enter the vCenter Server service account inform	mation.	
Configure the vCenter Server service to run in t account in the domain.	the SYSTEM account or in a user-specified	
Use SYSTEM Account		
Account name:	administrator	
Account password:	••••••	
Eully Qualified Domain Name:	vCenter-1.cisco.local	
SECURITY ADVISORY: The vCenter Server insta to user-specified accounts.	aller grants the "Log on as a service" right	
InstallShield		
< B	Back Next > Cancel	

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

HWWare vCenter Server			
vCenter Server Linked Mode Options Install this VMware vCenter Server instance in linked mode or standalone mode.			
To configure linked mode, install the first vCenter Server instance in standalone mode. Install subsequent vCenter Server instances in linked mode.			
Create a standalone VMware vCenter Server instance			
Use this option for standalone mode or for the first vCenter Server installation when you are forming a new linked mode group.			
○ Join a ¥Mware vCenter Server group using linked mode to share information			
Use this option for the second and subsequent vCenter Server installations when you are forming a linked mode group.			
InstallShield			
< Back Next > Cancel			

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

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

🛃 VMware vCenter Server	×
<b>Configure Ports</b> Enter the connection information for vCenter Server.	e
HTTPS Port:	443
HITP Port:	80
Heartbeat Port (UDP):	902
Web Services HTTP Port:	8080
Web Services HTTPS Port:	8443
Web Services Change Service Notification Port:	60099
LDAP Port:	389
SSL P <u>o</u> rt:	636
InstallShield	
< Back	Next > Cancel

• 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.

VMware vCenter Server		×
Configure Ports for Inventory Service Enter port numbers for Inventory Service,		Q
HTTPS Port:	10442	
Service Management Port:	10109	
Linked Mode Communication Port:	10111	
InstallShield	< Back Next >	Cancel

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

🛃 ¥Mware vCenter Server			×	
vCenter Server JYM Memory           Select vCenter Server Web services JVM memory configuration.				
To optimally configure your deployment, please select which vCenter Server configuration best describes your setup.				
Inventory Size		Maximum Memory		
<ul> <li>Small (less than 100 host machines)</li> </ul>	ts or 1000 virtual	1024 MB		
C Medium (100-400 hosts o machines)	or 1000-4000 virtual	2048 MB		
C Large (more than 400 ho machines)	osts or 4000 virtual	3072 MB		
InstallShield				
	< Back	Next >	Cancel	

· 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.



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.

🕗 vCenter-1.cisco.local - vSphere Client			
File Edit View Inventory Administra	ation Plug-ins Help		
🕒 🖸 🏠 Home 🕨 🛃 Inv	entory 🕨 🛐 Hosts and Clusters		
📁 🕸 🖬 🖬 🛁 🦉			
🖃 🛃 vCenter-1.cisco.local	10k		
□ <u>10k</u> 10k-5J	Getting Started Summary Virtual Machines		
	Create a datacenter     Add a host		
	Add a host		
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.

Add a host
A host is a computer that uses virtualization software, such as ESX or ESXi, to run virtual machines. Adding a host to the inventory brings it under vCenter Server management.
You need a computer running ESX or ESXi software. If you don't have ESX or ESXi software, visit the VMware Web site for information about this product.
To add a host, you need to know the location of the host on the network and the administrative account (typically Administrator or root).
To continue vCenter Server setup, click Add a host.

**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**.

🛃 Add Host Wizard	
Specify Connection Settings Type in the information used to co	onnect to this host.
<b>Connection Settings</b> Host Summary Virtual Machine Location Ready to Complete	Connection Enter the name or IP address of the host to add to vCenter. Host: test-c220m3-1.cisco.local
	Authorization         Enter the administrative account information for the host. vSphere Client will use this information to connect to the host and establish a permanent account for its operations.         Username:       root         Password:       ********

i	Tech Tip
To hav	e a host appear by name, be sure to add the host into your DNS and add the
host to	o 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.

Security A	Mert	×
2	Unable to verify the authenticity of the specified host. The SHA1 thumbprint of the certificate is: D8:F9:52:ED:8C:0E:93:53:6F:84:87:71:3B:E3:DF:C8:BD:8A:D2:7 E Do you wish to proceed with connecting anyway? Choose "Yes" if you trust the host. The above information will be remembered until the host is removed from the inventory. Choose "No" to abort connecting to the host at this time.	
		_
	Yes No	

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

🛃 Add Host Wizard			_ 🗆 🗵
Host Information Review the product information for th	e specified host.		
Connection Settings Host Summary Assign License Lockdown Mode Virtual Machine Location Ready to Complete	You have chosen to Name: Vendor: Model: Version: Virtual Machines:	add the following host to vCenter: test-c220m3-1.cisco.local Cisco Systems Inc UCSC-C220-M35 VMware ESXI 5.0.0 build-623860	

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

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

🗗 Add Host Wizard		_ 🗆 ×
Assign License Assign an existing or a new lice	inse key to this host.	
Connection Settings Host Summary	Assign an existing license key to this host	
Assign License Lockdown Mode Virtual Machine Location Ready to Complete	Product Available □ Evaluation Mode (No License Key)	
	C Assign a new license key to this host Enter Key Product: Evaluation Mode Capacity: - Available: - Expires: 1/31/2013 Label:	

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.

🛃 Add Host Wizard		
<b>Virtual Machine Location</b> Select a location in the vCenter Server i	nventory for the host's virtual machines.	
Connection Settings Host Summary Assign License Lockdown Mode <b>Virtual Machine Location</b> Ready to Complete	Select a location for this host's virtual machines.	

**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.

🚰 Add Host Wizard			_ 🗆 🗵
Ready to Complete Review the options you have selected and	click Finish to add I	the host.	
Connection Settings Host Summary Assign License Lockdown Mode Virtual Machine Location Ready to Complete	Review this summ Host: Version: Networks: Datastores: Lockdown Mode:	ary and click Finish. test-c220m3-1.cisco.local VMware ESXI 5.0.0 build-623860 VM Network Servers_1 C220M3-2-Storage Openfiler(Software) Disabled	

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

## Procedure 5 License vCenter

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

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

Admi	nistration Plug-ins Help	
	Custom Attributes	
	vCenter Server Settings	
	Role	Þ
	Session	Þ
	Edit Message of the Day	
	Export System Logs	

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.

Licensing Statistics Runtime Settings Active Directory Mail SIMIP Ports Timeout Settings	VCenter License     Assign an existing license key to this vCenter Server     Product     Available     Evaluation Mode     (No License Key)
Logging Options Database Database Retention Policy SSL Settings Advanced Settings	Assign a new license key to this vCenter Server      Enter Key  Product: - Capacity: - Capacity: - Expires: - Label: -
	License Server ESX 3.x/ESXI 3.5 hosts and some vCenter add-ons are licensed using a license server. Enter the address of the license server to only license ESX 3.x/ESXI 3.5 hosts or vCenter add-ons.

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

🔂 Add License Key	x
New license key:	
Optional label for the new license key:	
	OK Cancel

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.

lardware	Licensed Features	
Processors	ESX Server License Type	Edit
Memory		
Storage	Product: Evaluation Mode Evalues: 1/31/2013	
Networking	Expires: 1/31/2013	
Storage Adapters	Product Features:	
Network Adapters	Up to 32-way virtual SMP vCenter agent for VMware bost	
Network Adapters	vStorage APIs	
Advanced Settings	VMsafe	
Power Management	VSphere HA	
after and	vMotion	
bitware	vSphere FT	
Licensed Features	vSphere Data Recovery	
Time Configuration	voniela zones voniere DRS	
DNS and Routing	Storage vMotion	
Authoritisation Services	MPIO / Third-Party Multi-Pathing	
Addiendeddon Dervices	vSphere Distributed Switch Host profiles	
Power management	Remote virtual Serial Port Concentrator	
Virtual Machine Startup/Shutdown	Storage I/O Control	
Virtual Machine Swapfile Location	Direct Path vMotion	
Security Profile	VAAI Shared Smart Card Reader	
Host Cache Configuration	Storage DRS	
System Resource Allocation	Profile-Driven Storage	
Agent VM Settings	vMotion Metro	
Agent vin Detungs	vopriere Auto Deploy vSobere View Accelerator	

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

Assign Li	cense: test-c2	20m3-1.cisco.	ocal			×
<ul> <li>Assign</li> </ul>	an existing licen:	se key to this host				
Produ	ct			Available		
E Ev	valuation Mode					
	(No License )	(ey)				
O Assian	a new license ke	eu to this host				
riooign	1					
En	ter Key					
Product:	Evaluation Mod	e				
Capacity:	-					
Available: Evoires:	-					
Label:	175172015					
Help				ок	Cancel	

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

🛃 Add License Key	X
New license key:	
Optional label for the new license key:	
	OK Cancel

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.

File Edit View Inventory Administration Plug-ins Help								
🖸 🔝 🏠 Home 🕨 🎇 Administration 🕨 🤗 Licensing								
Manage vSphere Licenses     ■	🐉 Manage vSphere Licenses							
Licensing								
Management Reporting								
View by: <ul> <li>Product</li> <li>C License key</li> <li>C Asset</li> </ul>								
Product	Assigned	Capacity	Label	Expires				
Evaluation Mode	2	Unlimited						
	1 instances	1 instances						
WMware vSphere 5 Enterprise Plus (unlimited cores per CPU)	40 CPUs	60 CPUs						



1. Install VUM

**PROCESS** 

- 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.

## CO 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**.

🙀 YMware vSphere Update M	anager X						
vCenter Server Information							
Please provide the necessary inf Update Manager will need this in	ormation about vCenter Server below. VMware vSphere formation to connect to the vCenter Server at startup.						
VMware vCenter Server Inform	nation						
IP Address / Name:	HTTP Port:						
vCenter-1.cisco.local	80						
<u>U</u> sername:	Password:						
administrator	••••••						
InstallShield							
	< Back Next > Cancel						

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

🙀 VMware vSphere Update Manager	×
Database Options Select an ODBC data source for VMware vSphere Update Manager.	2
VMware vSphere Update Manager requires a database.	
Install a Microsoft SQL Server 2008 R2 Express instance (for small scale deploy)	ments)
O Use an existing supported database	
Data Source Name (DSN): (Please create a 32 bit system DSN)	7
NOTE: Update Manager requires a 32 bit system DSN with supported types of data and versions of drivers.	bases
< Back Next >	Cancel

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

🔐 VMware vSphere Up	late Manager		X
VMware vSphere Upd	ate Manager Port Settings		
Enter the connection in	formation for Update Manager		
Specify how this VMwa make sure this IP addr	re vSphere Update Manager sho ess or host name can be accesso	ould be identified on the i ed from both vCenter Sei	network. Please rver and hosts.
10.4.48.212			
Setup will open the po service is running on t	ts in firewall if the Windows Fire ne system.	wall/Internet Connection	Sharing
<u>S</u> OAP Port:	<u>W</u> eb Port:	SS <u>L</u> Port:	
8084	9084	9087	
Tes, I have Intern	et connection and I want to conf	igure proxy settings now	
	< Back	Next >	Cancel

**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.

🛃 VMware vSphere Update Manager			×
<b>Ready to Install the Program</b> The wizard is ready to begin installation	Π.		2
Click Install to begin the installation.			
If you want to review or change any o exit the wizard.	of your installatio	n settings, click Bac	k, Click Cancel to
InstallShield			
	< Back	Install	Cancel

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**.

🖏 Services						 l×
File Action View	Help					
🧇 🔿 🔟 🤹 🖬	» 🛛 🖬 🕨 🔳 💵					
Services (Local)	Name 🔺	Description	Status	Startup Type	Log On As	
	🔍 VMware Snapshot Provider	VMware Sn		Manual	Local System	
	🔍 VMware Tools Service	Provides s	Started	Automatic	Local System	
	🔅 VMware vSphere Update Manager Service	VMware vS	Started	Automatic	Local System	
	🔍 VMware vSphere Update Manager UFA Ser	VMware Up	Started	Manual	Local System	

**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.

Howare vSphere Update	Manager Client 5.0 Update 1 🛛 🗙					
	Welcome to the InstallShield Wizard for VMware vSphere Update Manager Client 5.0 Update 1					
R.	The InstallShield(R) Wizard will install VMware vSphere Update Manager Client 5.0 Update 1 on your computer. To continue, click Next.					
<sup>VMware vSphere™</sup> Update Manager Client	WARNING: This program is protected by copyright law and international treaties.					
	< Back Next > Cancel					

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**.

🚰 Plug-in Manager						
Plug-in Name	Vendor	Version	Status	Description	Progress	Errors
Installed Plug-ins						
🐣 VMware vCenter Storage Monitoring Service	VMware Inc.	5.0	Enabled	Storage Monitoring and		
				Reporting		
🥞 vCenter Hardware Status	VMware, Inc.	5.0	Enabled	Displays the hardware status of		
				hosts (CIM monitoring)		
🐣 vCenter Service Status	VMware, Inc.	5.0	Enabled	Displays the health status of		
				vCenter services		
🔮 VMware vSphere Update Manager Extension	VMware, Inc.	5.0.0	Enabled	VMware vSphere Update		
				Manager extension		
Available Plug-ins						

## 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.

🛃 Schedule Update Dow	nload		_ 🗆 🗡
Schedule Task Select the time and	d frequency of the tas	k.	
Schedule Task Email Notification	Task Name	VMware vSphere Update Manager Update Download	
Ready to Complete	Task Description	A predefined scheduled task to download software updates.	
	Frequency:	Daily Start Time	
		9:28 PM	
		Run every 1 day(s).	

**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.

Update Manager Administration fo	or vCenter-1.cisco.local	
Getting Started Baselines and Group	ps Configuration Events Notifications Patch Repository ESXI Images VA Upgrades	
Settings	Download Settings Complian	ce View
Network Connectivity Download Settings Download Schedule Unification Schedule	Download Sources     Ownload sources     download new patches and VA upgrades either at intervals specified in Download     Schedule or immediately by clicking the Download Now button below     Add Download Source	
Nooncadon Check Schedule	Enabled Update Type Component Download Source Description Connectivity Status	
Virtual Machine Settings	VMware ESX https://hostupdate.vmware.com/software/V. Download vSphere ESX. Connected	
ESX Host/Cluster Settings	VMware ESX https://www.vmware.com/PatchManageme Download ESX 3x patc Connected	
vApp Settings	Custom ESX https://hostupdate.vm/ware.com/software/V. Download vSphere ESX. Connected     Connected Control Cont	
	C Use a shared repository What's this? Validate URL Download New Apply	
	Note: you can also Import Patches manually from a local .zip file	
	Proxy Settings	
	Use proxy     Proxy requires authentication	
	Proxy: Username:	
	Port: 0 Password:	
	Test Connection Apply	

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

🛃 vCenter-1.cisco.local - vSphere Client								
File Edit View Inventory Administration Plug-ins Help								
🖸 💽 🏠 Home 🕨 🖏 Management 🕨 🐯 Sch	🖸 🖸 home 🕨 🧃 Management 🕨 🐼 Scheduled Tasks 🔍 🖉 vCenter-1.cisco.local							
🐼 New 🛷 Properties 🔉 Remove	🐼 New 💯 Properties 🛛 🕄 Remove							
Name	Description	Last run	Next run					
VMware vSphere Update Manager Update Download	A predefined scheduled task to download software updates.	12/2/2012 9:28:00 PM	12/3/2012 9:28:00 PM					
VMware vSphere Update Manager Check Notification	A predefined scheduled task to check update notifications.	12/3/2012 1:33:00 PM	12/3/2012 2:33:00 PM					

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.

🛃 vCenter-1.cisco.local - vSphere Client				
File Edit View Inventory Administration Plug-ins	Help			
💽 💽 Anne 🕨 🖷 Management 🕨	📆 Scheduled Tasks 🕨 🛃 vCenter-1.cisco.local		🖅 🔹 Search Inventor	у 🔍
🐼 New 😿 Properties 😫 Remove				
Name	Description	Last run	Next run	
VMware vSphere Update Manager Update Download	A predefined scheduled task to download sof	tware updates. 12/3/2012 1:5	0:40 PM 12/3/2012 9:28:00 PM	
VMware vSphere Update Manager Check Notification	A predefined scheduled task to check update	notifications. 12/3/2012 1:3	3:00 PM 12/3/2012 2:33:00 PM	
Recent Tasks		Name, T	arget or Status contains: +	Clear ×
Name Target	Status Details	Initiated by	vCenter Server Requested S	tart Ti 🤝 🛛 Start Time
Download patch definit 2 vCenter-1.cisco	Completed	VMware vSp	VCenter-1.cisco 12/3/2012 1	:50:40 PM 12/3/2012 1:
🗞 Run scheduled task 🛛 🚱 vCenter-1.cisco	Completed	Administrator	VCenter-1.cisco 12/3/2012 1	:50:40 PM 12/3/2012 1:

**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**.

🚰 vCenter-1.cisco.local - vSphere (	Elient		×
File Edit View Inventory Administr	ration Plug-ins Help		
🖸 🖸 🔥 Home 🕨 👸 In	ventory 🕨 🎁 Hosts and Clusters		🛃 🛛 Search Inventory 🔍
a e 🗄 🕏 🗑 🏘			
Center-1.cisco.local	test-c220m3-1.cisco.local VMware E5Xi, 5.0.0, 623860	Evaluation (59 days remaining)	
	Resource Allocation Performance Configuration Tasks 8	& Events Alarms Permissions Maps Storage	Views Hardware Status Update Manager 🛛 🕸
		Name contains:	lear Scan Attach Help Admin View
	Attached Baseline Groups	Attached Baselines / Type	Host Compliance # Hosts
			No Baselines Attached
			<u> </u>

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



**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.

🛃 Confirm Scan	×
Scan the selected hosts for:	
Patches and Extensions	
Help	Scan Cancel

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

test-c220m3-1.cisco.local ¥Mware ESXi, 5.0.0, 623	860   Evaluation (59 days	remaining)			
Resource Allocation Performance Configuration	Tasks & Events 🔷 Alarms 🗸 P	ermissions Maps Sto	orage Views 🔪 Har	dware Status Upo	late Manager 🛛 🛛 🕬
	Nan	ne contains:	Clear Scan.	Attach H	lelp Admin View
Attached Baseline Groups	Attached Baselines	🛆 Туре		Host Compliance	# Hosts
😵 All Groups and Independent Baselines	🕨 🕺 Ali		•	All Applicable Ho	osts 1
	😵 Critical Host Patch	ies (Predefined) Patch		😵 Non-Compliant	1
	😵 Non-Critical Host 🖡	Patches (Prede Patch		Å Incompatible	0
				② Unknown	0
				🗸 Compliant	0
				Non-Compliant	
1					
All Groups and Independent Baselines -> All	-> 😵 Non-Compliant and	🔺 Incompatible and	l 🕜 Unknown a	and	
Host Name	Patcl	hes Upgrade	es Exte	ensions L	ast Patch Scan Ti
🖟 test-c220m3-1.cisco.local	😵 1	4 - Details		1	2/3/2012 2:00:19
Hide Hosts				[v]Stage	Remediate

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.

Remediate					_	
Remediation Selection Select the target object	s of your remediation.					
Remediation Selection Patches and Extensions	Select the baselines or baseline groups to re	emedial	e.			
Schedule	Baseline Groups and Types	B	aselines		1	
Host Remediation Options	Name		Name		🛆 Туре	
Ready to Complete	Baseline Groups		Critical Host Patches (Pre	defined)	Host Patches	
	C Patch Baselines			(r (coonino)		
	Host ~ Version		Patches	Extensions	Upgrades	-
	kest-c220m3-1.cisco.l. VMware ESXi	5.0.0	14 (0 staged)			

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

atches and Extensions Select the specific patc	hes and extensions that you w	vant to apply.					
emediation Selection atches and Extensions	Your remediation includes a change, any patch that you	dynamic baseline. 1 u exclude now will no	The exact list of a ot be applied.	applicable patches	might change before	e remediation occu	rs. Even if the list d
hedule ost Remediation Options				Patch Name, Ty	pe or Vendor contair	ns: •	Clea
eady to Complete	Patch Name Type	Severity	Category	Impact	Release Date	Vendor	Patch ID I
	✓ Updates esx… Patch	Critical	Security	Reboot	5/3/2012 1:00:0	VMware, Inc.	ESXi500-20 1
	🔽 Updates esx Patch	Critical	Security	Reboot	6/14/2012 1:00:	VMware, Inc.	ESXi500-20 1
	🔽 Updates VM Patch	Important	BugFix		4/12/2012 1:00:	VMware, Inc.	ESXi500-20 Y
	🔽 Updates esx Patch	Important	Security	Reboot	7/12/2012 1:00:	VMware, Inc.	ESXi500-20 1
	Updates too Patch	Important	Security		7/12/2012 1:00:	VMware, Inc.	ESXi500-20 1
	🔽 Updates esx Patch	Important	BugFix	Reboot	7/12/2012 1:00:	VMware, Inc.	ESXi500-20 1
	Updates too Patch	Important	BugFix		7/12/2012 1:00:	VMware, Inc.	ESXi500-20 1
	Updates scs Patch	Important	BugFix	Reboot, Ma	7/12/2012 1:00:	VMware, Inc.	ESXi500-20 Y
	🔽 Updates mis Patch	Important	BugFix	Reboot	7/12/2012 1:00:	VMware, Inc.	ESXi500-20 1
	Updates net Patch	Important	BugFix	Reboot, Ma	7/12/2012 1:00:	VMware, Inc.	ESXi500-20 1
	🔽 Updates esx Patch	Important	Security	Reboot	9/27/2012 1:00:	VMware, Inc.	ESXi500-20 1
	🔽 Updates esx Patch	Important	BugFix	Reboot	9/27/2012 1:00:	VMware, Inc.	ESXi500-20 1
	🔽 Updates too Patch	Important	BugFix		9/27/2012 1:00:	VMware, Inc.	ESXi500-20 \
	Undates mis., Patch	Important	BudEix	Reboot	9/27/2012 1:00:	VMware, Inc.	ESXi500-20 Y

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

Remediate		_ 0
Schedule Specify the time of the rer	nediation task.	
Remediation Selection Patches and Extensions Schedule Host Remediation Options Ready to Complete	Task Name:       test-c220m3-1.cisco.local         Task Description:       Apply Patches         Remediation Time:       Remediate the selected hosts:         If Immediately       Immediately         If At time:       12/-3/2012_2:05:00 PM	

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



Host Remediation Options Specify the maintenance mo	ode options of the remediation task.
Remediation Selection Patches and Extensions Schedule Host Remediation Options Ready to Complete	Maintenance Mode Options:         ▲ These options also apply to hosts in clusters.         Before host remediation, ESX/ESXI hosts might need to enter maintenance mode. Virtual machines and virtual appliances must be shut down or migrated. To reduce the host remediation downtime, you can select to shut down or suspend the virtual machines and appliances before remediation from the drop-down menu below.         Power state:       Power Off virtual machines         ✓       Retry entering maintenance mode in case of failure         Retry delay:       5         ✓       Disable any removable media devices connected to the virtual machines on the host.         ESXI 5.x Patch Settings       Enable patch remediation of powered on PXE booted ESXI hosts         ▲       PXE booted ESXI hosts revert to their original state after a reboot. To keep new software and patches on stateless hosts after a reboot, use a PXE boot image that contains the updates.

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

🛃 Remediate		
Ready to Complete Review the remediation :	settings before you complete th	e wizard.
Remediation Selection Patches and Extensions Schedule Host Remediation Options Ready to Complete	Host: Scheduling: Maintenance Mode Options:	test-c220m3-1.cisco.local Task Name - test-c220m3-1.cisco.local Remediate immediately Power Oth virtual machines Retry every 5 Minutes 3 Retries Settries
	Patch Baselines (2)     Non-Critical Host Pat Critical Host Patch     Critical Host Patches     Patches [14]     Updates tools-light     Updates tools-light     Updates esx-base     Updates esx-base     Updates tools-light     Updates esx-base     Updates esx-base     Updates esx-base	ches (Predefined) (Predefined) Is

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.



## **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

i

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.

August 2013

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

	Power		•
	Guest		٠
	Snapshot		•
2	Open Console		
₿	Edit Settings		
	Migrate		
**	Clone		
_	Template		٠
	Fault Tolerance		۲
	Add Permission	Ctrl+P	
	Alarm		٠
	Report Performance		
	Rename		
	Open in New Window	Ctrl+Alt+N	
	Remove from Inventory		
	Delete from Disk		

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

🚰 Migrate Virtual Machine		_ 🗆 🗙
Select Migration Type Change the virtual machine's hos	t, datastore or both.	
Select Migration Type Storage Ready to Complete	Change host         Move the virtual machine to another host.         Change datastore         Move the virtual machine's storage to another datastore.         Change both host and datastore         Move the virtual machine to another host and move its storage to another datastore.         Image the virtual machine must be powered off to change the VM's host and datastore.	

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

elect Migration Type	Select a virtual disk for	mat:						
Storage	Same format as source			•				
eady to Complete	Select a destination sto	rage for the virtu	ual machine files:					
	VM Storage Profile:	o not change the	e profiles	- 🔨 \Lambda				
	Name	Drive Type	Capacity	Provisioned	Free	Туре	Thin Provisioning	[
	C220M3-2-Sto.	Non-SSD	557.75 GB	45.05 GB	545.67 GB	VMFS5	Supported	
	Openfiler(Soft.	. Unknown	9.09 TB	6.22 TB	2.87 TB	NFS	Supported	_
		. Noresso	99/73 GD			WH-25	Supported	
	Disable Storage D	RS for this virtua	I machine			CCIIII	Supported	
	Disable Storage D Select a datastore:	RS for this virtue	I machine	ovisioned	Free	Туре	Supported	
	Disable Storage D Select a datastore: Name	RS for this virtua	I machine	ovisioned	Free	Туре	Thin Provisioning	
	Disable Storage D Select a datastore: Name	RS for this virtue	I machine	ovisioned	Free	Туре	Thin Provisioning	

**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.

Port Group Properties	
Network Label:	vMotion
VLAN ID (Optional):	161
	✓ Use this port group for vMotion
	Use this port group for Fault Tolerance logging
	Use this port group for management traffic

Step 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.

🛃 Migrate Virtual Machine 👘		_ 🗆 🗙
Select Migration Type Change the virtual machine	's host, datastore or both.	
Select Migration Type Select Destination vMotion Priority Ready to Complete	<ul> <li>Change host         Move the virtual machine to another host.</li> <li>Change datastore         Move the virtual machine's storage to another datastore.</li> <li>C Change both host and datastore         Move the virtual machine to another host and move its storage to another datastore.         Move the virtual machine must be powered off to change the VM's host and datastore.     </li> </ul>	

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

🛃 Migrate Virtual Machine 👘		
Select Destination Select the destination host	or cluster for this virtual machine migration.	
Select Migration Type Select Destination vMotion Priority Ready to Complete	IOK     test-c220m3-1.cisco.local     test-c220m3-2.cisco.local	

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

🛃 Migrate Virtual Machine 👘		_ 🗆 X
<b>vMotion Priority</b> Set the priority of the vMo	otion migrations, relative to the other operations on the destination host.	
Select Migration Type Select Destination vMotion Priority Ready to Complete	<ul> <li>High priority (Recommended)</li> <li>Standard priority</li> <li>High priority vMotions are favored over standard priority vMotions and are expected to perform better.</li> <li>If using an ESX 4.0 host or ESXI 4.0 host, click Help for additional information.</li> </ul>	

**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 CVD 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.



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

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. This process will use a manual installation method to accommodate an existing VMware environment where multiple network and management interfaces may exist.

## CO Reader Tip

For simple or new Nexus 1000V and VMware installation environments, the Cisco Nexus 1000V Installer Application may provide a simpler VSM deployment process. For more information, see:

http://www.cisco.com/assets/TD/switches/datacenter/nexus1000/sw/ 4\_2\_1\_s\_v\_2\_1\_1/install/workflow/nexus\_1000v\_r\_4\_2\_1\_S\_V\_2\_1\_1.html

PROCESS

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 design guide uses the Layer 3 mode of operation for VSM-to-VEM communication.

## Procedure 1 Install the first VSM

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

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

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

Table 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 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.

i	Tech Tip
You car	n install the software from the OVA or OVF image. Here you use the OVA
installat	tion file, because it allows you to apply initial configurations to the VSM,
includin	ng the VSM domain ID, admin user password, management IP address, subnet
mask, a	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.

	-VMkernel Port	Physica	l Adapters			
Ρ	Management Network 👲 🔶	• • •	vmnic1	20000	Full	5
	vmk0:10.4.63.102   VLAN ID:163	L- 🖷	vmnic0	20000	Full	두
_	Virtual Machine Port Group					
μ	N1kv_Control_Packet					
	VLAN ID: 160					
	Virtual Machine Port Group					
P	N1kv_Management 👳 🔶					
	VLAN ID: 163					
	Virtual Machine Port Group					
P	Servers_1 👳 🔶					
	VIAN ID: 149					

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

New	► rentory ► 🕅 Hosts	and Clusters
Deploy OVF Templa	te	
Export	•	
Report	•	chas1-s7.cisco.local VMware E
Browse VA Marketp	lace	Getting Started Summary Vir
Print Maps	Þ.	Hardware
Exit		Processors
VMFEX_te	sting	Memory
🗉 💋 🛛 VXI		Storage
	tisco.local	<ul> <li>Networking</li> </ul>
	enter	Storage Adapters
		Network Adapters
		Advanced Settings
		Advanced Settings Power Management
		Advanced Settings Power Management Software
		Advanced Settings Power Management Software Licensed Features
		Advanced Settings Power Management Software Licensed Features Time Configuration
		Advanced Settings Power Management Software Licensed Features Time Configuration DNS and Routing

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

Deploy OVF Template		_ 🗆 ×
Source Select the source location.		
Source OVF Template Details Name and Location Storage Disk Format Ready to Complete	Deploy from a file or URL .2.1.SV2.1.1a\VSM\Install\nexus-1000v.4.2.1.SV2.1.1a.ovd ▼ Browse Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.	

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

🛃 Deploy OVF Template		
OVF Template Details Verify OVF template details		
Source OVF Template Details End User License Agreement	Product:	Nexus1000V-4.2.1.SV2.1.1a
Name and Location Deployment Configuration	Version:	4.2(1)5V2(1.1a)
Storage Disk Format	Vendor:	Cisco Systems Inc
Network Mapping Properties	Publisher:	No certificate present
Ready to Complete	Download size:	122.2 MB
	Size on disk:	Unknown (thin provisioned) 3.0 GB (thick provisioned)
	Description:	Cisco Nexus 1000V Virtual Supervisor Module

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

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

Deploy Over remplate		
Name and Location Specify a name and locatio	n for the deployed template	
Source OVF Template Details	Name: DC-N1kv-VSM-1	
End User License Agreement Name and Location Deployment Configuration	The name can contain up to 80 characters and it must be unique within the inventory folder.	
Storage Disk Format Network Mapping	Inventory Location:	
Properties Ready to Complete		

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.

Deploy OVF Template Storage Where do you want to sto	re the virtual machine f	iles?			
<u>Source</u> OVF Template Details End User License Agreement	Select a destination s VM Storage Profile:	torage for the virtu	ual machine files:		
Name and Location	Name	Drive Type	Capacity Provisioned	Free Type	Thin Prov
Deployment Configuration	🔋 chas1-s7-loca	l Non-SSD	552.00 GB 973.00 MB	551.05 GB VMFS5	Supporte
Disk Format Disk Format Network Mapping Properties Ready to Complete	BHARED-STO	Non-SSD	99.75 GB 1.98 GB	97.77 GB VMF55	Supporte

**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.

🗗 Deploy O¥F Template			
<b>Disk Format</b> In which format do you wa	nt to store the virtual disks?		
<u>Source</u> OVF Template Details	Datastore:	chas1-s7-local-disk	
End User License Agreement Name and Location Deployment Configuration	Available space (GB):	551.0	
Storage Disk Format Network Mapping Properties Ready to Complete	C Thick Provision Lazy Ze Thick Provision Eager Z Thin Provision	roed eroed	

**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**.

Network Mapping What networks should the	deployed template use?		
Source OVF Template Details End User License Agreement	Map the networks used in this OVF	template to networks in your inventory	
Name and Location	Source Networks	Destination Networks	
Deployment Configuration	Control	N1kv_Control_Packet	
Storage Disk Formation	Management N1kv_Management		
Network Mapping Properties Ready to Complete	Packet	N1kv_Control_Packet	
	Description:		
	This network provides connectivity Module. Please associate it with th mgmt0" is configured within the VS	r (ssh/teinet/scp) to the Cisco Nexus 1000V Virtual Supervisor e portgroup that corresponds to the subnet, the "interface M.	4
	Warning: Multiple source networks	are mapped to the bost betwork: N1ky, Control, Packet	

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

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

Deploy OVF Template		_ [
Properties Customize the software solul	ion for this deployment.	
Source OVF Template Details End User License Agreement Name and Location Deployment. Configuration Storage Disk Format Network Mapping Properties Ready to Complete	b. Nexus 1000V Admin User Password         Password         Enter the password Must contain at least one capital, one lowercase, one number.         Enter password         Confirm password         ********         Confirm password         ************************************	

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

🖉 Deploy OVF Template		
Ready to Complete Are these the options you	want to use?	
Source OVE Template Details End User License Acreement Name and Location Deployment. Configuration Storage Disk Format Network Mapping Properties Ready to Complete	When you click Finish, the deploym Deployment settings: OVF file: Download size: Size on disk: Name: Folder: Deployment Configuration: Host/Cluster: Datastore: Disk provisioning: Network Mapping: IP Allocation: Property: Property: Property: Property: Property: Property: Property: Property: Property: Property:	C:(Downloads)Wexus1000v.4.2.1.5V2.1.1a\Wexus1000v.4 122.2 MB 3.0 GB DC-MINV-VSM-1 10k Nexus1000V Installer chas1=57-local-disk Thick Provision Eager Zeroed "Control" Fo"NIA_Control_Packet" "Management" to "NILv_Control_Packet" "Packet" to "NILv_Control_Packet" Fixed, IPv4 Domaintd = 12 ManagementIpV4 = 10.4.63.28 ManagementIpV4 = 10.4.63.1
Help		< Back Finish Cancel

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).

Following files are available for download :					
-					
Cisco Nexus 1000V Installer Application					
<ul> <li>Launch Installer Application (deprecated)</li> </ul>					
Cisco Nexus 1000V Extension					
◦ cisco_nexus_1000v_extension.xml					
VEM Software					
Description File					
ESXi 5.1 or later cisco-vem-v152-4.2.1.2.1.1a.0-3.1.1.zip					
ESXi 5.0 or later cisco-vem-v152-4.2.1.2.1.1a.0-3.0.1.zip					
ESX/ESXi 4.1.0 or later cisco-vem-v152-4.2.1.2.1.1a.0-2.0.1.zip					
ESXi 5.1 or later cross_cisco-vem-v152-4.2.1.2.1.1a.0-3.1.1.vib					
ESXi 5.0 or later cross_cisco-vem-v152-4.2.1.2.1.1a.0-3.0.1.vib					
ESX/ESXi 4.1.0 or later cross_cisco-vem-v152-4.2.1.2.1.1a.0-2.0.1.vib					

**Step 2:** Under the Cisco Nexus 1000V Extension, right-click on the **cisco\_nexus\_1000v\_extension.xml** file, select the **Save target as** option, and then save the xml file to the local directory of the machine from where you launch vSphere Client.

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

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

🛃 Plug-in Manager						_ 🗆 🗡
			-			
Plug-in Name Vendor	Version	Status	Description	Progress	Errors	
Installed Plug-ins						
🦂 VMware vCenter Storage Mon VMware Inc.	5.0	Enabled	Storage Monitoring and			
			Reporting			
🗳 VMware vSphere Update Ma VMware, Inc.	5.0.0	Enabled	VMware vSphere Update			
			Manager extension			
vCenter Hardware Status VMware, Inc.	5.0	Enabled	Displays the hardware status of			
			hosts (CIM monitoring)			
vCenter Service Status VMware, Inc.	5.0	Enabled	Displays the health status of			
			vCenter services			
Available Plug-ins						
👌 Cisco-UCSM-dbc91092-0286 Cisco Systems I	. 1.0.0	Download and I				
1						
Help						Close

**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**.

🗗 Register Plug-in		×
Current vCenter Server:	vCenter.cisco.local	
	_	
Provide an input plug-in xi	nl file which needs to be registered with vCenter Server.	
File name: C:\Users\vsa	thiam\Downloads\N1kv\cisco_nexus_1000v_extension.xml Brows	e
View Xml: (read-only)		
- cevtensionData		▲
- <obi <="" th="" versionid="uber" xmlns="u&lt;/td&gt;&lt;th&gt;(m:vim25" xsi:type="Extension"><td></td></obi>		
xmlns:xsi="	1ttp://www.w3.org/2001/XMLSchema-instance">	
– <descriptior< p=""></descriptior<>	>	
<label></label>		
<summary< td=""><th>1&gt;</th><td></td></summary<>	1>	
<th>.n&gt;</th> <td></td>	.n>	
<key>ciscu</key>	_Nexus_1000v_707033274	
Version>1.	U.U. Version	
<subjectn< td=""><th>lame&gt;/C=US/ST=CA/O=Cisco/OU=NexusCertificate</th><td>/CN=Cisco Nexus 1000V</td></subjectn<>	lame>/C=US/ST=CA/O=Cisco/OU=NexusCertificate	/CN=Cisco Nexus 1000V
- <server></server>		····
<url></url>		
– <descripti< td=""><th>on&gt;</th><td></td></descripti<>	on>	
<label <="" td=""><th>&gt;</th><td></td></label>	>	
<summa< td=""><th>ary /&gt;</th><td></td></summa<>	ary />	
<th>cion&gt;</th> <td></td>	cion>	
<company< td=""><th>/&gt;Cisco Systems Inc.</th><td></td></company<>	/>Cisco Systems Inc.	
<type>D\</type>	/S	
<adminem< td=""><th>al /&gt;</th><td></td></adminem<>	al />	
- <client></client>		
<uri></uri>		
- Cuescripti		
•		
Help		Register Plug-in Cancel

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

Security Warning	
Certificate Warnings An untrusted certificate is provided as part of plug certificate will be used by vCenter Server to author policy, this issue might not represent a security co	g-in registration xml. Post-registration, this enticate the plug-in. Depending on your security pncern.
Click Ignore to continue using the certificate.	
View Certificate	Ignore Cancel

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

i

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.

```
\texttt{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.


**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.

View	vSphere Standard Switch vSph	ere Distributed Switch				
Net	Networking					
Stan	dard Switch: vSwitch0	Remove Properties				
P	VMkernel Port Management Network	Physical Adapters				
	vmk0 : 10.4.63.103   VLAN ID: 163	📙 🖵 📟 vmnic0 20000 Full 🖓				
P	Virtual Machine Port Group Servers_1					
	VLAN ID: 148					
P	-Virtual Machine Port Group N1kv_Control_Packet	+				
	VLAN ID: 160					
þ	Virtual Machine Port Group N1kv_Management					
	VLAN ID: 163					

**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**.

Name and Location Specify a name and locatio	n for the deployed template	
Source OVF Template Details End User License Agreement Name and Location Deployment Configuration	Name: DC-N1kv-VSM-2 The name can contain up to 80 characters and it must be unique within the inventory folder.	
Disk Format Network Mapping Properties Ready to Complete	Inventory Location:	

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

Deploy OVF Template Deployment Configuration Select a deployment configur	ation.
Source OVF Template Details End User License Agreement Name and Location Deployment Configuration Storage Disk Format Network Mapping Properties Ready to Complete	Configuration: Nexus 1000V Secondary Use this deployment option to pair the Nexus 1000V VSM with a secondary VSM in a HA pair. If this option is selected, please only enter the selected properties as prompted in the Properties section ahead ignoring Property (c-e).

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

Step 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**.

🛃 Deploy OVF Template		_ 🗆 ×
Properties Customize the software solut	ion for this deployment.	
Source OVE Template Details End User License Agreement Name and Location Disk.Format Network: Mapping Properties Ready to Complete	a. VSM Domain ID         Domain1d         Enter the Domain Id (1-4095).         [12         b. Nexus 1000V Admin User Password         Password         Enter the password. Must contain at least one capital, one lowercase, one number.         Enter the password         Enter the password         @confirm password         @exercise         Confirm password         @exercise         Enter the VSM IP in the following form: 192.168.0.10         @otdlewing form: 192.168.0.10         @otdlewing form: 192.168.0.10         @otdlewing form: 255.255.255.0         @otdlewing form: 255.255.255.0	
Help	< Back Next >	Cancel

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

🚰 Deploy OVF Template		
Ready to Complete Are these the options you	want to use?	
Source OVF Template Details End User License Agreement Name and Location Disk Format Network Mapping Properties Ready to Complete	When you click Finish, the deploym Deployment settings: OVF file: Download size: Size on disk: Name: Folder: Deployment Configuration: Host/Cluster: Datastore: Disk provisioning: Network Mapping: Network Mapping: Network Mapping: PAllocation: Property: Proper	ent task will be started. C:\Downloads\Nexus1000v.4.2.1.5V2.1.1a\Nexus1000v.4 122.2 MB 3.0 GB DC-N1kv-VSM-2 10k Nexus 1000V Secondary chas1-s8.cisco.local chas1-s8-ic
Help		< Back Finish Cancel

**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). If you configured centralized authentication in Step 13 of the "Configure the primary VSM" procedure, you must log in using a username and password that has administrative privileges.

**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 --- ----- ------Virtual Supervisor Module Nexus1000V active \* 1 0 2 0 Virtual Supervisor Module Nexus1000V ha-standby Mod Sw Hw \_\_\_\_ \_\_\_\_\_ 1 4.2(1)SV2(1.1a) 0.0 2 4.2(1)SV2(1.1a) 0.0 Mod MAC-Address(es) Serial-Num \_\_\_\_ \_\_\_\_\_ 1 00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8 NA 2 00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8 NA Mod Server-IP Server-UUID Server-Name \_\_\_\_ \_\_\_\_\_ 10.4.63.28 1 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.

August 2013



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

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		
160	1kv-Control	Cisco Nexus 1000V Control		
161	vMotion	VMware vMotion		
162	iSCSI	iSCSI transport traffic		
163	DC-Management	Data Center Management Traffic		

Table 5 - VLANs for Cisco Nexus 1000V Series switch

**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). If you configured centralized authentication in Step 13 of the "Configure the primary VSM" procedure, you must log in using a username and password that has administrative privileges.

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 149-155
DC-N1kv-VSM(config-vlan)# vlan 160
DC-N1kv-VSM(config-vlan)# name 1kv-Control
DC-N1kv-VSM(config-vlan)# vlan 161
DC-N1kv-VSM(config-vlan)# name vMotion
DC-N1kv-VSM(config-vlan)# vlan 162
DC-N1kv-VSM(config-vlan)# name iSCSI
DC-N1kv-VSM(config-vlan)# vlan 163
DC-N1kv-VSM(config-vlan)# name DC-Management
```

The control and management VLANs are defined as system VLANs, as are VMware VMkernel iSCSI VLANs connecting to storage and VLANs used with vMotion traffic. Port profiles that contain system VLANs are defined as *system port profiles*. In the deployment in this guide, the Cisco UCS C-Series server is physically connected to two different switches in a fabric extender (FEX) 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 CVD 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 148-155,160-163
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 11 - 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\_V1148
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 I3control** 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.

🎄 Cisco Unified Co	omputing System Man	ager - FI6248UP												. 🗆 >
- Fault Summary	V	Δ			🧿 🍈 🛤 New - 🎴 😧 Options	00	Pending Activities	0 Ext						diade
0	12	9	14	16	>> = LAN + O LAN Cloud + = NLANS = VLANS									
Equipment Server	< LAN SAN M Adm	o.			VLANS									
edation in parter				1	🕰 Filter 👄 Export 😹 Print									
	Filter: Al	•			Name	[ ID	Tune	Transport	Mative	VI AN Sharing	Primary VI AN Name	M dtinast Policy Name	imi	
± =					VIANDC Management (163)	163	1990	Ether	No	None	Prindly VLMA Nono	Profocase Policy Name		
					ULANEW Incide 1 (154)	154	Lan	Ether	No.	None				
			<u>^</u>		VIANTW_Bride_2 (151)	100	Lan	Ether	No.	None				
E CAN CO	uu nic ă				MANEW Creater (153)	163	Lan	Ether	No.	None				
E ess Fabr	nic B				VIAN N1ka Control (160)	160	Lan	Ether	No	None				
	System Class				UI AN Servers 1 (149)	149	Lan	Other	Ale	Alama				+
LAN	Pin Groups				VLAN Servers 2 (140)	140	Lan	Ether	No.	Mana				
🕀 🚿 Thre	shold Policies				VLAN DE VEIS_2 (147)	167	Lan	Ether	No	Mana				
VLA1	N Groups				Station (1)	1.07	Lan	Ether	Ver	None				10
	NS				VLAN LOCAT (162)	162	Lan	Ether	100	None				
	VLAN DC_Management (1)	63)			ULANI, Making (101)	100	Con .	China	A14	Name				
	VLAN PW_Inside_1 (154)				- VLAN 1190001(181)	101	can	coler	140	14.3.10				
	VLAN PW_DISUE_2 (155)													
	VLAN NI ky-Coptrol (160)												-	
	VLAN Servers 1 (148)				A.W								-	
	VLAN Servers 2 (149)				Details									
	VLAN VDI_Clients (157)				General Org Permissions VLAN Gr	oup Membership	Faults Events							
=	VLAN default (1)													
- 3	VLAN ISCSI (162)				Fault Summary									
	VLAN vMotion (161)											WWD:		
Applance	es .				0 0 0	0						Extent The		
internal	LAN mal Fabria A				- Octions									
ince	riidi Fabric A													
E S The	schold Policies													

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 Unified Computing System Design 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

August 2013

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**.

Network Connectivity Download Settings Download Schedule	Download Sources     Orrect connection to Internet - download new patches and VA upgrades either at intervals specified in Download     Schedule or immediately by clicking the Download Now button below	Add Download Source
Notification Check Schedule Virtual Machine Settings ESX Host/Cluster Settings vApp Settings	Enabled         Ubdat.         Com         Download Source           IV         VMware ESX         https://hostupdate.vmware.com/software/VLMPRCOUCTION/main/vmw-depol-inde           IV         VMware ESX         https://hostupdate.vmware.com/software/VLMPRCOUCTION/main/vmw-depol-inde           IV         VMware ESX         https://hostupdate.vmware.com/software/VLMPRCOUCTION/main/vmw-depol-inde           IV         Custom ESX         https://hostupdate.vmware.com/software/VLMPRCOUCTION/csco-main/csco-depol           IV         V/thware VAs         http://hostup-updates.vmware.com/soil-catalogIndex.xml	Descripti Connectivity State Downloa Connected Downloa Connected Downloa Connected Downloa 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**.

Add Host to vSphere Distribute	d Switch				
Select Hosts and Physical Ada	pters	-L			
select nosts and physical ada	pters to add to this vsphere distributed swit	cn.			
Select Host and Physical Adap	ters			Settings	<ul> <li>View Incompatible Hos</li> </ul>
Network Connectivity	Host/Physical adapters	In use by switch	Settings	Uplink port group	
irtual Machine Networking	🖃 🗹 📋 c210m2-1.cisco.local		View Details		
eady to Complete	Select physical adapters				
	🗹 📖 vmnic0	vSwitch1	View Details	10G-CSeries	
	🗹 📖 vmnic1	vSwitch1	View Details	10G-CSeries	
	Vmnic2	vSwitch0	View Details	ESXI-Mgmnt-Uplink	
	Vmnic3	vSwitch0	View Details	ESXi-Mgmnt-Uplink	
	표 🔲 📋 chas1-s1.cisco.local		View Details		
	🖃 🗹 📋 chas1-s6.cisco.local		View Details		
	Select physical adapters				
	Vmnic0	vSwitch0	View Details	System-Uplink	
	Vmnic1	vSwitch0	View Details	System-Uplink	
	🗉 🔲 📋 chas1-s7.cisco.local		View Details		
	🕀 🗖 📋 chas1-s8.cisco.local		View Details		
	🗄 🗖 📋 chas2-s1.cisco.local		View Details		
	🖅 🔲 🗐 chas2-s3.cisco.local		View Details		

**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.

Add Host to vSphere Distributed S	Switch						
Select port group to provide net	vork connectivity for the adapters o	on the vSphere distrib	uted switch.				
Select Host and Divisical Adapters	Assign adapters to a destin	nation port group to m	igrate them. Ctrl+click to multi-	select.			
Network Connectivity	A Virtual NICs marked with th	ne warning sign might	lose network connectivity unles	s they are migrated to the vSphere			
Virtual Machine Networking	distributed switch. Select a destination port group in order to migrate them.						
Ready to Complete	Host/Virtual adapter	Switch	Source port group	Destination port group			
	🗉 🖟 c210m2-1.cisco.local						
	🜇 vmk0	vSwitch0	Management Network	n1kv-L3			
	🗾 vmk1	vSwitch1	vMotion	vMotion			
	🗾 vmk2	vSwitch1	iSCSI	ISCSI			
	🖃 🖟 chas1-s6.cisco.local						
	🛐 vmk0	vSwitch0	Management Network	n1kv-L3			
	📷 vmk1	vSwitch0	iSCSI	ISCSI			
	vmk2	vSwitch0	vMotion	vMotion			



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.

🗿 Add Host to vSphere Distributed Sv	vitch				
Virtual Machine Networking Select virtual machines or network	adapters to migrate to the vSph	nere distributed switch.			
Select Host and Physical Adapters Network Connectivity Virtual Machine Networking Ready to Complete	Migrate virtual machine in     Assign VMs or network a     Host/Virtual machine/Networi     C210m2-1.cisco.loc     C210m2-1.cisco.loc     Win2008-Test1     Network ada	etworking Japters to a destination port a adapter NIC count al 1 pter 1	group to migrate then Source port group Servers_1	n. Ctrl+click to multi-select. Destination port group Servers_VI148 Servers_VI148	
	Network adapter details           Win2008-Test1           Host:           Network adapter 1           MAC address:	c210m2-1.cisco.local			Assign port group
	Adapter type:	VMXNET 3			
Help				< Back	Next > Cancel

**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.

Hardware	View: vSphere Standard Switch vSphere Distributed Switch	
Processors	Networking	Refres
Memory		
Storage	Distributed Switch: N1kvVSM	Manage Virtual Adapters Manage Physical Adapters Properties
<ul> <li>Networking</li> </ul>		
Storage Adapters	N1kvV5M	
Network Adapters		
Advanced Settings	👳 iSCSI 🚯 🍖	Unused_Or_Quarantine_Uplink
Power Management	VMkernel Ports (1)	
C-Burren	vmk2 : 10.4.62.95 🚯 🗕 🔂	+ System-Lolink
Suitware	Virtual Machines (0)	
Licensed Features		
Time Configuration	😨 n1kv-L3 🚯 🏀	ESXI-Mgmnt-Uplink (1)
DNS and Routing	WMkernel Ports (1)	Image: Second
Authentication Services	vmk0 : 10.4.63.95 🚯 🕂 🕞	Image: Contract of the second seco
Power Management	Virtual Machines (0)	
Virtual Machine Startup/Shutdown	Converse Ult 49	- Tug-CSeries
Virtual Machine Swapfile Location		UpLink00 (1 NIC Adapter)
Security Profile	Virtual Machines (1)	UpLink01 (1 NIC Adapter)
Host Cache Configuration	WIN2008-Test1	
System Resource Allocation	🗣 Unused Or Ouarantine V 🚯 🍖	
Agent VM Settings	Virtual Machines (0)	
Advanced Settings		
	👳 vMotion 🕕 🍫	
	- VMkernel Ports (1)	
	vmk1 : 10.4.61.95	
	Virtual Machines (0)	



# **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 5.0 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.

## 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

### 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

**PROCESS** 

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 Unified Computing System Design 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 Unified Computing System Design 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)

🏯 Create Dynamic vNIC Connection Policy	×
Create Dynamic vNIC Connection Policy	0
Name: IDM_to_FI_4-Link Description: VMFEX Policy for VMware Number of Dynamic vNICS: 54 Adapter Policy: VMWarePassThru  Protection: Protected Pref A C Protected Pref B • Protected	
OK	Cancel

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.

📥 Create BIOS Policy		×
Unified C	omputing System Manager	
Create BIOS Policy	Main	9
V <u>Main</u> Processor     Intel Directed IO     Bas Memory     Serial Port     USB     Pect Configuration     Boot Options     Server Management	Name: VMwarePassThru Reboot on BIOS Settings Change: Quiet Boot: C disabled C enabled C Platform Default Post Error Pause: C disabled C enabled C Platform Default Resume Ac On Power Loss: C stay-off C last-state C reset C Platform Default Front Panel Lockout: C disabled C enabled Platform Default	

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

📥 Create BIOS Policy			X
Unified C	omputing	System Manager	
Create BIOS Policy	Processor		0
2. √ <u>Processor</u> 3. □ <u>Intel Directed IO</u>	Turbo Boost:	C disabled C enabled C Platform Default	
4. □ <u>RAS Memory</u> 5. □ <u>Serial Port</u>	Enhanced Intel Speedstep:	C disabled C enabled © Platform Default	
6. ∐ <u>USB</u> 7. □PCI Configuration	Hyper Threading:	C disabled C enabled C Platform Default	
8. Boot Options	Core Multi Processing:	Platform Default	
9. D <u>Server Management</u>	Execute Disabled Bit:	○ disabled ○ enabled ○ Platform Default	
	Virtualization Technology (VT):	C disabled  enabled C Platform Default	
	Direct Cache Access:	C disabled  enabled  Platform Default	
	Processor ⊂ State:	C disabled C enabled  Platform Default	
	Processor C1E:	C disabled C enabled  Platform Default	
	Processor C3 Report:	C disabled C acpi-c2 C acpi-c3 C Platform Default	
	Processor C6 Report:	C disabled C enabled C Platform Default	
	Processor C7 Report:	C disabled C enabled  Platform Default	
	CPU Performance:	C enterprise C high-throughput C hpc • Platform Default	
	Max Variable MTRR Setting:	🔿 auto-max 🔿 8 💿 Platform Default	

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

📥 Create BIOS Policy			X
Unified C	omputing	System Mana	ger
Create BIOS Policy	Intel Directed IO		0
2. √ <u>Processor</u>			
3. √ <u>Intel Directed IO</u> 4. □ PAS Memory	VT For Directed IO:	C disabled      enabled      C Platform Default	
5. Serial Port	Interrupt Remap:	○ disabled ⊙ enabled ○ Platform Default	
6. U <u>USB</u> 7. D <u>PCI Configuration</u>	Coherency Support:	🔿 disabled 💿 enabled 🔿 Platform Default	
8. Boot Options	ATS Support:	🔿 disabled 💿 enabled 🔿 Platform Default	
<ol> <li>Server Management</li> </ol>	Pass Through DMA Support: O	C disabled    enabled    Platform Default	

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

📥 Create BIOS Policy		×
Unified C	omputing System Manager	
Create BIOS Policy 1. V <u>Main</u>	Server Management	0
2. √ <u>Processor</u> 3. √ <u>Intel Directed IO</u> 4. √ <u>RAS Memory</u> 5. √ <u>Serial Port</u> 6. √ <u>USB</u> 7. √ <u>PCI Configuration</u> 8. √ <u>Boot Options</u> 9. √ <u>Server Management</u>	Assert Nmi On Serr: Clasabled Clasabled Platform Default Assert Nmi On Perr: disabled Platform Default OS Boot Watchdog Timer: disabled Platform Default Console Redirection: Platform Default Flow Control: none rts-cts Platform Default BALD Rate: Platform Default Terminal Type: Platform Default Legacy OS Redirect: disabled Platform Default	
	< Prev Next > Finish	Cancel

#### 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**.

>> 🥪 Servers 🕨 💐 Service Profiles 🛌	🛕 root > 🥶 Service Profile VMFEX-Server-1 🥶 Service Pro	file VMFEX-Server-
General Storage Network SCSI vNIC	Is Boot Order Virtual Machines FC Zones Policies Server Details FSM VIF Paths Faults Events	
Actions	Policies	
🔊 Change Serial over LAN Policy	BIO5 Policy	۲
	BIOS Policy . VMwarePassThru 🔍 💶 Create BIOS Policy BIOS Policy Instance:	
	Firmware Policies	۲
	IPMI Access Profile Policy	8
	Power Control Policy	۲
	Scrub Policy	8
	Serial over LAN Policy	8
	Stats Policy	8



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.

📥 Change Dynamic vNIC Connection Policy		×
Change Dynamic vNIC Connection Policy		0
Select the Dynamic vNIC Connection Policy: Use a Dynamic vNIC Connection Policy	-	
Dynamic vNIC Connection Policy		
Dynamic vNIC: IOM_to_FI_4-Link 🔽		
0		



#### **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.

🚰 Datastore Browser - [LOCAL-DISK-54	1				_ O ×
💩 🕼 💕 🛢 🛢 😫 🗙	: @				
Folders Search	[LOCAL-DISK-S4] Downloads				
	Name	Size	Туре	Path	Modifie
Downloads	cross_cisco-vem-v132-4.2.1.1	3,242.01 KB	File	[LOCAL-DISK-S4] Downloads	12/10/

**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.

emote Access		
y default, remote clients are pr	revented from accessing services on this host, and local clients are prevented from	
loless configured otherwise da	amone will start automatically	
riless coningureu ocherwise, ua	senions will start auconiacically.	
Label	Daemon	
I/O Redirector (Active Director;	y Se Stopped	
Network Login Server (Active D	Direc Stopped	
lbtd	Running	
vpxa	Running	
ESXi Shell	Stopped	
Local Security Authentication Se	jerv Stopped	
NTP Daemon	Stopped	
SSH	Stopped	
Direct Console UI	Running	
CIM Server	H (TSM-55H) Options	
St	tatus	
Service Properties	Stopped	
	Jopped	
General		
General	tartup Policy	
General St	Rattup Policy	
General Service: C Package Information C	Tartup Policy	
General Service: C Package Information C	tartup Policy	
General St Service: C Package Information C	Tartup Policy Start automatically if any ports are open, and stop when all ports are closed Start and stop with host Start and stop manually	
General Service: Package Information	Sopped itartup Policy Start automatically if any ports are open, and stop when all ports are closed Start and stop with host Start and stop manually ervice Commands	]
General Service: Package Information	Stopped Startup Policy Start automatically if any ports are open, and stop when all ports are closed Start and stop with host Start and stop manually ervice Commands Start Stop Restart	]
General Service: Package Information	Stopped Startup Policy — Start automatically if any ports are open, and stop when all ports are closed Start and stop with host Start and stop manually ervice Commands Start Stop Restart	
General S Service: C Package Information C	Stopped Startup Policy Start automatically if any ports are open, and stop when all ports are closed Start and stop with host Start and stop manually iervice Commands Start Stop Restart	]
General S Service: C Package Information C Se	Stopped Startup Policy Start automatically if any ports are open, and stop when all ports are closed Start and stop with host Start and stop manually ervice Commands Start Stop Restart	
General Si Service: C Package Information C	Stopped Start up Policy Start automatically if any ports are open, and stop when all ports are closed Start and stop with host Start and stop manually iervice Commands Start Stop Restart	]
General Si Service: C Package Information C	Stopped       Startup Policy       Start automatically if any ports are open, and stop when all ports are closed       Start and stop with host       Start and stop manually       iervice Commands       Start       Start       Stop       Restart	

**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.

```
# cd /var/log/vmware
```

/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 MTUUplinksvSwitch012841281500vmnic0,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.



Once the plug-in registration process completes, return to this wizard and click the Next button below

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**.

Export vCenter Extension	×
Save Location: C:\VMFEX	
OK Cancel Help	

**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, in the empty space, right-click, and then click **New Plug-in**.

Plug-	in Manager							
Plug-ir	n Name	Vendor	Version	Status	Description	Progress	Errors	
Insta	lled Plug-ins							
3	VMware vCenter Storage Mon	VMware Inc.	5.0	Enabled	Storage Monitoring and			
					Reporting			
3	VMware vSphere Update Ma	VMware, Inc.	5.0.0	Enabled	VMware vSphere Update			
					Manager extension			
3	vCenter Hardware Status	VMware, Inc.	5.0	Enabled	Displays the hardware status of			
					hosts (CIM monitoring)			
3	vCenter Service Status	VMware, Inc.	5.0	Enabled	Displays the health status of			
					vCenter services			
Availa	able Plug-ins							
3	Cisco_Nexus_1000V_759878	Cisco Systems, I	1.0.0	No client side d				
	Ne	w Plug.ip						
		Windy min						

**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.

📥 Configure ¥Mware Integration	2
Unified C	omputing System Manager
Configure VMware Integration	Define VMware Distributed Virtual Switch(DVS)
<ol> <li>Ansoan August In Trease Server</li> <li><u>Perfore Wware</u></li> <li><u>Distributed Writual</u></li> <li><u>Bowner Port Profile</u></li> <li><u>Apply Port Profiles to</u> <u>Writual Machines in vCenter</u></li> </ol>	VCenter Server VCenter Server Name: 10k-vCenter Description: VCenter Server Hostname or IP Address: 10.4.48.211 Datacenter
	vCenter Datacenter Name: 10k Description: 10k Datacenter
	DVS Folder Folder Name: VM-FEX Description:
	DVS DVS Name: VM-FEX-10k Description: DVS C Disable C Enable

*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**.



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

	Define Port Profile				•
I. √ <u>Install Plug-in on vCenter</u> <u>Server</u> Z. √ <u>Define VMware Distributed</u> <u>Wrtual Switch(DVS)</u> 3. √ <u>Define Port Profile</u> 4	Port Profile Name: DC_Ma	nagement	_		
<ul> <li>Apply Part Profiles to <u>Virtual Machines in vCenter</u> <u>Server</u>.</li> </ul>	Vetwork Control Policy: CIOP-En- Max Ports: 64 Pin Group: <not set<="" th=""><th>t&gt;</th><th></th><th></th><th></th></not>	t>			
	Select	Name	Native VLAN	.₽	
		default	0		
		DC_Management	0		
		FW_Inside_1	0		
		FW_Inside_2	0		
		FW_Outside	0		
		N1kv-Control	0		
		Servers_1	0		
		Servers_2	0		
		VDI_Clients	0		
		iSCSI	0	T	
	Profile Client Name: DC_M Description: Datacenter: 10k Folder: VM-FE Distributed Virtual Switch:	fanagement × X X X X X X X			

**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:** On the General tab, in the Properties section, for Host Network IO Performance, select **High Performance**, click **Save Changes**, and then click **OK**.

Ligh_portormoneo	modo allowe tr	offic to and from	$m \sim 1/N/t \sim h$	avenace the co	ttward DV/S on	d hyporylicor
I IIUII-DEITOITTAILCE	ו מווטעפ מווטעא נו	מחוכ נט מחט חטו	II a vivi lo k	שלאלא אות אות אות אות אות אות אות אות אות או	חנשמופ סעט מוו	
5 1						- )

>> All 🕴 🚍 Port Profiles 🕴 🚍	> All 🕴 🗏 Port Profiles 👌 🗐 Port Profile DC_Management 📃 Port Profile DC_Management			
General VM LANs Profile Clier	nts   Virtual Machines   Events			
Actions	Properties			
🚦 Create Profile Client	Name: DC_Management			
-( Modify VLANs	Description:			
🗂 Delete	QoS Policy: <not set=""></not>			
	Network Control Policy: CDP-En-LinkLoss			
	Max Ports: 64			
	Host Network IO Performance: O None  High Performance			
	Pin Group: <not set=""></not>			

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**.

1	Тес	h Tip					
If the	e virtual r	machine (	can tac	, the traffic, i	t is r	ot necessary to	select Native VLAN
				, ,		,	
Create Po	ort Profile					X	
reate	Port Profi	ile				0	
acate		ic.					
	Name:	Servers_2_VI14	)				
	Description:	Servers in VLAN	149			-	
	QoS Policy:	<pre>not set&gt;</pre>	-				
Netv	vork Control Policy:	CDP-En-LinkLoss	-				
	Max Ports:	0					
lock Mohuer	rk IO Derfermenser	C None C High	Performance				
IUSCINECIMU	rk to Performance:		renomiance				
	Pin Group:	<not set=""></not>	•				
Select		Name		Native VLAN			
	default	i ano		0			
	DC_Management			0			
	FW_Inside_1			0			
	FW_Inside_2			0			
	FW_Outside			<u> </u>			
	N1kv-Control			0			
	Servers_1			0			
	bervers_2						
	VDI_Clients			0			
	IDC01			0			
	MHOODIT			U			

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

📥 Create Profile Client 🛛				×
Create Profile	Client			0
Name:	Servers_2_VI	149		
Description:	Port Profile Cli	ent for D¥S ¥M	1-FEX-10k (in ¥LAN 149)	
Datacenter:	10k	-		
Folder:	VM-FEX	-		
Distributed Virtual Switch:	VM-FEX-10k	-		
,	D			

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 12 - Port profiles in Cisco UCS Manager

>> All > = Port Profiles		=	Port Profiles
Port Profiles Faults Events FSM			
🛨 🖃 🕰 Filter 🖨 Export 😓 Print			
Name	QoS Policy Name	MAC	E\$
Port Profile DC_Management			
Port Profile Management-Kernel			
Port Profile iSCSI			
Port Profile vMotion			

Figure 13 - 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.

Add Host to vSphere Distributed Switch					
Select Hosts and Physical Adapters Select hosts and physical adapters I	<b>s</b> to add to this vSphere distributed switch.				
Select Host and Physical Adapters			Settings	View Incompatible Hosts	
Network Connectivity	Host/Physical adapters	In use by switch	Settings	Uplink port group	
Virtual Machine Networking	🛨 🔲 📋 test-c220m3-1.cisco.lo		View Details		
Ready to Complete	🛨 🔲 📋 test-c220m3-2.cisco.lo		View Details		
	🖃 🗹 📋 test-chas1-s4.cisco.local		View Details		
	Select physical adapters				
	Vmnic0	vSwitch0	View Details	uplink-pg-VM-FEX-10k	
	Vmnic1	vSwitch0	View Details	uplink-pg-VM-FEX-10k	

• 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.

Add Host to vSphere Distributed S	witch			
Network Connectivity Select port group to provide netw	ork connectivity for the adapters o	n the vSphere distrit	outed switch.	
Select Host and Physical Adapters Network Connectivity Virtual Machine Networking	<ul> <li>Assign adapters to a destin</li> <li>Virtual NICs marked with th distributed switch. Select a</li> </ul>	ation port group to i e warning sign might destination port gro	nigrate them. Ctrl+click to multi-s lose network connectivity unless up in order to migrate them.	elect. they are migrated to the vSphere
Ready to Complete	Host/Virtual adapter	Switch	Source port group	Destination port group
	🖃 🚡 test-chas1-s4.cisco.lo	cal		
	vmk0	vSwitch0	Management Network	DC_Management 🗾
	1			

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

i

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.

🚰 Add Host to vSphere Distributed Sw	itch				_ 🗆 🗡
Virtual Machine Networking Select virtual machines or network	adapters to migrate to the vSphere distribu	ited switch.			
Select Host and Physical Adapters Network Connectivity Virtual Machine Networking Ready to Complete	Migrate virtual machine networking     Assign VMs or network adapters to a     Host/Virtual machine/Network adapter     Elect-chas1-s4.cisco.local     E    Est-cVMFEX-S1	a destination port NIC count   1	group to migrate them Source port group	. Ctrl+click to multi-select. Destination port group Servers_1_VI148	

• 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.

🛃 Add Host to vSphere Distributed Sw	itch		_	
Ready to Complete Verify the settings for the new vSp	here distributed switch.			
Select Host and Physical Adapters Network Connectivity Virtual Machine Networking Ready to Complete	VM-FEX-10k         © DC_Management         UMMernel Ports (1)         vmk0 : 10.4.63.99         Virtual Machines (0)         © deleted-pg-VM-FEX-10k         Virtual Machines (0)         © ISCSI         Virtual Machines (0)         © Servers_1_VI148         Uvitual Machines (1)         TEST-VMFEX-S1         © VMotion         Virtual Machines (0)	\$	Uplink-pg-VM-FEX-10k Uplink00 (1 NIC Adapter) Vmnic0 test-chas1-s4.cisco.local Uplink01 (1 NIC Adapter) Vmnic1 test-chas1-s4.cisco.local Uplink02 (0 NIC Adapters) New Port test-chas1-s4.cisco.local Uplink03 (0 NIC Adapters) New Port test-chas1-s4.cisco.local Uplink03 (0 NIC Adapters) New Port test-chas1-s4.cisco.local Uplink05 (0 NIC Adapters) New Port test-chas1-s4.cisco.local Uplink05 (0 NIC Adapters) New Port test-chas1-s4.cisco.local Uplink05 (0 NIC Adapters) New Port test-chas1-s4.cisco.local Uplink07 (0 NIC Adapters) New Port test-chas1-s4.cisco.local Uplink07 (0 NIC Adapters) New Port test-chas1-s4.cisco.local Uplink07 (0 NIC Adapters) New Port test-chas1-s4.cisco.local Uplink09 (0 NIC Adapters) New Port test-chas1-s4.cisco.local	
Help			< Back Finish Cance	

**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.

test-chas1-s4.cisco.local VMware ESXi, Getting Started Summary Virtual Mach	5.0.0, 623860   Evaluation (58 days remaining) ines Resource Allocation Performance <mark>Configuration</mark> Tasks & Events Alarms Permissions Maps	S Storage Views Hardware Status Update Manager
Hardware Processors Memory Storage	View: vsphere Standard Switch Vsphere Distributed Switch Networking	Refresh Properties
Networking     Stronge Adapters     Network Adapters     Advanced Settings     Power Management     Usensed Features     Time Configuration     OKS and Routing     Authentication Services     Power Management     Virtual Machine Sarapit Shutdown     Virtual Machine Sarapit Excention     Society Profile     Hest Cache Configuration     System Resource Adoction     System Resource Adoction     Agent VM Settings     Advanced Settings	View         Manage Virtual Adapters         Manage Virtual Machines (0)         Management         Management	loge Physical Adapters Properties

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.

🚰 TEST-VMFEX-S1 - Virtual N	Machine Properties	
Hardware Options Resource	S Profiles VServices	Virtual Machine Version: 8
Settings	Summary	Resource Allocation
CPU	0 MHz	
Memory	4096 MB (All locked)	Reserve all guest memory (All locked)
Disk	Normal	
Advanced CPU	HT Sharing: Any	Shares: Normal 40960 📼
Advanced Memory	NUMA Nodes: 2	Reservation: - 4096 🛱 MB
		Limit: 60968 📰 MB
		Limit based on parent resource pool or current host

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 the VM DirectPath I/O feature is active.

Tech Tip

i

For the Windows operating system virtual machine used in this example, the adapter type must be VMXNET 3 for DirectPath I/O (High Performance Operation). If you want to change the adapter type for the virtual machine, refer to Step 6 in the "Run the Add Network Wizard" procedure.

TEST-VMFEX-S1 - Virtual Machin	e Properties	
Hardware Options Resources Prof	iles vServices	Virtual Machine Version: 8
	Add Remove	Device Status
Hardware	Summary	Connect at power on
Memory CPUs Video card VMCI device SCSI controller 0 Hard disk 1 CD/DVD drive 1 Floppy drive 1 Network adapter 1	4096 MB 1 Video card Restricted LSI Logic SAS Virtual Disk [Openfiler(Software)] M Client Device Servers_1_VI148 (VM-F	Adapter Type Current adapter: VMXNET 3 MAC Address 00:50:56:94:4e:86 Automatic Manual DirectPath I/O Status: Active 1
		Network Connection Network label: Servers_1_VI148 (VM-FEX-10k) Port: 1564 Switch to advanced settings

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.

# 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(1.1a)
	Nexus 1000V VSM on Physical Media	N1K-VSMK9-404S12=	
VMware	ESXi	ESXi	5.0U2

## **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(3) 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	
	Cisco Nexus 5500 Layer 3 Enterprise Software License	N55-LAN1K9	
	Cisco Nexus 5500 Storage Protocols Services License, 8 ports	N55-8P-SSK9	
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)
	Cisco ASA 5585-X Security Plus IPS Edition SSP-20 and IPS SSP-20 bundle	ASA5585-S20P20X-K9	IPS 7.1(7) E4
	Cisco ASA 5585-X Security Plus IPS Edition SSP-10 and IPS SSP-10 bundle	ASA5585-S10P10XK9	

## **Storage Network Extension**

<b>Functional Area</b>	Product Description	Part Numbers	Software
Fibre-channel	Cisco MDS 9148 Multilayer Fibre Channel Switch	DS-C9148D-8G16P-K9	NX-OS 5.0(8)
Switch	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 96-port Fabric Interconnect	UCS-FI-6296UP	2.1(1b) Cisco UCS Release
	Cisco UCS up to 48-port Fabric Interconnect	UCS-FI-6248UP	
UCS B-Series Blade Servers	Cisco UCS Blade Server Chassis	N20-C6508	2.1(1b) 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 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	1.5.1f Cisco UCS CIMC Release
	Cisco UCS C240 M3 Rack Mount Server	UCSC-C240-M3S	
	Cisco UCS C460 M2 Rack Mount Server	UCSC-BASE-M2-C460	
	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
!Command: show running-config
version 4.2(1)SV2(1.1a)
svs switch edition essential
no feature telnet
feature tacacs+
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 "*****"
aaa group server tacacs+ tacacs
    server 10.4.48.15
    use-vrf management
    source-interface mgmt0
hostname N1kvVSM
errdisable recovery cause failed-port-state
vem 3
 host vmware id b4196721-282b-994b-87d9-9bb06fb24d0b
vem 4
 host vmware id 8575281e-91ad-11e2-00ff-000000001af
snmp-server user admin network-admin auth md5 *****
priv ***** localizedkey
snmp-server community cisco123 group network-admin
snmp-server community cisco group network-operator
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 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 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 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 V1148 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 vethernet n1kv-L3
  capability 13control
 vmware port-group
 switchport mode access
 switchport access vlan 163
  no shutdown
  system vlan 163
  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 System-Uplink
 vem 4
interface port-channel2
 inherit port-profile 10G CSeries
 vem 3
interface port-channel3
 inherit port-profile ESXi-Mgmnt-Uplink
 vem 3
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 "28 03 ... c6 5e 91"
  vmware vm mac 0025.B5FF.01DF
interface Vethernet2
  inherit port-profile n1kv-L3
  description VMware VMkernel, vmk0
  vmware dvport 129 dvswitch uuid "28 03 ... 5e 91"
  vmware vm mac C464.1339.22B0
interface Ethernet3/1
  inherit port-profile ESXi-Mgmnt-Uplink
interface Ethernet3/3
  inherit port-profile 10G CSeries
interface Ethernet3/4
  inherit port-profile 10G CSeries
interface Ethernet4/1
  inherit port-profile System-Uplink
interface Ethernet4/2
  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.SV2.1.1a.bin sup-1
boot system bootflash:/nexus-1000v.4.2.1.SV2.1.1a.bin sup-1
boot kickstart bootflash:/nexus-1000v-kickstart.4.2.1.SV2.1.1a.bin sup-2
boot system bootflash:/nexus-1000v.4.2.1.SV2.1.1a.bin sup-2
svs-domain
  domain id 12
  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 "28 03 ... 5e 91" 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
```

## Feedback

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

•1|1•1|1• CISCO

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.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2013 Cisco Systems, Inc. All rights reserved.

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

B-0000555-1 08/13