# Table of Contents

**Preface** ........................................................................................................................................1

**CVD Navigator** .............................................................................................................................2
  Use Cases ........................................................................................................................................ 2
  Scope ............................................................................................................................................... 2
  Proficiency ...................................................................................................................................... 3

**Introduction** .................................................................................................................................4
  Technology Use Cases .................................................................................................................... 4
    Use Case: Virtualize Server Hardware and Network Connectivity ............................................. 5
    Use Case: Centralize Server Configuration and Management ....................................................... 5
  Design Overview .............................................................................................................................. 5
    Application Growth ....................................................................................................................... 6
    Increasing Storage Requirements .................................................................................................. 6
    Managing Processing Resources ................................................................................................... 6
    Availability and Business Continuance .......................................................................................... 6
    Ethernet Foundation .................................................................................................................... 8
    Storage Networking ....................................................................................................................... 8
    Computing Systems ...................................................................................................................... 10
    Cisco Unified Computing System Components .......................................................................... 10
    Cisco UCS Manager ..................................................................................................................... 11
    Cisco UCS C-Series Rack-Mount Servers .................................................................................... 12
    Third-Party Computing Systems .................................................................................................. 13
    Server Virtualization and Cisco UCS ............................................................................................ 13

**Deployment Details** .................................................................................................................... 14
  Data Center Core Network Infrastructure ....................................................................................... 14
  Configuring the Ethernet Network Infrastructure ............................................................................. 15
  Configuring the Fibre Channel or FCoE Network Infrastructure ..................................................... 18
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS B-Series Blade Server System</td>
<td>23</td>
</tr>
<tr>
<td>Completing the Initial System Setup</td>
<td>24</td>
</tr>
<tr>
<td>Configuring Communications Connections Using UCS Manager</td>
<td>28</td>
</tr>
<tr>
<td>Configuring Common System Address Pools and VLANs</td>
<td>45</td>
</tr>
<tr>
<td>Configuring Virtual Adapter Templates</td>
<td>53</td>
</tr>
<tr>
<td>Configuring Server Boot Policy</td>
<td>57</td>
</tr>
<tr>
<td>Creating an Initial Boot Service Profile for Local Boot</td>
<td>64</td>
</tr>
<tr>
<td>Creating a Service Profile for SAN Boot</td>
<td>70</td>
</tr>
<tr>
<td>Creating Multiple Service Profiles through Templates</td>
<td>74</td>
</tr>
<tr>
<td>Cisco UCS C-Series Rack-Mount Server</td>
<td>77</td>
</tr>
<tr>
<td>Configuring Cisco Integrated Management Controller</td>
<td>78</td>
</tr>
<tr>
<td>Updating Firmware for Cisco UCS C-Series Server</td>
<td>80</td>
</tr>
<tr>
<td>Configuring LSI RAID</td>
<td>87</td>
</tr>
<tr>
<td>Configuring Ethernet and FCoE Connectivity</td>
<td>89</td>
</tr>
<tr>
<td>Integrating Cisco UCS C-Series into the Cisco UCS Manager Environment</td>
<td>94</td>
</tr>
<tr>
<td>Appendix A: Product List</td>
<td>102</td>
</tr>
<tr>
<td>Appendix B: Changes</td>
<td>103</td>
</tr>
</tbody>
</table>
Cisco Validated Designs (CVDs) present systems that are based on common use cases or engineering priorities. CVDs incorporate a broad set of technologies, features, and applications that address customer needs. Cisco engineers have comprehensively tested and documented each design in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested design 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 existing CVDs but also include product features and functionality across Cisco products and sometimes 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.

**CVD Foundation Series**

This CVD Foundation guide is a part of the August 2014 Series. As Cisco develops a CVD Foundation series, the guides themselves are tested together, in the same network lab. This approach assures that the guides in a series are fully compatible with one another. Each series describes a lab-validated, complete system.

The CVD Foundation series incorporates wired and wireless LAN, WAN, data center, security, and network management technologies. Using the CVD Foundation simplifies system integration, allowing you to select solutions that solve an organization’s problems—without worrying about the technical complexity.

To ensure the compatibility of designs in the CVD Foundation, you should use guides that belong to the same release. For the most recent CVD Foundation guides, please visit the CVD Foundation web site.

**Comments and Questions**

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

- **Virtualize Server Hardware and Network Connectivity**—Organizations can use virtualized resource pools of server hardware, network adapters, and storage in order to reduce the cost and time of deploying new applications.

- **Centralize Server Configuration and Management**—Application servers are often placed in a variety of locations, such as across racks in the data center and at remote sites. However, IT operations can be more efficient if server resources can be managed from a central location with a reduced set of tools.

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

Scope

This guide covers the following areas of technology and products:

- Configuration of the data center foundation Ethernet and storage network for connectivity to the Cisco UCS B-Series Blade Server system for high throughput and resilience

- Configuration of the Cisco UCS B-Series Blade Server system from the ground up to a point where the bare metal server is ready for an operating system or hypervisor installation

- Configuration and management of all elements of the Cisco UCS B-Series and C-Series servers with the Cisco Unified Computing System Manager

- Configuration and management of Cisco UCS Rack-Mount Servers with the integrated management controller for standalone applications

- Establishment of connectivity to Ethernet and storage resources with reduced cabling and complexity by using virtual network adapters

- Boot from SAN for stateless computing environments

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

Related CVD Guides

To view the related CVD guides, click the titles or visit the CVD Foundation web site.
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
Introduction

This Unified Computing System Design Guide builds upon the foundation laid out in the Data Center Technology Design Guide.

This guide includes the following modules:

- The first module explains how to program the foundation data center for connectivity to the Cisco UCS B-Series Blade Server system for maximum throughput and resiliency. This module covers Ethernet, Fibre Channel, and Fibre Channel over Ethernet connections between the UCS B-Series Blade Server system and the data center core network deployed in the Data Center Technology Design Guide.

- The Cisco UCS B-Series Blade Server system module shows how the system is programmed from the ground up to a point where the “bare metal” server is ready for an operating system or hypervisor software installation. This module shows how the Cisco Unified Computing System Manager (UCS Manager) is used to program all elements of the system—from connectivity to the data center core, to building profiles to assign the various aspects of the server boot, communications, and storage to the physical blade server hardware.

- The Cisco UCS C-Series Rack-Mount Server module shows how to use the Cisco Integrated Management Controller (CIMC) to remotely configure and prepare a server to a point where it is ready to load an operating system or hypervisor software. Similar to the Cisco UCS B-Series Blade Server system module, this section shows how to establish connectivity to the data center core to support Ethernet and Fibre Channel communications by using converged network adapters that add flexibility to server connectivity and reduce cabling and complexity. This module also includes guidance on managing the UCS C-Series server with the same Cisco UCS Manager that controls the B-Series servers for a single method of managing both server types.

- The appendices provide the complete list of products used in the lab testing of this architecture, as well as the software revisions used on the products.

Technology Use Cases

As an organization begins to grow, the number of servers required to handle the information-processing tasks of the organization grows as well. Using the full capabilities of the investment in server resources can help an organization add new applications while controlling costs as they move from a small server room environment to a more scalable data center design. Server virtualization has become a common approach to allow an organization to access the untapped processing capacity available in processor technology. Streamlining the management of server hardware and its interaction with networking and storage equipment is another important component of using this investment in an efficient manner.

Scaling a data center with conventional servers, networking equipment, and storage resources can pose a significant challenge to a growing organization. Multiple hardware platforms and technologies must be integrated to deliver the expected levels of performance and availability to application end users. These components in the data center also need to be managed and maintained, typically with a diverse set of management tools that have different interfaces and approaches. In larger organizations, often multiple teams of people are involved in managing applications, servers, storage, and networking. In many smaller organizations, the lines between these tasks are blurred, and often a single, smaller team—or even one individual—may need to handle many of these tasks in a day.
Use Case: Virtualize Server Hardware and Network Connectivity

Some applications require enough processing and memory that you need to dedicate an entire server to running them, while others benefit from hypervisors to optimize workloads and storage. The key is to optimize your server environment for both requirements.

This design guide enables the following data center capabilities:

- **Pooled resources for applications**—Create server profiles that define hardware and networking requirements, and then apply the profile to a physical server blade in order to create an operational server on-demand.

- **Simple access to network transport**—Configure blade server access to Ethernet and centralized storage at the system level during deployment, including addressing pools, in order to allow quick and easy allocation of new servers.

- **Reduced hardware requirements**—Virtual network adapters on servers can provide multiple Ethernet or SAN connections with a single adapter in order to reduce the number and type of physical adapters required on a server.

- **Boot from SAN for stateless computing**—By moving operating system and data files to the SAN combined with hardware independence of provisioning servers through service profiles, you can achieve stateless computing.

Use Case: Centralize Server Configuration and Management

Application servers for an organization are often placed in a variety of locations, posing an operational burden for IT management. The ability to centrally manage Cisco UCS servers located in a data center or a remote site can reduce the time and expense required to manage an organization’s server population.

This design guide enables the following application server capabilities:

- **Single management point for blade server systems**—Use the Cisco UCS Manager to provision all aspects of a Cisco UCS blade server system and scale up to twenty blade server chassis in a single domain.

- **Extend management to rack mount servers**—Connect blade server chassis and Cisco UCS rack mount servers in the data center to a common fabric and manage them with a common GUI, deployment method, and monitoring system.

- **Simple access to remote-site server console**—Using Cisco Integrated Management Console, manage remotely located rack mount servers from a browser interface.

Design Overview

Scaling a data center with conventional servers, networking equipment, and storage resources can pose a significant challenge to a growing organization. Multiple hardware platforms and technologies must be integrated in order to deliver the expected levels of performance and availability to application end users. These components in the data center also need to be managed and maintained, typically with a diverse set of management tools that have different interfaces and approaches. In larger organizations, often multiple teams of people are involved in managing applications, servers, storage, and networking. In many smaller organizations, the lines between these tasks are blurred, and often a single, smaller team—or even one individual—may need to handle many of these tasks in a day.

Business agility in the data center is a growing concern for organizations. The ability to reduce the time necessary to deploy new applications or expand existing applications to a larger footprint to handle increasing workloads contributes to the success of a project. The compute environment needs to be consistent in order to reduce operational requirements, yet flexible enough to accommodate the different requirements of applications and the operating system.
This guide addresses many of the data center issues encountered by growing organizations with respect to server resources and their interaction with network and storage systems.

**Application Growth**

The Cisco Unified Computing System model provides for using a simple GUI for rapid deployment of additional physical servers that share common attributes. Using the Cisco UCS Manager service profiles, you can define the “personality” of an individual server—including boot characteristics, interface addresses, and even firmware versions—separately from any physical hardware. You can also generate service profiles from a template and keep them linked to the template to facilitate updates across multiple servers in the future. This gives you the ability to create a new server by cloning an existing service profile or using a template. It also means that it only takes a few minutes to deploy a new server, and you can limit physical server hardware to a flexible and common pool of spare parts as your data center grows.

**Increasing Storage Requirements**

The most efficient way to manage the investment in additional storage capacity is to move to a centralized storage model. The Cisco Unified Computing System model decouples the computing functions of the server farm from the storage systems, which provides greater flexibility for system growth and migration. System storage and boot disk are accessible from either the local disk that is available on each server or through access to centralized storage located on the Ethernet IP network or Fibre Channel or Fibre Channel over Ethernet storage area network (SAN).

**Managing Processing Resources**

Some applications require enough processing and memory that you might decide to dedicate an entire server or even a cluster of servers to support the workload. Other applications may start out on a single server where the processor and memory are underutilized, resulting in excess or wasted resources. In the case where applications need a separate operating environment but not an entire server for processing and memory resources, server virtualization is the key to combining applications and optimizing resources. Server virtualization technologies insert a hypervisor layer between the server operating systems and the hardware, allowing a single physical server to run multiple instances of different “guest” operating systems such as Microsoft Windows or Linux. This increases the utilization of the processors on the physical servers, which helps to optimize this costly resource.

The architecture of the Cisco Unified Computing System model is optimized to support the use of hypervisor-based systems or the direct installation of a base operating system such as Windows or Linux. The service profile structure of Cisco UCS, along with a centralized storage model, allows you the portability of server definitions to different hardware with or without a hypervisor system in place. The Cisco Unified Computing System model provides scalable connectivity options for not only Cisco UCS Series 5100 Blade Server Chassis but also Cisco UCS C-Series Rack-Mount Servers, as well as connectivity options to support third-party servers.

**Availability and Business Continuance**

The CVD data center foundation has been designed to ensure availability with the use of resilient network devices, links, and service models. The Cisco Unified Computing System model extends this resiliency to the servers themselves through the capabilities of Cisco Unified Computing System.

Cisco Unified Computing System uses service profiles to provide a consistent interface for managing all server resource requirements as a logical entity, independent of the specific hardware module that is used to provide the processing capacity. This service profile approach is applied consistently on both virtualized servers and “bare metal” servers, which do not run a hypervisor.
This capability allows the entire personality of a given logical server to be ported easily to a different physical server module independent of any virtualization software when LAN or SAN boot are in use. This approach increases overall availability and dramatically reduces the time required to replace the function of an individual server module that has failed.

*Figure 1 - Cisco Unified Computing System CVD architecture*
This architecture is designed to allow your existing server farm to migrate into a scalable Ethernet and storage transport based on the CVD reference design. Figure 1 shows the data center components of this architecture and their interaction with the headquarters LAN core.

**Ethernet Foundation**

The *Unified Computing System Design Guide* is designed as an extension of the *Data Center Technology Design Guide*. The basis of the Cisco Unified Computing System architecture is an Ethernet switch fabric that consists of two Cisco Nexus 5500UP switches, as shown in Figure 1. This data center switching fabric provides Layer 2 and Layer 3 Ethernet switching services to attached devices and, in turn, communicates with the LAN Ethernet core by using redundant Layer 3 links.

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 Spanning Tree Protocol, which is a standard component of Layer-2 bridging, does not need to block any of the links in the topology to prevent bridging loops. Additional Gigabit Ethernet and 10-Gigabit Ethernet switch port density may be added to the switch fabric by using Cisco Nexus 2000 Series Fabric Extenders. The vPC and fabric extender technologies provide the flexibility for extending VLANs across the data center for a resilient, virtualized computing environment.

**Storage Networking**

The Cisco Unified Computing System model is also adaptable to multiple ways of accessing centralized storage. Two alternatives for storage access are included in the overall architecture. One approach uses a pure Ethernet IP network to connect the servers to both their user community and the shared storage array. Communication between the servers and storage over IP can be accomplished by using an Internet Small Computer System Interface (iSCSI), which is a block-oriented protocol encapsulated over IP, or traditional network-attached storage (NAS) protocols such as Common Internet File System (CIFS) or network file server (NFS). LAN-based storage access follows the path through the Cisco Nexus 5500 Series Switching Fabric shown in Figure 1.

A more traditional but advanced alternative for providing shared storage access is using a Fibre Channel SAN built using the data center core Cisco Nexus 5500UP switches or the Cisco MDS 9100 Series for larger SAN environments. Fibre Channel over Ethernet (FCoE) builds on the lossless Ethernet infrastructure to provide a converged network infrastructure. For resilient access, SANs are normally built with two distinct fabric switches that are not cross-connected. Currently, Fibre Channel offers the widest support for various disk-array platforms and also support for boot-from-SAN.

The Cisco UCS 6200 Series Fabric Interconnects also maintain separate Fibre Channel fabrics, so each fabric is attached to one of the data center core switches running either SAN A or SAN B as shown in Figure 2. When Fibre Channel is used for storage access from Cisco UCS B-Series Blade Servers, the system provides virtual host bus adapters (vHBAs) to the service profiles to be presented to the host operating system. The Cisco UCS fabric interconnect can now connect to the data center core switches with FCoE uplinks as of Cisco UCS Manager release 2.1(1a). This guide will show how you can use Fibre Channel or FCoE uplinks from the Cisco UCS fabric interconnect to the data center core switches.
On the Cisco UCS fabric interconnect, the Fibre Channel ports that connect to the data center core SAN operate in N-port Virtualization mode. All Fibre Channel switching happens upstream at the data center core switches running N-Port Identifier Virtualization (NPIV). NPIV allows multiple Fibre Channel port IDs to share a common physical port. Though there are multiple Fibre Channel ports on the fabric interconnects, local Fibre Channel switching between these ports is not covered in this guide.

You can connect the Cisco UCS C-Series Rack-Mount Servers to the Fibre Channel SAN by using dedicated host bus adapters (HBAs) that attach directly to the SAN switches. Alternatively, you can use a converged network adapter, which allows Ethernet data and Fibre Channel over Ethernet (FCoE) storage traffic to share the same physical set of cabling. This Unified Wire approach allows these servers to connect directly to the Cisco Nexus 5500UP Series switches or a Cisco Nexus Fabric Extender for data traffic, as well as SAN A and SAN B highly available storage access, shown in Figure 3. The Cisco Nexus 5500UP switch fabric is responsible for splitting FCoE traffic off to the Fibre Channel attached storage array. Many storage arrays now include FCoE connectivity as an option and can be directly connected to the data center core.

Figure 2 - Cisco UCS 6200 fabric interconnect to SAN core

Figure 3 - Cisco UCS C-Series server to SAN core using FCoE
Many available shared storage systems offer multi-protocol access to the system, including iSCSI, Fibre Channel, FCoE, CIFS, and NFS. Multiple methods can be combined on the same storage system to meet the access requirements of a variety of server implementations. This flexibility also helps facilitate migration from legacy third-party server implementations onto Cisco UCS.

Computing Systems

The primary computing platforms targeted for the Cisco Unified Computing System reference architecture are Cisco UCS B-Series Blade Servers and Cisco UCS C-Series Rack-Mount Servers.

The Cisco UCS 5100 Series Blade Server Chassis is a blade-server style enclosure supporting compact, slide-in server modules, but architecturally it is a significantly different approach from traditional blade-server systems on the market. Most blade server systems essentially take the components that would have been in a standalone data center rack, such as a number of standardized rack-mount servers with a pair of redundant top-of-rack switches, and attempt to condense them into a single sheet-metal box. Some of these implementations even include localized storage arrays within the chassis. That approach achieves higher system density but retains most of the complexity of traditional rack systems in a smaller form factor. Also, the number of management interfaces and switching devices multiplies with each new chassis.

By extending a single low-latency network fabric directly into multiple enclosures, Cisco has removed the management complexity and cable-management issues associated with blade switching or pass-through module implementations common to blade servers. By consolidating storage traffic along the same fabric using lossless FCoE technology, Cisco UCS even further simplifies the topology by using the fabric interconnects as a common aggregation point for Ethernet data traffic and storage-specific Fibre Channel traffic. On top of this vastly simplified physical architecture, Cisco UCS Manager extends a single management interface across the physical blade servers and all of their associated data and storage networking requirements. The Cisco UCS Manager can also extend the single management interface to Cisco UCS C-Series servers when those servers are interconnected to the UCS Fabric Interconnects.

Cisco Unified Computing System Components

The Cisco Unified Computing System has a unique architecture that integrates compute, data network access, and storage network access into a common set of components under a single-pane-of-glass management interface. The primary components included within this architecture are as follows:

- **Cisco UCS Fabric Interconnect**—The Cisco UCS 6200 Series fabric interconnects provide both network connectivity and management capabilities to the other components in the system. It is recommended that the fabric interconnects are clustered together as a pair, providing resilient management access—as well as 10-Gb Ethernet, Fibre Channel, and FCoE capabilities—to the system. The Cisco UCS 6200 fabric interconnect provides the flexibility of unified ports, enabling a port to run Ethernet or Fibre Channel.

- **Cisco UCS Fabric Extender**—The Cisco UCS 2200 Series Fabric Extenders, also referred to as I/O modules, are installed directly within the Cisco UCS 5100 Series Blade Server Chassis enclosure. These modules logically extend the fabric from the fabric interconnects into each of the enclosures for Ethernet, FCoE, and management purposes. The fabric extenders simplify cabling requirements from the blade servers installed within the system chassis.

- **Cisco UCS 5100 Series Blade Server Chassis**—The Cisco UCS 5100 Series Blade Server Chassis provides an enclosure to house up to eight half-width or four full-width blade servers, their associated fabric extenders, and four power supplies for system resiliency.

Tech Tip

As of Cisco UCS release 2.1(1), a single pair of fabric interconnects may connect to and manage up to twenty Cisco UCS 5100 Series Blade Server Chassis.
Cisco UCS B-Series Blade Servers—Cisco B-Series Blade Servers implement Intel Xeon Series processors and are available in both a half-width or full-width format. The Cisco UCS B22, B200, and B230 blade servers require a half-slot within the enclosure, providing high-density, high-performance computing resources in an easily managed system. The Cisco UCS B250, B420, and B440 blade servers require a full slot and offer extended memory, increased processing power, increased local storage, and higher I/O throughput.

Cisco UCS B-Series Network Adapters—The Cisco UCS B-Series Blade Servers accept a variety of mezzanine adapter cards that allow the switching fabric to provide multiple interfaces to a server. These adapter cards fall into three categories:

- **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 can present up to two 10-Gigabit Ethernet interfaces to a server, along with two Fibre Channel interfaces.

- **Virtual interface cards**—The Cisco virtual interface cards (VICs) feature new technology from Cisco, allowing additional network interfaces to be dynamically presented to the server. This adapter supports Cisco VN-Link technology in hardware, which allows each virtual adapter to appear as a separate virtual interface on the fabric interconnects. The architecture of the VIC is capable of supporting up to 256 total virtual interfaces split between virtual network interface cards (vNICs) and vHBAs. The number of virtual interfaces currently supported depends on the UCS infrastructure, including the fabric interconnect, I/O module, VIC model, and version of Cisco UCS Manager.

**Cisco UCS Manager**

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

The Cisco UCS Manager GUI provides role-based access control (RBAC) to allow multiple levels of users granular administrative rights to system objects. Users can be restricted to certain portions of the system based on locale, which corresponds to an optional organizational structure that can be created within the system. Users can also be classified based on their access levels or areas of expertise, such as “Storage Administrator,” “Server Equipment Administrator,” or “Read-Only”. RBAC allows the comprehensive capabilities of the Cisco UCS Manager GUI to be properly shared across multiple individuals or teams within your organization in a flexible, secure manner.

Cisco UCS Manager provides unified, embedded management of all software and hardware components. Every instance of Cisco UCS Manager and all of the components managed by it form a domain. For organizations that deploy multiple Cisco UCS domains, Cisco UCS Central software provides a centralized user interface that allows you to manage multiple, globally distributed Cisco UCS domains with thousands of servers. Cisco UCS Central integrates with Cisco UCS Manager and utilizes it to provide global configuration capabilities for pools, policies, and firmware.
Cisco UCS C-Series Rack-Mount Servers

Cisco UCS C-Series servers extend Cisco Unified Computing System innovations and benefits to the rack-mount server form factor. 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 office requirements, or they can be used as an approach to deploy rack-mounted servers on an incremental basis. The Cisco UCS C-Series servers also implement Intel Xeon processor technology and are available in multiple models with options for processing power, local storage size, and I/O throughput requirements. They offer Cisco innovations such as extended memory and network-aware VN-Link technologies.

The Cisco Integrated Management Controller (CIMC) is the management service for Cisco 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 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 perform the following server management tasks, including (but not limited to):

- Power on, power off, power cycle, reset, and shut down the server
- Configure the server boot order
- View server properties and sensors
- Configure network-related settings, including network interface card (NIC) properties and network security
- Configure communication services, including HTTP, SSH, SNMP, and Intelligent Platform Management Interface (IPMI) over LAN
- Update CIMC firmware
- Monitor faults, alarms, and server status

The Cisco UCS C-Series servers can be managed by the Cisco UCS Manager if they are deployed connected to the fabric interconnects via Cisco 2232PP fabric extenders as shown in Figure 4. This type of deployment enables the flexibility of both rack-mounted and blade servers with a single-pane-of-glass management of all Cisco UCS servers in the data center. The newer Cisco UCS C-Series M3 model servers can be managed with a single wire connected to the Cisco 2232PP fabric extenders when the server is using the new Cisco UCS VIC 1225 virtual interface card.
Third-Party Computing Systems

Third-party rack server and blade server systems may also be connected to the data center topology with the available 10-Gigabit Ethernet interfaces on the Cisco Nexus 5500 Series switches, or interfaces on the Cisco Nexus 2000 Series Fabric Extenders that support Gigabit Ethernet and 10-Gigabit Ethernet connectivity, depending on the model selected. To support existing applications and facilitate smooth migration to servers that support the Cisco Unified Computing System features, you can easily integrate a previously installed base of running servers into the data center architecture.

Server Virtualization and Cisco UCS

Server virtualization technologies allow a single physical server to run multiple virtual instances of a guest operating system, creating virtual machines. Running multiple virtual machines on server hardware helps to increase processor utilization levels, while still allowing each virtual machine to be viewed as independent from a security, configuration, and troubleshooting perspective.

Cisco Unified Computing System server platforms provide unique advantages that complement the implementation of server virtualization technologies. The Cisco UCS servers with Cisco UCS Manager allow the personality of a server instance to be easily ported to different physical hardware, similar to porting a virtual machine to a different host. Cisco UCS Manager provides the capability to directly integrate network interfaces to the hypervisor system for dynamic network interface allocation to virtual machines. This is currently supported with VMware ESX 4.0 Update 1 and above. Cisco Extended Memory Technology allows individual servers to scale to large numbers of virtual machines, reducing support and licensing costs.

Cisco UCS servers have been certified with multiple hypervisor systems, including VMware ESX, Microsoft Hyper-V, and Citrix Xen. Please contact your Cisco Systems or authorized partner sales representative to verify the specifics of your implementation requirements with current hardware and software versions.
How to Read Commands

This guide uses the following conventions for commands that you enter at the command-line interface (CLI).

Commands to enter at a CLI prompt:
configure terminal

Commands that specify a value for a variable:
ntp server 10.10.48.17

Commands with variables that you must define:
class-map [highest class name]

Commands at a CLI or script prompt:
Router# enable

Long commands that line wrap are underlined. Enter them as one command:
police rate 10000 pps burst 10000 packets conform-action

Noteworthy parts of system output (or of device configuration files) are highlighted:
interface Vlan64
ip address 10.5.204.5 255.255.255.0

The following sections provide detailed, step-by-step instructions to configure the basic elements of the Cisco Unified Computing System model. If you are a new user, you can use these common best-practice configurations to quickly configure a new system for basic operations. This is a flexible configuration, so additional information is provided, including pointers to more detailed documentation that you can use for more advanced system configurations.

Data Center Core Network Infrastructure

The foundation data center core network infrastructure for the Cisco Unified Computing System topology is based on the Data Center Technology Design Guide. The following Ethernet, Fibre Channel, and FCoE network setup processes prepare the data center core for connecting to a Cisco UCS B-Series Blade Server system.

Cisco UCS C-Series Rack-Mount Servers may be connected to the data center infrastructure, using available interfaces on the Cisco Nexus 5500UP switches or through the Cisco Nexus 2000 Series Fabric Extenders. You can configure switching access or trunk port modes according to the settings appropriate for the installed operating system. The Cisco UCS C-Series servers may also be connected to the fabric interconnects that provide connectivity for the Cisco UCS B-Series servers for a single control point provided by Cisco UCS Manager.
Configuring the Ethernet Network Infrastructure

1. Configure Nexus 5500 port channels

The Cisco UCS B-Series Blade Servers and Cisco UCS 5100 Series Blade Server Chassis operate in conjunction with the Cisco UCS 6200 Series Fabric Interconnects to appear as a group of end-node servers to the data center Ethernet switching fabric. In the Cisco Unified Computing System architecture, the fabric interconnects for Ethernet traffic are connected directly to the Cisco Nexus 5500UP Series Ethernet switching fabric running vPC for the best combination of throughput and resiliency.

Configuration examples in this guide show the use of a port channel with four physical 10-Gigabit Ethernet ports from each Cisco UCS Fabric Interconnect to the Cisco Nexus 5500 vPC pair. These interfaces are numbered Ethernet 1/9 through 1/12 on each Cisco Nexus 5500 Series switch, and ports 17 through 20 on each fabric interconnect in the example configurations. The port channel from each fabric interconnect spans the two physical Cisco Nexus 5500 switches for resilient connectivity, as shown in the figure below. You can use interface numbers specific to your implementation to achieve the same cabling structure.

Figure 5 – Data center core to fabric interconnect Ethernet cabling

This illustration shows the use of integrated ports on the Cisco UCS fabric interconnects in the validation network for Ethernet uplink connections. Expansion module Ethernet ports may also be used as uplink ports.
Procedure 1  Configure Nexus 5500 port channels

Step 1: Ensure that the LACP feature is enabled for EtherChannel operation.

feature lacp

Step 2: Configure the physical interfaces to the port channels on the data center core Cisco Nexus 5500UP-A switch.

interface Ethernet1/9
    description Link to FI-A eth1/17
    channel-group 50 mode active
    no shutdown

interface Ethernet1/10
    description Link to FI-A eth1/18
    channel-group 50 mode active
    no shutdown

interface Ethernet1/11
    description Link to FI-B eth1/17
    channel-group 51 mode active
    no shutdown

interface Ethernet1/12
    description Link to FI-B eth1/18
    channel-group 51 mode active
    no shutdown

When you assign the channel group to a physical interface, the switch’s operating system creates the logical EtherChannel (port-channel) interface. Next, you configure the logical port-channel interfaces, and the physical interfaces tied to the port channel will inherit the settings.

Step 3: Configure the port channels on the data center core Cisco Nexus 5500UP-A switch.

The port channels are created as vPC port channels, because the fabric interconnects are dual-homed EtherChannels to both data center core switches.

interface port-channel50
    switchport mode trunk
    switchport trunk allowed vlan 148-163
    spanning-tree port type edge trunk
    service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
    vpc 50

interface port-channel51
    switchport mode trunk
    switchport trunk allowed vlan 148-163
    spanning-tree port type edge trunk
    service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
    vpc 51
Tech Tip

Setting the spanning-tree port type to "edge trunk" is appropriate for the recommended default fabric interconnect configuration of End Host Mode. If the fabric interconnect is configured in switched mode, leave the Cisco Nexus 5500 port type set to "normal" for standard Spanning Tree Protocol loop prevention.

The port-channel interfaces do not become active until you complete the corresponding configuration on the Cisco UCS fabric interconnects, which is covered in Procedure 2, “Define Ethernet uplink ports.”

Step 4: Configure the physical interfaces for the port channels, and the port channels on data center core Cisco Nexus 5500UP-B switch.

```plaintext
interface Ethernet1/9
    description Link to FI-A eth1/19
    channel-group 50 mode active
    no shutdown
!
interface Ethernet1/10
    description Link to FI-A eth1/20
    channel-group 50 mode active
    no shutdown
!
interface Ethernet1/11
    description Link to FI-B eth1/19
    channel-group 51 mode active
    no shutdown
!
interface Ethernet1/12
    description Link to FI-B eth1/20
    channel-group 51 mode active
    no shutdown
!
interface port-channel50
    switchport mode trunk
    switchport trunk allowed vlan 148-163
    spanning-tree port type edge trunk
    service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
    vpc 50
!
interface port-channel51
    switchport mode trunk
    switchport trunk allowed vlan 148-163
    spanning-tree port type edge trunk
    service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
    vpc 51
```
Configuring the Fibre Channel or FCoE Network Infrastructure

1. Configure SAN port channels

If you will access all of your storage strictly over Ethernet by using iSCSI or NAS protocols, it is not necessary to define or attach Fibre Channel uplinks; you can skip this process.

Complete the following process to prepare the data center core Cisco Nexus 5500UP switches to support a Fibre Channel or FCoE SAN connection to the Cisco UCS Fabric Interconnects. As of Cisco UCS Release 2.1(1a), the Cisco UCS 6200 Series Fabric Interconnects support either a Fibre Channel or FCoE SAN connection to the data center core switching fabric. Configuration instructions and Fibre Channel SAN numbering provided in this guide are based on the foundation of the Fibre Channel infrastructure in the Data Center Technology Design Guide topology.

**Table 1 - Fibre Channel VSAN to FCoE VLAN mapping**

<table>
<thead>
<tr>
<th>Data center core switch</th>
<th>VSAN</th>
<th>FCoE VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Nexus 5500UP-A</td>
<td>4</td>
<td>304</td>
</tr>
<tr>
<td>Cisco Nexus 5500UP-B</td>
<td>5</td>
<td>305</td>
</tr>
</tbody>
</table>

The following procedure options provide guidance for Fibre Channel (FC) or FCoE connectivity from the data center core to the Cisco UCS Fabric Interconnect. Both procedures configure the SAN extension for operation where the Cisco UCS Fabric Interconnects are operating in the default SAN FC and Ethernet LAN switching End-Host mode.

**Procedure 1** Configure SAN port channels

If you want to use native Fibre Channel to extend the SAN from the data center core to the Cisco UCS Fabric Interconnect, complete Option 1. If you want to use FCoE to extend the SAN from the data center core to the Cisco UCS Fabric Interconnect, complete Option 2.

**Option 1: Configure Fibre Channel SAN port channels**

*Figure 6 - Fibre Channel connection between the data center core and fabric interconnects*
To prepare the data center core Cisco Nexus 5500UP switches for Fibre Channel connectivity to the fabric interconnect, you must enable NPIV. This may have already been done during programming according to the Data Center Technology Design Guide.

**Step 1:** On the data center core Cisco Nexus 5500UP-A switch, enable NPIV, Fibre Channel port channel trunking, and Fibre Channel or FCoE switching operation.

```bash
feature npiv
feature fport-channel-trunk
feature fcoe
```

The `feature fcoe` command is required to enable both Fibre Channel and FCoE on the Cisco Nexus 5500UP switches.

**Step 2:** Create a SAN port channel to connect the fabric interconnect to the data center core Cisco Nexus 5500UP-A switch.

With NPIV enabled, you must assign a virtual SAN (VSAN) to the SAN port channels that connect to the fabric interconnects. You use the same VSAN numbering established in the Data Center Technology Design Guide.

```bash
interface san-port-channel 29
  channel mode active
  switchport trunk mode on
  switchport trunk allowed vsan 1
  switchport trunk allowed vsan add 4
```

**Step 3:** Add the SAN port channel to an existing VSAN database on the data center core Cisco Nexus 5500UP-A switch.

```bash
vsan database
  vsan 4 interface san-port-channel 29
```

**Step 4:** On the data center core Cisco Nexus 5500UP-A switch, configure the SAN port channel on physical interfaces.

The Fibre Channel ports on the Cisco Nexus 5500UP switches are set to negotiate speed by default.

```bash
interface fc1/29
  switchport trunk mode on
  channel-group 29 force

interface fc1/30
  switchport trunk mode on
  channel-group 29 force
```

**Step 5:** Apply the following configuration to the data center core Cisco Nexus 5500UP-B switch. Note the different VSAN number value used for the Cisco Nexus 5500UP-B switch.

```bash
feature npiv
feature fport-channel-trunk
feature fcoe

interface san-port-channel 29
  channel mode active
  switchport trunk mode on
```
switchport trunk allowed vsan 1
switchport trunk allowed vsan add 5
!
vsan database
  vsan 5 interface san-port-channel 29
!
interface fc1/29
  switchport trunk mode on
  channel-group 29 force
!
interface fc1/30
  switchport trunk mode on
  channel-group 29 force

**Tech Tip**

The Fibre Channel SAN port channel interfaces configured in these steps will not show a status of “up” until you complete the upcoming configuration of the fabric interconnects for Fibre Channel operation in Procedure 3, “Configure SAN uplinks” in the “Configuring Communications Connections Using UCS Manager” process.

**Option 2: Configure FCoE SAN port channels**

If you want to use FCoE in order to extend the SAN from the data center core to the Cisco UCS Fabric Interconnect, use this procedure. The EtherChannel links for FCoE are different than the EtherChannel links for only Ethernet traffic, created in the previous “Configuring the Ethernet Network Infrastructure” process.

*Figure 7 - FCoE connection between the data center core and fabric interconnects*

If you have already configured your Cisco Nexus 5500UP switches for FCoE operation by following the “Configuring the Data Center Core” procedure in the Data Center Technology Design Guide, you may skip to Step 5.
Step 1: On the data center core Cisco Nexus 5500UP-A switch, enable NPIV and Fibre Channel or FCoE switching operation, and then ensure that LACP is enabled.

```plaintext
feature lacp
feature npiv
feature fcoe
```

The `feature fcoe` command is required to enable both Fibre Channel and FCoE on the Cisco Nexus 5500UP switches.

Step 2: If you have not already configured your Cisco Nexus 5500UP switches for QoS by following the Configuring the Data Center Core procedure in the Data Center Technology Design Guide, you must enable quality of service (QoS) for FCoE operation on the Cisco Nexus 5500UP.

Four lines of QoS statements map the baseline system QoS policies for FCoE. Without these commands, the virtual FC interface will not function when activated. If you followed the Data Center Technology Design Guide to deploy your network, you should have already executed a more comprehensive QoS policy, which includes FCoE traffic classification, so you can skip this step. If you use the commands below for the baseline FCoE QoS operation, you will overwrite your existing QoS policy.

```plaintext
system qos
service-policy type qos input fcoe-default-in-policy
service-policy type queuing input fcoe-default-in-policy
service-policy type queuing output fcoe-default-out-policy
service-policy type network-qos fcoe-default-nq-policy
end
```

Tech Tip

All FC and FCoE control and data traffic is automatically classified into the FCoE system class, which provides a no-drop service. On the Cisco Nexus 5010 and Cisco Nexus 5020, this class is created automatically when the system starts up. The class is named class-fcoe in the CLI.

Step 3: On the data center core Cisco Nexus 5500UP-A switch, ensure that an FCoE VLAN has been created. This VLAN that will carry FCoE traffic to the fabric interconnects.

```plaintext
vlan 304
    name FCoE-VLAN_304
exit
```

Step 4: On the data center core Cisco Nexus 5500UP-A switch, ensure that VSAN 4 has been created and map VLAN 304 to VSAN 4. VLAN 304 carries all VSAN 4 traffic over the trunk.

```plaintext
vsan database
    vsan 4
    vsan 4 name General-Storage
exit
!
vlan 304
    fcoe vsan 4
exit
```
**Step 5:** Configure a new port channel on the physical interfaces on the Cisco Nexus 5500UP-A switch, connecting FCoE transport to the fabric interconnects. Cisco Nexus Operating System automatically creates the port channel associated with the channel group.

```plaintext
interface ethernet 2/1
  description FCoE Link to FI-A eth1/33
  channel-group 33 mode active
  no shutdown

interface ethernet 2/2
  description FCoE Link to FI-A eth1/34
  channel-group 33 mode active
  no shutdown
```

**Step 6:** Configure the port channel created by the previous step to trunk, and allow the FCoE VLAN (304).

```plaintext
interface port-channel 33
  description FCoE EtherChannel Link to FI-A
  switchport mode trunk
  switchport trunk allowed vlan 304
  spanning-tree port type edge trunk
```

> **Caution**

In order to prevent spanning tree loops, only use `spanning-tree port type edge trunk` when the Cisco UCS Fabric Interconnects are operating in the default Ethernet LAN switching End-Host mode.

**Step 7:** On the data center core Cisco Nexus 5500UP-A switch, create a virtual Fibre Channel (vfc) interface, bind it to the port channel created in the previous step, and then configure the interface to trunk VSAN 4.

```plaintext
interface vfc 33
  bind interface port-channel 33
  switchport trunk allowed vsan 4
  switchport mode F
  no shutdown
```

**Step 8:** Apply the following configuration to the data center core Cisco Nexus 5500UP-B switch, and ensure that QoS is enabled for FCoE operation as done in Step 2 above. Note the different VSAN number value used for the Cisco Nexus 5500UP-B switch.

```plaintext
feature lacp
feature npiv
feature fcoe

vlan 305
  name FCoE-VLAN_305
  exit
  !
vsan database
vsan 5
vsan 5 name General-Storage
exit
!
vlan 305
cfcoe vsan 5
exit
!
interface ethernet 2/1
description FCoE Link to FI-B eth1/33
channel-group 33 mode active
no shutdown
!
interface ethernet 2/2
description FCoE Link to FI-B eth1/34
channel-group 33 mode active
no shutdown
!
interface port-channel 33
description FCoE EtherChannel Link to FI-B
switchport mode trunk
switchport trunk allowed vlan 305
spanning-tree port type edge trunk
!
interface vfc 33
bind interface port-channel 33
switchport trunk allowed vsan 5
switchport mode F
no shutdown

Cisco UCS B-Series Blade Server System
The Cisco UCS B-Series Blade Server system is the heart of the Cisco Unified Computing System architecture. This section provides information on initial system setup and basic service profile configuration to prepare your first running server to boot on one of the blade server modules. Additional information is provided for setting up service profiles with multiple interfaces and boot-from-SAN configurations.
Completing the Initial System Setup

1. Complete cabling and ensure connectivity
2. Configure management switch ports
3. Complete initial fabric interconnect setup

**Procedure 1**  
Complete cabling and ensure connectivity

The Cisco UCS fabric interconnects act as the concentration point for all cabling to and from the UCS 5100 Series Blade Server Chassis.

**Step 1:** Connect the two fabric interconnects together using the integrated ports labeled L1/L2. These ports are used for replication of cluster information between the two fabric interconnects, not the forwarding of data traffic.

**Step 2:** Attach the management Ethernet ports from each fabric interconnect to the out-of-band Ethernet management network created in the *Data Center Technology Design Guide* (or appropriate Ethernet segment) where they can be accessed for overall administration of the system.

**Step 3:** Populate each blade chassis with two fabric extenders (*I/O modules*) to provide connectivity back to the fabric interconnects.

**Step 4:** From the Cisco UCS 5100 Blade Server Chassis, connect one I/O module to the first fabric interconnect. Connect the second I/O module to the second fabric interconnect. After you have configured the fabric interconnects, they will be designated as “A” and “B” fabric interconnects.

You can connect the I/O modules to the fabric interconnects by using one, two, four, or eight cables per module. For system resiliency and throughput, it is recommended that you use a minimum of two connections per I/O module.
Ports 1 through 4 on the fabric interconnects are shown as an example. Additional blade chassis may be connected via their integrated I/O modules into any of the baseboard ports on the fabric interconnect. It is recommended that for maximum virtual NIC scalability, connect the I/O module to the fabric interconnect with all I/O module ports included in a group of 8 fabric interconnect ports; that is all I/O module ports connect to fabric interconnect ports 1-8, or 9-16, or 17-24, etc.

**Procedure 2 Configure management switch ports**

In the Data Center Technology Design Guide, an Ethernet out-of-band management network was created. The management ports for the Cisco UCS fabric interconnects should connect to this switch and use IP addressing from the management VLAN. The ports on the management switch should be configured for connecting to the fabric interconnect management ports, as described in this procedure.

**Step 1:** Configure the ports connected to Cisco UCS.

```bash
interface GigabitEthernet1/0/7
switchport access vlan 163
switchport mode access
!
interface GigabitEthernet1/0/8
switchport access vlan 163
switchport mode access
```

With this configuration, when both the fabric interconnects are up and configured with the management IP addresses, they are able to ping the Cisco Nexus 5500 switches.

**Procedure 3 Complete initial fabric interconnect setup**

You can easily accomplish the initial configuration of the fabric interconnects through the Basic System Configuration dialog that launches when you power on a new or unconfigured fabric interconnect.

**Tech Tip**

This guide assumes you are configuring a new or unconfigured unit. If you want to erase the configuration of a Cisco UCS Fabric Interconnect, access the local management CLI and use the erase configuration command:

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# erase configuration
```

**Step 1:** Connect a terminal to the console port of the first fabric interconnect to be configured, and then press Enter.
**Step 2:** In the Basic System Configuration Dialog, enter information as shown below, and then establish a password for the admin account.

```
---- Basic System Configuration Dialog ----
This setup utility will guide you through the basic configuration of the system.
Only minimal configuration including IP connectivity to the Fabric interconnect
and its clustering mode is performed through these steps.
Type Ctrl-C at any time to abort configuration and reboot system. To back track
or make modifications to already entered values, complete input till end of
section and answer no when prompted to apply configuration.
Enter the configuration method. (console/gui) ? **console**
Enter the setup mode; setup newly or restore from backup. (setup/restore) ? **setup**
You have chosen to setup a new Fabric interconnect. Continue? (y/n): **y**
Enforce strong password? (y/n) [y]: **y**
Enter the password for "admin": [xxxxx]
Confirm the password for "admin": [xxxxx]
```

Next, you are prompted to confirm whether the fabric interconnect is part of a cluster. The Cisco UCS cluster consists of two fabric interconnects, and all associated configuration is replicated between the two for all devices in the system.

**Step 3:** Create a new cluster.

```
Is this Fabric interconnect part of a cluster(select 'no' for standalone)? (yes/no) [n]: **yes**
```

Each fabric interconnect has a unique physical IP address. A shared cluster IP address is used to access Cisco UCS Manager after the system initialization is completed. The fabric interconnects are assigned one of two unique fabric IDs for both Ethernet and Fibre Channel networking.

**Step 4:** Choose fabric A for the first fabric interconnect that you are setting up.

```
Enter the switch fabric (A/B) []: **A**
```

The system name is shared across both fabrics, so "-a" or "-b" is automatically appended to the name that you specify in the Basic System Configuration Dialog when you set up one of the fabric interconnects.

**Step 5:** Name the Cisco UCS system.

```
Enter the system name: **cvd-ucs**
```

**Step 6:** Apply the following example configuration as you respond to the prompts.

```
Physical Switch Mgmt0 IPv4 address : **10.4.63.29**
Physical Switch Mgmt0 IPv4 netmask : **255.255.255.0**
IPv4 address of the default gateway : **10.4.63.1**
Cluster IPv4 address : **10.4.63.31**
Configure the DNS Server IPv4 address? (yes/no) [n]: **n**
Configure the default domain name? (yes/no) [n]: **n**
Join centralized management environment (UCS Central)? (yes/no) [n]: **n**
```
Step 7: The Basic System Configuration Dialog displays a summary of the configuration options that you chose. Verify the accuracy of the settings. Unless the settings require correction, enter yes to apply the configuration. The system assumes the new identity that you configured.

Following configurations will be applied:

- Switch Fabric=A
- System Name=cvd-ucs
- Enforced Strong Password=yes
- Physical Switch Mgmt0 IP Address=10.4.63.29
- Physical Switch Mgmt0 IP Netmask=255.255.255.0
- Default Gateway=10.4.63.1
- Cluster Enabled=yes
- Cluster IP Address=10.4.63.31

NOTE: Cluster IP will be configured only after both Fabric Interconnects are initialized

Apply and save the configuration (select ‘no’ if you want to re-enter)? (yes/no): yes
Applying configuration. Please wait.
Configuration file – Ok

After the system has booted, you can add the second fabric interconnect to the cluster. Because you have already defined the cluster, you only need to acknowledge the prompts to add the second fabric interconnect to the cluster and set a unique IP address.

Step 8: Connect a terminal to the console port of the second fabric interconnect to be configured, and then press Enter.

Step 9: In the Basic System Configuration Dialog that follows, enter the information as shown below, enter the admin password you configured on the first fabric interconnect to establish a connection to the peer, enter the management IP address for the second fabric interconnect, and then save the configuration.

Enter the configuration method. (console/gui) ? console
Installer has detected the presence of a peer Fabric interconnect. This Fabric interconnect will be added to the cluster. Continue (y/n) ? y
Enter the admin password of the peer Fabric interconnect: [xxxxx]
Connecting to peer Fabric interconnect... done
Retrieving config from peer Fabric interconnect... done
Peer Fabric interconnect Mgmt0 IP Address: 10.4.63.29
Peer Fabric interconnect Mgmt0 IP Netmask: 255.255.255.128
Cluser IP address: 10.4.63.31
Physical Switch Mgmt0 IPv4 address : 10.4.63.30
Apply and save the configuration (select ‘no’ if you want to re-enter)? (yes/no): yes
Applying configuration. Please wait.
Configuration file – Ok
From this point forward, this guide primarily shows the use of the Cisco UCS Manager GUI for management of the system; however, you should become familiar with the console in case you need very low-bandwidth remote access or a separate mode of access for administrative tasks such as code upgrades or system troubleshooting.

Configuring Communications Connections Using UCS Manager

1. Configure fabric-to-I/O-module links
2. Define Ethernet uplink ports
3. Configure SAN uplinks

Cisco UCS Manager is the management service for all of the components in a Cisco UCS instance. Cisco UCS Manager runs on the fabric interconnects and keeps configuration data synchronized between the resilient pair. The primary access method covered here for using Cisco UCS Manager is the Java-based GUI client, which you launch from a web browser.

Figure 8 - Cisco UCS Manager GUI
The Cisco UCS Manager GUI consists of a navigation pane on the left side of the screen and a work pane on the right side of the screen. The navigation pane allows you to browse through containers and objects and to drill down easily through layers of system management. In addition, the following tabs appear across the top of the navigation pane:

- **Equipment**—Inventory of hardware components and hardware-specific configuration
- **Servers**—Service profile configuration and related components such as policies and pools
- **LAN**—LAN-specific configuration for Ethernet and IP networking capabilities
- **SAN**—SAN-specific configuration for Fibre Channel networking capabilities
- **VM**—Configuration specific to linking to external server virtualization software, currently supported for VMware
- **Admin**—User management tasks, fault management, and troubleshooting

The tabs displayed in the navigation pane are always present as you move through the system and in conjunction with the tree structure shown within the pane itself. They are the primary mechanisms for navigating the system.

After you choose a section of the Cisco UCS Manager GUI in the navigation pane, information and configuration options appear in the work pane on the right side of the screen. In the work pane, tabs divide information into categories. The work pane tabs that appear vary according to the context chosen in the navigation pane.

Any computer that you want to use to run the Cisco UCS Manager client must meet or exceed the minimum system requirements listed in the “Release Notes for Cisco UCS Software,” which can be found on: www.cisco.com.

### Procedure 1  Configure fabric-to-I/O-module links

On a newly installed system, one of your first tasks is to define which ports on the fabric interconnects are attached to the I/O modules in each chassis (these are referred to as server ports). This allows Cisco UCS Manager to discover the attached system components and build a view of the entire system.

**Step 1:** Using a browser, access the cluster IP address that you assigned during initial setup in Procedure 3 “Complete initial fabric interconnect setup” of the “Completing the Initial System Setup” process.

This example configuration uses 10.4.63.31 from the setup script. Authenticate by using the configured username and password, and view the initial screen.

**Step 2:** Choose **Launch UCS Manager**. The Cisco UCS Manager Java application downloads.

**Step 3:** In the navigation pane, click the **Equipment** tab, and then click the **Policies** tab in the work pane. On the **Policies** tab, another set of tabs appears. By default, the **Global Policies** tab displays the Chassis Discovery Policy.

**Tech Tip**

Link Grouping Preference of Port Channel is only supported on Cisco UCS 2200 Series Fabric Extenders and is recommended for most applications when using this model.
Step 4: In the Action list, choose the appropriate number of links for your configuration, and then click **Save Changes** at the bottom of the work pane.

**Tech Tip**

The chassis discovery policy may be set at 1, 2, 4, or max, which is 8 links per fabric; the default value is one. This design sets the value to two. You can add more links; this only defines the minimum number of I/O module links that must be active to discover a chassis.

Step 5: In the navigation pane, click the **Equipment** tab, and then expand Fabric Interconnects > Fabric Interconnect A > Fixed Module > Ethernet Ports.

Objects are displayed representing each of the physical ports on the base fabric interconnect system.

Step 6: Choose the desired port by clicking the port object, or choose several sequential ports by clicking additional ports while pressing the **Shift** key.
Step 7: Right-click the selected port or group of ports, and then choose **Configure as Server Port**.

![Image of Cisco UCS Manager interface]

Step 8: On the “Successfully configured…” message, click **OK**.

Step 9: In the navigation pane, expand the tree to **Fabric Interconnect B**, and then follow Step 5 through Step 8 to configure the resilient links from Fabric B.

After Cisco UCS Manager has discovered each of the chassis attached to your system, you can use the Equipment tab in the navigation pane to verify that each chassis, I/O module, and server is properly reflected. If they do not show up, or they indicate an error condition, right-click the chassis number, choose **Acknowledge Chassis**, and in the pop-up window, click **OK**. After the discovery process is done, you can see the result on the Main Topology View tab in the work pane.

![Image of Cisco UCS Manager interface showing Main Topology View]
Procedure 2 Define Ethernet uplink ports

In the Cisco Unified Computing System reference design, Ethernet uplink ports connect the fabric interconnects to the Cisco Nexus 5500UP switches via 10-Gigabit Ethernet links. These links carry IP-based client and server traffic, server-to-server traffic between IP subnets, and Ethernet-based storage access such as iSCSI or NAS traffic. You may use ports from either the base fabric interconnects or expansion modules as uplink ports.

Step 1: On the Equipment tab in the navigation pane, locate the ports that are physically connected to the upstream switches.

Step 2: Choose each port that you selected for your implementation (or choose sequential ports by clicking additional ports while pressing the Shift key), right-click, and then choose Configure as Uplink Port.

This design implemented a port-channel configuration on the upstream Cisco Nexus 5500UP Series switches as described in the Procedure 1 “Configure Nexus 5500 port channels” earlier in this guide. You must perform similar port-channel configuration for the Ethernet uplink ports for the fabric interconnects.

Step 3: In the navigation pane, click the LAN tab, expand LAN > LAN Cloud > Fabric A, and then select the Port Channels container.

Step 4: Click Add (green plus sign).
Step 5: Enter an ID and Name for the new port channel, and then click Next. For example, enter an ID 50 and a name of Fabric-A-PC-50.

Step 6: In the Ports list, select the Ethernet ports to use as uplinks.

Step 7: Click the right arrows (>>) button. This adds the ports to the Ports in the port channel list on the right. This design uses ports Slot-1, ports 17 through 20.

Pay close attention to the Slot ID column when you select the ports to be added to the port channel. Integrated ports are listed with a slot ID of 1. If you are using an expansion module, scroll down to find ports listed with a slot ID of 2.

Step 8: Click Finish. This completes the creation of the Ethernet uplink port channel for Fabric A.

Step 9: Create a port channel for Fabric B by repeating Step 1 through Step 8. In Step 5, use a unique port-channel ID (for example, 51) and name (for example Fabric-B-PC-51).

Port channel IDs are locally significant to each device; therefore, as shown, the ID used to identify a port channel to the fabric interconnect does not have to match the ID used for the channels on the Cisco Nexus 5500 switch configuration. In some cases, it may be beneficial for operational support to use consistent numbering for representation of these channels.

Procedure 3 Configure SAN uplinks

If you will access all of your storage strictly over Ethernet by using iSCSI or NAS protocols, it is not necessary to define or attach Fibre Channel uplinks, and you can skip the Fibre Channel and FCoE uplink procedures.

If you want to use native Fibre Channel to extend the SAN from the data center core to the Cisco UCS Fabric Interconnect, complete Option 1 of this procedure. If you want to use FCoE to extend the SAN from the data center core to the Cisco UCS Fabric Interconnect, complete Option 2 of this procedure.
Option 1: Configure Fibre Channel SAN uplinks

On a Cisco UCS 6200 fabric interconnect, the baseboard ports are universal ports that can run in the default Ethernet interface mode or can be changed to operate in Fibre Channel mode. If you will be using Fibre Channel SAN connectivity from your Cisco UCS 6200 fabric interconnect, the following steps configure ports for Fibre Channel mode.

Tech Tip

Changing the universal port mode operation from Ethernet to Fibre Channel operation causes the fabric interconnect to reboot. The remaining fabric interconnect remains active and able to pass traffic. If this is a new system, this should not pose a risk; if this is an existing system with active servers dual-homed, servers continue to communicate via the remaining active fabric interconnect.

Step 1: In the navigation pane, click the Equipment tab, expand Fabric Interconnect, and then select the subordinate fabric interconnect, which in this case is Fabric Interconnect B.

This deployment uses the subordinate fabric interconnect first to avoid losing GUI access to the fabric. Then it switches fabric interconnect roles and configures Fabric Interconnect A.

Step 2: In the work pane, click Configure Unified Ports. A popup warning message appears.

Step 3: Click Yes. This acknowledges the operation.
Step 4: On the Configure Fixed Module Ports screen, beneath the graphic of the Fixed Module Ports, move the slider from right to left so that it includes the two right-most ports (ports 47 and 48) for Fibre Channel operation, and then click Finish. This design uses two ports and the default Fibre Channel port mode operation of uplink.

The Successfully Configured Ports box appears.

Step 5: Click OK. The Fabric Interconnect-B reboots. While Fabric Interconnect-B is rebooting the Overall Status shows inoperable until it has completed the reboot and returns to operational state. Once Fabric Interconnect-B returns to an Operable status, proceed to the next step.

Step 6: Log in to the Fabric Interconnect Cluster with an SSH CLI session to the IP address 10.4.63.31, as defined in Step 6 of the “Complete initial fabric interconnect setup” procedure.
Step 7: To avoid a long GUI access timeout when configuring Fabric Interconnect-A Fibre Channel port mode, configure Fabric Interconnect-B to be the primary.

    login as: admin
  Cisco UCS 6200 Series Fabric Interconnect
Using keyboard-interactive authentication.
Password: [password]
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2012, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

Step 8: Verify that Fabric Interconnect-A is now the primary.

    cvd-ucs-A# show cluster state
  Cluster Id: 0x99fd3a5684de11e1-0xa340547fee243524
    A: UP, PRIMARY
    B: UP, SUBORDINATE
    HA READY

Step 9: Connect to the local management control process.

    cvd-ucs-A# connect local-mgmt
  Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2012, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

Step 10: Switch the primary role to fabric interconnect-B.

    cvd-ucs-A(local-mgmt)# cluster lead b
  Cluster Id: 0x99fd3a5684de11e1-0xa340547fee243524
  cvd-ucs-A(local-mgmt)#

This causes your SSH CLI session to disconnect and your Cisco UCS Manager GUI console access to lose connection.
Step 11: Click Re-Login on the GUI console access popup message, and then log in to Cisco UCS Manager again.

Step 12: In the navigation pane, click the Equipment tab, and then expand Fabric Interconnect. Note that Fabric Interconnect B is now the primary.

Step 13: Select the subordinate fabric interconnect, which in this case in Fabric Interconnect A.

Step 14: Follow Step 2 and Step 4 above to configure Fibre Channel ports on Fabric Interconnect A.

Next, after you have completed the tasks and the Fabric Interconnect A has returned to operable state, you verify that you now have Fibre Channel uplink ports available to configure.

Step 15: On the SAN tab, expand SAN Cloud > Fabric A > Uplink FC Interfaces, and then expand Fabric B > Uplink FC Interfaces. You should see the Fibre Channel uplinks listed in the display.

Step 16: Connect the Fibre Channel configured ports on the Cisco UCS 6200 Fabric Interconnect to the data center core Cisco Nexus 5500 switch SAN.

Step 17: Disable unused ports by right-clicking the port name in the navigation pane, and then choosing Disable. When you disable unused ports, you clear any system alerts tied to the unused ports in both fabric interconnects A and B.

Next, you must create a VSAN and assign it to the Fibre Channel port to activate the port and transmit traffic. This VSAN should match the VSAN configured on the corresponding SAN fabric, as referred to in Table 1 “Fibre Channel VSAN to FCoE VLAN mapping.”

Step 18: In the navigation pane, click the SAN tab, and then expand SAN > SAN Cloud > VSANs.
Step 19: Right-click the SAN Cloud container, and then choose Create VSAN.

Step 20: Enter a Name for the VSAN, leave the default value selected for FC Zoning as Disabled, and then select Both Fabrics Configured Differently.
Step 21: Enter the VSAN IDs corresponding to the SAN-A and SAN-B VSANs configured in your SAN fabrics. In the Data Center Technology Design Guide, VSAN 4 is assigned to SAN-A, and VSAN 5 is assigned to SAN-B.

Step 22: For each fabric, enter the VLAN that the Fibre Channel traffic should use from the chassis to the fabric interconnects. VSAN ID 4 on Fabric A corresponds to FCoE VLAN 304 on the fabric interconnect, and VSAN ID 5 on Fabric B corresponds to FCoE VLAN 305 on the fabric interconnect.

Step 23: When you have configured the VSAN IDs in this section, click OK. A window shows the successful creation of the VSAN.

Now that you have created the VSAN, you can create a SAN port-channel to connect to the data center core Cisco Nexus 5500UP switches.

Step 24: In the navigation pane on the SAN tab, expand SAN Cloud, expand Fabric A, right-click FC Port Channels, and then choose Create Port Channel.

Step 25: Enter an ID and name for the port channel, and then click Next.
Step 26: In the Ports list, select the ports, and then click the right arrows (>>) button to move them to the Ports in the port channel list. Click Finish when you have added the physical uplink ports to the port channel.

![Unified Computing System Manager](image)

Step 27: On the “Successfully created...” message, click OK.

Step 28: Expand FC Port Channels. You can see the newly created port channel.

Step 29: In the main window, double-click the new port channel. The next step is to configure the VSAN assignment.

Step 30: In the work pane, on the General tab, inside the Properties box, in the VSAN list, choose the VSAN for SAN Fabric A on Fabric Interconnect A operation, and then click Save Changes.

![Unified Computing System Manager](image)

**Tech Tip**

If the port channel fails to come up, you may have to reset the corresponding ports on the data center core Cisco Nexus 5500UP switches. To do so via CLI, enter interface configuration mode for the SAN port channel 29, enter the shutdown command, and then enter the no shutdown command.

![Unified Computing System Manager](image)

Step 31: Repeat Step 24 through Step 30 for the VSAN for SAN Fabric B on Fabric Interconnect B.
Option 2: Configure FCoE SAN uplinks

If you want to use FCoE to extend the SAN from the data center core to the Cisco UCS Fabric Interconnect, as configured in Option 2: “Configure FCoE SAN port channels” earlier in this guide, use this procedure.

First you must create a VSAN and assign it to the FCoE port channel. This VSAN should match the VSAN configured on the corresponding SAN fabric as referred to in Table 1, “Fibre Channel VSAN to FCoE VLAN mapping.”

Step 1: In the navigation pane, click the SAN tab, and then expand SAN > SAN Cloud > VSANs.

Step 2: Right-click the SAN Cloud container, and then choose Create VSAN.
Step 3: Enter a Name for the VSAN, leave the default value selected for FC Zoning as Disabled, and then select Both Fabrics Configured Differently.

Step 4: Enter the VSAN IDs corresponding to the SAN–A and SAN–B VSANs configured in your SAN fabrics. In the Data Center Technology Design Guide, VSAN 4 is assigned to SAN–A, and VSAN 5 is assigned to SAN–B.

Step 5: For each fabric, enter the VLAN that the Fibre Channel traffic should use from the chassis to the fabric interconnects. VSAN ID 4 on Fabric A corresponds to FCoE VLAN 304 on the fabric interconnect, and VSAN ID 5 on Fabric B corresponds to FCoE VLAN 305 on the fabric interconnect.

Step 6: When you have configured the VSAN IDs in this section, click OK. A window shows the successful creation of the VSAN.

Now that you have created the VSAN, you can create an FCoE SAN port-channel to connect to the data center core Cisco Nexus 5500UP switches.

Step 7: In the navigation pane, on the Equipment tab, locate the ports on Fabric A that are physically connected to the data center core Cisco Nexus 5500 switches for FCoE SAN traffic. These ports were configured on the data center core in Option 2: “Configure FCoE SAN port channels.”

Step 8: Choose each port that you selected for your implementation (or choose sequential ports by clicking additional ports while pressing the Shift key), right–click, and then choose Configure as FCoE Uplink Port.

Step 9: In the confirmation message, click Yes to configure the port as FCoE Uplink Port.
Step 10: In the navigation pane, on the SAN tab, expand SAN Cloud, expand Fabric A, right-click FCoE Port Channels, and then choose Create FCoE Port Channel.

Step 11: Enter an ID and name for the port channel, and then click Next.
Step 12: In the Ports list, select the ports, and then click the right arrows (>>) button to move them to the Ports in the port channel list. Click Finish when you have added the physical uplink ports to the port channel.

Step 13: On the “Successfully created…” message, click OK.

Step 14: In the main window, double-click the new port channel. The next step is to configure the VSAN assignment.

Step 15: In the work pane, on the General tab, inside the Properties box, in the VSAN list, choose the VSAN for the SAN Fabric A on Fabric Interconnect A operation, and then click Save Changes.

Step 16: Repeat Step 7 through Step 15 for Fabric Interconnect B FCoE uplink ports and SAN port-channel creation.
Configuring Common System Address Pools and VLANs

1. Add a management IP address pool
2. Create UUID pool
3. Create WWNN pool
4. Create WWPN pools
5. Create MAC pool
6. Create VLANs

When configuring the Cisco UCS Management address pools for a fabric interconnect pair, it is advised to customize some addressing to your environment so that you can more easily configure and identify addresses related to a fabric interconnect or UCS Manager domain. However it is recommended to preserve the IEEE assigned organizationally unique identifier (OUI) addressing when possible in order to avoid conflicts and operational issues. This design will use a hex pair of “FF” as the UCS Manager domain identifier for this fabric interconnect pair in the following fields:

- Universally unique identifier (UUID) suffix pool
- Fibre Channel World Wide Node Name (WWNN) and World Wide Port Name (WWPN) pools
- MAC address pool

In addition to the Cisco UCS Manager domain identifier, some pools will contain a UCS Fabric Interconnect identifier of 0A or 0B for Fabric Interconnect A and B respectively.

<table>
<thead>
<tr>
<th>WW Name field</th>
<th>Address</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>WW Node Name</td>
<td>20:FF:00:25:85:00:00:01</td>
<td>Preserve NAA=2 format prefix (20:)</td>
</tr>
<tr>
<td>WW Port Name FI-A</td>
<td>20:FF:00:25:85:0A:00:01</td>
<td>Fabric Interconnect-A WWPN range</td>
</tr>
<tr>
<td>WW Port Name FI-B</td>
<td>20:FF:00:25:85:0B:00:01</td>
<td>Fabric Interconnect-B WWPN range</td>
</tr>
</tbody>
</table>

The VLAN and IP address assignment in this process aligns to the addressing used in the Data Center Technology Design Guide as well as VLAN 160, which is used in the Virtualization with Cisco UCS, Nexus 1000V, and VMware Technology Design Guide. Actual VLANs and IP address assignment may vary based on your deployment requirements.
Table 3 - Design guide data center VLANs and IP address ranges

<table>
<thead>
<tr>
<th>VLAN</th>
<th>VLAN name</th>
<th>IP address</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>148</td>
<td>Servers_1</td>
<td>10.4.48.0/24</td>
<td>General network server use</td>
</tr>
<tr>
<td>149</td>
<td>Servers_2</td>
<td>10.4.49.0/24</td>
<td>General server use</td>
</tr>
<tr>
<td>150</td>
<td>Servers_3</td>
<td>10.4.50.0/24</td>
<td>General server use</td>
</tr>
<tr>
<td>154</td>
<td>FW_Inide_1</td>
<td>10.4.54.0/24</td>
<td>Firewall-protected servers</td>
</tr>
<tr>
<td>155</td>
<td>FW_Inide_2</td>
<td>10.4.55.0/24</td>
<td>Firewall and IPS protected servers</td>
</tr>
<tr>
<td>160</td>
<td>1kv-Control</td>
<td>10.4.60.0/24</td>
<td>Cisco Nexus 1000V Control</td>
</tr>
<tr>
<td>161</td>
<td>vMotion</td>
<td>10.4.61.0/24</td>
<td>Reserved for VMware vMotion traffic future use</td>
</tr>
<tr>
<td>162</td>
<td>iSCSI</td>
<td>10.4.62.0/24</td>
<td>Reserved for iSCSI storage traffic</td>
</tr>
<tr>
<td>163</td>
<td>DC-Management</td>
<td>10.4.63.0/24</td>
<td>Out-of-band data center management VLAN</td>
</tr>
</tbody>
</table>

**Procedure 1** Add a management IP address pool

The Cisco UCS Manager GUI provides a launching point to direct keyboard-video-mouse (KVM) access to control each of the blade servers within the system. To facilitate this remote management access, you must allocate a pool of IP addresses to the blade servers within the system. These addresses are used by the Cisco UCS KVM Console application to communicate with the individual blade servers. You must allocate this pool of addresses from the same IP subnet as the addresses assigned to the management interfaces of the fabric interconnects, because a common default gateway is used for their communication.

This procedure assigns an IP address pool from the DC-Management IP address range listed in Table 3.

**Step 1:** In the navigation pane, click the **LAN** tab, expand **LAN > Pools > root > IP Pools**, and then choose **IP Pool ext-mgmt**.

![Image of IP Pool ext-mgmt](image)

**Step 2:** In the work pane, on the **General** tab, click **Create Block of IPv4 Addresses**.

![Image of Create Block of IPv4 Addresses](image)
Step 3: Allocate a contiguous block of IP addresses by specifying the starting address in the From box, the Size of the block, the Subnet Mask, and the Default Gateway, and then click OK. The size of the block needs to be large enough to assign one address to each server connected to the fabric. In this example, you can use 32 addresses for the size of the block.

Step 4: After you complete the initial setup, ensure that the system firmware is updated to the most current version or to the version recommended for your installation.

Reader Tip

Detailed information on upgrading firmware is available at:

Procedure 2 Create UUID pool

Step 1: In the navigation pane, click the Servers tab, expand Servers > Pools > root > UUID Suffix Pools, and then choose Pool default.
A universally unique identifier (UUID) suffix pool is a collection of SMBIOS UUIDs that are available to be assigned to servers. The first number of digits that constitute the prefix of the UUID are fixed. The remaining digits, the UUID suffix, are variable. A UUID suffix pool avoids conflicts by ensuring that these variable values are unique for each server associated with a service profile that uses that particular pool. It is recommended that you do not alter the UUID prefix, and only customize the UUID suffix for your identification requirements.

**Step 2:** On the General tab, under the Actions pane, select **Create a Block of UUID Suffixes**.

**Step 3:** In the Create a Block of UUID Suffixes window, in the From box, enter a unique, randomized base value as a starting point. This guide assigns the Cisco UCS Manager domain an identifier of “FF” in the suffix field.

You can find UUID generation tools that are compliant with RFC 4122 on the Internet. For an example, see: [http://www.famkruthof.net/uuid/uuidgen](http://www.famkruthof.net/uuid/uuidgen)

**Step 4:** In the Size box, enter a number larger than the number of servers or service profiles that you require to use the same pool. If future expansion is required, you can add multiple UUID suffix blocks to the same pool. For a base system startup, a simple, small pool is sufficient. This example uses 512.

**Step 5:** Click OK.

**Procedure 3** Create WWNN pool

A World Wide Names (WWN) pool is a collection of WWNs for use by the Fibre Channel vHBA in a Cisco UCS domain. You must provision a pool of World Wide Node Names (WWNNs) in the system, and you must assign the WWNNs in the pool to servers that need to access the Fibre Channel SAN. You assign one WWNN from the pool to each server. Each WWNN corresponds to the identity of a Fibre Channel end-node. World Wide Port Names (WWPNs) are assigned to the vHBA.
Step 1: In the Cisco UCM Manager navigation pane, click the SAN tab, and then expand SAN > Pools > Root > WWNN Pools.

Step 2: Right-click WWNN Pools, and then select Create WWNN Pool.

Step 3: Enter a Name and Description for the new pool, and then click Next.

Step 4: In the Add WWN Blocks work pane click Add.

Step 5: In the Create WWNN Block window, in the From box, enter a WWN prefix. The system provides a prefix to help ensure uniqueness of the WWNN values on the SAN. Assign the last three segments of the base WWNN value in colon-delimited notation, as needed for your system. This guide assigns the Cisco UCS Manager domain an identifier of “FF” in the second hex pair of the WWN block, thereby preserving the required “20” hex pair in the first block, and the OUI identifier of “00:25:B5” in hex pairs 3 through 5.

Reader Tip

For more information on WWN, WWNN, and WWPN, see the Cisco UCS Manager GUI Configuration Guide:

Step 6: In the Size box, specify the number of node names required, and then click OK.
Step 7: Click Finish. This completes the creation of the new WWNN pool. If you include a pool of WWNNs in a service profile, the associated server is assigned a WWNN from that pool.

**Procedure 4  Create WWPN pools**

Both Fibre Channel port and node addressing assignments are required in order for Cisco UCS to provide access through the SAN fabric to the disk array. Using WWPNs and WWNNs that are independent from the physical hardware allows you to assign the service profile to any server in the Cisco UCS system. This allows the server to assume the correct server identity and SAN access privileges. Similar to the WWNN pool that you created in Procedure 3, you must provision a pool of WWPNs for the system to assign port addresses consistently when you add new service profiles to the system. A given device can have only one WWNN but many WWPN’s. We will create two pools for WWPNs, one for Fabric A and other for Fabric B.

Step 1: In the Cisco UCM Manager navigation pane, click the SAN tab, and then expand SAN > Pools > Root > WWPN Pools.

Step 2: Right-click WWPN Pools, and then select Create WWPN Pool.

Step 3: Enter a Name and Description for the pool, and then click Next.

Step 4: On the WWN Blocks page, click Add. This creates a new WWPN block.

Step 5: In the Create WWN Block window, in the From box, assign a unique WWPN value that identifies that the WWPN pool belongs to Fabric A, according to Table 2.

Step 6: In the Size box, specify the number of port names required in the pool, and then click OK.
Step 7: Click Finish.

Step 8: Repeat the above steps to create WWPN pool for Fabric B, following the addressing assigned in Table 2.

**Procedure 5  Create MAC pool**

A MAC pool is collection of MAC addresses that are unique in their Layer 2 environment and are assigned to the vNICs on a server. This pool of MAC addresses is used by vNIC interfaces in service profiles. Using a pool of MAC addresses instead of hardware-based MAC addresses allows a service profile to retain the same MAC address for its network interfaces, even when it is assigned to a new blade server in the system.

Similar to the Cisco UCS domain addressing used in the previous procedures in this process, you assign a domain identifier of “FF” for this UCS domain. It is recommended that you retain the OUI value in the MAC address field (00:25:B5) and assign any unique identifiers to the right of this portion of the address field.

**Step 1:** In the Cisco UCM Manager navigation pane, click the **LAN** tab, and then expand **LAN > Pools > Root > MAC Pools**.

**Step 2:** Under **MAC Pools** section, select **MAC POOL default**.

![Image of MAC POOL default](Attachment)

**Step 3:** Right-click **MAC POOL default**, and then select **Create a Block of MAC Addresses**. The Create a Block of MAC Addresses window allows you to define the starting address and the number of addresses to include in the block. Next, you create a block of addresses large enough to allocate one address to each vNIC that will exist in the system.

**Step 4:** In the **First MAC Address** box, add the starting address for the MAC address block, and then in the **Size** box, enter the number of addresses to allocate.
Step 5: Click OK, and then click OK to acknowledge creation of the pool.

**Procedure 6  Create VLANs**

The VLANs created for the data center design are replicated here for your reference. Actual VLANs and IP address assignment may vary based on your deployment requirements.

<table>
<thead>
<tr>
<th>VLAN</th>
<th>VLAN name</th>
<th>IP address</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>148</td>
<td>Servers_1</td>
<td>10.4.48.0/24</td>
<td>General network server use</td>
</tr>
<tr>
<td>149</td>
<td>Servers_2</td>
<td>10.4.49.0/24</td>
<td>General server use</td>
</tr>
<tr>
<td>150</td>
<td>Servers_3</td>
<td>10.4.50.0/24</td>
<td>General server use</td>
</tr>
<tr>
<td>154</td>
<td>FW_Inside_1</td>
<td>10.4.54.0/24</td>
<td>Firewall-protected servers</td>
</tr>
<tr>
<td>155</td>
<td>FW_Inside_2</td>
<td>10.4.55.0/24</td>
<td>Firewall and IPS protected servers</td>
</tr>
<tr>
<td>160</td>
<td>1kv-Control</td>
<td>10.4.60.0/24</td>
<td>Cisco Nexus 1000V Control</td>
</tr>
<tr>
<td>161</td>
<td>vMotion</td>
<td>10.4.61.0/24</td>
<td>Reserved for VMware vMotion traffic future use</td>
</tr>
<tr>
<td>162</td>
<td>iSCSI</td>
<td>10.4.62.0/24</td>
<td>Reserved for iSCSI storage traffic</td>
</tr>
<tr>
<td>163</td>
<td>DC-Management</td>
<td>10.4.63.0/24</td>
<td>Out-of-band data center management VLAN</td>
</tr>
</tbody>
</table>

Step 1: In the Cisco UCM Manager navigation pane, click the LAN tab, and then select LAN Cloud.

Step 2: Right-click LAN Cloud, and then select Create VLANs.

Step 3: Enter a VLAN Name, select Common/Global, options for scope of VLAN and enter the VLAN ID, and then click OK.

Step 4: In the Create VLANs dialog box that pops up, you will note that VLAN was successfully created. Click OK.
Step 5: Create the remaining VLANs by following Step 1 through Step 4.

<table>
<thead>
<tr>
<th>Tech Tip</th>
</tr>
</thead>
</table>

Most single operating systems that have been installed directly on a server use a single VLAN for server-to-network operation. In hypervisor installations where multiple applications or servers will be hosted, trunking multiple VLANs is more likely.

**Configuring Virtual Adapter Templates**

1. Create Network Control Policy
2. Create vNIC templates
3. Create vHBA templates

This process will configure a basic Network Control Policy, an Ethernet vNIC template, and a Fibre Channel SAN vHBA template.

**Procedure 1** Create Network Control Policy

Cisco Discovery Protocol (CDP) should be enabled in order to help troubleshoot any connectivity problems on both physical and virtual adapters. Create a policy to enable CDP.

**Step 1:** In the navigation pane, click the LAN tab, and then expand LAN > Policies > root > Network Control Policies.

**Step 2:** Right-click Network Control Policies, and then choose Create Network Control Policy.

**Step 3:** In the Create Network Control Policy dialog box, enter a name for the policy, select Enabled for CDP, and then click OK.
Procedure 2  Create vNIC templates

A vNIC template defines how a vNIC on a server connects to the LAN. You create two vNIC templates, one associated to Fabric A and another associated to Fabric B.

Step 1: In the navigation pane, click the LAN tab, and then expand LAN > Policies > root > vNIC Templates.

Step 2: Right-click vNIC Templates, and then choose Create vNIC Template.

Step 3: Enter a name for vNIC template, and then for Fabric ID, select Fabric A.

Step 4: Under Target, ensure only Adapter is selected, select Updating Template as the Template Type, and then select all VLANs that needs to be assigned to the vNIC.

Step 5: In the MAC Pool list, select default.

Step 6: In the Network Control Policy list, select the policy created in Procedure 1. This template will be added to the Service Profiles in the later sections. By selecting Updating Template as the Template type, vNICs created from this template are updated if the template changes.
Fabric failover is appropriate for configurations with a single host operating system installed directly on the blade server. For a virtualized environment, it is recommended instead that you disable fabric failover, present multiple vNICs to the hypervisor, and allow the hypervisor system to manage the failover of traffic in the event of a loss of connection to one of the fabric interconnects. See the Virtualization with Cisco UCS, Nexus 1000V, and VMware Technology Design Guide for more information on presenting multiple vNICs to a hypervisor explanation.

Step 7: Click OK.

Step 8: Repeat Step 1 through Step 7 in order to create a vNIC template for vNICs that connect to Fabric B.

Procedure 3 Create vHBA templates

The vHBA template defines how a vHBA on a server connects to the Fibre Channel SAN.

Step 1: In the navigation pane, click the SAN tab, and then expand SAN > Policies > root > vHBA Templates.

Step 2: Right-click vHBA Templates, and then choose Create vHBA Template.
Step 3: Enter the following information and then click OK:

- Name—vHBA-Fabric-A
- Fabric ID—A
- Select VSAN—General Storage, which was created in Procedure 3 “Configure SAN uplinks.”
- Template Type—Initial Template
- WWPN Pool—CVD-WWPN-FabA, which was created in Procedure 4 “Create WWPN pools.”

Step 4: Repeat Step 2 through Step 3 in order to create a vHBA template for vHBAs that connect to Fabric B, using the following information:

- Name—vHBA-Fabric-B
- Fabric ID—B
- Select VSAN—General Storage which was created in Procedure 3 “Configure SAN uplinks.”
- Template Type—Initial Template
- WWPN Pool—CVD-WWPN-FabB which was created in Procedure 4 “Create WWPN pools.”
**Configuring Server Boot Policy**

1. Create local disk configuration policy
2. Create a local boot policy
3. Create a SAN boot policy

In this process, you will create:

- A Local Disk policy for servers that have physically local hard drives.
- A No Local Disk policy for servers that have no physically local hard drives and will utilize SAN boot.
- A Local Boot policy for servers that will boot from removable media such as Compact Disks (CD) or a local hard drive.
- A SAN Boot policy for servers that will boot from removable media such as CDs or a SAN boot target LUN.

Building multiple policies will provide flexibility for different hardware environments in your Cisco UCS domain.

**Procedure 1** Create local disk configuration policy

The local disk configuration policy allows the service profile to define how the block storage is structured on the local disks installed in each Cisco UCS blade server. A common configuration is to have two locally installed disks in each blade, set up for mirrored storage.

**Step 1:** In the navigation pane, click the **Servers** tab, and then expand **Servers > Policies > root > Local Disk Configuration Policies**.

**Step 2:** Right-click **Local Disk Configuration Policies**, and then select **Create Local Disk Configuration Policy**.

**Step 3:** Enter a **Name** and **Description** for the policy, and then in the **Mode** list, choose **Raid 1 Mirrored**.

**Step 4:** Ensure **Protect Configuration** is selected. If selected, the server retains the configuration in the local disk configuration policy even if the server is disassociated from the service profile.
Step 5: Click OK, and then acknowledge the creation.

To prepare for servers that boot from SAN, you create a policy that will not configure and install any Local Disk for your blade server.

Step 6: In the navigation pane, click the Servers tab, and then expand Servers > Policies > root > Local Disk Configuration Policies.

Step 7: Right-click Local Disk Configuration Policies, and then select Create Local Disk Configuration Policy.

Step 8: Enter a Name and Description for the policy, and then in the Mode list, choose No Local Storage.

![Create Local Disk Configuration Policy]

Step 9: Click OK, and acknowledge the creation.

**Procedure 2 Create a local boot policy**

The server boot order policy allows you to control the priority of different boot devices, to which the server will have access. In this procedure, you will first configure a basic boot policy that boots first from removable media—in this case, an attached CD or DVD drive—and then from the internal disk.

Step 1: In the navigation pane, click the Servers tab, and then expand Servers > Policies > root > Boot Policies.

Step 2: Right-click Boot Policies, and select Create Boot Policy.

Step 3: In the Create Boot Policy window, enter the Name and Description for the boot policy.

Step 4: Clear the Enforce vNIC/vHBA/iSCSI Name check box. Cisco UCS Manager uses the priority specified in the vNIC or vHBA.

Step 5: Click the down arrows on the Local Devices container, click Add CD-ROM first, and then click Add Local Disk.

The order of the devices in the list is displayed as a number in the Order column of the table.
Procedure 3  Create a SAN boot policy

The following steps will guide you to create boot-from-SAN policy. The policy will include a boot order that starts with any attached removable media, such as CD or DVD, and then will specify target WWPN of the storage system that houses the server boot LUN.

In addition to the configuration on the Cisco UCS for SAN boot, you will need to configure a LUN on your storage array, and Fibre Channel zoning on the data center core for the server to storage array connections according to the Data Center Technology Design Guide.

On storage arrays with redundant storage controllers, you may have up to four paths to the target LUN (LUN 0) for boot, two paths over SAN-A and two paths over SAN-B. If your storage array does not have redundant storage controllers, you only have two paths, one path over SAN-A and one over SAN-B. Only one of the paths will be configured as primary.

Table 5 - Example vHBA SAN boot target connections

<table>
<thead>
<tr>
<th>vHBA</th>
<th>Target type</th>
<th>Boot target WWPN</th>
<th>Target array controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>fc0</td>
<td>Primary</td>
<td>50:06:01:61:3C:E0:60:E2</td>
<td>A</td>
</tr>
<tr>
<td>fc0</td>
<td>Secondary</td>
<td>50:06:01:69:3C:E0:60:E2</td>
<td>B</td>
</tr>
<tr>
<td>fc1</td>
<td>Primary</td>
<td>50:06:01:60:3C:E0:60:E2</td>
<td>A</td>
</tr>
<tr>
<td>fc1</td>
<td>Secondary</td>
<td>50:06:01:68:3C:E0:60:E2</td>
<td>B</td>
</tr>
</tbody>
</table>

Step 1: In the navigation pane, click the Servers tab, and then expand Servers > Policies > root > Boot Policies.

Step 2: Right-click Boot Policies, and then select Create Boot Policy.

Step 3: In the Create Boot Policy window, enter the Name and Description for the boot policy.

Step 4: Clear the Enforce vNIC/vHBA/iSCSI Name check box. Cisco UCS Manager will use the priority specified in the vNIC or vHBA.
Step 5: Click the down arrows on the Local Devices container, and then click Add CD-ROM first.

Step 6: In the left pane, click vHBAs, and then click Add SAN Boot.

**Tech Tip**

When you create a boot policy that targets the WWPN of the storage system, the boot policy may be reused across multiple service profiles. Many storage systems can present a different LUN as a boot LUN or LUN 0 to different initiators, based on the initiator WWPN address. Referencing a common boot policy promotes configuration consistency across similar service profiles.

Step 7: In the Add SAN Boot window, in the vHBA box, enter a name (Example: fc0) that you will be defining for the vHBA of your system. For Type, select Primary, and then click OK.

**Tech Tip**

Because the boot policy references the vHBA by name, you must name interfaces consistently across service profiles that need to share a common boot policy definition.

Make note of the vHBA names you use, as you will use the same name for vHBA in your service profiles in a later procedure.

Step 8: In the Create Boot Policy window, click Add SAN Boot Target.
**Step 9**: In the Add SAN Boot Target dialog box, in the **Boot Target LUN** box, enter the specific LUN number for the system to boot. Typically, the boot LUN is presented by the storage system as LUN 0 to the requesting initiator.

**Step 10**: In the **Boot Target WWPN** box, enter the proper SAN target WWPN of FC adapter interface of target array controller A using SAN-A, and then click **OK**.

![Add SAN Boot Target](image1)

**Step 11**: Click **Add SAN Boot Target**.

**Step 12**: In the Add San Boot Target dialog box, keep the **Boot Target LUN** as 0.

**Step 13**: In the Boot Target WWPN box, enter the proper SAN target WWPN of FC adapter interface of target array controller B using SAN-A, and then click **OK**.

![Add SAN Boot Target](image2)

Now you will add SAN Boot targets for your second vHBA.

**Step 14**: In the left pane, click **vHBAs**, and then click **Add SAN Boot**.
Step 15: In the Add SAN Boot window, in the vHBA box, enter a name (Example: fc1) that you will be defining for the second vHBA of your system, and then click OK. The type will be set to Secondary.

Step 16: Click Add SAN Boot Target.

Step 17: In the Add SAN Boot Target dialog box, in the Boot Target WWPN box, enter the proper SAN target WWPN of FC adapter interface of target array controller A using SAN-B, and then click OK.

Step 18: Click Add SAN Boot Target.

Step 19: In the Add SAN Boot Target dialog box, deep the value for Boot Target LUN as 0.

Step 20: In the Boot Target WWPN box, enter the proper SAN target WWPN of FC adapter interface of target array controller B using SAN-B, click OK, and then click OK to create the policy.
You can configure redundant access to the boot LUN for some operating systems during installation; on others it must be added after you have completed the initial installation.

For example: Windows requires a single HBA during installation until multipath drivers are installed. For more information, see:

Other operating systems have different requirements. Please refer to your specific operating system documentation for handling redundant SAN connections.

The following summary screen shows multiple vHBAs configured with multiple paths to the SAN target boot LUN 0.
Creating an Initial Boot Service Profile for Local Boot

1. Create Service Profile for Local boot
2. Assign service profile and policies

One of the core concepts of Cisco UCS Manager is the service profile. A service profile defines all characteristics that are normally presented by a physical server to a host operating system or a hypervisor, including the presence of network interfaces and their addresses, host adapters and their addresses, boot order, disk configuration, and firmware versions. The profile can be assigned to one or more physical blade servers within the chassis. In this way, what is traditionally thought of as the personality of a given server or host is tied to the service profile rather than to the physical server blade where the profile is running. This is particularly true if network-based or SAN-based boot is configured for the profile. If local-boot is configured for the profile, the boot images installed on the local hard drives of the physical blade do tie the identity of the service profile to a given physical server blade.

There are multiple supporting objects within the Cisco UCS Manager GUI to streamline the creation of a service profile. These objects contain items such as pools of MAC addresses for Ethernet, World Wide Port Names (WWPNs) for Fibre Channel, disk configurations, VLANs, VSANs, etc. These objects are stored by the system so that they may be referenced by multiple service profiles, so you do not need to redefine them as you create each new profile.

This process provides an example of how to create a basic service profile for initial installation and boot of a host operating system or a hypervisor. Throughout this process, you create reusable system objects to facilitate faster creation of additional profiles that share similar characteristics. For simplicity, in this process you configure a basic boot policy using local mirrored disks. This initial profile creates the base system setup upon which you can build additional, more advanced profiles. Later sections in this guide show options for network-based or SAN-based boot.

**Procedure 1** Create Service Profile for Local boot

**Step 1:** On the Servers tab in the navigation pane, expand the containers underneath Service Profiles, and then select the Root container.

**Step 2:** On the General tab in the work pane, click Create Service Profile (expert), and then on the Identify Service Profile page, enter a name for the service profile in the Name box.
Step 3: In the UUID section, in the UUID Assignment list, choose the UUID suffix pool you created in Procedure 2 “Create UUID pool”, and then click Next.

Step 4: In the Networking section, Leave the **Dynamic vNIC Connection Policy** list set to its default, and next to **How would you like to configure LAN connectivity?**, select **Expert**.

Step 5: Click **Add** to add vNICs to the server.

Step 6: In the Create vNIC window, in the **Name** box, enter a name for the vNIC. For the example configuration, this guide uses **eth0** as the interface name; representing Ethernet 0.

Step 7: Select **Use vNIC Template**. In the **vNIC Template** list, select the vNIC Template created for Fabric A in Procedure 2 “Create vNIC templates.”
Step 8: In the **Adapter policy** list, select a policy from a list of pre-defined policies set according to the OS vendor’s optimal performance suggestions. This example uses the Ethernet Adapter policy for VMware.

Step 9: Click **OK**. This adds the vNIC.

Step 10: Repeat Step 5 through Step 9 in order to add a second vNIC, eth 1, using the vNIC template for Fabric B, created in Procedure 2 “Create vNIC templates.”

Step 11: On the Networking page, click **Next**.

Step 12: On the Storage page, in the **Local Storage** list, select the local disk configuration policy created in Procedure 1 “Create local disk configuration policy” for local disks installed in the Cisco UCS blade server.
Step 13: Next to How would you like to configure SAN connectivity?, select Expert.

Step 14: In the WWNN Assignment list, select the WWNN pool created in Procedure 3 “Create WWNN pool.”

Step 15: Click Add to add vHBA to the server.

Step 16: In the Create vHBA window, in the Name box, enter a name for the vHBA. For the example configuration, this guide uses fc0 as the interface name; representing vHBA 0.

Step 17: Select Use vHBA Template. In the vHBA Template list, select the vHBA Template created for Fabric A in Procedure 3 “Create vHBA templates.”

Step 18: In the Adapter policy list, select a policy from a list of pre-defined policies set according to the OS vendor’s optimal performance suggestions. This example uses Fibre Channel Adapter policy for VMware.
Step 19: Repeat Step 15 through Step 18 in order to add a second vHBA, fc1. Select the vHBA Template created for Fabric B in Procedure 3 “Create vHBA templates.”

Step 20: On the Storage page, click Next.

Step 21: On the Zoning page, do not make any changes. Click Next.

Step 22: On the vNIC/vHBA Place page, leave the defaults, and then click Next. The system places the virtual interfaces on the physical interfaces that exist on the blade servers with which this profile will be associated.

Step 23: On the Server Boot Order page, in the Boot policy list, select the boot policy created in Procedure 2 “Create a local boot policy,” which is configured to first boot from CD/DVD drive and then from the internal disk. Click Next.
Step 24: On the Maintenance Policy page, leave all default settings, and then click Next.

Step 25: On the Server Assignment page, in the **Server Assignment** list, select **Assign Later**, and then click Next.

Step 26: On the Operational Policies page, leave all default settings, and then click Finish.

Step 27: On the successful completion message, click OK. This exits the Service Profile Creation Wizard.

---

**Procedure 2** Assign service profile and policies

Cisco UCS has the ability to assign a service profile directly to a specific server, pre-provision an unused chassis slot, assign the profile to a pool of servers, or assign the profile to a physical blade server later.

**Step 1:** In the navigation pane, click the **Equipment** tab, and then click the **Chassis#** from which you want to select the server.

**Step 2:** Expand **Servers**, and then click the server you want. By default, the General tab displays.

**Step 3:** On the General page, in the Actions section, click the **Associate Service Profile** link.

**Step 4:** In the Associate Service Profile window, select the service profile from the list of available service profiles, and then click OK. This associates the service profile to the selected server.

**Step 5:** If you want to check the progress on the service profile that is being applied on the server, in the work pane, click the **FSM** tab. When progress status reaches 100%, it completes the service profile association to a server.
**Step 6:** After the service profile is applied to a server, you can now boot the server to install an operating system. The operating system installation media is available by either locally attached removable media, or KVM Console Virtual Media.

---

**Reader Tip**

For further details on how to install VMware on a server, please refer to the Virtualization with Cisco UCS, Nexus 1000V, and VMware Technology Design Guide.

The installation begins as is typical for the given operating system.

---

**Creating a Service Profile for SAN Boot**

1. Create service profile for SAN boot
2. Associate server to service profile

Booting service profiles directly from a Fibre Channel SAN can provide key advantages for ensuring server and application availability. With all operating system files and application data specific to the server stored on the SAN, your organization benefits from SAN disk redundancy and backup practices. This approach works in conjunction with the hardware independence provided by Cisco UCS-specific constructs such as shared pools of Ethernet and Fibre Channel addressing. Together, these attributes provide the ability to move a service profile among blade servers within the system programmatically, with no physical intervention required. This concept is known as stateless computing.

Fibre Channel uses World Wide Node Names (WWNN) and World Wide Port Names (WWPN) to communicate over the SAN. This process illustrates how to create a new service profile for SAN boot based on the existing example profile that you created in the previous process, “Creating an Initial Boot Service Profile for Local Boot.”

**Procedure 1  Create service profile for SAN boot**

In this procedure, you clone the service profile that you created in the previous process, “Creating an Initial Boot Service Profile for Local Boot.”

**Step 1:** On the **Servers** tab in the navigation pane, right-click the name of the profile you created in the previous process (Example: Servers_Local_Disk), and then choose **Create a Clone**.

**Step 2:** In the **Clone Name** box, enter a name that clearly identifies the profile as a SAN boot server instance (Example: Servers_SAN_Boot), and then click **OK**.

**Step 3:** On the **Servers** tab in the navigation pane, click on the service profile you created in the previous step.
Step 4: Click the **Storage** tab, and then click the **vHBAs** tab. Under the Actions pane, click **Change Local Disk Configuration Policy**.

![Cisco Unified Computing System Manager - vuds](image)

Step 5: In the Change Local Disk Configuration Policy window, in the **Select the Local Disk Configuration Policy** list, select the **No_Disk** configuration policy you created in Procedure 1 “Create local disk configuration policy,” and then click **OK**.

![Change Local Disk Configuration Policy](image)

Step 6: Click the **Boot Order** tab in the work pane, and then in the Actions area, click **Modify Boot Policy**.

![Modify Boot Policy](image)

Step 7: In the Modify Boot Policy window, under **Boot Policy** list, select the policy created for SAN boot in Procedure 3 “Create a SAN boot policy,” and then click **OK**. This assigns the new boot policy to the profile.

---

Deployment Details  
August 2014 Series
After you select the new boot policy, the work pane shows the new boot order information, including the correct target LUN ID and WWPN number.

![Modify Boot Policy](image)

**Procedure 2**  
**Associate server to service profile**

After the service profile is created and boot policy is assigned, associate the service profile to an open server on the chassis.

**Step 1:** In the navigation pane, click the **Equipment** tab, and then click the **Chassis** from which you want to select the server.

**Step 2:** Expand **Servers**, and then click the server you want. By default, the General tab displays.

**Step 3:** On the General page, in the Actions section, click the **Associate Service Profile** link.

**Step 4:** In the Associate Service Profile window, select the service profile from the list of available service profiles, and then click **OK**. This associates the service profile to the selected server.

![Associate Service Profile](image)
Step 5: If you want to check the progress on the service profile that is being applied on the server, in the work pane, click the FSM tab. When progress status reaches 100%, it completes the service profile association to a server.

![Step 5](image)

Step 6: After the service profile is applied to a server, you can now boot the server to install an operating system. The operating system installation media is available by either locally attached removable media, or KVM Console Virtual Media.

![Reader Tip](image)

For further details on how to install VMware on a server, please refer to the Virtualization with Cisco UCS, Nexus 1000V, and VMware Technology Design Guide.

The installation begins as is typical for the given operating system.

Step 7: When you choose a target disk destination for the installation, ensure that the new LUN 0, accessible over the Fibre Channel SAN, is selected.

Step 8: If you want, you can provision the SAN to expose multiple LUNs to a given initiator. For example, you can use separate LUNs to house operating system boot files and files that contain application-specific data or database contents. In a hypervisor environment, a LUN specific to an individual profile is presented as a boot LUN. A larger LUN, accessible to multiple initiators, is used to house virtual machine-specific files. In this way, multiple virtualized servers can access the virtual machine files.
Creating Multiple Service Profiles through Templates

1. Create a service profile template
2. Create a service profile from a template

Service profile templates are one of the ways to simplify the creation of new service profiles. The template approach ensures that consistent policies within the system are applied to a given service or application by using the same basic parameters—such as the number of vNICs and vHBAs—and with identity information drawn from the same pools. These templates may be configured as one of two types of service profile templates:

- **Initial templates**—A service profile created from an initial template initially inherits all the properties of the template, but after you create the profile, it is no longer connected to the template. If any changes were to be made to one or more profiles created from this template, you must change each profile individually.

- **Updating templates**—A service profile created from an updating template inherits all of the properties of the template and remains connected to the template. Any change to the template automatically updates the service profiles created from the template. The updating template feature is a powerful tool for managing updates to multiple servers with minimal administrative overhead.

The following procedures describe how to create a service profile template and then create a service profile from the template.

**Procedure 1** Create a service profile template

**Step 1:** In the Cisco UCS Manager navigation pane, click the **Servers** tab, expand **Service Profile Templates**, and then click the organization **root**.

**Step 2:** In the work pane, on the General tab, click **Create Service Profile Template**.

**Step 3:** In the Create Service Profile Template window, enter the **Name** of the template.
Step 4: Verify that the Initial Template option (default value) is selected.

Step 5: In the UUID Assignment list, choose an existing UUID pool, and then click Next.

Step 6: Follow the steps in Procedure 1, “Create Service Profile for Local boot”, to fill all required fields for the Storage, Networking, Zoning, vNIC/vHBA Placement, Server Boot Order, and Maintenance Policy pages, and then on the Server Assignment page, click Next.

The difference between creating a service profile versus creating a service profile template is that the template only allows you to choose a server pool in the Server Assignment window, but not for the individual blade server.

Step 7: On the Operational Policies page, leave the default settings, and then click Finish.

**Procedure 2** Create a service profile from a template

Step 1: In Cisco UCS Manager, click the Servers tab in the navigation pane, expand Service Profile Templates, and then click the organization where the new service profile template was created earlier under root.
Step 2: Right-click the service profile template from which you want to create the profiles, and then click **Create Service Profiles From Template**.

Step 3: In the **Create Service Profiles from Template** window, enter a **Naming Prefix** for the new profiles, enter the **Number** of profiles you want to create (or leave the default value of 2), and then click **OK**.

Step 4: On the message “Successfully created service profiles from template,” click **OK**.
Step 5: In the navigation pane under **Servers > Service Profiles > root**, verify that your new service profiles were created.

This completes the creation of service profiles from a service profile template.

**Cisco UCS C-Series Rack-Mount Server**

This module covers deploying the Cisco UCS C-Series Rack-Mount Server. This module includes information on initial system setup and basic configuration to prepare your server to communicate over Ethernet and FCoE using Cisco Integrated Management Controller (CIMC) to configure server settings. This module also includes details on integrating the Cisco UCS C-Series server with the Cisco Unified Computing System and allowing the server to be managed by Cisco UCS Manager. CIMC is the management service for the Cisco UCS C-Series servers. CIMC runs within the server and allows you to use a web-based GUI or SSH-based CLI to 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.

Cisco UCS C-Series Rack-Mount Servers may be connected to the data center infrastructure using available interfaces on the Cisco Nexus 5500UP Series Switches or through the Cisco Nexus 2000 Series Fabric Extenders. Switching access or trunk port modes may be configured according to the settings appropriate for the installed operating system.

The final process in this module details how the Cisco UCS C-Series server can be integrated into the Cisco Unified Computing System and be managed by the same Cisco UCS Manager that controls the UCS B-Series blade servers by connecting to a UCS Fabric Interconnect through a Cisco Nexus 2232PP Fabric Extender. This integration provides a single management interface to Cisco UCS B-Series and C-Series servers.

---

**Reader Tip**

Details on supported C-Series servers and network adapter cards for UCS integration with Cisco UCS Manager 2.2(1d), as well as the installation instructions for your specific C-Series server, can be found at:

If you are deploying your Cisco UCS C-Series servers for UCS-managed integration, complete the following processes only:

- Configuring Cisco Integrated Management Controller
- Updating Firmware for Cisco UCS C-Series Server
- Integrating Cisco UCS C-Series into the Cisco UCS Manager Environment

**Configuring Cisco Integrated Management Controller**

1. Configure management access

**Procedure 1** Configure management access

To access the CIMC controller remotely, you must either statically assign a management IP address or have a DHCP server servicing the VLAN or subnet to which the server is connected. This procedure assigns a static IP address to the server and requires the following information:

- IP address—**10.4.63.66**
- Subnet mask—**255.255.255.0**
- Default gateway—**10.4.63.1**
- Password

**Step 1:** Connect a keyboard, video display, and mouse to the server for the initial setup, and then power up the server.

**Step 2:** When the server boots up, you have the option to set up BIOS, boot menu, network boot, and CIMC Configuration. While in BIOS, press **F8** to start CIMC Configuration.

```
Processor(s) Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz
Total Memory = 64 GB  Effective Memory = 64 GB
Memory Operating Speed 1333 MHz

Entering CIMC Configuration Utility...
```
**Step 3:** Under NIC mode, press the **Spacebar**. This enables Dedicated.

The 10/100 management ports included on the server are used to access CIMC. The management ports are connected to the out-of-band Ethernet management network, which is detailed in the Data Center Technology Design Guide.

![CIMC Configuration Utility](image)

**Tech Tip**

To manage the Cisco UCS C-Series server as a standalone server using dedicated Ethernet ports for CIMC access, choose NIC mode **Dedicated**. To access CIMC via Cisco Card, or to manage the server when connected to a Cisco UCS fabric interconnect, see the following guide for more information:


Details for managing a Cisco UCS C-Series server with Cisco UCS Manager appear later in this guide, in the “Integrating Cisco UCS C-Series into the Cisco UCS Manager Environment” process.

**Step 4:** Under IPV4 (Basic), press the **Spacebar**. This action disables the default **DHCP enabled**. Then enter CIMC IP, Subnetmask, and the default Gateway.

**Step 5:** Under NIC redundancy, verify that **Active-Standby** is enabled.

**Tech Tip**

If you are using a server with a single management NIC, like the Cisco C200 Series, select a **NIC redundancy** of **None**.

**Step 6:** Under Default User (Basic), enter a default password. The default username is **admin**.
Step 7: Press F10. This saves the settings.

Step 8: Press F5 (Refresh). This reflects the latest configuration.

Step 9: Wait until the new settings appear, and then press Esc to exit and reboot the server.

---

### Updating Firmware for Cisco UCS C-Series Server

1. Configure virtual media
2. Upgrade UCS C-Series server firmware

It is recommended that you update your Cisco UCS C-Series servers with the latest firmware and BIOS.

Support for integrating a Cisco UCS C-Series server with Cisco UCS to be managed by Cisco UCS Manager running release 2.2(1d) or later is listed in Table 7 below.

#### Table 6 - Cisco UCS C Series server firmware used in this CVD

<table>
<thead>
<tr>
<th>Server type</th>
<th>Host Upgrade utility version</th>
<th>Virtual interface card type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS C220 M3</td>
<td>1.5(4f)</td>
<td>Cisco UCS VIC 1225</td>
</tr>
<tr>
<td>Cisco UCS C240 M3</td>
<td>1.5(4f)</td>
<td>Cisco UCS VIC 1225</td>
</tr>
</tbody>
</table>

#### Table 7 - Cisco UCS C-Series integration with UCS Manager firmware requirements

<table>
<thead>
<tr>
<th>Server model</th>
<th>Integration type</th>
<th>CIMC version</th>
<th>BIOS version</th>
<th>VIC firmware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS C220 M3</td>
<td>Single wire</td>
<td>1.4(6)</td>
<td>1.4(7a)</td>
<td>2.1(0.457a)</td>
</tr>
<tr>
<td>Cisco UCS C240 M3</td>
<td>Single wire</td>
<td>1.4(6)</td>
<td>1.4(7a)</td>
<td>2.1(0.457a)</td>
</tr>
<tr>
<td>Cisco UCS C200 M2</td>
<td>Dual wire</td>
<td>1.4(3c) minimum</td>
<td>–</td>
<td>2.0(2g)</td>
</tr>
<tr>
<td>Cisco UCS C210 M2</td>
<td>Dual wire</td>
<td>1.4(3c) minimum</td>
<td>–</td>
<td>2.0(2g)</td>
</tr>
</tbody>
</table>

Details on supported Cisco UCS C-Series servers, network adapter cards, and firmware requirements for Cisco UCS integration, as well as the installation instructions for your specific C-Series server, can be found at:


Note that Cisco UCS Manager single-wire-management integration requires a Cisco UCS Virtual Interface Card 1225.
Procedure 1  Configure virtual media

**Step 1:** In a browser, enter the IP address you configured earlier in Step 4 of the “Configure management access” procedure under the “Configuring Cisco Integrated Management Controller” process. This opens the CIMC login page.

You receive a Security Certificate warning in your browser on initial login before you can connect to the login screen.

**Step 2:** Click Accept. This acknowledges the certificate warning.

**Step 3:** Log in by using the default username **admin** and the password you configured earlier.

<table>
<thead>
<tr>
<th>Tech Tip</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can launch the CIMC GUI and manage the server from any remote host that meets these minimum requirements: Java 1.6 or later, HTTP and HTTPS enabled, and Adobe Flash Player 10 or later.</td>
</tr>
</tbody>
</table>

**Step 4:** On the Server tab, click **Remote Presence**.

**Step 5:** On the Virtual Media tab, verify that **Enabled** is selected.

<table>
<thead>
<tr>
<th>Tech Tip</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you do not select <strong>Enabled</strong>, you will receive the error “Either Virtual Media is detached or ...” when you try to map a remote disk.</td>
</tr>
</tbody>
</table>

**Step 6:** Click **Save Changes**.
Procedure 2  Upgrade UCS C-Series server firmware

You can use the Cisco Host Upgrade utility to upgrade the following firmware:

- CIMC
- System BIOS
- LAN on motherboard
- LSI
- Cisco UCS Virtual Interface Card

Step 1: Download the Cisco UCS Host Upgrade utility ISO file from [www.cisco.com](http://www.cisco.com). The version of Cisco UCS used in this guide is Server Firmware version 2.0(1a) for a Cisco UCS C-Series C220 M3 Rack Server.

Step 2: Locate the ISO file corresponding to the model of your server, download the file, and store it locally on your hard disk.

Step 3: In the CIMC Console, on the Server tab, click Summary, and then click Launch KVM Console.
Step 4: In the KVM Console dialog box, select the Virtual Media tab. The virtual media feature allows for media on your desktop to be available to the remote host.

![KVM Console Virtual Media](image)

Step 5: Click Add Image, and in the Open dialog box, select the Host Upgrade utility ISO file that you downloaded in Step 2.

![Add Image](image)

Step 6: Select the check box in the Mapped column for the ISO file. Do not click Exit when complete. Instead, proceed to the next step.

![Select Check Box](image)

Step 7: In the KVM Console, click the KVM tab, and then, from the Macros > Static Macros menu, select Ctrl-Alt-Del. The server reboots.

![KVM Console KVM Tab](image)

Step 8: During the server's power-on self-test, press F6. Use the arrow key to select Cisco VvKVM-Mapped vDVD1.22, and then press Enter. Do not close the virtual media screen while it is in use.

![Server Reboot](image)
After the server boots from the selected device, the following screen is displayed as the host loads the ISO image from the virtual disk drive.

**Step 9:** After the server loads the upgrade utility and displays the Cisco end-user license agreement (EULA), press \textit{y} to accept the EULA.

**Step 10:** In the Host Upgrade utility screen, in the Controls section, select \textbf{Update All}. This upgrades CIMC, BIOS, LAN on motherboard (LOM), LSI, VIC firmware, and Peripheral Component Interconnect (PCI) adapters.

**Step 11:** In the confirmation window, click \textbf{Yes} to update firmware on all components.
**Step 12:** To proceed with the firmware update, click Yes in the confirmation window.

![Confirmation dialog box]

**Step 13:** The Cisco IMC Secure Boot option allows you to only install and boot signed Cisco images. Click No to disable Secure Boot. It can be enabled later if desired.

![Confirmation dialog box]

Enabling Cisco IMC Secure Boot option implies:

1. You can install and boot only signed Cisco IMC firmware images on the server.
2. You cannot install and boot Cisco IMC versions prior to 1.5 (3x).
3. You cannot disable this option later on.

**IMPORTANT:** After installing the firmware with the Secure Boot option enabled, activate the image before performing regular server-based tasks. The Secure Boot option is enabled only when the firmware installation is complete and you have activated the image.

**NOTE:** If CIMC secure boot was already enabled, then "No" will not have any effect.

Do you want to enable Cisco IMC secure boot?

![Confirmation dialog box]
The firmware upgrade begins, and the status can be monitored as in the following figure.

**Step 14:** Once the BIOS upgrade completes, the server power cycles and boots up. Log in to CIMC to reestablish the connection.

**Step 15:** Verify under Server Properties that the BIOS Version has been updated, and under CIMC that the Firmware Version has been updated.
Configuring LSI RAID

1. Configure the LSI RAID adapter

If you are going to connect your Cisco UCS C-Series Server to a Cisco UCS Fabric Interconnect and manage it with Cisco UCS Manager, you may skip this process and continue with the next process “Updating Firmware for Cisco UCS C-Series Server.”

This process is based on using the new LSI RAID adapter configuration tool available in CIMC version 1.5.

**Procedure 1  Configure the LSI RAID adapter**

The LSI Integrated Mirroring feature is used to safeguard critical information by mirroring a set of data on two or more disks. In the event of a drive failure, data can be recovered from the mirrored drive, and the failed drive can be replaced. The server used in this lab setup has four identical, 500-GB hard drives with one optional LSI RAID controller. This procedure configures the four drives for RAID 1 (mirroring).

### Reader Tip

The following setup uses the LSI Integrated Mirroring feature. For a more elaborate RAID setup, see more specific LSI documentation at:

http://www.lsi.com

**Step 1:** In a browser, enter the CIMC IP address that you configured in Step 4 of Procedure 1, “Configure management access.”

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

**Step 3:** Click the Storage tab, and select the PCIe MegaRAID card.

**Step 4:** Under the Controller Info tab, in the Actions pane, select Create Virtual Drive from Unused Physical Drives.
**Step 5:** On the Create Virtual Drive from Unused Physical Drives dialog box, select the **RAID Level** (Example: RAID Level 1), select the physical drives to include in the Drive Group, and then click the **>>** button.

**Step 6:** Once the physical drives have been included in the RAID 1 Drive group, under the Drive Groups pane, select the **Drive Group**, and then click **Create Virtual Drive**.
Step 7: Click the Virtual Drive Info tab, and then in the Actions pane, click Initialize.

Step 8: On the Initialize Virtual Drive dialog box, in the Initialize type list, choose Fast Initialize, and then click Initialize VD.

Step 9: Once initialization is complete, reboot the server. The new RAID configuration is recognized.

Configuring Ethernet and FCoE Connectivity

1. Configure vNICs
2. Configure vHBAs

If you are going to connect your Cisco UCS C-Series Server to a Cisco UCS Fabric Interconnect and manage it with Cisco UCS Manager, you may skip this process and continue with the next process “Integrating Cisco UCS C-Series into the Cisco UCS Manager Environment.”

FCoE is an extension of the Fibre Channel SAN onto a lossless Ethernet fabric. This allows you to consolidate NICs and HBAs onto a single converged network adapter.

The FCoE-connected server is controlled by two drivers for Fibre Channel and Ethernet, respectively. Fibre Channel traffic over Ethernet is transparent to the operating system of the server. It operates as a Small Computer System Interface (SCSI) Initiator running over FCoE acting as if the server were connected over native Fibre Channel. In the following setup, you enable the Cisco UCS C-Series server to make use of FCoE capabilities.
This is done by configuring vNICs and vHBAs, which enables the server to pass Ethernet and Fibre Channel traffic. With the help of adapter virtualization (network interface virtualization), it is possible to create multiple Ethernet and Fibre Channel adapters. Through Peripheral Component Interconnect Express (PCIe) virtualization, the adapter shows multiple Ethernet and Fibre Channel adapters to the server. The server can scan the PCIe bus and can find all the virtual adapters that have been provisioned.

Procedure 1  Configure vNICs

Step 1: In the CIMC console navigation pane, click the Server tab, and then click Inventory.

Step 2: On the Cisco VIC Adapters tab, click the adapter.

Step 3: On the General tab in the tabbed menu below the Adapter Cards area, verify that FIP Mode is set to Enabled. If the FIP mode is not enabled, click Modify Adapter Properties, select Enable FIP Mode, and then click Save Changes. FIP mode ensures that the adapter is compatible with current FCoE standards.
Step 4: On the tabbed menu below the Adapter Card area, click the **vNICs** tab. In the Host Ethernet Interfaces area, select a vNIC from the table.

![Adapter Card with vNICs tab](image)

Step 5: Click **Properties**. The vNIC Properties dialog box appears.

![vNIC Properties dialog box](image)

Most single operating system installations that have been installed directly on a server use a single VLAN for server-to-network operation. For a server environment where multiple VLANs will need to be available to the operating system, as is the case for VMware ESXi, you use a VLAN mode of Trunk.

Step 6: In the **VLAN Mode** list, choose **Trunk**.

The upstream data-center core switch ports to which the two physical ports of the Cisco UCS P81E VIC or Cisco UCS VIC 1225 adapter are connected should also be configured to match the VLAN selection as either a single VLAN or trunk ports. VLAN trunks on the adapter card carry traffic from all VLANs by default. The upstream data center core switch typically has VLAN-1 as the native VLAN by default.

Step 7: If you are not passing any data traffic on VLAN-1 to the host, leave **Default VLAN** set to **NONE**.

Step 8: Repeat Step 4 through Step 7 for the second vNIC, and ensure that the vNIC properties are the same as you set in Step 6 and Step 7.
Procedure 2  Configure vHBAs

The Cisco UCS VIC 1225 and Cisco UCS P81E VIC converged network adapters include two physical 10-Gigabit Ethernet ports and have two vHBAs created by default. The two vHBAs labeled as fc0 and fc1 are connected to the upstream data-center core switches Cisco Nexus 5500-A and Nexus 5500-B, respectively, as configured in the Data Center Technology Design Guide. VSAN allows logical partitioning of the physical SAN infrastructure. It is recommended that you dedicate a separate VLAN for FCoE traffic corresponding to each VSAN. The following table shows the FCoE VLAN for each VSAN as was set up in the Data Center Technology Design Guide.

Table 8 - Data center core switch VSAN and FCoE VLAN values

<table>
<thead>
<tr>
<th>Data center core switch</th>
<th>VSAN</th>
<th>FCoE VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Nexus 5500-A</td>
<td>4</td>
<td>304</td>
</tr>
<tr>
<td>Cisco Nexus 5500-B</td>
<td>5</td>
<td>305</td>
</tr>
</tbody>
</table>

FCoE Initialization Protocol (FIP) is the control plane protocol used to establish the FCoE virtual link between the Ethernet-attached Fibre Channel node and the FCoE switch. FIP performs FCoE VLAN discovery by sending untagged frames to its neighbor. It provides a way for the host to log into and log out from the FCoE switch. Note that FIP VLAN discovery is not supported by Linux or VMware ESX server. Because of this, the FCoE VLAN has to be configured on the vHBA from the CIMC console. More details about the Fibre Channel and FCoE setup can be found in the Data Center Technology Design Guide.

Step 1: In the Adapter Cards area, select the available adapter card.

![Adapter Card 1](image)

Step 2: On the tabbed menu below the Adapter Card area, click the vHBAs tab, and in the Host Fibre Channel Interfaces area, select the vHBA labeled fc0 from the table, and then click Properties.
Step 3: In the Default VLAN field, select the second option button, and then enter the FCoE VLAN, which in this case is VLAN 304 (as shown in Table 8 earlier in this procedure).

Step 4: Click Save Changes.

Step 5: In the Host Fibre Channel Interfaces area, select the vHBA labeled as fc1 from the table, and then click Properties.

Step 6: In the Default VLAN field, select the second option button, and then enter the FCoE VLAN, which in this case is VLAN 305. This value must match with the FCoE VLAN configured in the upstream connected switch.

Step 7: Click Save Changes.

Step 8: In the navigation pane, click the Server tab, click Summary, and then in the work pane, under Actions, click Power Cycle Server. You must reboot the server for changes to take effect.
Step 9: On the “Power cycle the server?” message, click OK.

After the server reboots, it is ready to have an operating system installed.

Reader Tip
How to configure a VMware environment is explained in detail in the Virtualization with Cisco UCS, Nexus 1000V, and VMware Technology Design Guide.

Integrating Cisco UCS C-Series into the Cisco UCS Manager Environment

1. Connect Cisco Nexus 2232PP FEX
2. Configuring single-wire management
3. Configuring dual-wire management
4. Associate service profile to server

The previous process for the Cisco UCS C-Series prepared the server for connectivity directly to the Cisco Nexus 2000 Series Fabric Extenders and Nexus 5000 Series Switches data center foundation, where the C-Series server would be managed as a standalone device. This section describes deploying infrastructure to allow the C-series server to connect to the fabric interconnects of the Cisco UCS B-Series environment and to allow you to manage both the B-Series and C-Series servers from Cisco UCS Manager and transport traffic through the Fabric Interconnect.

Reader Tip
Details on supported Cisco UCS C-Series servers and network adapter cards for Cisco UCS integration, as well as the installation instructions for your specific C-Series server, can be found at: http://www.cisco.com/en/US/products/ps11736/products_installation_and_configuration_guides_list.html
This design guide is using Cisco UCS Manager Release 2.2(1d). With UCS Manager Release 2.1(1a) and later, there are now two modes of managing the UCS C-Series server connected to the fabric interconnects:

- **Single-wire-management**—Requires the Cisco UCS VIC1225 Virtual Interface Card, which can carry both data traffic and management traffic on the same interface cable. The Cisco UCS VIC 1225 is supported on the Cisco UCS C-Series M3 model servers and select M2 model servers.

- **Dual-wire-management**—Is supported in the Cisco UCS Manager release 2.1 and earlier releases. Shared LAN on Motherboard (LOM) ports on the rack server are used exclusively for carrying management traffic. A separate cable connected to one of the ports on the PCIe card or Cisco UCS P81E Virtual Interface Card carries the data traffic. The Cisco UCS VIC 1225 supports dual-wire-management as well.

The Cisco UCS C-Series servers connect to the UCS Fabric Interconnects via Cisco Nexus 2232PP Fabric Extenders (FEX), as shown in Figure 10. For dual-wire management, the C-Series server requires four connections to the FEX: two management links and two data traffic links. For single-wire management, the C-Series server requires only two connections, one to each FEX. The Nexus 2232PP FEX allows higher-density server connectivity and can support both data and management traffic flows to the fabric. In this design, the Nexus 2232PP FEX can connect up to 32 UCS C-Series servers by using single-wire management, or 16 UCS C-Series servers by using dual-wire management.

*Figure 10 – Cisco UCS C-Series server to UCS Fabric connection details*

The quantity of FEX to fabric uplinks must be equal to or greater than the minimum number of links specified in the Chassis Discovery Policy set in Step 3 of the “Configure fabric-to-I/O-module links” procedure earlier in this guide.
**Procedure 1** Connect Cisco Nexus 2232PP FEX

**Step 1:** Connect FEX uplink ports to fabric interconnects, as follows:

- Connect FEX-A uplinks p1 through p4 to Fabric Interconnect-A (FI-A).
- Connect FEX-B uplinks p1 through p4 to Fabric Interconnect-B (FI-B).

You can use up to 8 FEX uplinks to a fabric interconnect for maximum throughput, and a minimum of 2 is required for the Chassis Discovery Policy set in Step 3 of the “Configure fabric-to-I/O-module links” procedure earlier in this guide. It is recommended that for maximum virtual NIC scalability, that a FEX connect to the fabric interconnect with all FEX uplink ports included in a group of 8 fabric interconnect ports; that is all FEX uplink ports connect to fabric interconnect ports 1-8, or 9-16, or 17-24, etc.

**Tech Tip**

The number of vNICs and vHBAs that can be defined on virtual interface cards in the servers connected to the FEX is dependent on the number of uplinks and the connectivity to the fabric interconnect. For more information see: [http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c-series_integration/ucsm2-2/b_C-Series-Integration_UCSM2-2/b_C-Series-Integration_UCSM2-2_chapter_01.html#reference_7F381038303B4825ACD303765905086A](http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c-series_integration/ucsm2-2/b_C-Series-Integration_UCSM2-2/b_C-Series-Integration_UCSM2-2_chapter_01.html#reference_7F381038303B4825ACD303765905086A)

**Step 2:** Using a browser, access the cluster IP address **10.4.63.31** that you assigned during initial setup in Procedure 3 “Complete initial fabric interconnect setup” of the “Completing the Initial System Setup” process, and then choose **Launch**. The Cisco UCS Manager Java application downloads.

**Step 3:** In the navigation pane, click the **Equipment** tab, and then expand **Fabric Interconnects > Fabric Interconnect A > Fixed Module > Ethernet Ports**.

Objects are displayed representing each of the physical ports on the base fabric interconnect system. This deployment uses ports 13, 14, 15 and 16 of fabric interconnect ports to FEX.
Step 4: Right-click the selected port or group of ports, and then choose Configure as Server Port.

Step 5: On the “Successfully Configured...” message, click OK.

Step 6: Repeat Step 3 and Step 4 on Fabric Interconnect B.

Step 7: Connect power to FEX-A and FEX-B.

Step 8: In the navigation pane, expand Equipment > Rack-Mounts > FEX. The Cisco Nexus 2232PP FEXs should appear with automatically generated FEX numbering. In the screen below the new FEXs are FEX 3 and FEX 4.

It will take a few minutes for the FEX to power up, download software from the fabric interconnect, and report to the system. If you click a FEX, the status in the work pane should appear as Operable.
**Procedure 2  Configuring single-wire management**

If you are configuring for dual-wire-management, you can skip this procedure and proceed to the next procedure.

Single-wire-management requires the Cisco UCS VIC 1225, which can carry both data traffic and management traffic on the same interface cable. The Cisco UCS VIC 1225 is supported on the Cisco UCS C-Series M3 model servers and select M2 model servers. You must ensure that the Cisco UCS C-Series server CIMC settings are set to factory default prior to attempting single-wire management integration.

In this deployment, you connect one of the Cisco UCS VIC 1225 adapter 10-Gb Ethernet interfaces to each FEX, FEX-A and FEX-B, deployed in Procedure 1, as shown in Figure 10.

**Step 1:** Connect a 10-Gb Small Form-Factor Pluggable Plus (SFP+) cable between the 10-Gb adapter card Port 1 in the server and a port on FEX-A. You can use any port on the FEX.

**Step 2:** Connect a 10-Gb SFP+ cable between the 10-Gb adapter card Port 2 in the server and a port on FEX-B. You can use any port on the FEX.

**Step 3:** Power on or reboot the server. Cisco UCS Manager dynamically discovers the server.

**Step 4:** In the navigation pane, expand **Equipment > Rack-Mounts > Servers**. Server 1 is listed.

**Step 5:** Click **Server 1**. The connectivity for the Cisco UCS C-Series Server 1 is shown in the work pane.
Step 6: Click the General tab. The operational status and the properties of the physical Server 1 are displayed.

**Procedure 3** Configuring dual-wire management

Dual-wire-management is supported in the Cisco UCS Manager release 2.1 and releases earlier than 2.1, which meets the adapter card and Cisco UCS C-Series server requirements. Shared LAN on Motherboard (LOM) ports on the rack server are used exclusively for carrying management traffic. A separate cable connected to one of the ports on the PCIe card or Cisco UCS P81E Virtual Interface Card carries the data traffic. You must ensure that the Cisco UCS C-Series server CIMC settings are set to factory default prior to attempting dual-wire management integration.

**Reader Tip**

For more information about dual-wire-management and support on releases prior to Cisco UCS Manager 2.2, please see: http://www.cisco.com/en/US/products/ps11736/products_installation_and_configuration_guides_list.html

In this procedure, you connect the Cisco UCS C-Series server management traffic path to FEX-A and FEX-B that you deployed in Procedure 1, as shown in Figure 10. In Step 1 and Step 2, you must use Cisco UCS C-Series Ethernet LOM ports for server management traffic, and not the CIMC management ports.

Step 1: Insert one GLC-T transceiver into a port of FEX-A. You can use any port on the FEX. Connect an RJ-45 Ethernet cable between the 1-Gb Ethernet LOM port Eth 1 on the rear panel of the server and the transceiver that you inserted in FEX-A.
Step 2: Insert one GLC-T transceiver into a port of FEX-B. You can use any port on the FEX. Connect an RJ-45 Ethernet cable between the 1-Gb Ethernet LOM port Eth 2 on the rear panel of the server and the transceiver that you inserted in FEX-B.

Next, connect the data traffic path to FEX-A and FEX-B that you deployed in Procedure 1, as shown in Figure 10.

Step 3: Connect a 10-Gb Small Form-Factor Pluggable Plus (SFP+) cable between the 10-Gb adapter card Port 1 in the server and a port on FEX-A. You can use any port on the FEX.

Step 4: Connect a 10-Gb SFP+ cable between the 10-Gb adapter card Port 2 in the server and a port on FEX-B. You can use any port on the FEX.

Step 5: Power on or reboot the server. Cisco UCS Manager dynamically discovers the server.

Step 6: In the navigation pane, expand Equipment > Rack-Mounts > Servers. Server 2 is listed.

Step 7: Click the server (Example: Server 2). The connectivity for the Cisco UCS C-Series Server 2 is shown in the work pane.
Step 8: Click the General tab. The operational status and the properties of the physical Server 2 are displayed.

![Cisco UCS C-Series server integration to Cisco UCS Manager environment](image)

**Procedure 4**  
**Associate service profile to server**

You can now attach a previously defined service profile to the Cisco UCS C-Series server the same way you are able to do with a Cisco UCS B-Series server, as detailed in Procedure 2, “Associate server to service profile.”

**Step 1:** In the work pane, click the General tab, and then, in the Actions field, click Associate Service Profile.

**Step 2:** Select a service profile for your server from the list of available service profiles, and then click OK. The physical server blade boots up with the assigned service profile.

![Associate Service Profile](image)

This completes the Cisco UCS C-Series server integration to Cisco UCS Manager environment. You can now build and assign profiles for C-Series servers the same way as a B-Series server, as detailed earlier in this guide.
## Data Center Core

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product Description</th>
<th>Part Numbers</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Switch</td>
<td>Cisco Nexus 5596 up to 96-port 10Gbe, FCoE, and Fibre Channel SFP+</td>
<td>N5K-C5596UP-FA</td>
<td>NX-OS 7.0(2) N1(1) Layer 3 License</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 5596 Layer 3 Switching Module</td>
<td>N55-M160L30V2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 5548 up to 48-port 10Gbe, FCoE, and Fibre Channel SFP+</td>
<td>N5K-C5548UP-FA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 5548 Layer 3 Switching Module</td>
<td>N55-D160L3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 5500 Layer 3 Enterprise Software License</td>
<td>N55-LAN1K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 5500 Storage Protocols Services License, 8 ports</td>
<td>N55-8P-SSK9</td>
<td></td>
</tr>
<tr>
<td>Ethernet Extension</td>
<td>Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T (enhanced) Fabric Extender</td>
<td>N2K-C2248TP-E</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T Fabric Extender</td>
<td>N2K-C2248TP-1GE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 2000 Series 32 1/10 Gbe SFP+, FCoE capable Fabric Extender</td>
<td>N2K-C2232PP-10GE</td>
<td></td>
</tr>
</tbody>
</table>

## Computing Resources

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product Description</th>
<th>Part Numbers</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCS Fabric Interconnect</td>
<td>Cisco UCS up to 96-port Fabric Interconnect</td>
<td>UCS-FI-6296UP</td>
<td>2.2(1d) Cisco UCS Release</td>
</tr>
<tr>
<td></td>
<td>Cisco UCS up to 48-port Fabric Interconnect</td>
<td>UCS-FI-6248UP</td>
<td></td>
</tr>
<tr>
<td>UCS B-Series Blade Servers</td>
<td>Cisco UCS Blade Server Chassis</td>
<td>N20-C6508</td>
<td>2.2(1d) Cisco UCS Release</td>
</tr>
<tr>
<td></td>
<td>Cisco UCS 8-port 10GbE Fabric Extender</td>
<td>UCS-IOM2208XP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco UCS 4-port 10GbE Fabric Extender</td>
<td>UCS-IOM2204XP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco UCS B200 M3 Blade Server</td>
<td>UCSB-B200-M3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco UCS B250 M2 Blade Server</td>
<td>N20-B6625-2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco UCS 1280 Virtual Interface Card</td>
<td>UCS-VIC-M82-8P</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco UCS M81KR Virtual Interface Card</td>
<td>N20-AC0002</td>
<td></td>
</tr>
<tr>
<td>UCS C-Series Rack-mount Servers</td>
<td>Cisco UCS C220 M3 Rack Mount Server</td>
<td>UCSC-C220-M3S</td>
<td>2.0(1a) Cisco UCS CIMC Release</td>
</tr>
<tr>
<td></td>
<td>Cisco UCS C240 M3 Rack Mount Server</td>
<td>UCSC-C240-M3S</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco UCS C460 M2 Rack Mount Server</td>
<td>UCSC-BASE-M2-C460</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco UCS 1225 Virtual Interface Card Dual Port 10Gb SFP+</td>
<td>UCSC-PCI-E-CSC-02</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco UCS P81E Virtual Interface Card Dual Port 10Gb SFP+</td>
<td>N2XX-ACPCI01</td>
<td></td>
</tr>
</tbody>
</table>
Appendix B: Changes

This appendix summarizes the changes Cisco made to this guide since its last edition.

- We updated the following software:
  - Cisco NX-OS 7.0(2)N1(1) on the Cisco Nexus 5500 Series Switches
  - Cisco UCS Release 2.2(1d) on the Cisco UCS 6200 Series Fabric Interconnects
  - Cisco UCS Release 2.2(1d) on the Cisco UCS B-Series Blade Servers
  - Cisco UCS CIMC 2.0(1a) on the Cisco UCS C-Series Rack-Mount Servers
Feedback

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