Newer Cisco SBA Guides Available

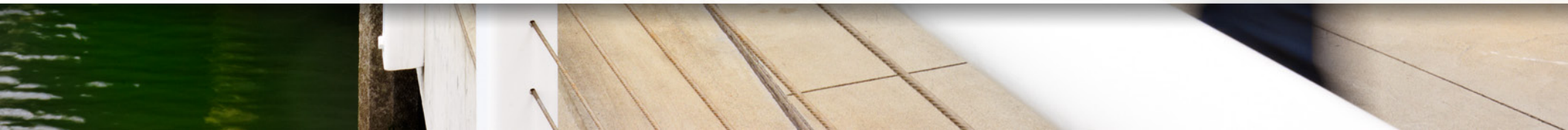
This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to http://www.cisco.com/go/sba

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

Unified Computing System Deployment Guide

SMART BUSINESS ARCHITECTURE

February 2012 Series



Preface

Who Should Read This Guide

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

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

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

Release Series

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

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

month year Series

For example, the series of guides that we released in August 2011 are the "August 2011 Series".

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

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

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

How to Read Commands

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

Commands to enter at a CLI appear as follows:

```
configure terminal
```

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

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

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

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

```
Router# enable
```

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

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

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

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

Comments and Questions

If you would like to comment on a guide or ask questions, please use the forum at the bottom of one of the following sites:

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

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

An RSS feed is available if you would like to be notified when new comments are posted.

Table of Contents

What's In This SBA Guide

About SBA

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

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

For more information, see the *How to Get Started with Cisco SBA* document:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/SBA_Getting_Started.pdf

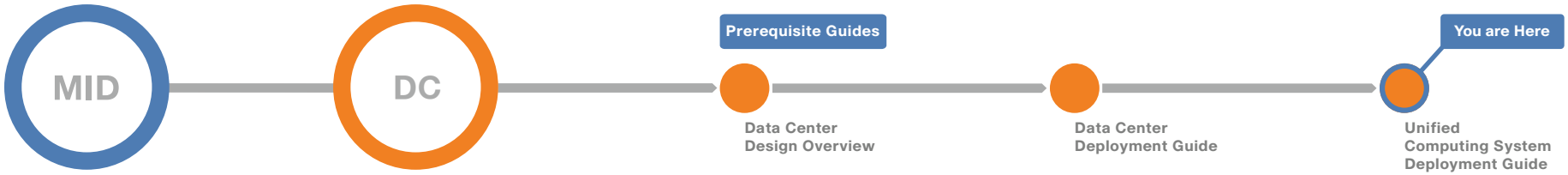
About This Guide

This *additional deployment guide* includes the following sections:

- **Business Overview**—The challenge that your organization faces. Business decision makers can use this section to understand the relevance of the solution to their organizations' operations.
- **Technology Overview**—How Cisco solves the challenge. Technical decision makers can use this section to understand how the solution works.
- **Deployment Details**—Step-by-step instructions for implementing the solution. Systems engineers can use this section to get the solution up and running quickly and reliably.

To learn what changed in this guide between the previous series and the current series, see Appendix B: Changes.

This guide presumes that you have read the prerequisites guides, as shown on the Route to Success below.



Route to Success

To ensure your success when implementing the designs in this guide, you should read any guides that this guide depends upon—shown to the left of this guide on the route above. Any guides that depend upon this guide are shown to the right of this guide.

For customer access to all SBA guides: http://www.cisco.com/go/sba
For partner access: http://www.cisco.com/go/sbachannel

Introduction

This *Unified Computing System Deployment Guide* for the midsize organization builds upon the foundation laid out in the *Cisco® SBA for Midsize Organizations—Data Center Deployment 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 and Fibre Channel connections between the UCS B-Series Blade Server system and the data center core network deployed in the *Data Center Deployment Guide*.
- The 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 (UCSM) 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 (Cisco IMC) 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 using converged network adapters that add flexibility to server connectivity, and reduce cabling and complexity.
- The Appendix provides the complete list of products used in the lab testing of this architecture, as well as the software revisions used on the products and a list of major changes since the last edition of this guide.

Business Overview

As a midsize 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 midsize data center. 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 a midsize organization, 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 to reduce operational requirements, yet flexible to accommodate the different requirements of applications and the operating system.

Application availability is key to an organization. Users depend on reaching the systems and information that are required to run the business just as much as they depend on having lights in the office or a power outlet to plug in a PC.

Technical Overview

Consistent with the SBA approach, Cisco offers a simplified reference model for managing a small server room as it grows into a full-fledged data center. This model benefits from the ease of use offered by the Cisco Unified Computing System. This guide has been lab-tested in conjunction with the architecture defined in the *Cisco SBA for Midsize Organizations—Data Center Deployment Guide*, available at: www.cisco.com/go/sba.

This guide addresses many of the same business issues encountered by growing organizations that are identified in the *Cisco SBA for Midsize Organizations—Data Center Deployment Guide* but it focuses on the server resources themselves and their interaction with network and storage systems.

Application Growth

The Cisco SBA 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 SBA 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 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.

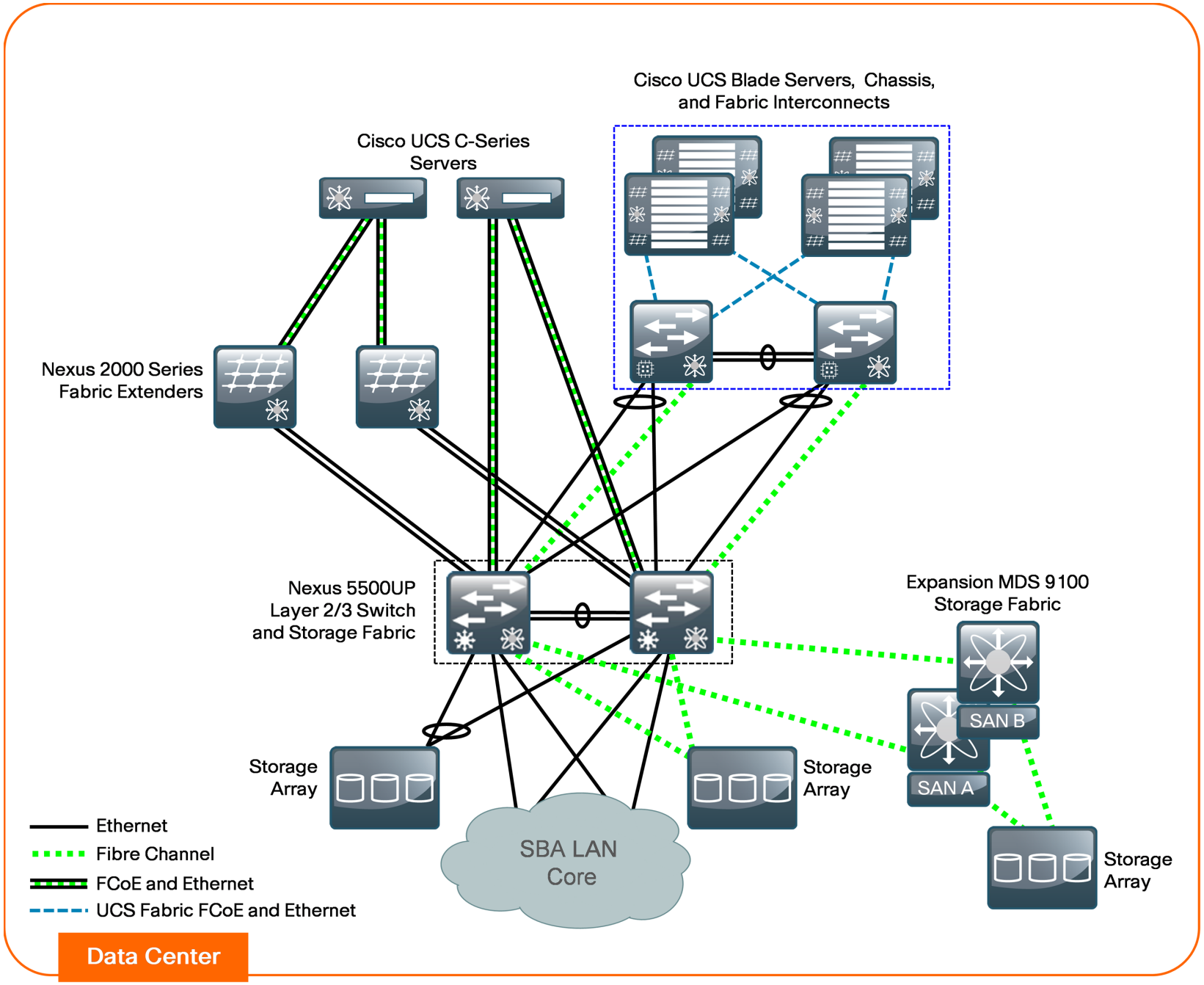
The architecture of the Cisco SBA Unified Computing System model is optimized to support the use of hypervisor-based systems or the direct installation of a base operating system such as Windows or Linux. The service profile structure of Cisco UCS, along with a centralized storage model, allows you the portability of server definitions to different hardware with or without a hypervisor system in place. Built on the data center infrastructure foundation defined in the *Cisco SBA for Midsize Organizations—Data Center Deployment Guide*, the SBA 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 Cisco SBA data center foundation has been designed to ensure availability with the use of resilient network devices, links, and service models. The Cisco SBA 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 SBA Unified Computing System architecture



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

Ethernet Foundation

The *Cisco SBA Unified Computing System Deployment Guide* is designed as an extension of the *Cisco SBA for Midsize Organizations—Data Center Deployment Guide*. The basis of the Cisco SBA 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 SBA 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 midsize data center for a resilient, virtualized computing environment.

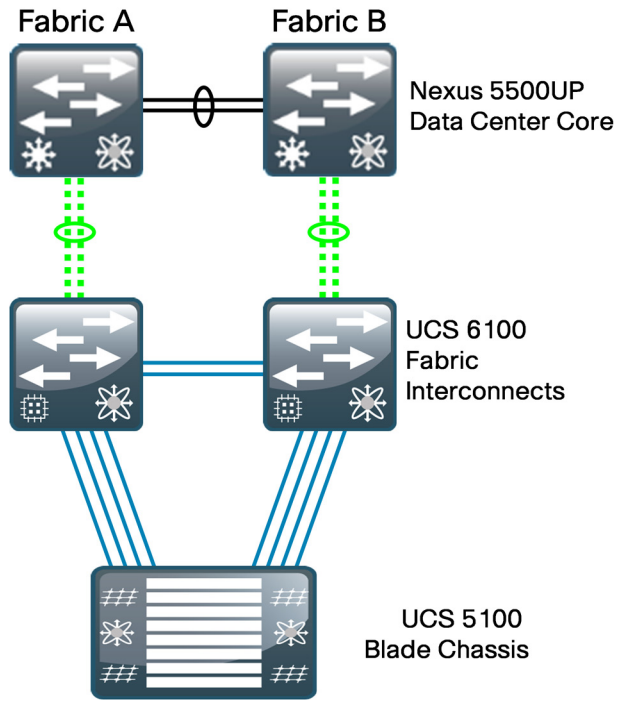
Storage Networking

The Cisco SBA 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 6100 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.

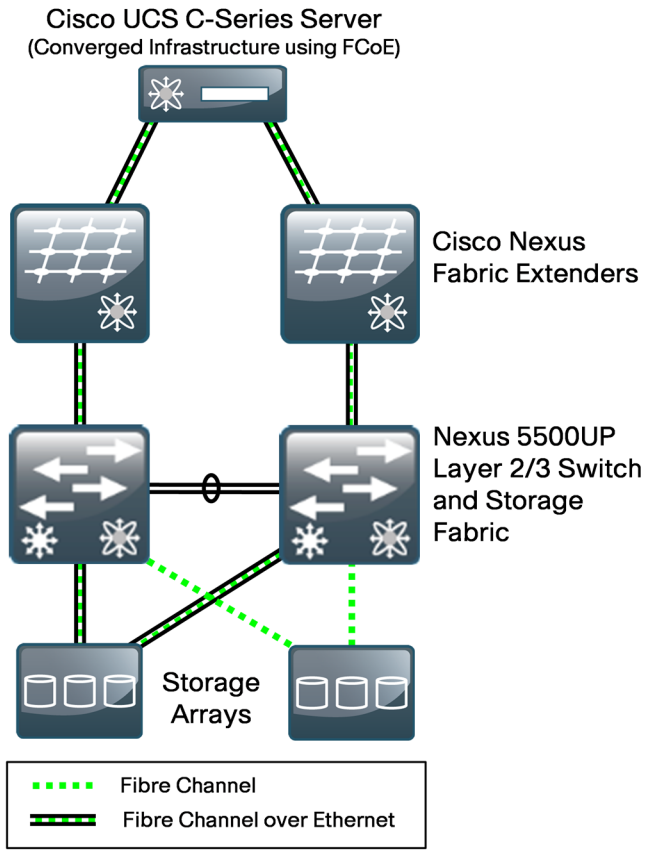
Figure 2 - Cisco UCS 6100 fabric interconnect to core SAN



On the Cisco UCS fabric interconnect, the Fibre Channel ports that connect to the Cisco MDS 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 only supported in a more limited deployment and is not covered in this guide.

You can connect the Cisco UCS C-Series Rack-Mount Servers to the Fibre Channel SAN using dedicated host bus adapters (HBAs) that attach directly to the SAN switches. Alternately, 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 3 - Cisco UCS C-Series server to core SAN 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 SBA 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 this 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.

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 6100 Series Fabric Interconnect—The Cisco UCS fabric interconnects provide both network connectivity and management capabilities to the other components in the system. The fabric interconnects are typically clustered together as a pair, providing resilient management access—as well as 10-Gb Ethernet, Fibre Channel, and FCoE capabilities—to the system.
- Cisco UCS 2100 Series Fabric Extender—The Cisco UCS 2100 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 2.0(1), up to twenty Cisco UCS 5100 Series Blade Server Chassis may be connected to and managed as one system by a single pair of fabric interconnects.

- 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 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 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 128 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, and version of UCSM.

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

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 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 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 like extended memory and network-aware VN-Link technologies.

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

Third-Party Computing Systems

Third-party rack server and blade server systems may also be connected to the Cisco SBA 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 Cisco SBA 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 B-Series Blade 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.

Notes

Deploying the SBA Unified Computing System Architecture

The following sections provide detailed, step-by-step instructions to configure the basic elements of the Cisco SBA 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 Cisco SBA midsize foundation data center core network infrastructure for the Cisco SBA Unified Computing System topology is based on the *Cisco SBA for Midsize Organizations—Data Center Deployment Guide*. The following Ethernet and Fibre Channel 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 SBA midsize 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.

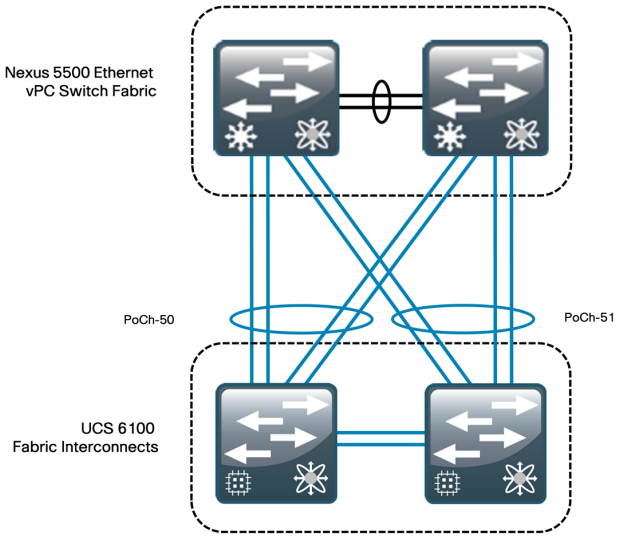
Process

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 6100 Series Fabric Interconnects to appear as a group of end-node servers to the data center Ethernet switching fabric. In the Cisco SBA 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 6100 Series 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.



Tech Tip

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: Configure the physical interfaces to the port channels on each of the two Cisco Nexus 5500 switches, which will be configured in vPC mode:

```
interface Ethernet1/9
  description Link to FI-A eth1/17
  channel-group 50 mode active

interface Ethernet1/10
  description Link to FI-A eth1/18
  channel-group 50 mode active

interface Ethernet1/11
  description Link to FI-B eth1/17
  channel-group 51 mode active

interface Ethernet1/12
  description Link to FI-B eth1/20
  channel-group 51 mode active
```

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 2: Configure the port channels on the Cisco Nexus 5500 switches.

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

```
interface port-channel50
  switchport mode trunk
  switchport trunk allowed vlan 148-151,154-155,159-162
  spanning-tree port type edge trunk
  vpc 50

interface port-channel51
  switchport mode trunk
  switchport trunk allowed vlan 148-151,154-155,159-162
  spanning-tree port type edge trunk
  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 Nexus 5500 port type set to "normal" for standard Spanning Tree Protocol loop prevention.

The port-channel interfaces will not become active until you complete the corresponding configuration on the Cisco UCS 6100 Series fabric interconnects, which is covered in Procedure 2, "Define Ethernet uplink ports" in the "Configuring Communications Connections using UCS Manager" process.

Process

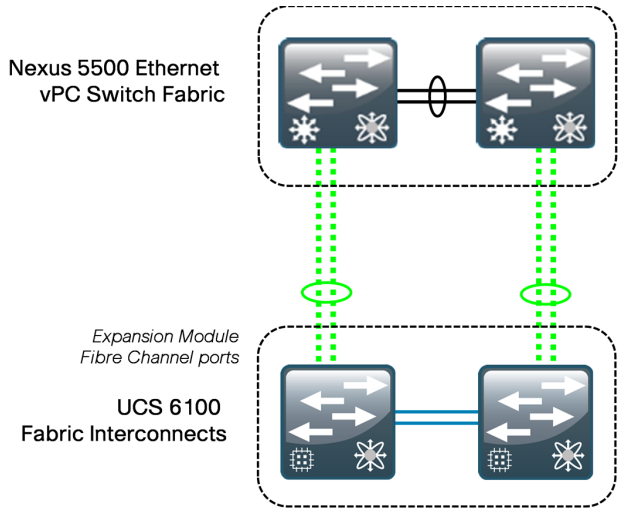
Configuring the Fibre Channel Network Infrastructure

1. Configure SAN port channels

Complete the following process to prepare the data center core Cisco Nexus 5500UP switches to support a Fibre Channel SAN connection to the UCS 6100 Series Fabric Interconnects. As of Cisco UCS Release 2.0(1t), the Cisco 6100 Series Fabric Interconnects support only a Gigabit Ethernet or 10–Gigabit Ethernet uplink connection, not FCoE, into the data center core switching fabric. Configuration instructions provided in this guide are based on the foundation of the Fibre Channel infrastructure in the *Cisco SBA for Midsize Organizations—Data Center Deployment Guide* topology.

Tech Tip

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.



Procedure 1 Configure SAN port channels

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 *Cisco SBA for Midsize Organizations—Data Center Deployment Guide.*

Step 1: Enable NPIV, Fibre Channel port channel trunking, and Fibre Channel/FCoE switching operation on each switch.

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

Step 2: Create a SAN port channel to connect to the fabric interface.

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 *Cisco SBA for Midsize Organizations—Data Center Deployment Guide.*

On the first data center core Cisco Nexus 5500UP switch:

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

On the second data center core Cisco Nexus 5500UP switch:

```
interface san-port-channel 29
channel mode active
switchport trunk mode off
switchport trunk allowed vsan 1
switchport trunk allowed vsan add 5
```

Step 3: Add the SAN port channels to an existing VSAN database.

On the first data center core Cisco Nexus 5500UP switch:

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

On the second data center core Cisco Nexus 5500UP switch:

```
vsan database
vsan 5 interface san-port-channel 29
```

Step 4: Configure the SAN port channel on physical interfaces.

The Fibre Channel ports on the Cisco Nexus 5500UP are set to negotiate speed by default. On each data center core Cisco Nexus 5500UP switch, configure the following:

```
interface fc1/29
switchport trunk mode off
channel-group 29 force
interface fc1/30
switchport trunk mode off
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 "Define Fibre Channel uplink" in the "Configuring Communications Connections using UCS Manager" process.

Cisco UCS B-Series Blade Server System

The Cisco UCS B-Series Blade Server system is the heart of the Cisco SBA 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.

Process

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 interconnect acts 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.

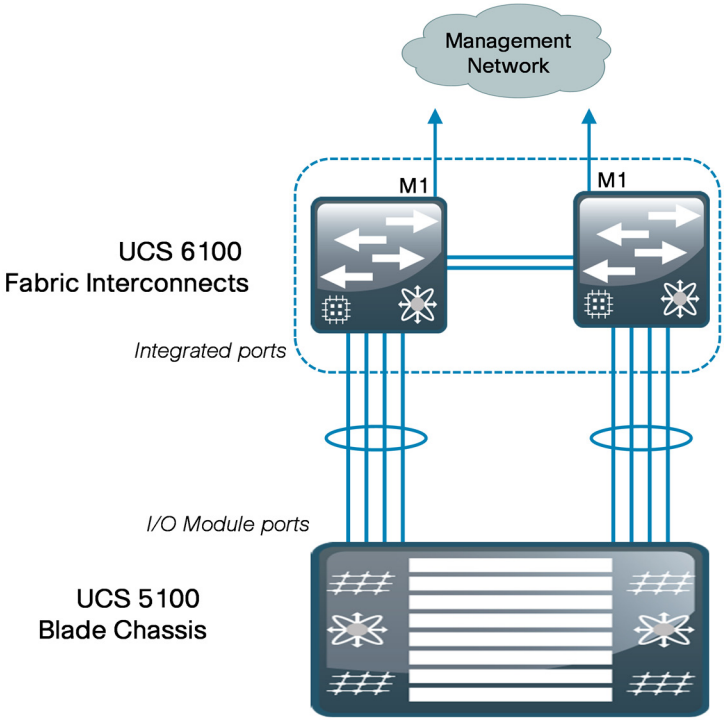
Step 2: Attach the Management Ethernet ports from each fabric interconnect to the out-of-band Ethernet management network created in the *Cisco SBA for Midsize Organizations—Data Center Deployment Guide* (or appropriate Ethernet segment) where they can be accessed for overall administration of the system.

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 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.

Tech Tip

You can connect the I/O modules to the fabric interconnects by using one, two, or four cables per module. For system resiliency and throughput, it is recommended that you use a minimum of two connections per I/O module.



Tech Tip

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. Expansion module ports on the 6100 Series fabric interconnects cannot be used as server facing ports.

Procedure 2 Configure management switch ports

In the *Cisco SBA for Midsize Organizations—Data Center Deployment 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 interface management ports, as described in this procedure.

Step 1: Configure the ports connected to UCS.

```
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 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 6100 Series 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": xxxxxxxx
Confirm the password for "admin": xxxxxxxx
```

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:  sba-ucs
```

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

```
Physical Switch Mgmt0 IPv4 address : 10.10.63.29
Physical Switch Mgmt0 IPv4 netmask : 255.255.255.128
IPv4 address of the default gateway : 10.10.63.1
Cluster IPv4 address : 10.10.63.31
Configure the DNS Server IPv4 address? (yes/no) [n]: n
Configure the default domain name? (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=sba-ucs
  Enforced Strong Password=yes
  Physical Switch Mgmt0 IP Address=10.10.63.29
  Physical Switch Mgmt0 IP Netmask=255.255.255.128
  Default Gateway=10.10.63.1

  Cluster Enabled=yes
  Cluster IP Address=10.10.63.31
  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 rebooted, 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:
  Connecting to peer Fabric interconnect... done
Retrieving config from peer Fabric interconnect...done
Peer Fabric interconnect Mgmt0 IP Address: 10.10.63.29
Peer Fabric interconnect Mgmt0 IP Netmask: 255.255.255.128
  Cluster IP address: 10.10.63.31
Physical Switch Mgmt0 IPv4 address : 10.10.63.30
Apply and save the configuration (select 'no' if you want to
re-enter)? (yes/no): yes
Applying configuration. Please wait.
Configuration file - Ok
```

Tech Tip

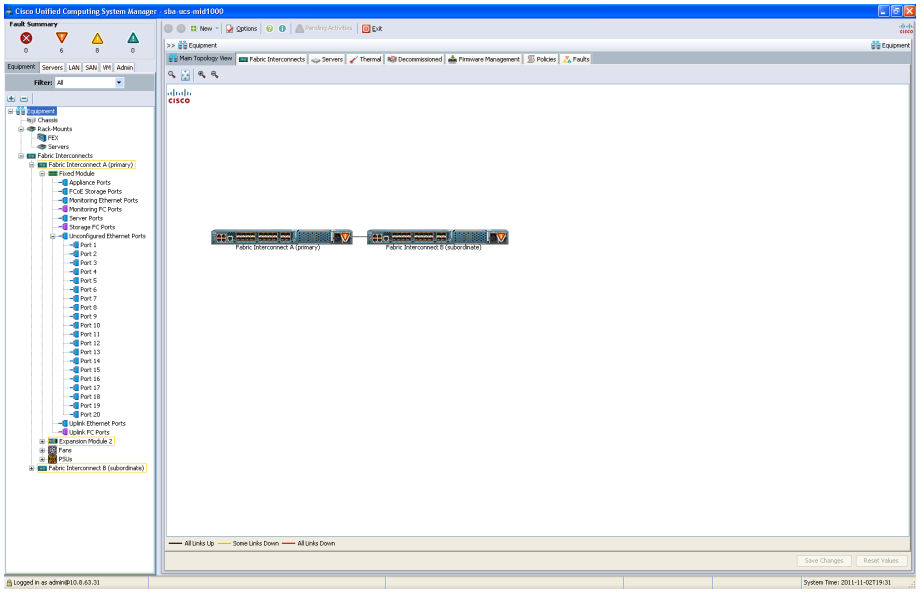
From this point forward, this guide primarily shows the use of the UCS Manager GUI for management of the system; however, you should become familiar with the console in case you need very low-bandwidth remote access or a separate mode of access for administrative tasks such as code upgrades or system troubleshooting.

Process

Configuring Communications Connections using UCS Manager

1. Configure fabric-to-I/O-module links
2. Define Ethernet uplink ports
3. Define Fibre Channel uplink ports
4. Add a management IP address pool

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.



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. Choose **Launch** to download the UCS Manager Java application.

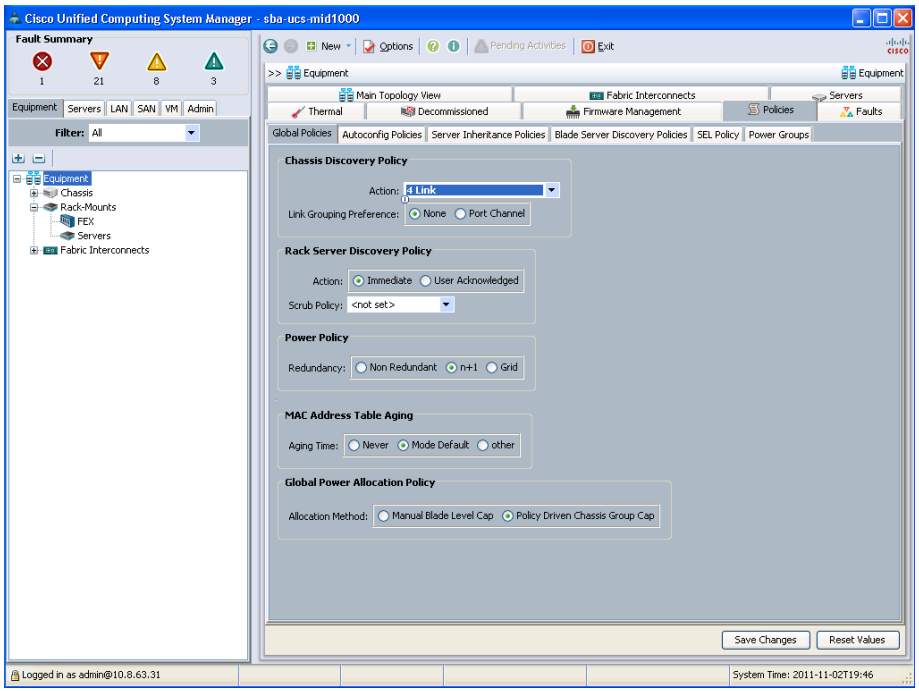
This example configuration uses 10.10.63.31 from the setup script. Authenticate by using the configured username and password, and view the initial screen.

Step 2: 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. This may be set at 1, 2, or 4 links per fabric, the default value is one.

Tech Tip

The Link Grouping Preference should be left at the default setting of None when using a 2104 model I/O module. Link Grouping Preference of Port Channel is only supported with the newer 2200 model I/O modules.

Step 3: 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.

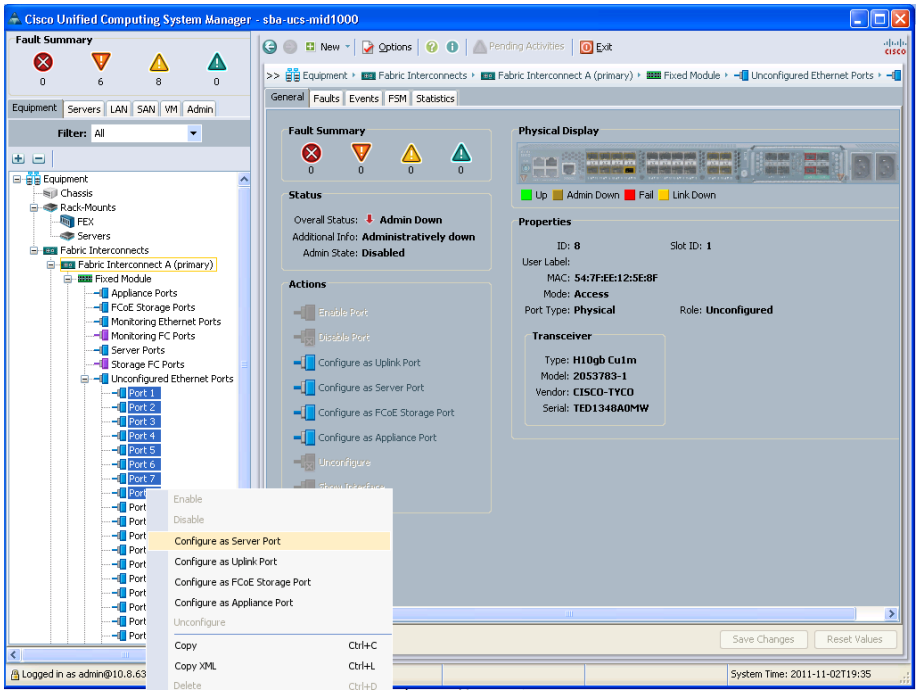


Step 4: In the navigation pane, click the **Equipment** tab, and then expand **Fabric Interconnects** > **Fabric Interconnect A** > **Fixed Module** > **Unconfigured Ethernet Ports**.

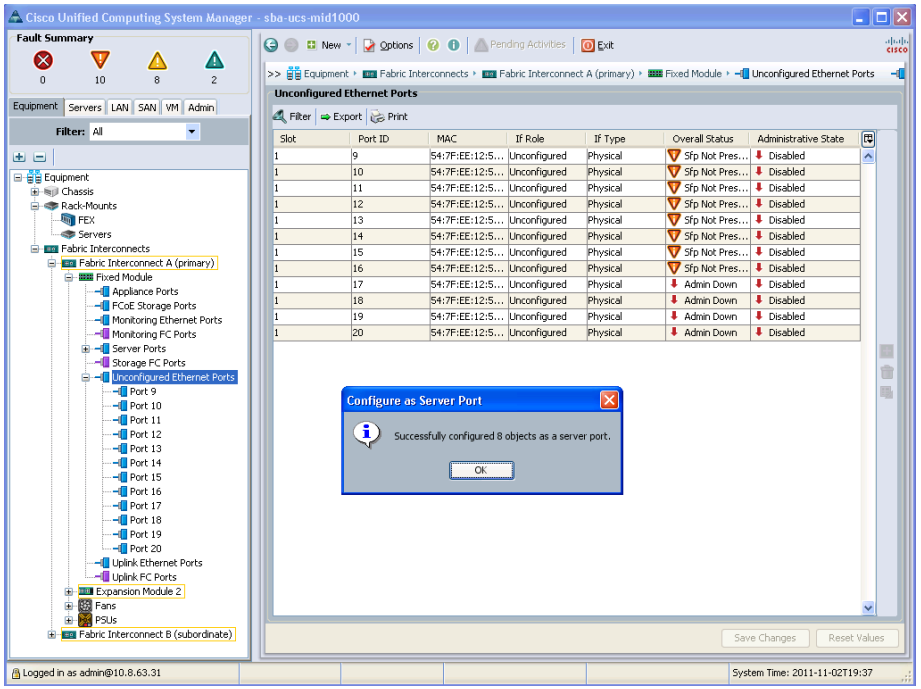
Objects are displayed representing each of the physical ports on the base fabric interconnect system.

Step 5: Choose the desired port by clicking the port object, or choose several sequential ports by clicking additional ports while pressing the **Shift** key.

Step 6: Right-click the selected port or group of ports, and then, choose **Configure as Server Port**

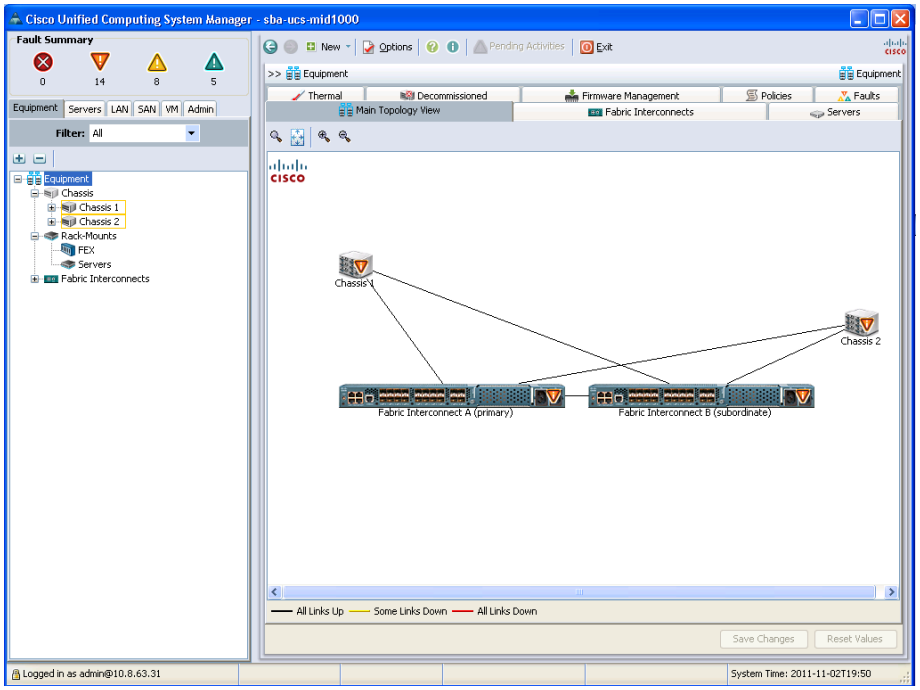


Step 7: On the "Successfully configured..." message, click **OK**.



Step 8: In the navigation pane, expand the tree to **Fabric Interconnect B**, and then follow Step 4 through Step 7 above 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, 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.

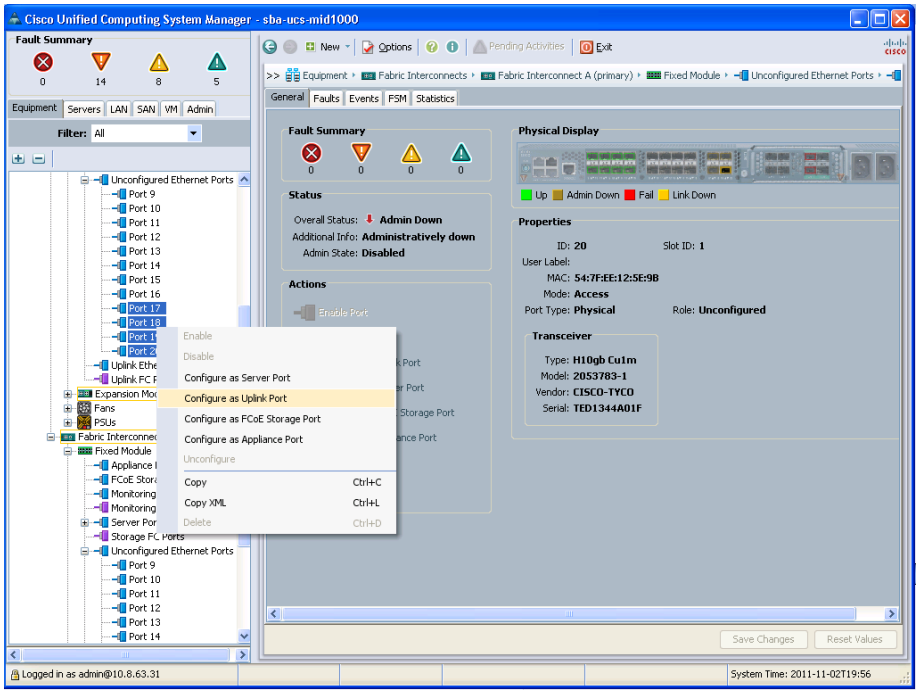


Procedure 2 Define Ethernet uplink ports

In the Cisco SBA 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/server traffic, server-to-server traffic between IP subnets, and Ethernet-based storage access such as iSCSI or NAS traffic. Ports from either the base fabric interconnects or expansion modules may be used as uplink ports.

Step 1: On the **Equipment** tab in the navigation pane, locate the ports that are physically connected to the upstream switches. These ports should initially be listed as unconfigured ports in the tree view.

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**.

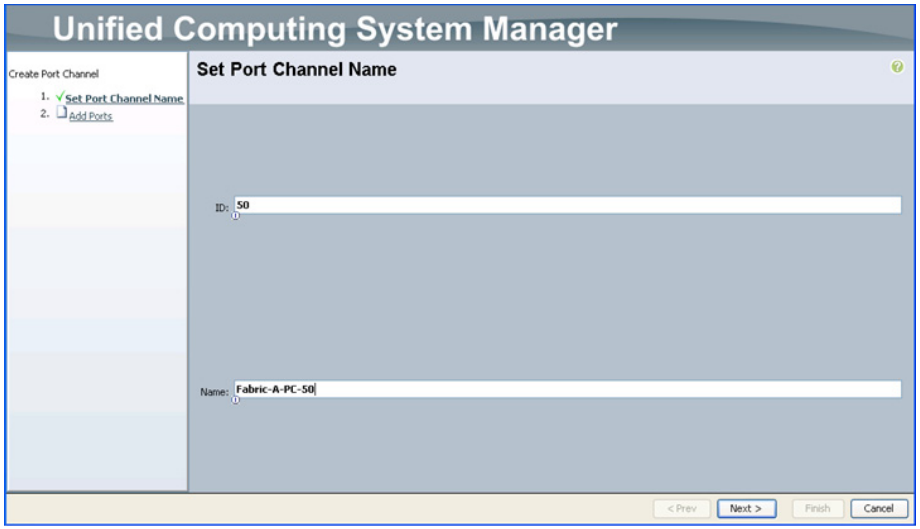


The SBA design implemented a port-channel configuration on the upstream Cisco Nexus 5500UP Series switches as described in the Procedure 1 "Configure Nexus 5500 port channels" earlier in this guide, You must perform similar port-channel configuration for the Ethernet uplink ports for the fabric interconnects.

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

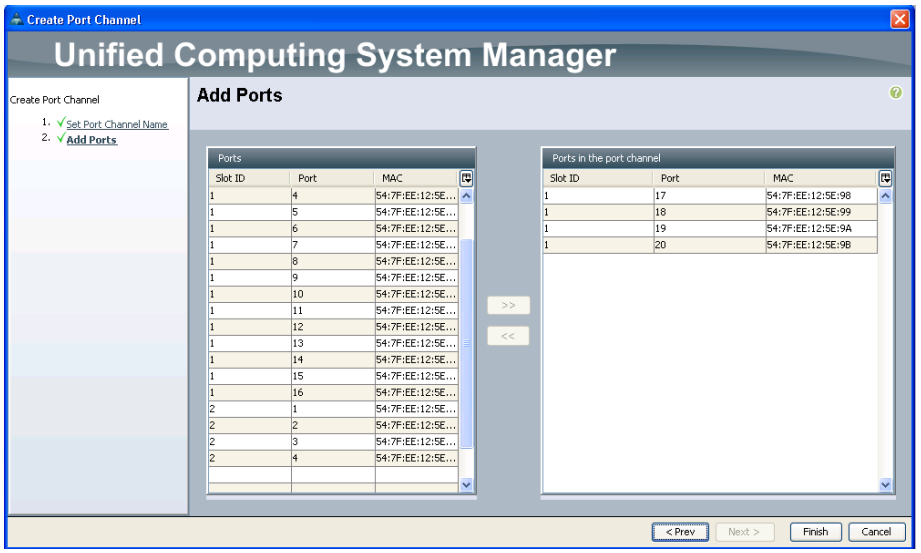
Step 4: Click **Add** (green plus sign).

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.



Tech Tip

Pay close attention to the Slot ID column when you select the ports to be added to the port channel. Integrated ports will be 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.

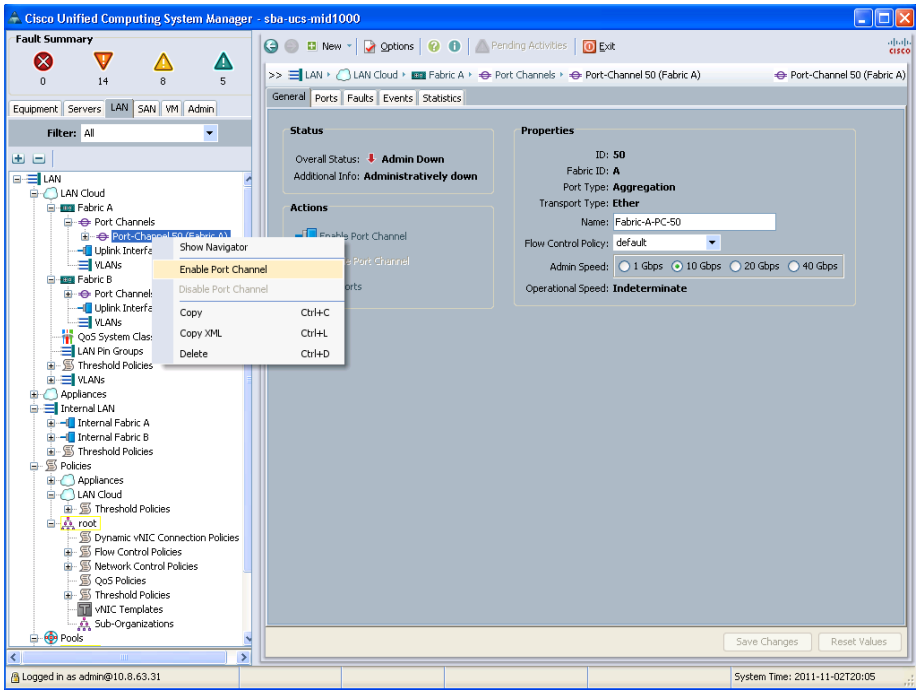
Step 8: Click **Finish**. This completes the creation of the Ethernet uplink port channel for Fabric A.

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.

After you have created the port channels, you must enable them before they will become active.

Step 10: In the navigation pane, expand **Port Channels**.

Step 11: For each port channel created above in both Fabrics A and B, choose and then right-click the port channel name, and then choose **Enable Port Channel**.



Tech Tip

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 configuration. In some cases, it may be beneficial for operational support to use consistent numbering for representation of these channels.

Procedure 3 Define Fibre Channel uplink ports

Fibre Channel uplink ports connect the fabric interconnects to the SAN, which in the Cisco SBA Unified Computing System reference topology is built by using the data center core Nexus 5500UP switches. In a larger SAN, you may also connect to Cisco MDS 9100 Series Switches. Fibre Channel uplink ports can also attach to a non-Cisco SAN switch, however guidance on that configuration is outside of the scope of this document.

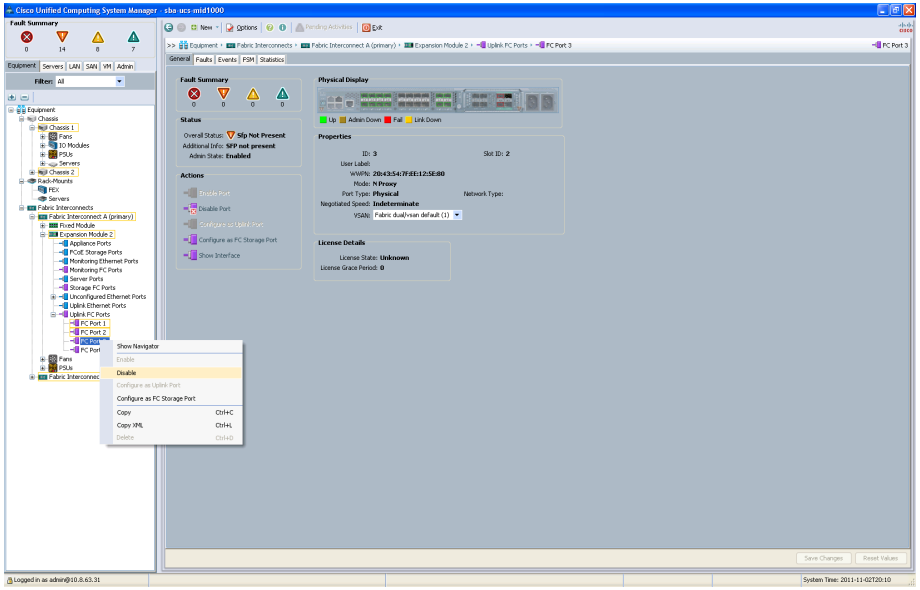
These links carry native Fibre Channel traffic to the SAN, and must be provisioned on expansion modules because there are no Fibre Channel ports on the base 6100 fabric interconnects. Because these ports can only be used as uplinks and not as server ports, they automatically appear in the Uplink FC Ports folder in the navigation pane underneath the fabric interconnect expansion modules. The Fibre Channel ports are enabled by default and will be configured as a SAN port-channel for added resilience, load balancing, and ease of adding additional links.

Tech Tip

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 procedure.

Step 1: Connect the desired ports from the Fibre Channel expansion module to the SAN.

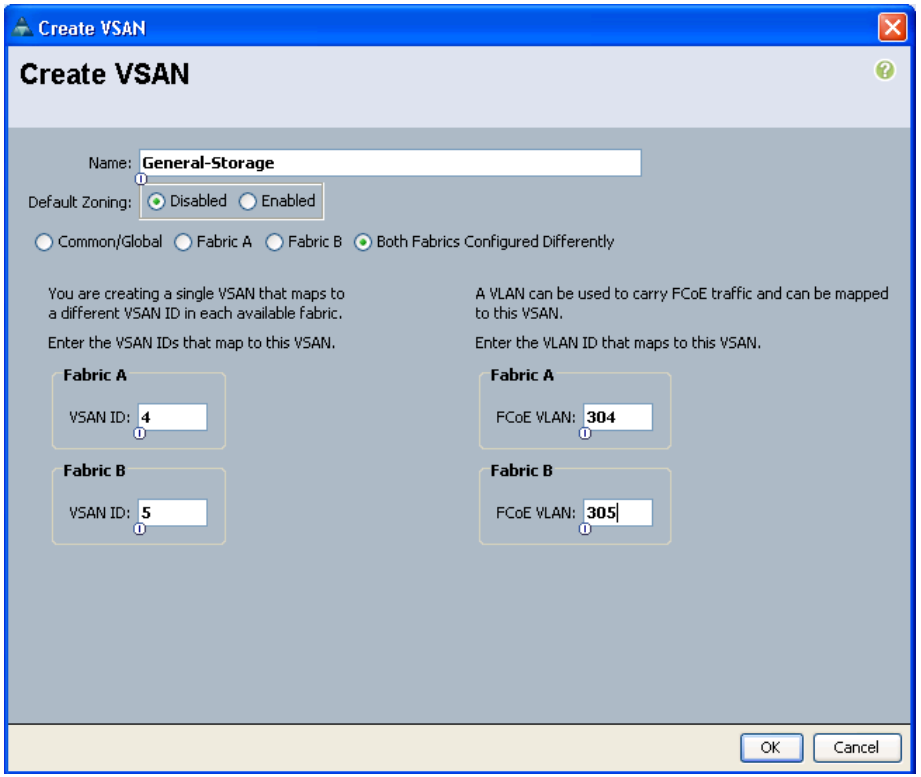
Step 2: Disable unused ports by right-clicking the port name in the navigation pane, and then choosing **Disable**. In this example, you disable ports 3 and 4. When you disable unused ports, you clear any system alerts tied to the unused ports in both fabric interconnects A and B.



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.

Step 3: In the navigation pane, click the **SAN** tab, and then expand **SAN** > **SAN Cloud** > **VSANs**.

Step 4: Right-click the **VSAN** container, and then choose **Create VSAN**.



Step 5: Enter a **Name** for the VSAN, leave the default value selected for **Default Zoning** as **Disabled**, and then select **Both Fabrics Configured Differently**.

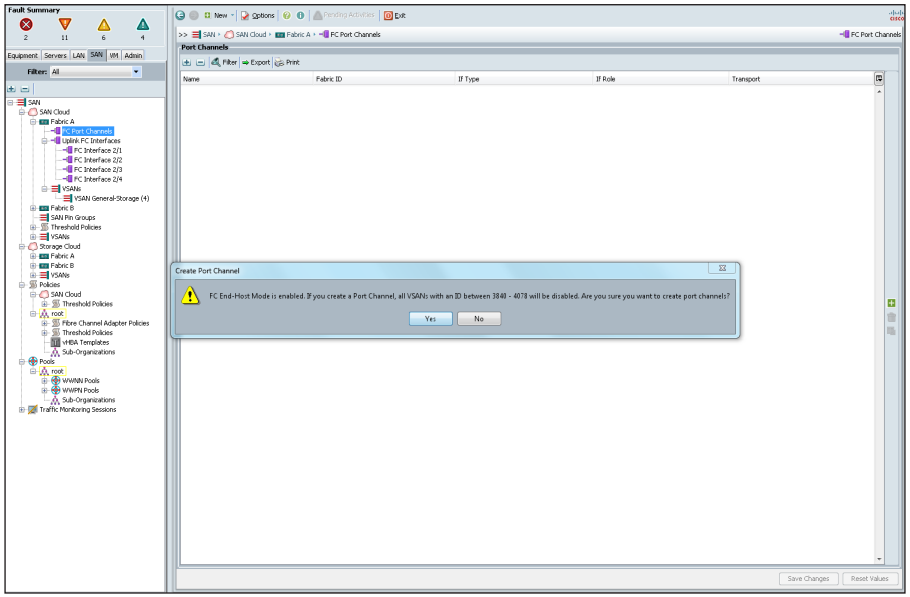
Step 6: Enter the VSAN IDs corresponding to the SAN-A and SAN-B VSANs configured in your SAN fabrics. In the *Cisco SBA for Midsize Organizations—Data Center Deployment Guide*, we assigned VSAN 4 to SAN-A and VSAN 5 to SAN-B.

Step 7: 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 8: When you have configured the VSAN IDs in this section, click **OK**. A window shows the successful creation of the VSAN.

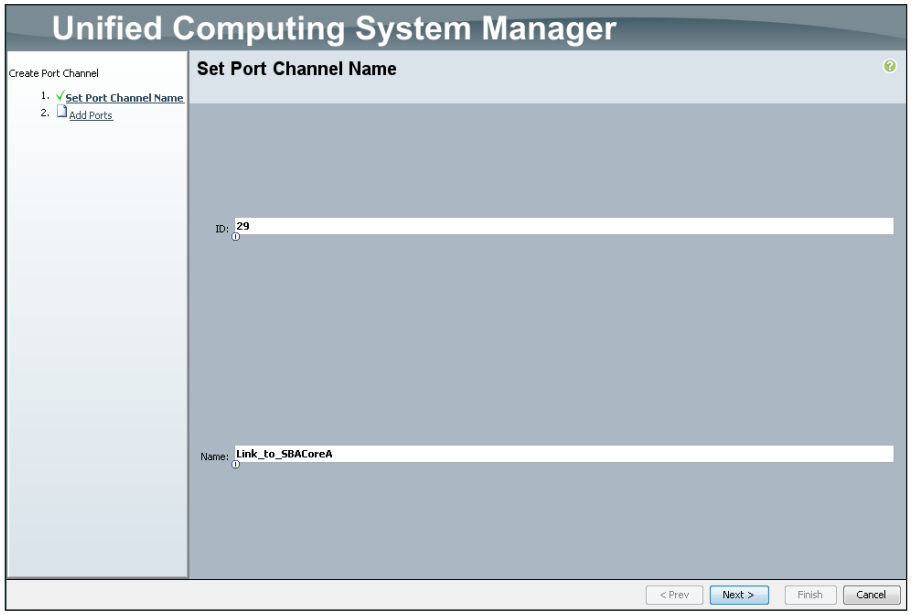
Now that you have created the VSAN, you can create a SAN port-channel to connect to the data center core Nexus 5500UP switches.

Step 9: In the navigation pane on the SAN tab, expand the SAN Cloud, expand Fabric A, right-click **FC Port Channels**, and then choose **Create Port Channel**.

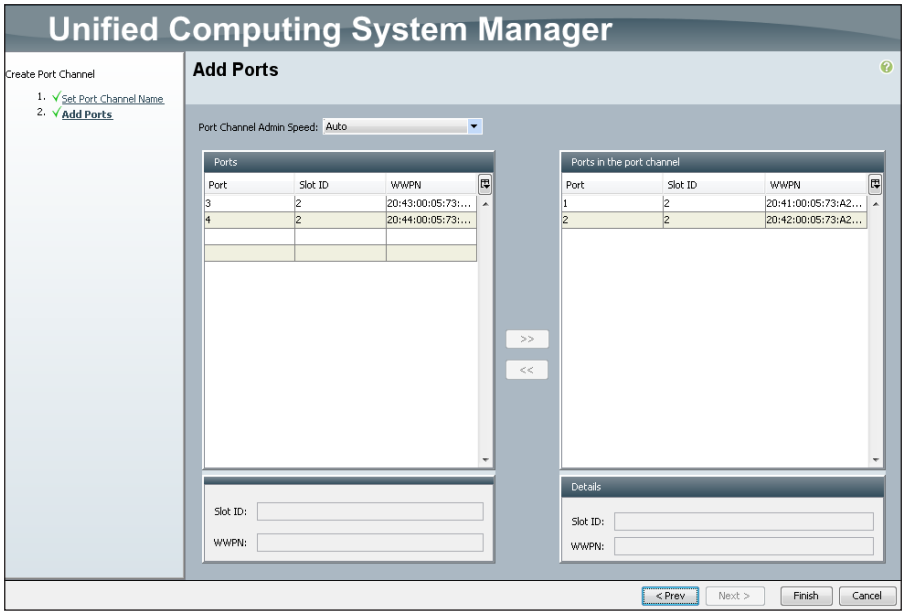


On the message that warns you of VSAN IDs that you cannot use if you create port channels, click **Yes**.

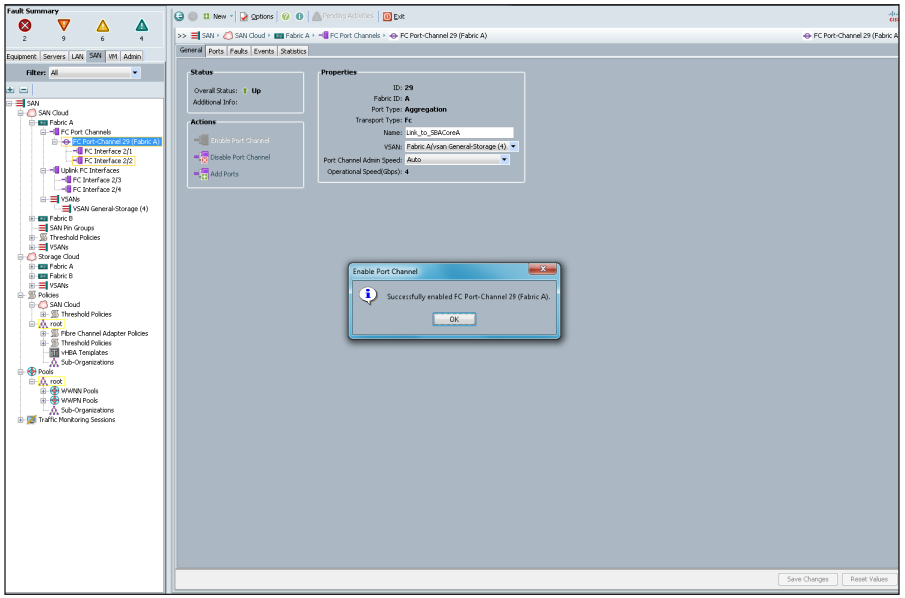
Step 10: Enter an ID and name for the port channel, and then click **Next**.



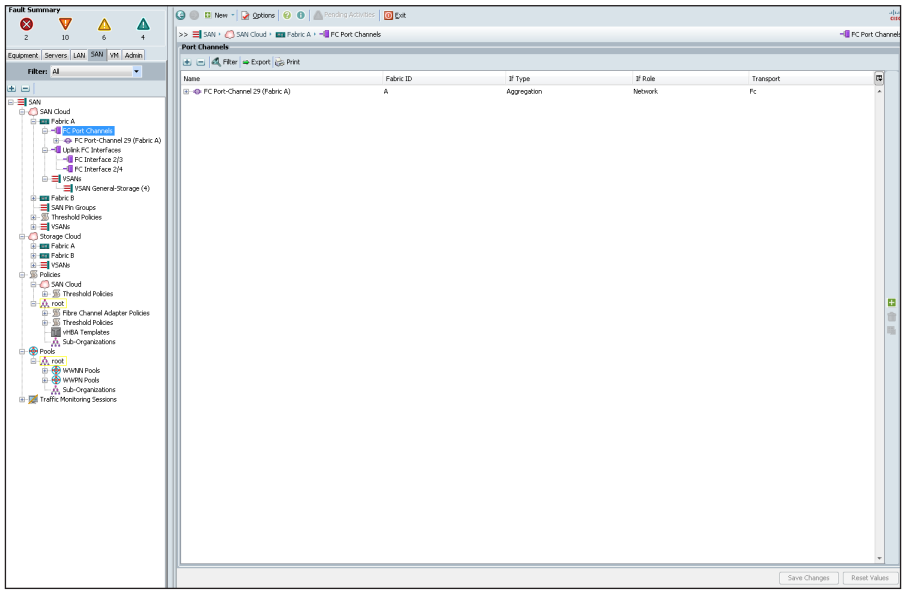
Step 11: In the **Ports** list, select the ports, and then click the right arrows (>>) button to move them to the **Ports in the port channel** list. Click **Finish** when you have added the physical uplink ports to the port channel.



Step 12: Click **OK** on the "Successfully created..." message.

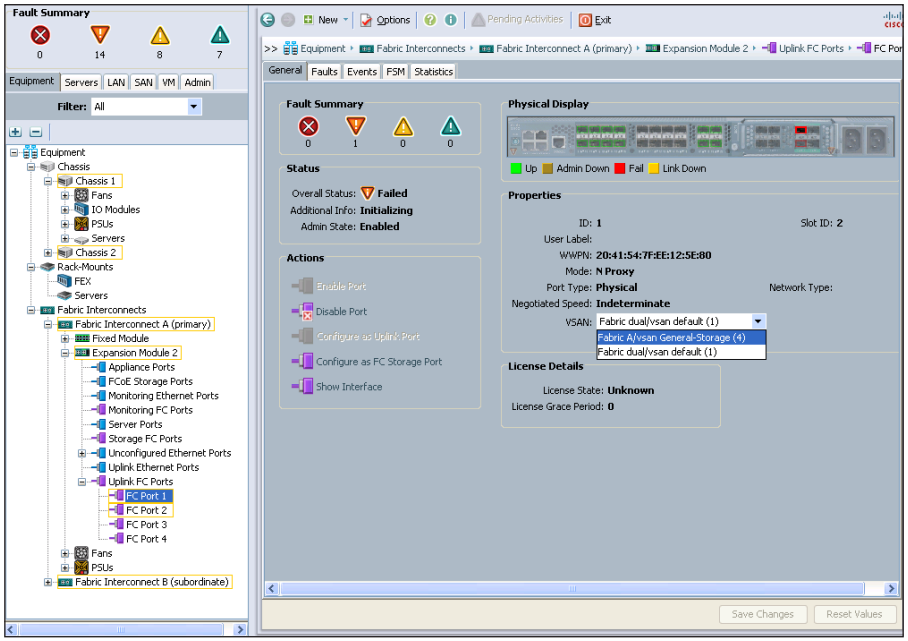


Step 13: Expand the **FC Port Channels**. You will see the newly created port channel.

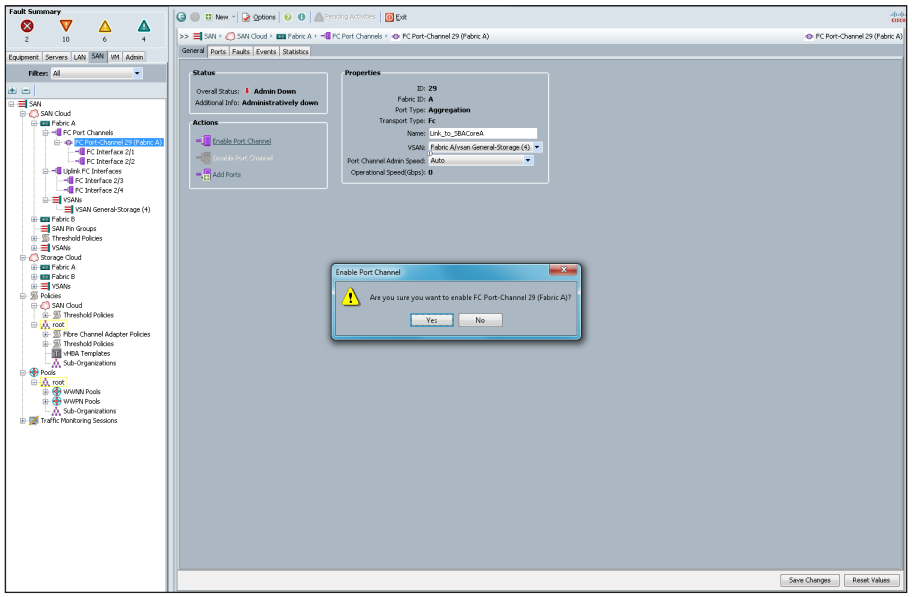


Step 14: Double click the new port channel in the main window. The next step is to configure the VSAN assignment.

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



Step 16: In the **Actions** box, Click **Enable Port Channel**, and on the message that appears, click **Yes**.



In a few seconds, the port channel Status should be displayed as UP.

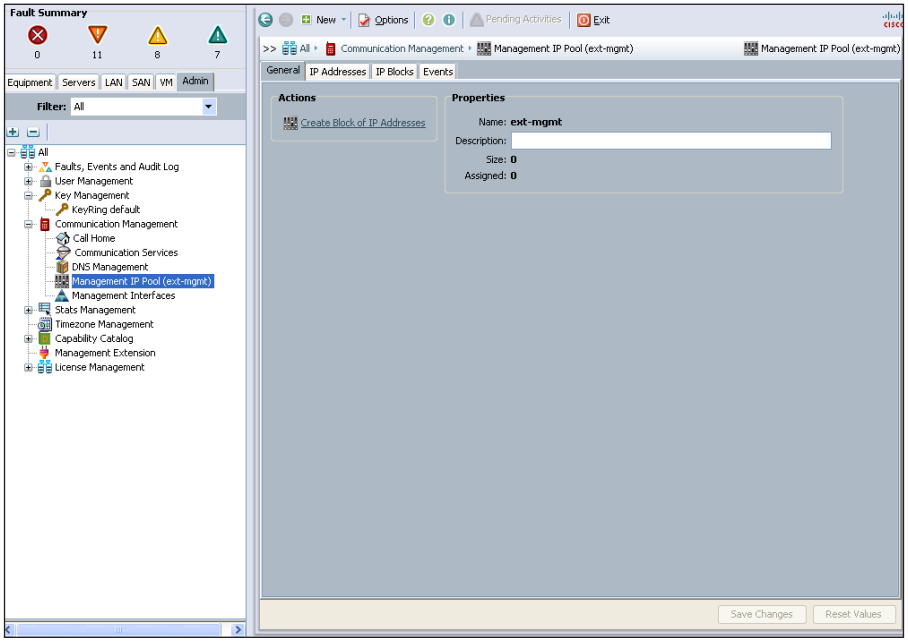
Tech Tip

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 port channel, enter the shutdown command, and then enter the no shutdown command. Repeat this procedure beginning at Step 9 for the VSAN for SAN Fabric B on Fabric Interconnect B.

Procedure 4 Add a management IP address pool

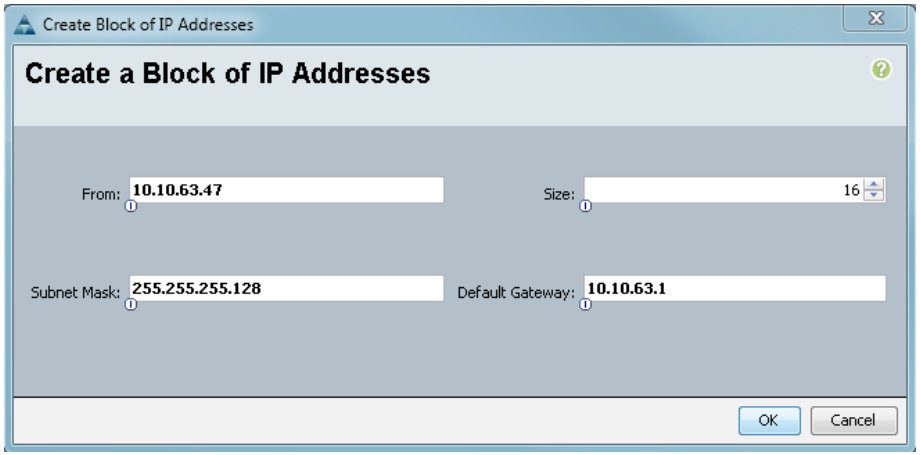
The Cisco UCS Manager GUI provides a launching point to direct keyboard-video-mouse (KVM) access to control each of the blade servers within the system. To facilitate this remote management access, you must allocate a pool of IP addresses to the blade servers within the system. These addresses are used 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.

Step 1: In the navigation pane, click the **Admin** tab, expand **All** > **Communication Management**, and then choose **Management IP Pool.**



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

Step 3: Allocate a contiguous block of IP addresses by specifying the starting address in the **From** field, and then specify the **Size of the block**, the **Subnet Mask**, and the **Default Gateway**, and then click **OK**. The size of the block will need to be large enough to assign one address to each server connected to the fabric. In this example, you can use **16** addresses for the size of the block.



Tech Tip

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. Detailed information on upgrading firmware is available at: http://www.cisco.com/en/US/products/ps10281/prod_installation_guides_list.html

Process

Creating an Initial Service Profile for Local Boot

1. Access the Service Profile Wizard
2. Create UUIDs
3. Configure storage
4. Complete networking configuration
5. Define the server boot order policy
6. 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 will 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 Access the Service Profile Wizard

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 on the Identify Service Profile page, enter a name for the service profile in the **Name** box.

The following procedures walk you through a wizard-based process for defining these attributes of the first service profile:

- Identification/universally unique identifier (UUID)
- Storage
- Networking
- vNIC/vHBA placement
- Server boot order
- Maintenance policy
- Server assignment
- Operational policies

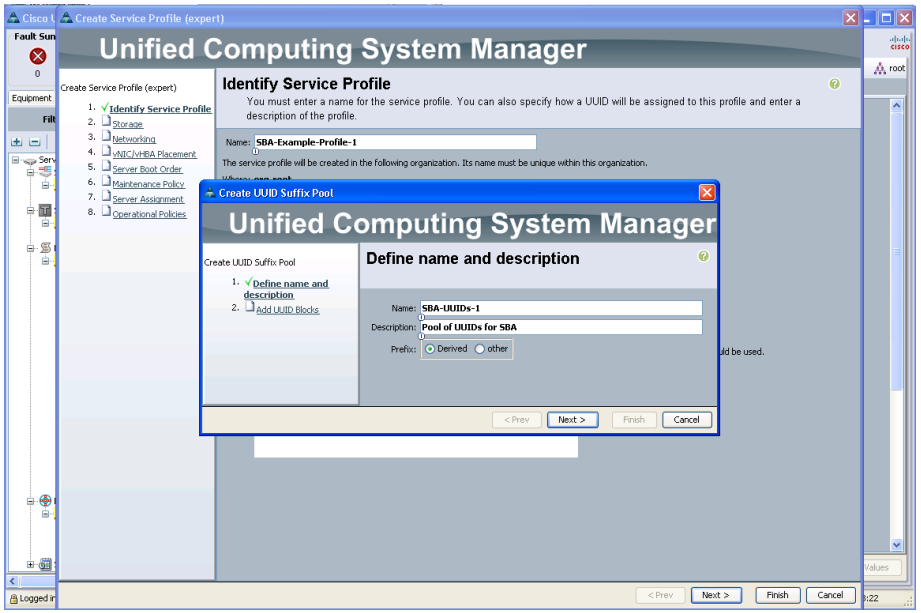
Procedure 2 Create UUIDs

Step 1: On the Identify Service Profile page, click **Create UUID Suffix Pool**.

Tech Tip

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.

Step 2: In the Create UUID Suffix Pool window, enter a **Name** and **Description** for the pool. Verify that the **Derived** radio button is selected to use a UUID prefix that is derived from server hardware.



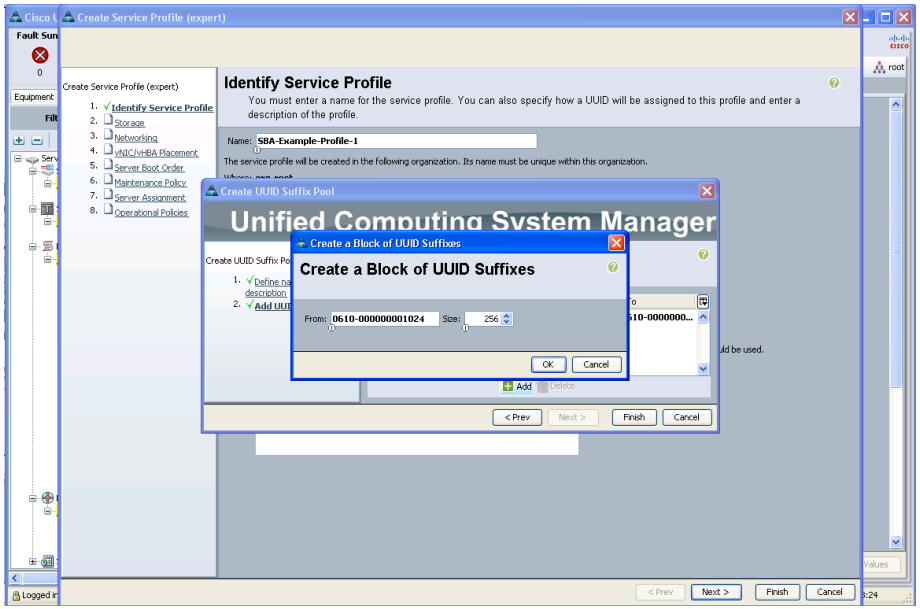
Step 3: Click **Next**, and then click **Add**.

Step 4: In the Create a Block of UUID Suffixes window, in the **From** field, enter a unique, randomized base value as a starting point.

Tech Tip

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

Step 5: In the **Size** field, enter a number larger than the number of servers or service profiles that you will 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 256.



Step 6: Click **OK**, and then click **Finish**.

Step 7: On the Identify Service Profile page, in the **UUID Suffix Pool** list, choose the UUID suffix pool you just created, and then click **Next**.

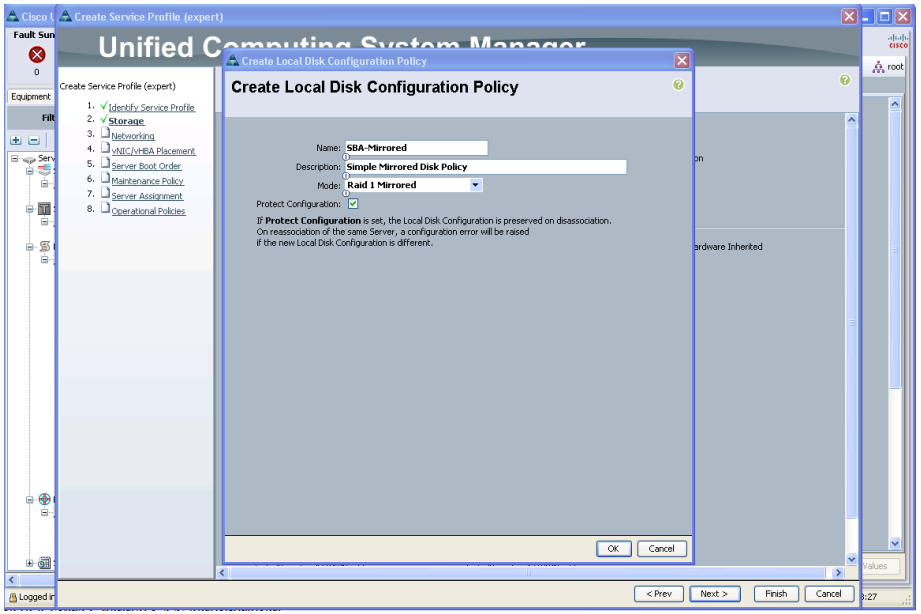
Procedure 3 Configure storage

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. To speed profile configuration and ensure consistency, you can create and save a local disk configuration policy as a reusable object.

Step 1: On the Storage tab, click **Create Local Disk Configuration Policy**.

Step 2: Enter a **Name** and **Description** for the policy, and in the **Mode** list, choose **Raid 1 Mirrored**.

Step 3: Ensure that **Protect Configuration** is selected.



Step 4: Click **OK**, acknowledge the creation, and then on the Storage page in the **Local Storage** list, choose the disk policy you just created.

Step 5: Next to **How would you like to configure SAN connectivity?**, select **No vHBAs**, and then click **Next**.

Tech Tip

For information about enabling a service profile to access Fibre Channel attached storage over a SAN, see the "Creating a Service Profile for SAN Boot," process, later in this guide.

Procedure 4 Complete networking configuration

The Networking page allows you to define vNICs that the system will present to the installed operating system in the same way that a standalone physical server presents hardware NICs installed in a PCI bus. The type of mezzanine card installed in the blade server affects how many vNICs may be defined in the profile and presented to the server operating system. Leave the Dynamic vNIC Connection Policy list at its default setting for this procedure.

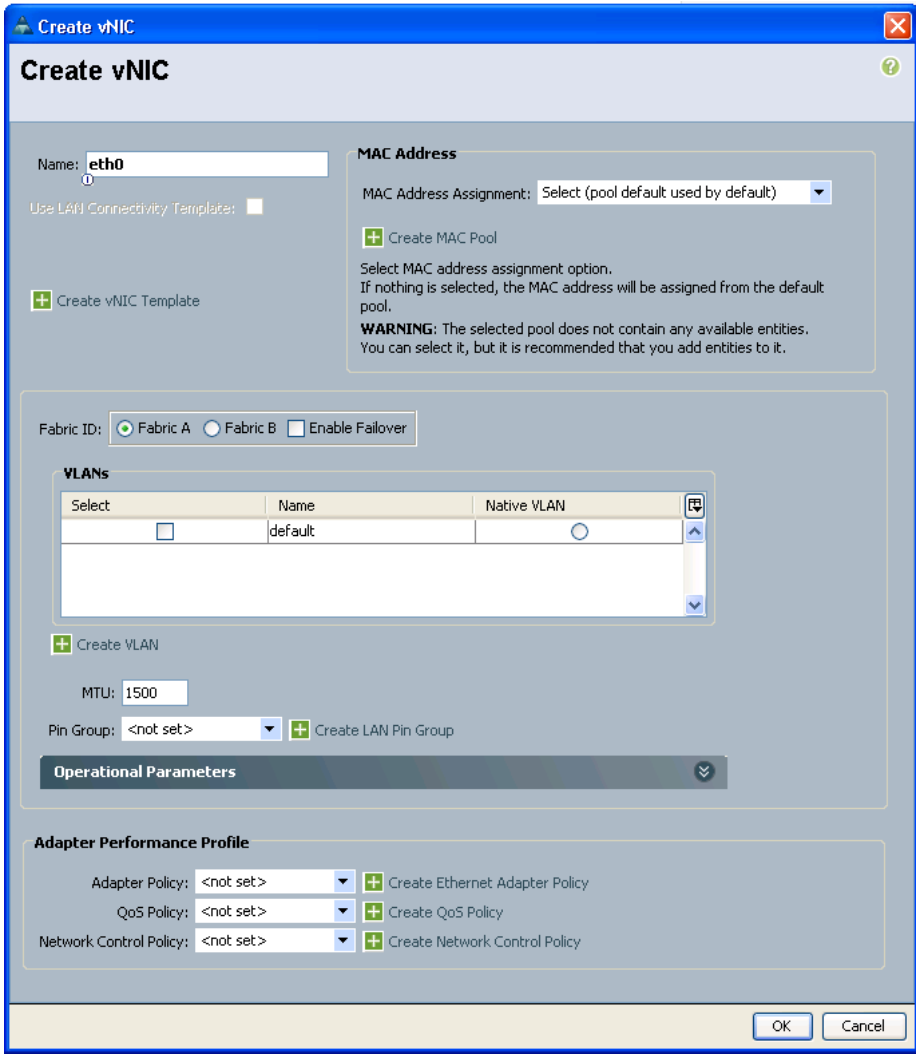
Tech Tip

Dynamic vNICs only apply to configurations that use the Cisco UCS M81KR Virtual Interface Card.

Step 1: Leave the **Dynamic vNIC Connection Policy** list set to its default, and next to **How would you like to configure LAN connectivity?**, select **Expert**. The expert mode allows you to walk through the creation of a MAC address pool instead of using the default MAC pool, which will not contain any address blocks on a new system.

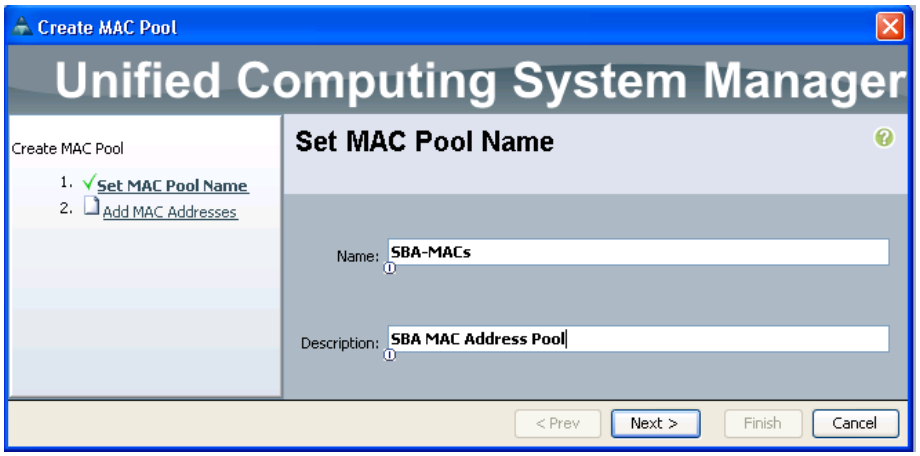
Step 2: Click **Add** at the bottom of the page.

Step 3: In the **Name** box, enter a name for the profile. For the example configuration, use **eth0** as the interface name; representing Ethernet 0.



Step 4: Under **MAC Address** section, click **Create MAC Pool.** This adds a pool of MAC addresses to be 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.

Step 5: Enter a **Name** and **Description** for the MAC pool, and then click **Next**.



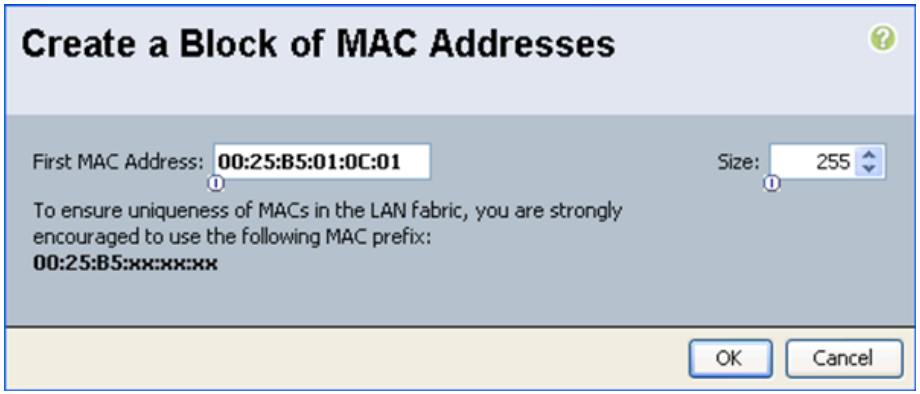
Step 6: At the bottom of the window, click **Add**.

Step 7: 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. Create a block of addresses large enough to allocate one address to each vNIC that will exist in the system.

Tech Tip

To assist with troubleshooting later, consider using multiple MAC address blocks with specific numbering conventions relevant to your implementation.

Step 8: In the **First MAC Address** box, add the starting address for the MAC address block, and in the **Size** box, enter the number of addresses to allocate.



Step 9: Click **OK**, click **Finish,** and then click **OK** to acknowledge creation of the pool.

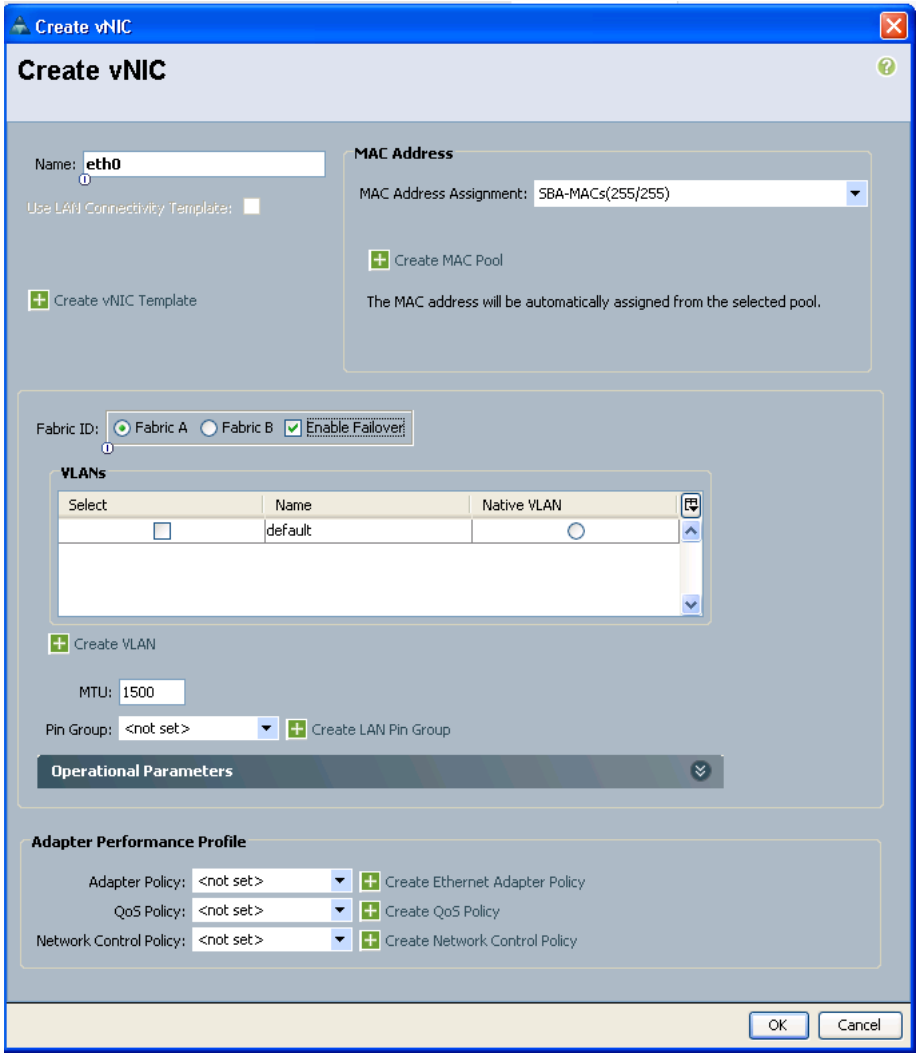
Step 10: In the Create vNIC window, in the **MAC Address Assignment** list, choose the name of the MAC address pool that you just created.

The next section of the Create vNIC screen allows you to define the vNIC traffic path through the fabric interconnects and identify which VLANs are present on the vNIC. The Cisco UCS system has the capability to present multiple vNICs to the installed operating system and pass the traffic from a specific vNIC to either fabric interconnect A or B. In addition, a fabric-failover capability is available on specific NIC hardware to allow the system to continue forwarding traffic through the other fabric interconnect if the primary selection has failed. For this basic service profile example, select fabric A as the primary traffic path and enable failover.

Tech Tip

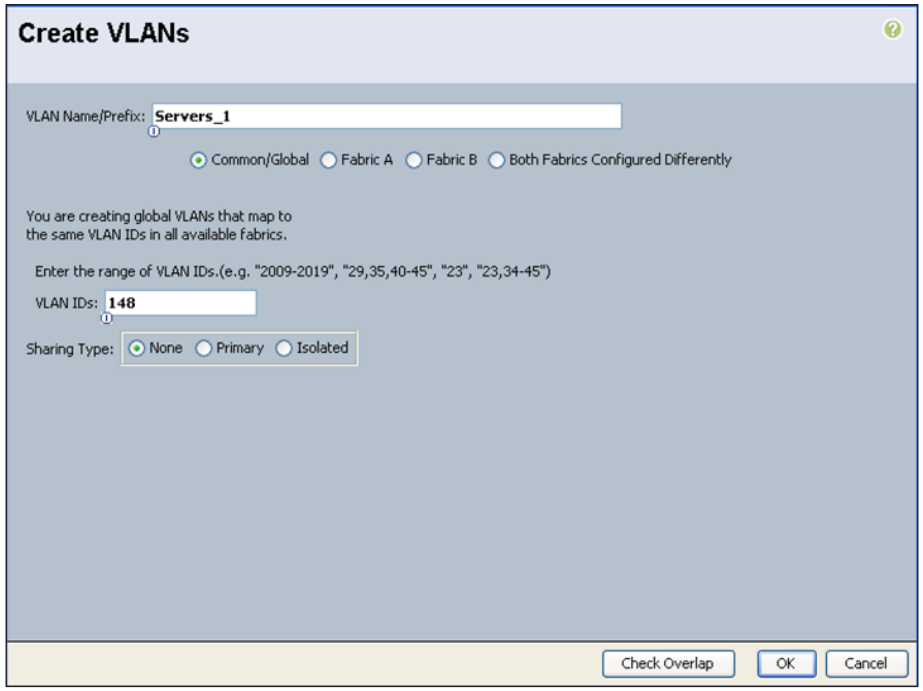
Fabric failover is appropriate for configurations with a single host operating system installed directly on the blade server. For a virtualized environment, we recommend instead that you disable fabric failover, present multiple vNICs to the hypervisor, and allow the hypervisor system to manage the failover of traffic in the event of a loss of connection to one of the fabric interconnects. See the *Cisco SBA for Midsize Organizations—Data Center Virtualization with UCS, Nexus 1000v and VMware Deployment Guide* for more information on presenting multiple vNICs to a hypervisor explanation.

Step 11: Next **to Fabric ID**, select the **Fabric A** option and the **Enable Failover** check box.



Step 12: Click **Create VLAN**. In the next step, you identify each VLAN needed in the Cisco UCS system. This is necessary to receive traffic from the server vNICs.

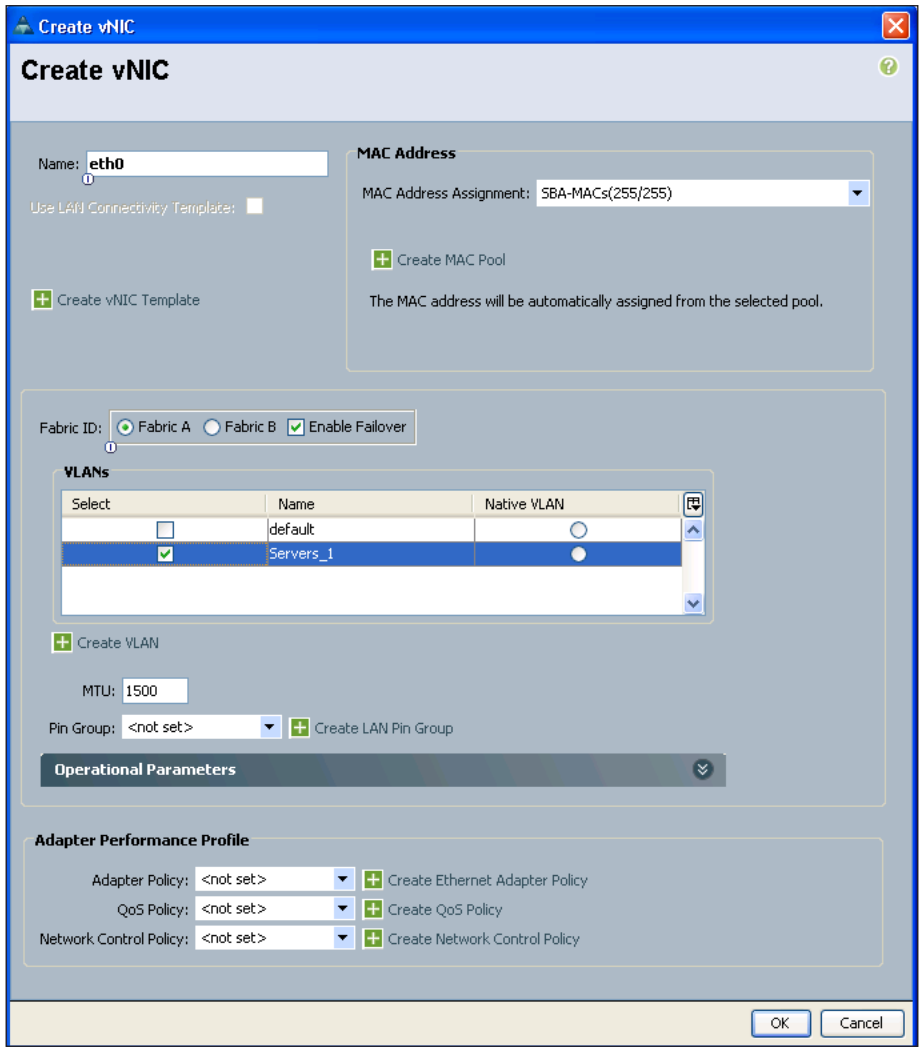
Step 13: In the Create VLANs window, enter the **VLAN Name/Prefix** and **VLAN IDs** for a group of VLAN IDs, verify that the **Common/Global** and **None** options are selected, and then click **OK**.



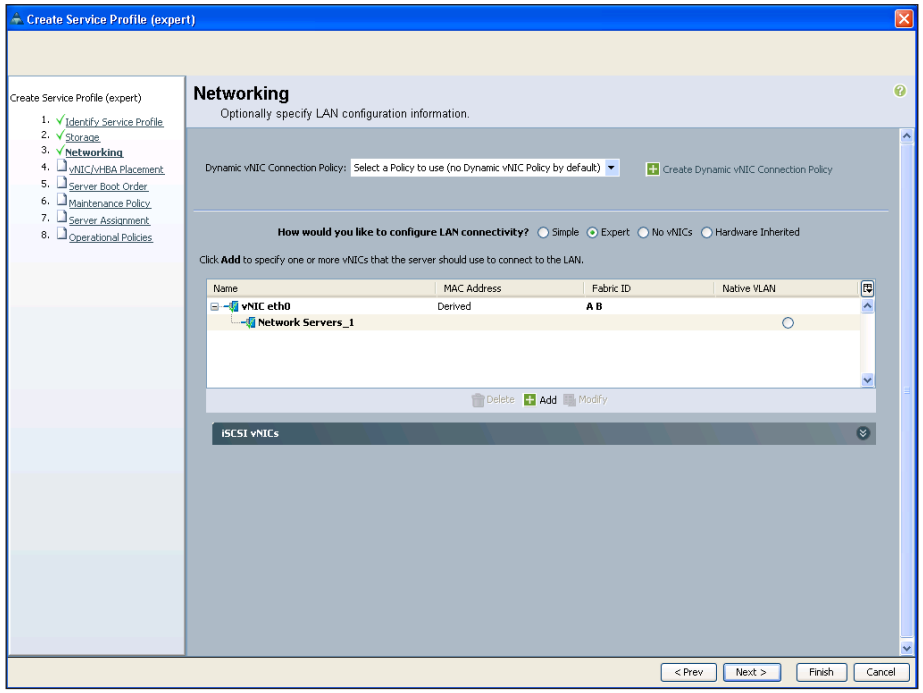
Tech Tip

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.

Step 14: In the **Create vNIC** window, in the **VLANs** list, choose the VLAN that you just created. Leave the **Native VLAN** column unselected.



Step 15: Leave the remainder of the fields in the Create vNIC window at the default settings, and then click **OK**. The next page shows the newly created vNIC, its fabric association, and the VLANs on which it forwards traffic.



Step 16: Verify the information displayed on the Networking page about the new vNIC as shown above and then click **Next**.

Step 17: On the vNIC/vHBA Placement page, leave the defaults, and then click **Next.** The system performs the placement of the virtual interfaces on the physical interfaces that exist on the blade servers with which this profile will be associated.

Procedure 5 Define the server boot order 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 configure a basic boot policy that boots from removable media—in this case, an attached CD/DVD drive—first, and then from the internal disk. More advanced configurations allow boot-from-LAN or boot-from-SAN. This guide covers boot-from-SAN in a later process.

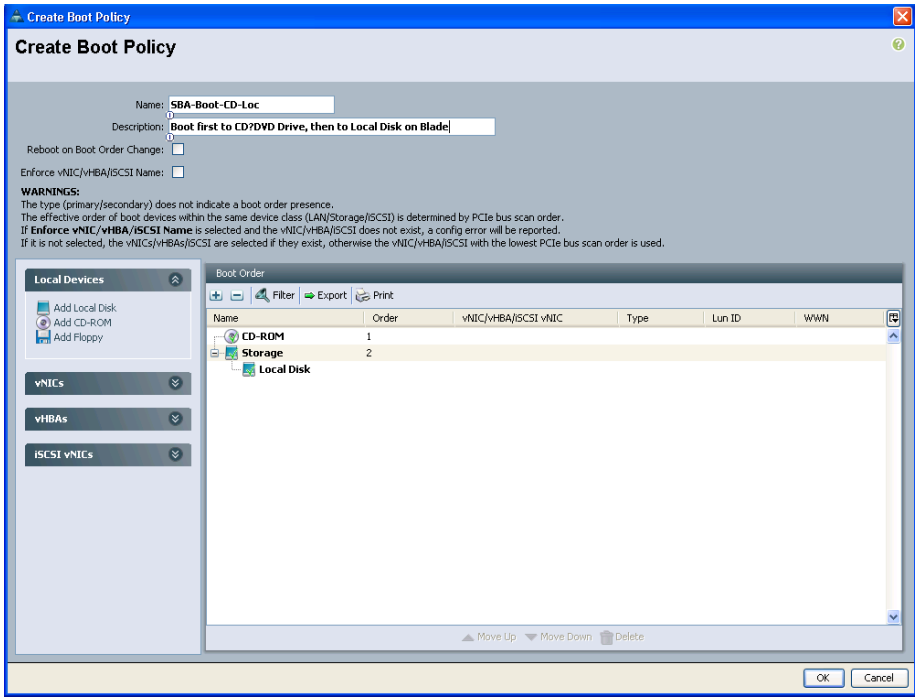
Step 1: On the Server Boot Order page, click **Create Boot Policy**.

Step 2: In the Create Boot Policy window, enter the **Name** and **Description** for the boot policy.

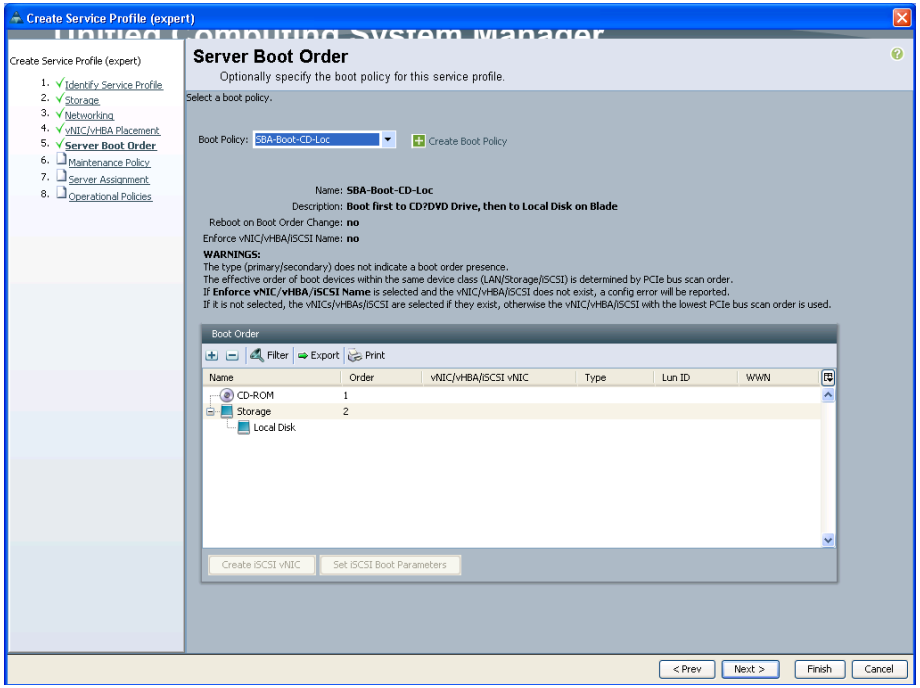
Step 3: Click the down arrows on the **Local Devices** container, click **Add CD-ROM** first, and then click **Add Local Disk.**

The order of the devices in the list is displayed as a number in the Order column of the table.

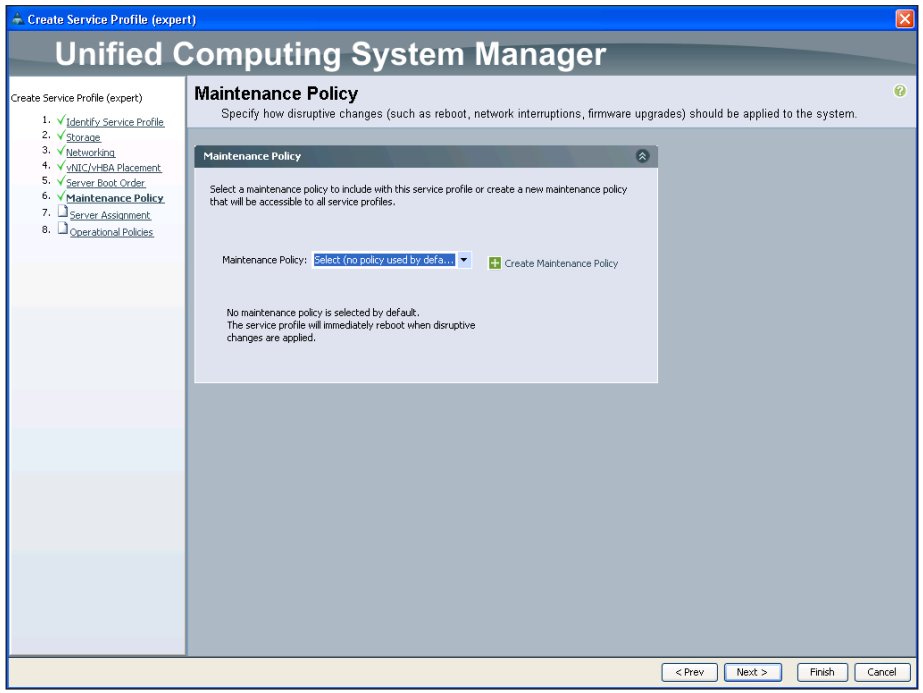
Step 4: Verify the choices, and then click **OK**.



Step 5: On the Server Boot Order page, in the **Boot Policy** list, choose the name of the policy you just created, and then click **Next**.



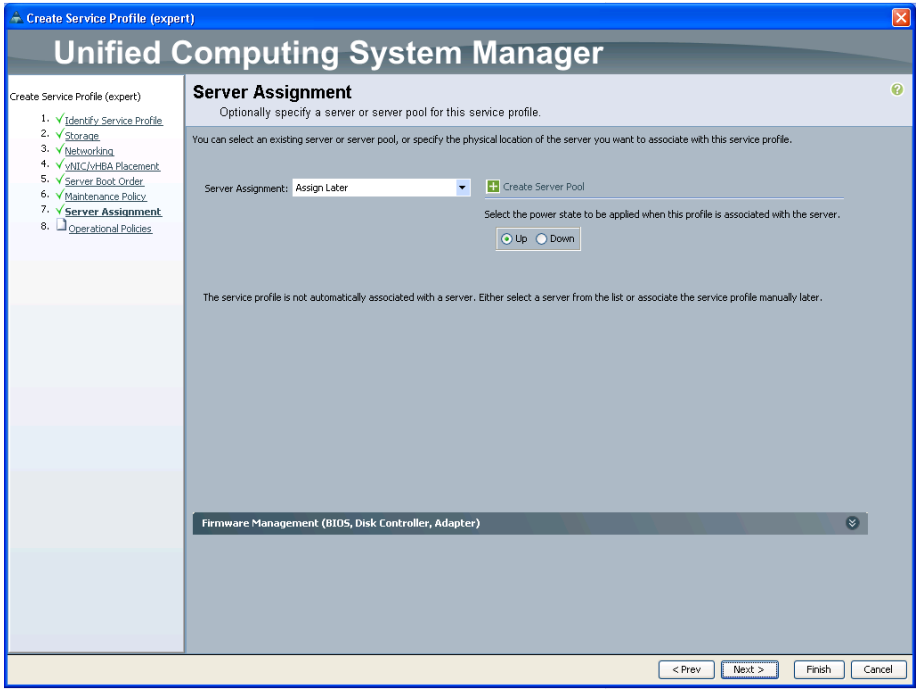
Step 6: On the **Maintenance Policy** page, leave all default settings, and then click **Next**.



Procedure 6 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. For purposes of this basic initial service profile, you will choose to assign the service profile later, and you will leave operational policies set to their defaults for now.

Step 1: On the Server Assignment page, in the **Server Assignment** list, choose **Assign Later**.



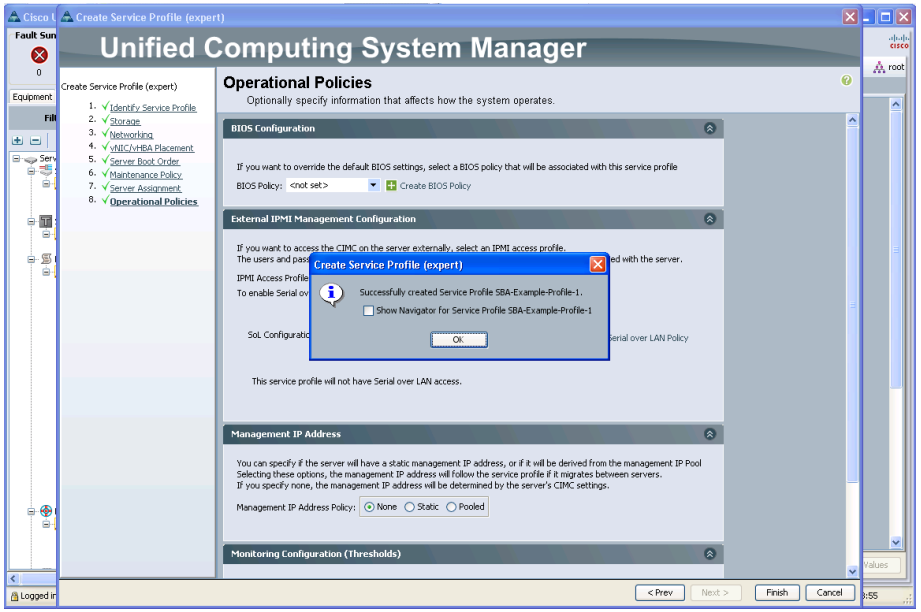
Step 2: Verify that the **Up** power state option is selected, and then click **Next**. This ensures that a physical blade server will be powered on when the service profile is eventually applied.

Step 3: On the **Operational Policies** page, leave all the defaults set as shown, and then click **Finish**.

Reader Tip

For more information, please refer to Cisco UCS product guides at http://www.cisco.com/en/US/partner/products/ps10281/tsd_products_support_series_home.html.

Step 4: This completes the creation of the initial service profile on the system. The system displays a message indicating successful completion of the Create Service Profile (expert) wizard. On the message, click **OK** to exit the Service Profile Creation Wizard.



Process

Creating a Service Profile for SAN Boot

1. Create a WWNN pool
2. Add a vHBA to the service profile
3. Create a WWPN pool
4. Assign the WWNN pool
5. Modify local disk policy
6. Modify the boot policy
7. 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 Service Profile for Local Boot."

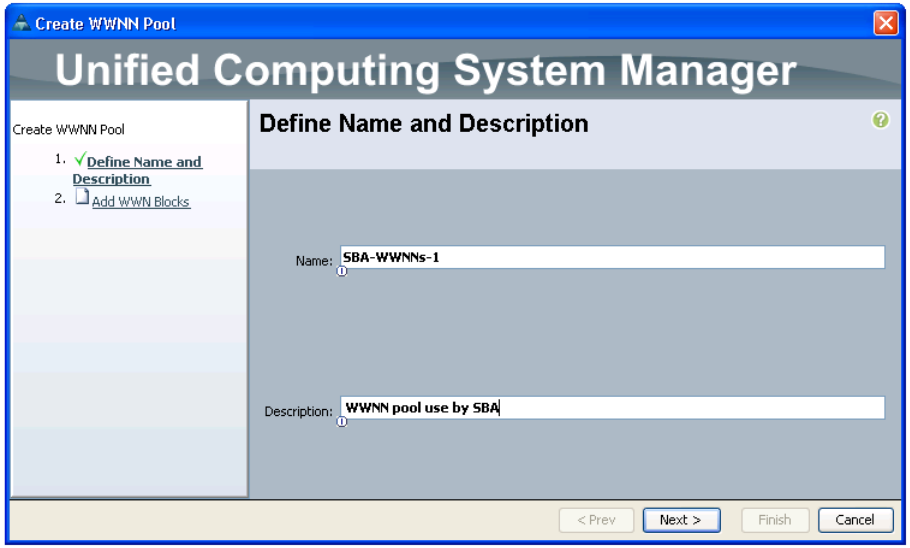
Procedure 1 Create a WWNN pool

First, you must provision a pool of WWNNs in the system. The WWNNs in the pool will be assigned to service profiles that need to access the Fibre Channel SAN. One WWNN is assigned from the pool to each service profile. Each WWNN corresponds to the identity of a Fibre Channel end-node.

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

Step 2: Under the section **Pool** in the work pane, click **Create WWNN Pool**.

Step 3: Enter a **Name** and **Description** for the new pool, and then click **Next**. The next step is to create a block of WWNN addresses by defining a starting point and the quantity of addresses in the block.

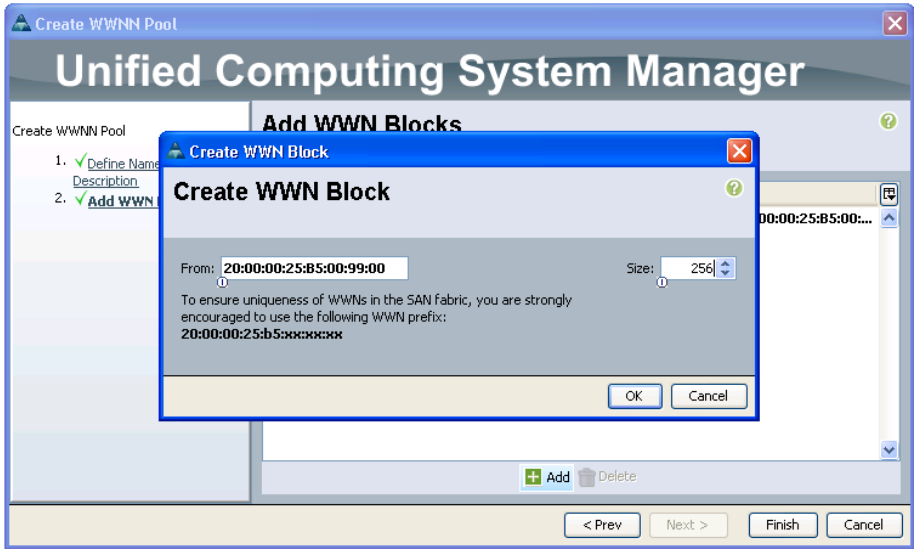


Step 4: In the **Create WWNN Block** window, in the **From** field, enter a WWN prefix. The system provides a prefix to help ensure uniqueness of the WWNN values on the SAN. Assign the last three segments of the base WWNN value in colon-delimited notation, as needed for your system.

Reader Tip

For more information on WWN, WWNN, and WWPN, see the *Cisco UCS Manager GUI Configuration Guide* at: http://www.cisco.com.

Step 5: In the **Size** field, specify the number of node names required, and then click **OK**.



Step 6: Click **Finish.** This completes the creation of the new WWNN pool. This pool will be referenced by the service profile you create for SAN boot in the following procedures.

Procedure 2 Add a vHBA to the service profile

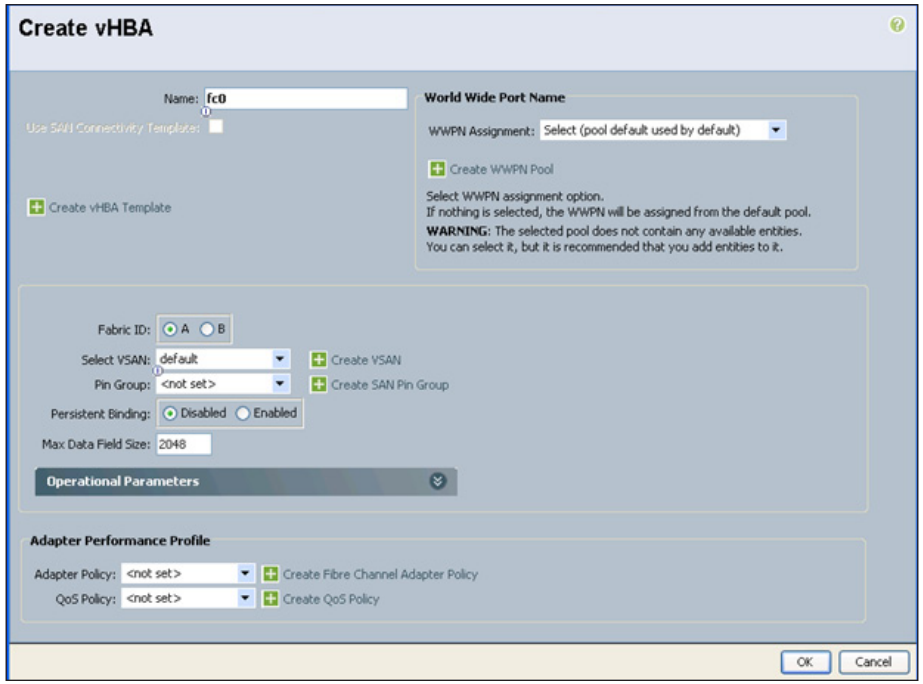
In this procedure, you clone the service profile that you created in the previous process, "Creating an Initial Service Profile for Local Boot." This allows you to reuse the storage and boot-order configuration of an existing profile and create a new profile with very little additional work.

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

Step 2: Enter a **Clone Name** that clearly identifies the profile as a SAN boot server instance, and then click **OK.**

Step 3: Click the name of the new profile in the navigation pane, and then click the **Storage** tab in the work pane. This tab is initially blank because we did not add any storage adapters in the profile that we created in the previous process.

Step 4: At the bottom of the screen, click **Add**. This will launch the Create vHBA window, which will create a vHBA for Fibre Channel storage access in this service profile..



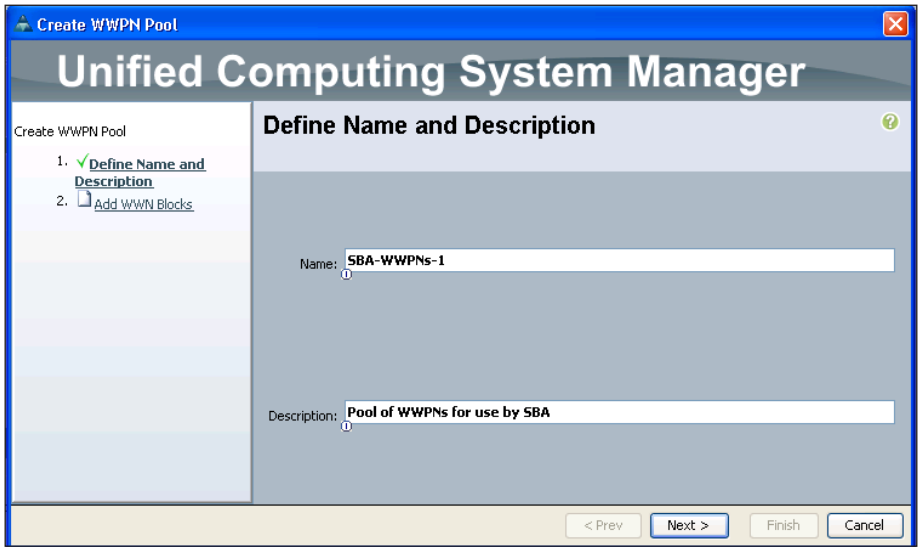
Step 5: Enter a **Name** for the vHBA. The example configuration uses the name **fc0**.

Procedure 3 Create a WWPN pool

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 1, you must provision a pool of WWPNs for the system to assign port addresses consistently when you add new service profiles to the system.

Step 1: On the **Create vHBA** screen, click **Create WWPN Pool**.

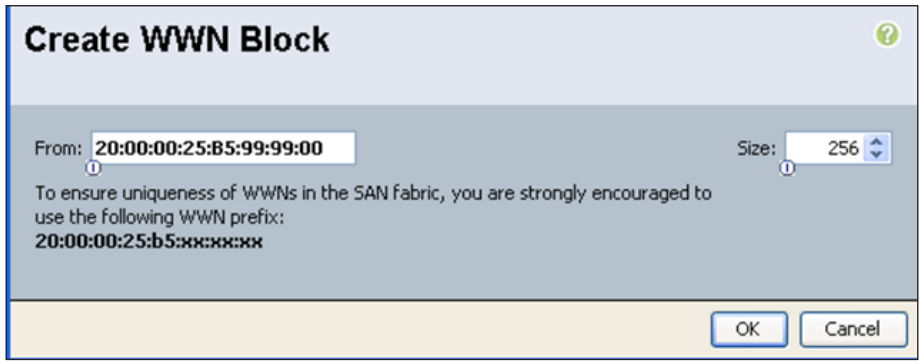
Step 2: Enter a **Name** and **Description** for the pool, and then click **Next**.



Step 3: Click **Add WWN Blocks** to create a new WWPN block.

Step 4: In the **Create WWN Blocks** window, in the **From** field, assign the last three segments of the base WWPN value in colon-delimited notation, as needed for your system. The system provides a prefix value to help ensure uniqueness of the WWPN values on the SAN.

Step 5: In the **Size** field, specify the number of port names required in the pool, and then click **OK**.



Step 6: Click **Finish**.

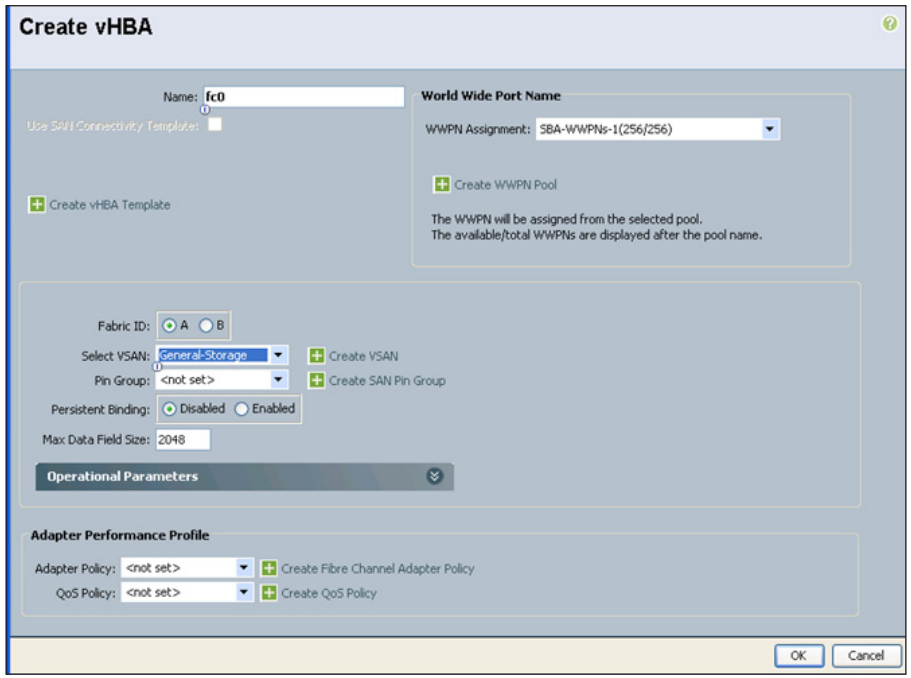
Step 7: In the **Create vHBA** window, in the **WWPN Assignment** list, choose the WWPN pool you just created.

Step 8: Because this is the first vHBA that you have added to this profile, leave the Fabric ID setting as **Fabric A**. If you add a second vHBA to the profile for SAN fault-tolerance, you should assign the second vHBA to Fabric B. In the tested design, we create another vHBA named fc1 and add it to Fabric B. Proceed to Step 4 of Procedure 2 "Add a vHBA to the service profile" to add the second vHBA and follow the steps to this point.

Next, you must configure this vHBA to communicate on a specific VSAN. VSANs allow multiple logical SAN networks to share a common physical Fibre Channel infrastructure. The desired VSAN numbering must match what you have created on your SAN network, and what was previously created in Procedure 3, "Define Fibre Channel uplink ports" in the "Configuring Communications Connections with UCS Manager" process.

Step 9: In the Create vHBA window, in the **Select VSAN** list, choose the VSAN for SAN-A that you created earlier for the vHBA.

Step 10: Leave the remaining fields in the Create vHBA window at their default settings, and then click **OK**.



Step 11: At the bottom of the Storage tab in the work pane, click **Save Changes**. This ensures that your changes are applied to the service profile.

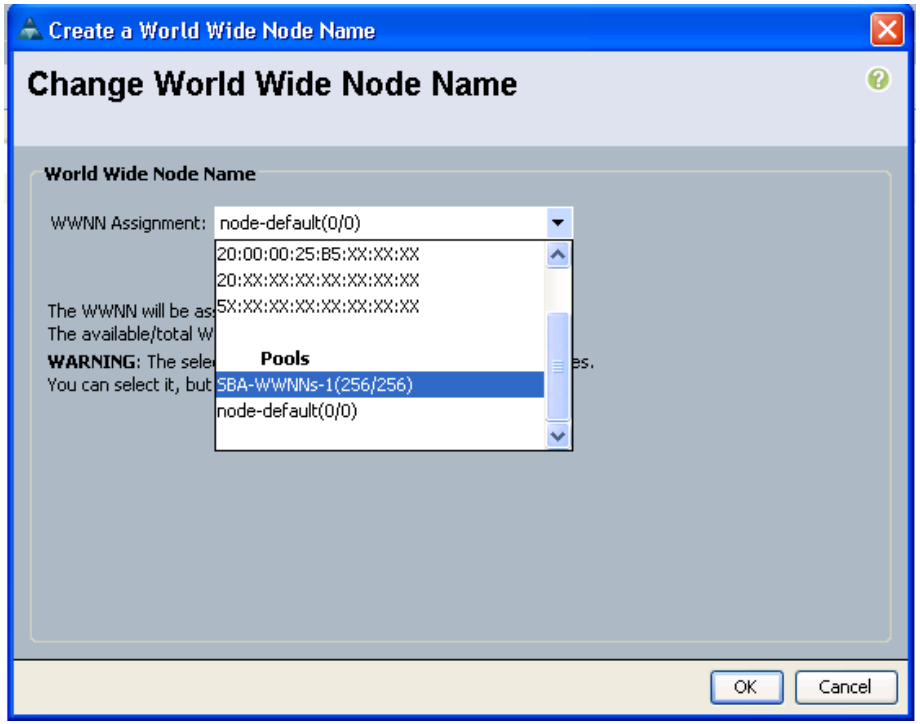
When you save and apply changes to the service profile, the system assigns a specific WWPN from the pool to the new vHBA. This WWPN is the Fibre Channel initiator value that must be assigned to the correct SAN zone to access the desired boot logical unit number (LUN) assigned by the SAN administrator. The storage system must also be properly configured in its LUN masking to expose the desired LUNs to this specific WWPN.

Procedure 4 Assign the WWNN pool

Now that you have defined a vHBA in the service profile to provide access to the Fibre Channel SAN, you must assign the WWNN pool to the profile.

Step 1: On the Storage tab of the work pane, in the Actions area, click **Change World Wide Node Name**.

Step 2: In the **WWNN Assignment** list, choose the WWNN pool name that you created.



Step 3: Click **OK**. On the Storage tab, the World Wide Node Name field now reflects the WWNN assigned to the profile from the pool and the name of the WWNN pool that you specified.

Procedure 5 Modify local disk policy

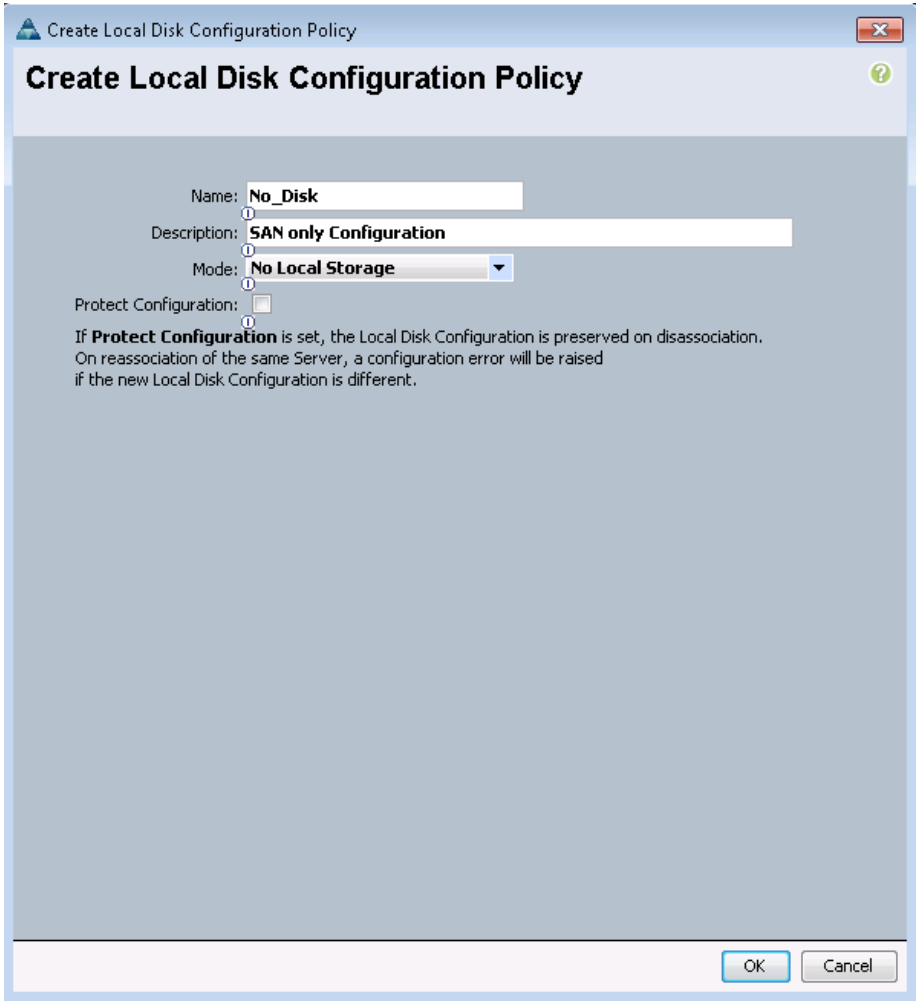
The boot order in a boot policy should include either a local disk or a SAN LUN, but not both, to avoid the possibility that the server will boot from the wrong storage type. Some operating systems will fail SAN boot if the local disk also contains a copy of the operating system. In this procedure, you create a policy which will not configure and install any Local Disk for your blade server.

Step 1: Navigate to **Servers > Policies > root > Local Disk Config Policies**.

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

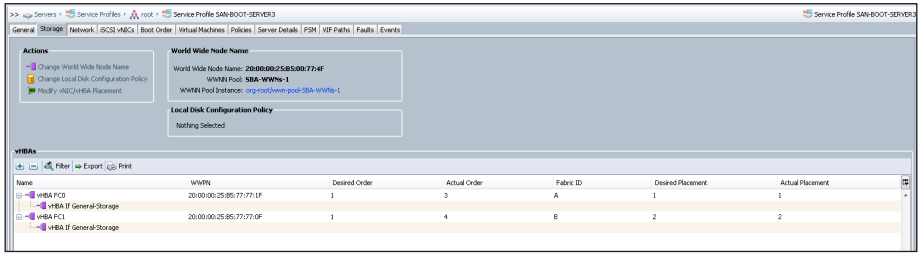
Step 3: In the Create Local Disk Configuration Policy window, enter a name for your policy such as No Disk.

Step 4: In the **Mode** list, choose **No Local Storage**, clear **Protect Configuration**, and then click **OK**.



Step 5: Navigate to **Servers** > **Service Profiles** > **root**, and then choose the SAN service profile that you created in Procedure 2.

Step 6: Click the **Storage** tab, and then click **Change Local Disk Configuration Policy**.



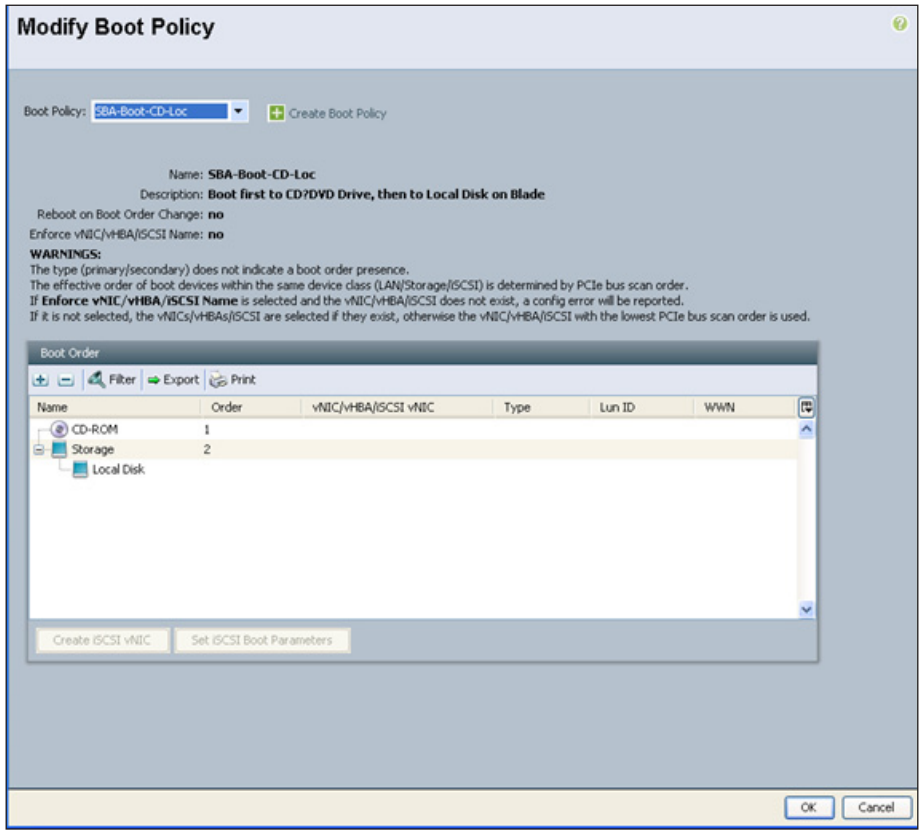
Step 7: In the Change Local Disk Configuration Policy window, select the **No_Disk** configuration policy you created earlier from the Select the Local Disk Configuration Policy list, and then click **OK**.

Procedure 6 Modify the boot policy

In this procedure, you update the profile to use the new vHBA storage adapter and the addresses assigned to it to access a new boot LUN over the SAN. The base profile that you created uses a simple boot policy with a boot order that starts with any attached removable media, such as CD or DVD, and then defaults to the local (internal) disk drives on the server. Now you create a new boot policy that is specific to accessing the target WWPN of the storage system that houses the server boot LUN.

Step 1: Click the **Boot Order** tab in the work pane, and then in the Actions area, click **Modify Boot Policy**.

Step 2: In the Modify Boot Policy window, click **Create Boot Policy**.

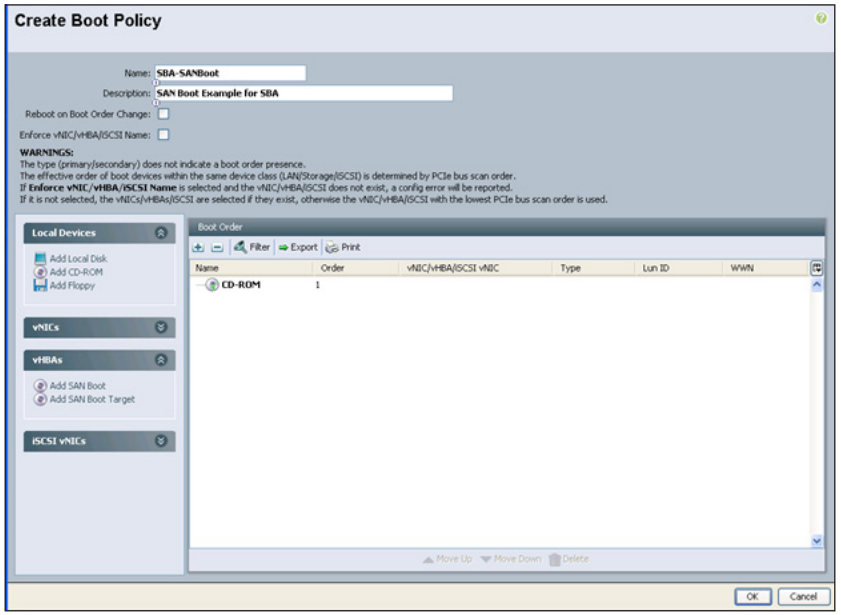


Tech Tip

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 3: In the Create Boot Policy window, enter a **Name** and **Description** for the new boot policy. You can use the choices in the left pane of the window to add different devices into the boot sequence.

Step 4: Click the down arrow next to **Local Devices**, and then click **Add CD ROM**. This allows the profile to first boot to a physically attached removable drive or a KVM Console Virtual Media drive, if present.



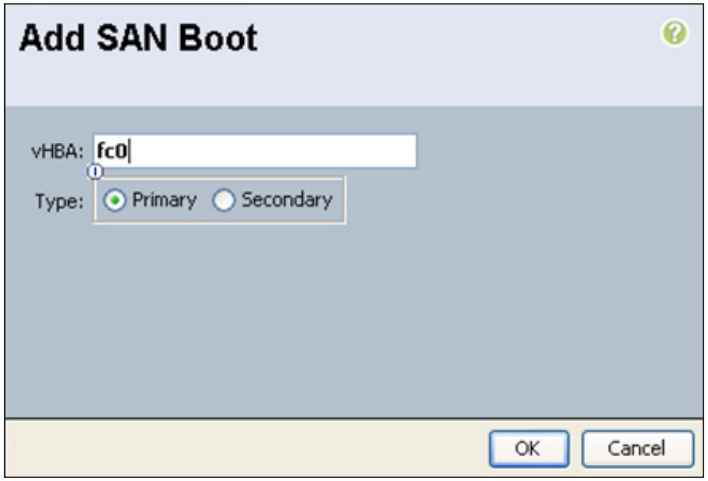
Step 5: In the left pane, click **vHBAs**, and then click **Add SAN Boot**.

Step 6: In the Add SAN Boot window, in the **vHBA** field, enter the correct name, leave the Type as Primary, and then click **OK**.

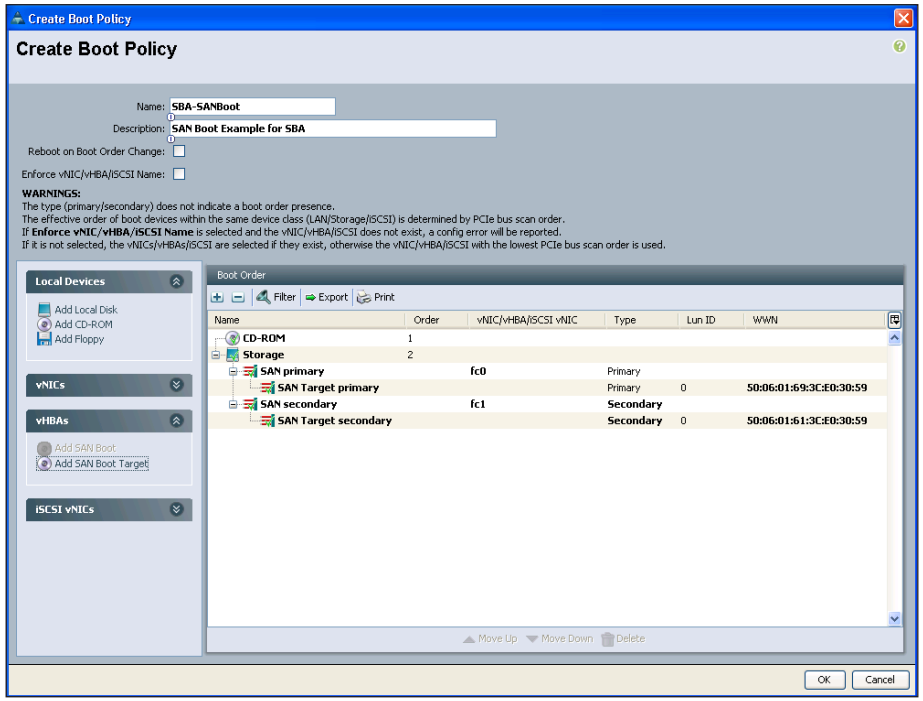
You must enter the same name that you used for defining the vHBA to the system in Procedure 2, "Add a vHBA to the service profile," earlier in this process. The example name provided was **fc0**.

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.



Step 7: In the Create Boot Policy window, click **Add SAN Boot Target**. to define the specific LUN number for the system to boot and the WWPN of the target storage system provided by your storage administrator. Typically, the boot LUN is presented by the storage system as LUN 0 to the requesting initiator. With the proper SAN target WWPN provided, the boot policy should appear similar to the figure below.



Step 8: To add a secondary vHBA using **fc1**, repeat Step 5 through Step 7.

Tech Tip

You can configure redundant access to the boot LUN for some operating systems on 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 http://www.microsoft.com/downloads/details.aspx?FamilyID=f4095fae-553d-4700-aafa-1cce38b5618f&displaylang=en

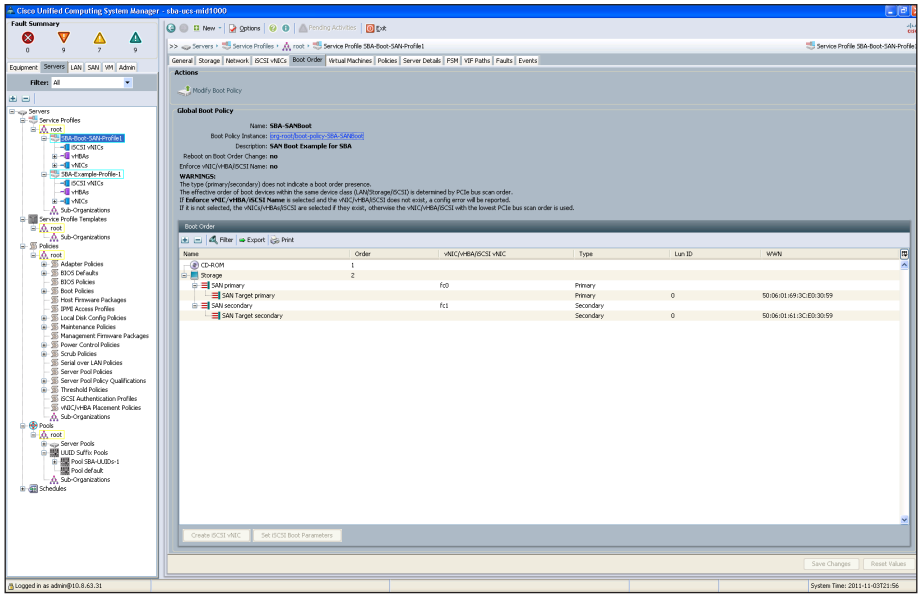
Other operating systems have different requirements. Please refer to your specific operating system documentation for handling redundant SAN connections.

Step 9: Click **OK**.

Step 10: In the Modify Boot Policy window, in the **Boot Policy** drop-down list, select the new boot policy. This assigns the new boot policy to the profile.

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.

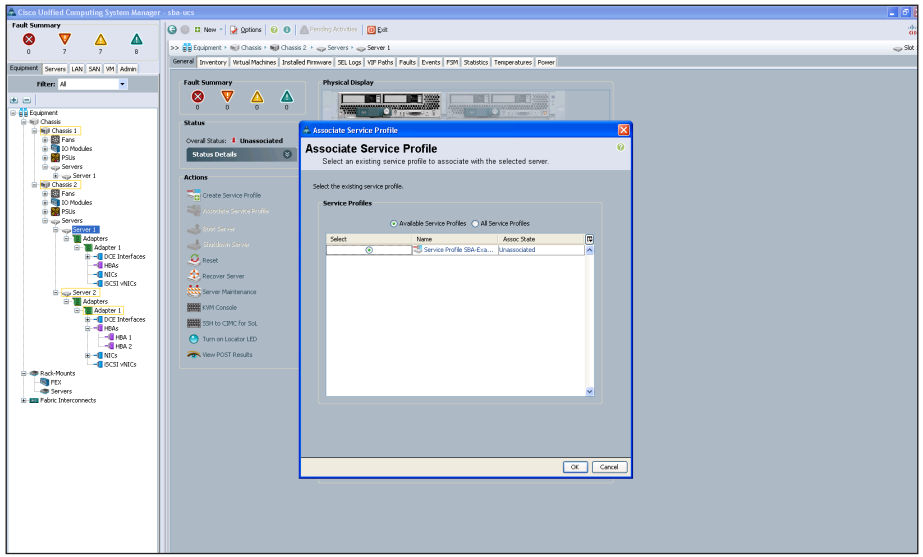
After you complete this step, you can apply the service profile to a server in Cisco UCS.



Procedure 7 Associate Server to Service Profile

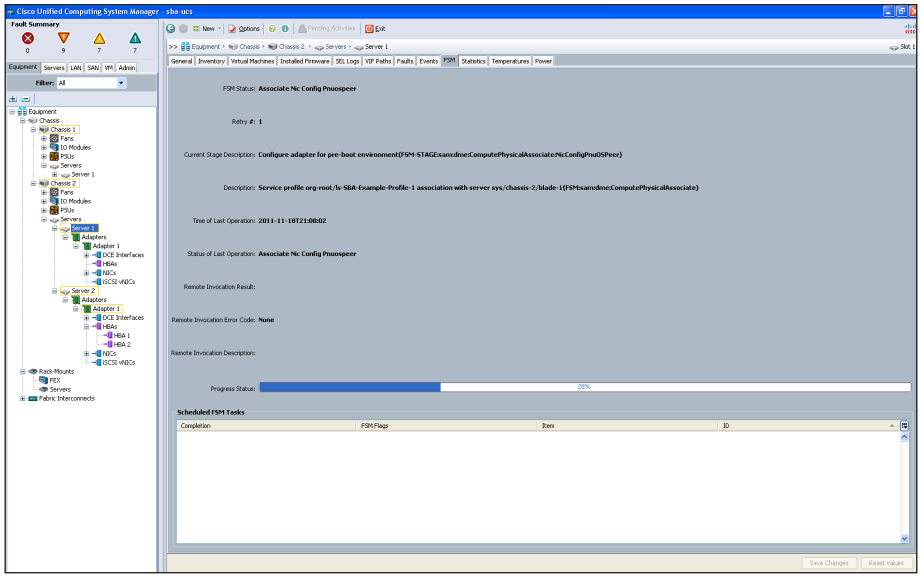
After the service profile is created and boot policy is assigned, associate the service profile to an open server on the chassis.

Step 1: In the navigation pane, click the **Equipment** tab, and then click a **Chassis#** you want to select the Server from. Expand the **Servers** and click on a **Server.** By default, the **General** tab displays. From the **Actions** section click on link **Associate Service Profile.**



Step 2: In the **Associate Service Profile** pop up window by default **Available Service Profiles** is selected which shows the list of unassociated and available Service Profiles. Select the **Name** of service profile from the provided list and click **OK.** This associates the Service Profile to the selected server.

Step 3: In the work pane click the **FSM** tab to check the progress on the Service profile that is being applied on the server. When **Progress Status** reaches 100%, it completes the service profile association to a Server.



After the service profile is applied to a server, you can boot the server, which requires the operating system installation media available by locally attached removable media or KVM Console Virtual Media. For further details on how to install VMware on a server please refer to *SBA Midsize Data Center Virtualization with UCS, Nexus 1000v and VMware Deployment Guide*.

The installation begins as is typical for the given operating system. When you choose a target disk destination for the installation, ensure that the new LUN 0, accessible over the Fibre Channel SAN, is selected. 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.

Process

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:

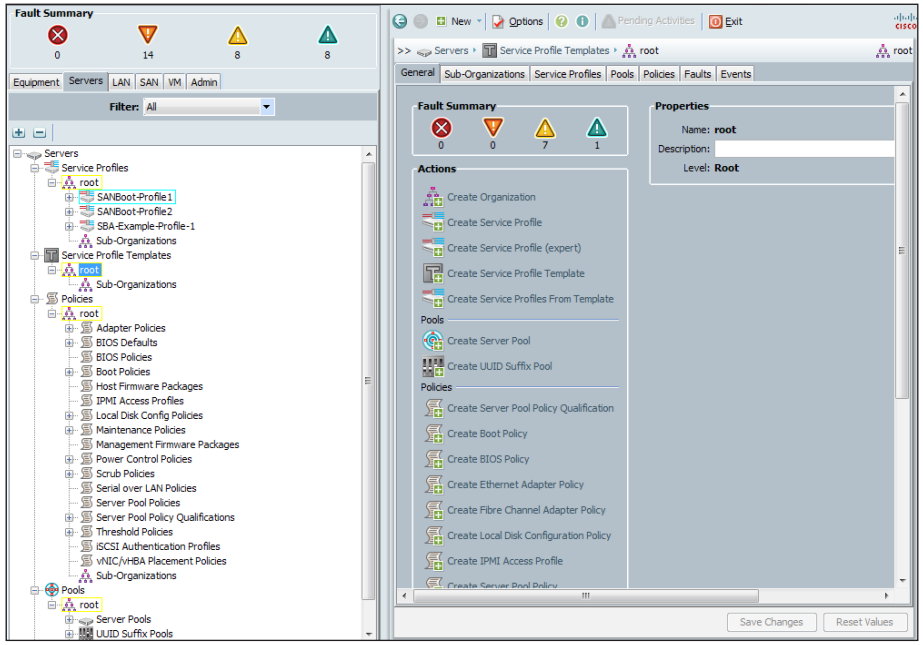
- **Initial templates—**A service profile created from an initial template initially inherits all the properties of the template, but after you create the profile, it is no longer connected to the template. If any changes were to be made to one or more profiles created from this template, you must change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

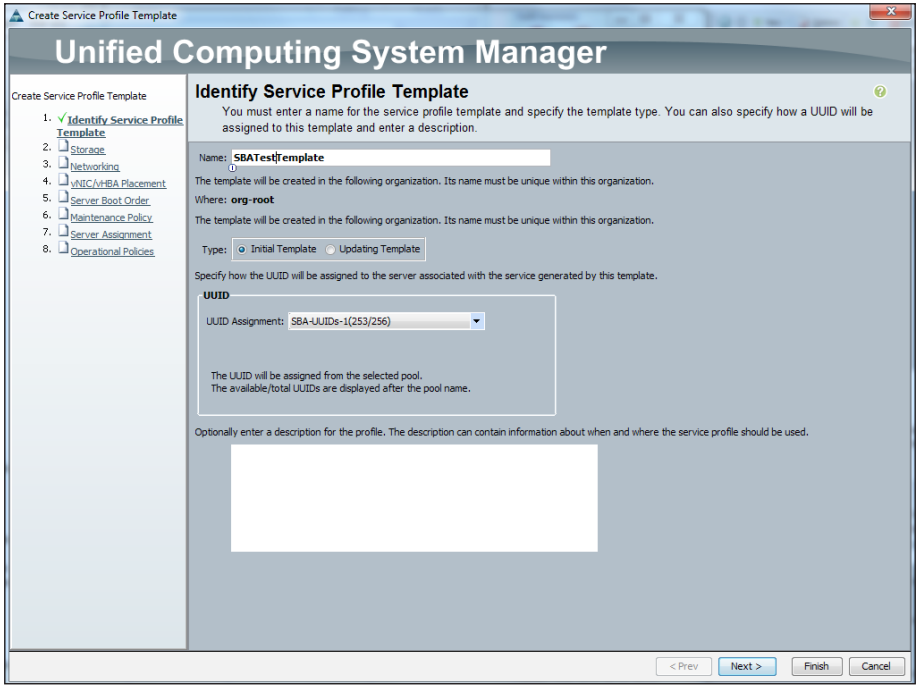
Step 2: In the work pane, on the General tab, click **Create Service Profile Template.** Alternatively you can right click on an existing profile and select **Create Service Profile Template**.



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.

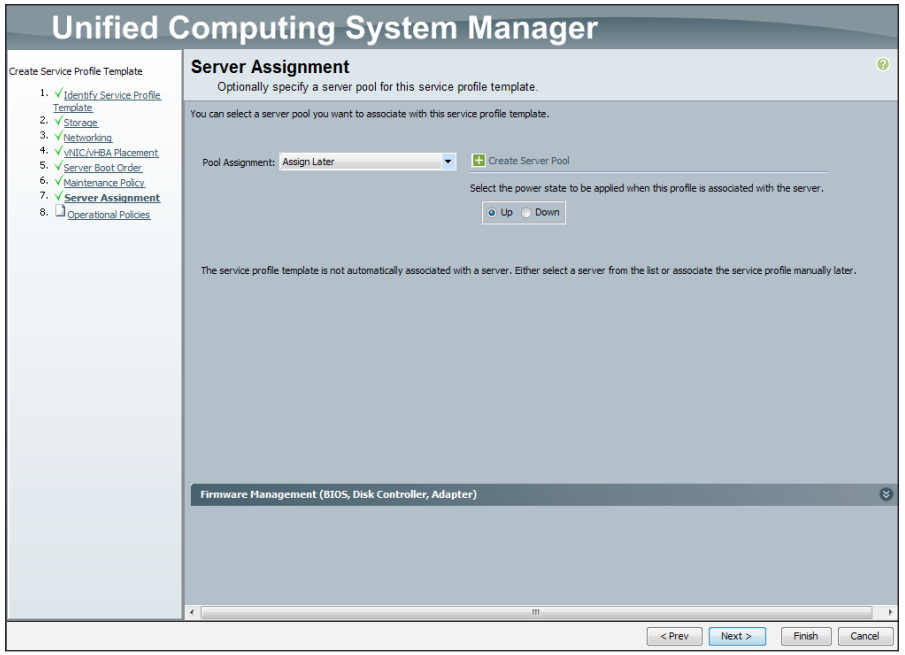
Step 5: In the **UUID Assignment** list, choose an existing UUID pool, and then click **Next**.



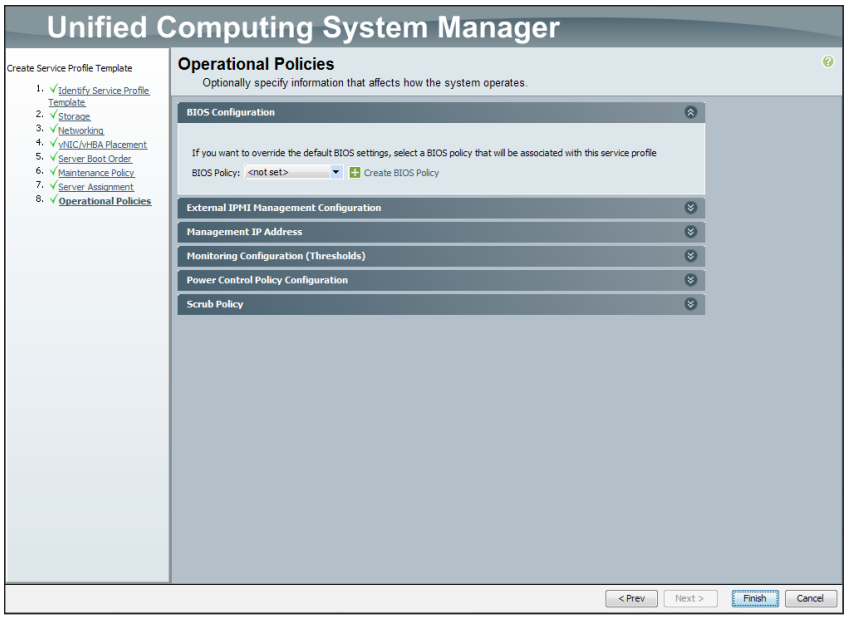
Step 6: Follow the steps listed under the respective procedures in the process "Creating an Initial Service Profile for Local Boot" to fill all required fields for the **Storage, Networking, vNIC/vHBA Placement, Server Boot Order**, and **Maintenance Policy**.

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: Click **Next**.



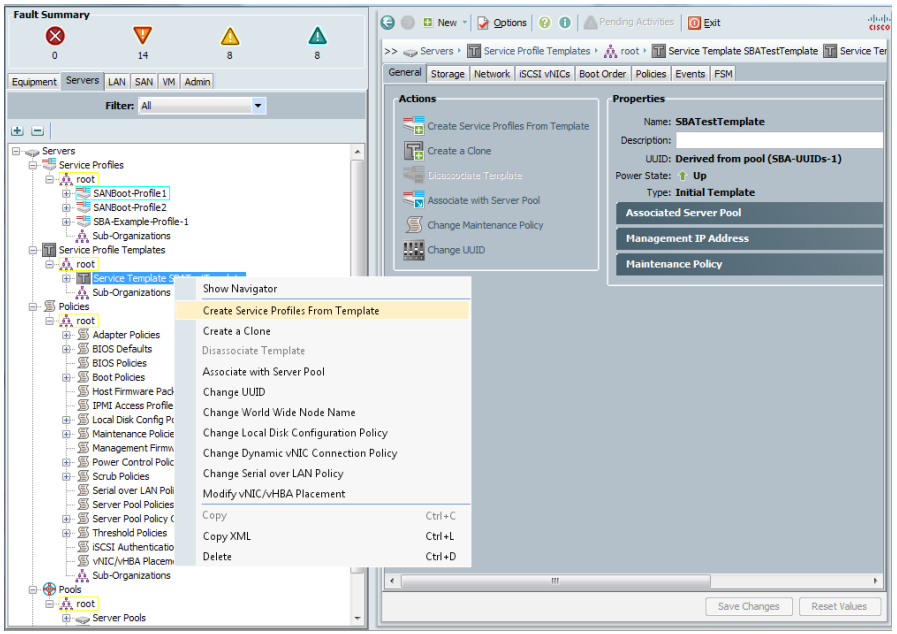
Step 8: Leave default settings for the **Operational Policies**, and then click **Finish**.



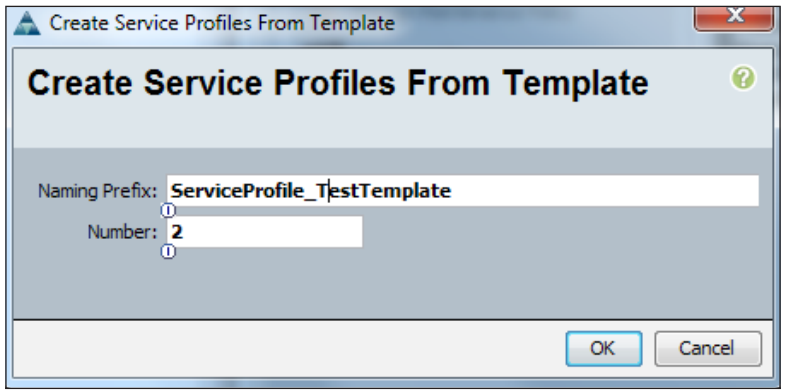
Procedure 2 Create a service profile from a template

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.**

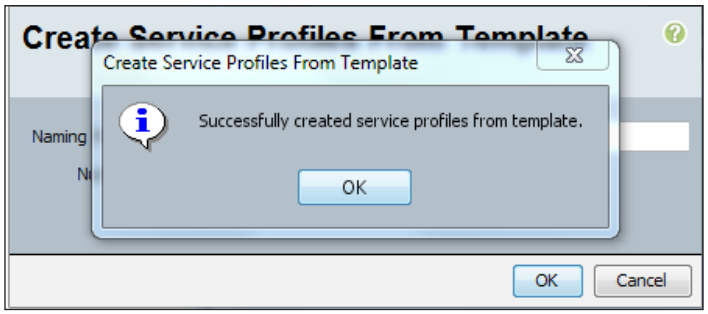
Step 2: Right-click the service profile template you want to create the profiles from. Alternatively choose **Create Service Profile From Template** in the work pane.



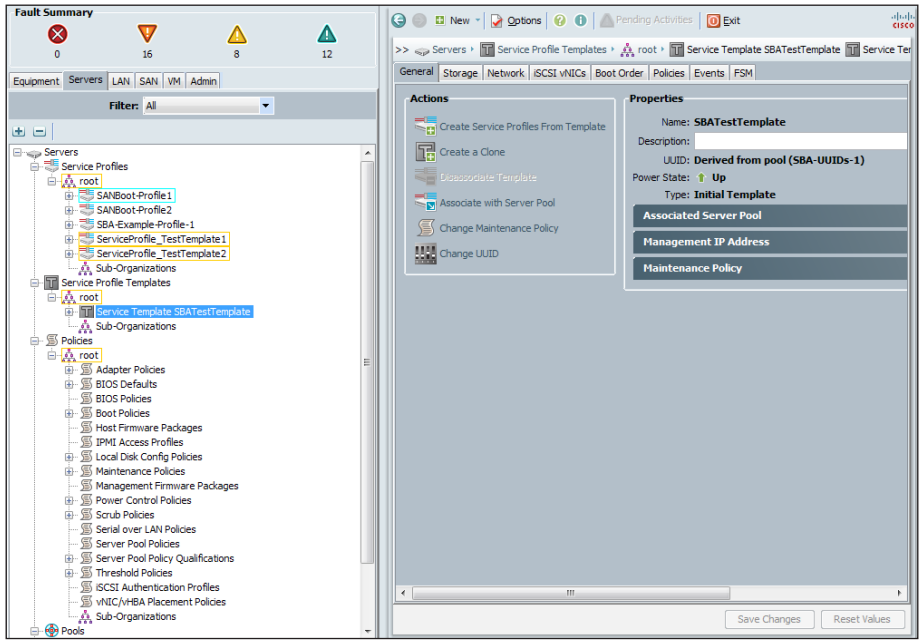
Step 3: In the **Create Service Profiles from Template** window, enter a **Naming Prefix** for the new profiles, enter the **Number** of profiles you want to create (or leave the default value of 2), and then click **OK**.



Step 4: Click **OK** on the message "Successfully created service profiles from template."



Step 5: In the navigation pane under Servers, select **Service Profiles** under the **root** organization and validate that your new service profiles were created.



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

Notes

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 (Cisco IMC) to configure server settings.

Cisco IMC is the management service for the Cisco UCS C-Series servers. Cisco IMC runs within the server. Cisco IMC 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 Cisco SBA midsize 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. Details for data center core port configurations are covered in the *Cisco SBA for Midsize Organizations—Data Center Deployment Guide*.

Process

Configuring Cisco IMC

1. Configure management access

Procedure 1 Configure management access

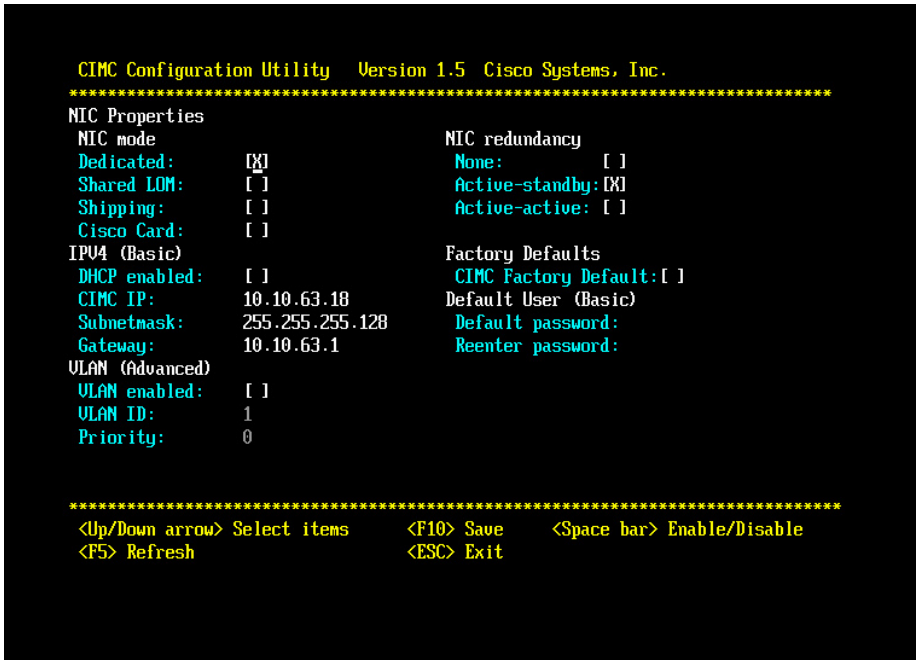
To access the Cisco IMC controller remotely, you must either statically assign a management IP address or have a DHCP server servicing the VLAN or subnet that the server is connected to. This procedure assigns a static IP address to the server and requires the following information:

- IP address—10.10.63.18
- Subnet mask—255.255.255.128
- Default gateway—10.10.63.1
- Password

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

Step 3: Under **NIC mode**, press **Spacebar** to enable **Dedicated**. The10/100 management ports included on the server are used to access Cisco IMC. The management ports are connected to the out-of-band Ethernet management network which is detailed in the *Cisco SBA for Midsize Organizations—Data Center Deployment Guide*.



Step 4: Under **IPV4 (Basic)**, press **Spacebar** to disable **DHCP enabled**, and then enter **CIMC IP**, **Subnetmask**, and the default **Gateway**.

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

Tech Tip

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

Step 6: Under **Default User (Basic)**, enter a default password. The default username is admin.

Step 7: Press **F10**, and then press **Esc** to exit.

Step 8: Press **F5** (Refresh) to reflect the latest configuration.

Step 9: Wait until the new settings appear, and then reboot the server.

Process

Configuring LSI RAID

1. Configure the LSI RAID adapter

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 two identical 300 GB hard drives with one optional LSI RAID controller. This procedure configures the two drives for RAID 1 (mirroring).

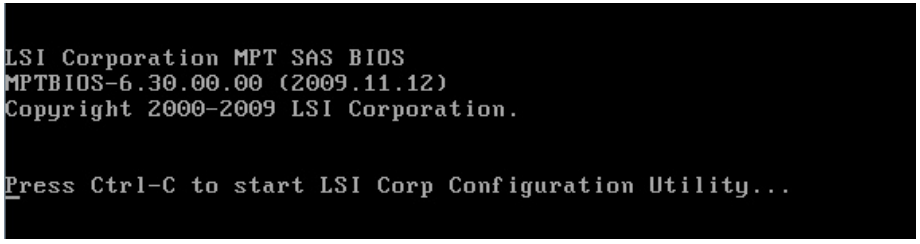
Reader Tip

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.

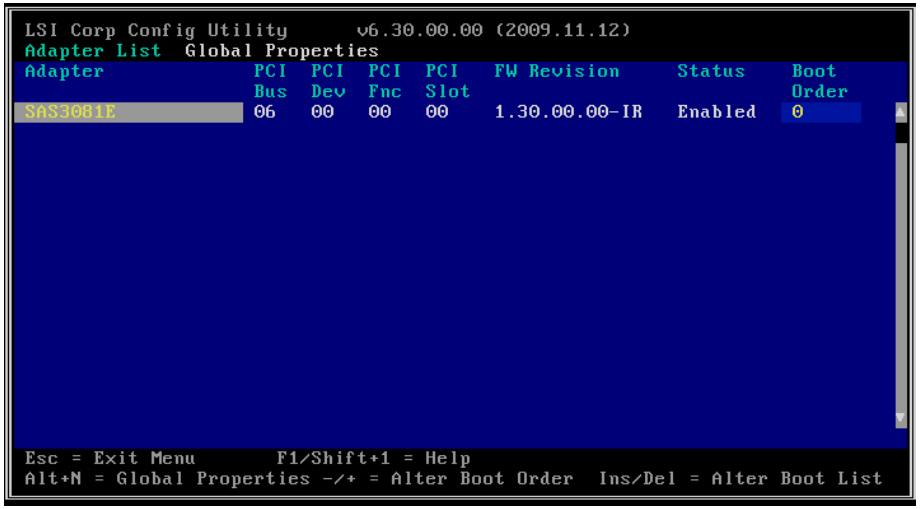
Step 1: After the server has started the boot process, look for the screen as shown in the figure below. When you see this screen, press **Ctrl-C**.

Tech Tip

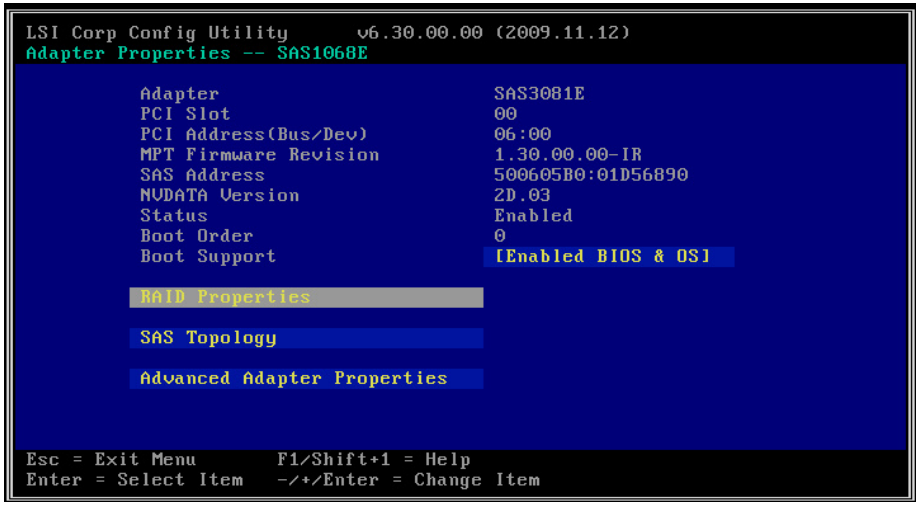
This guide was tested with LSI 1064E and LSI 1068E Raid Controllers. Servers provisioned with other Raid controllers like the LSI MegaRAID will use **Ctrl-H** to access the Raid web GUI setup screens.



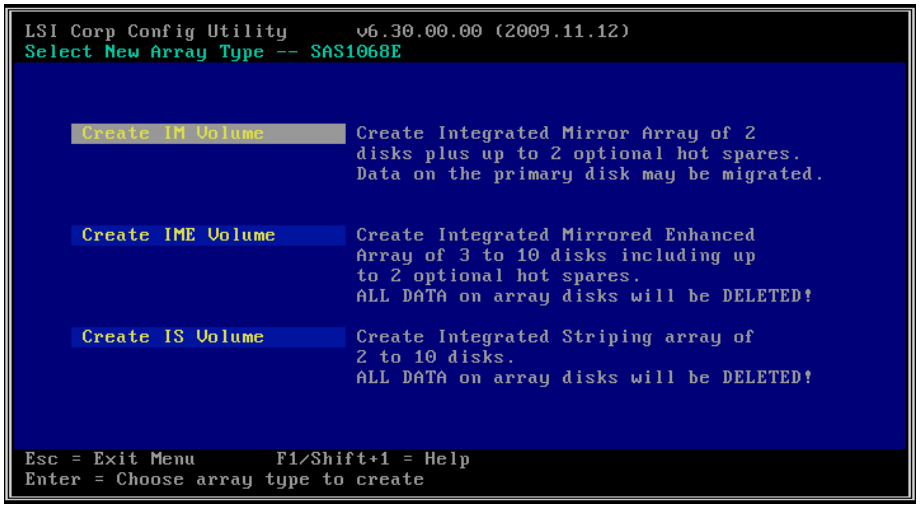
Step 2: Choose the controller, and then press **Enter**.



Step 3: On the Adapter Properties screen, choose **RAID Properties**, and then press **Enter**.

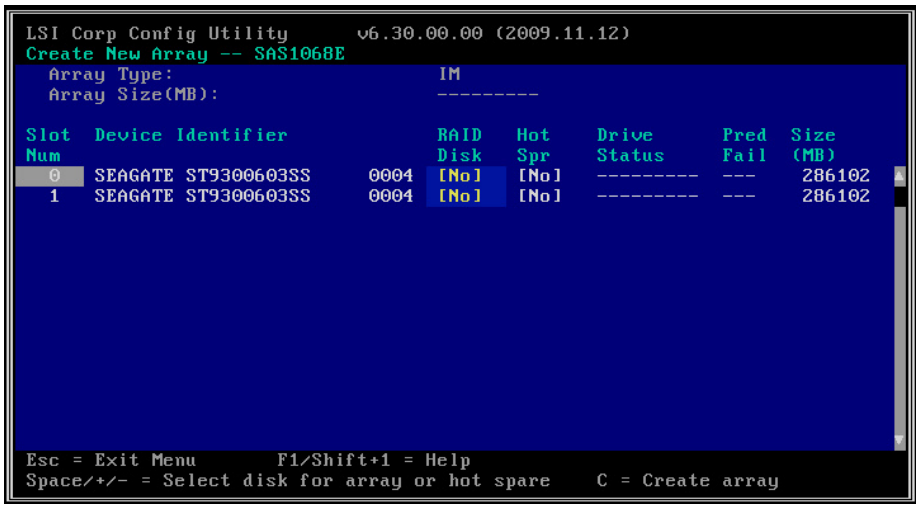


Step 4: On the Select New Array Type screen, choose **Create IM Volume**, and then press **Enter**.



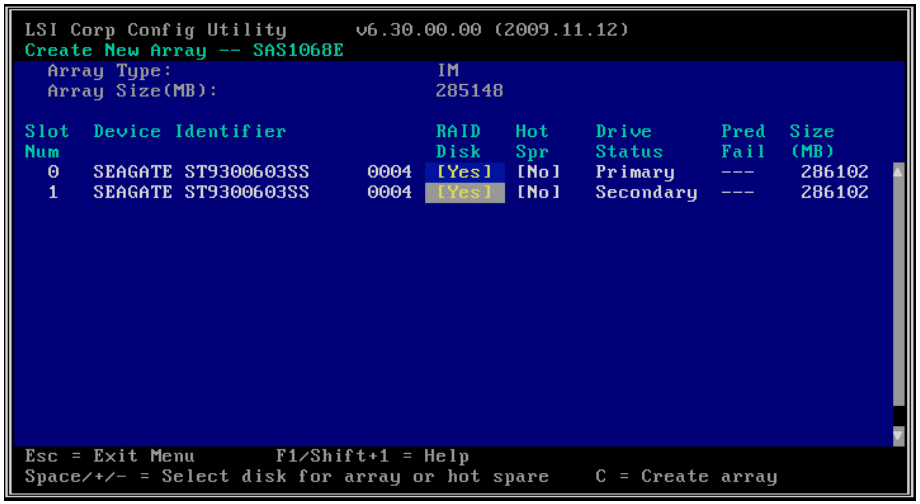
You now proceed to RAID configuration.

Step 5: On the **Create New Array** screen, choose the disk in slot number 0, use the **Tab** key to choose **RAID Disk**, and then press **Spacebar**.



Step 6: In the screen that appears, press **D**. The **RAID Disk** field will change from **No** to **Yes**.

Step 7: Repeat Step 5 and Step 6 for the disk in slot number 1.



Step 8: When both disks have been selected for RAID, press **C** to create the array.

Step 9: Press **Esc**, and then choose **Save and exit**. The host will reboot.

Process

Updating Firmware for Cisco UCS C-Series Server

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

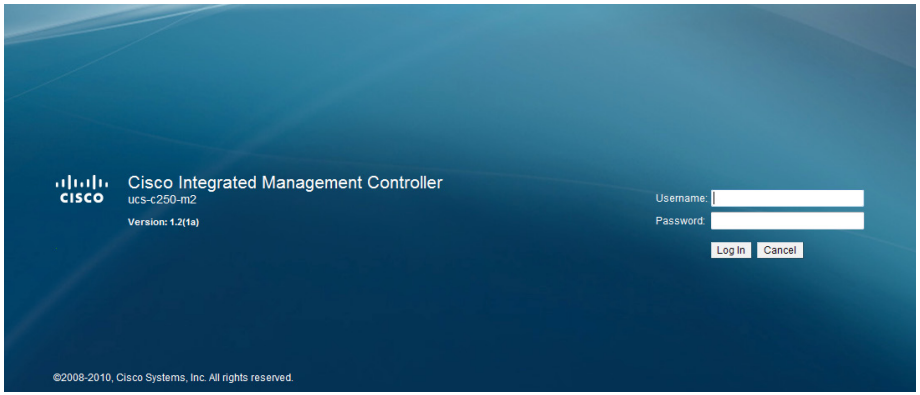
It is recommended that you update your Cisco UCS C-Series servers with the latest firmware and BIOS. The Cisco P81E VIC card requires Management Controller Firmware version 1.2.X or later. Support for configuration of FCoE over Network Interface Virtualization (NIV) needs Management Controller Firmware version 1.4.1 or later.

Procedure 1 Configure virtual media

Step 1: Open the Cisco IMC login page by entering the IP address you configured earlier in Step 4 of the "Configure the management network" procedure under the "Configuring Cisco IMC" process, in a browser.

Step 2: You will receive a Security Certificate warning in your browser on initial login before you can connect to the login screen. **Accept** the certificate.

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

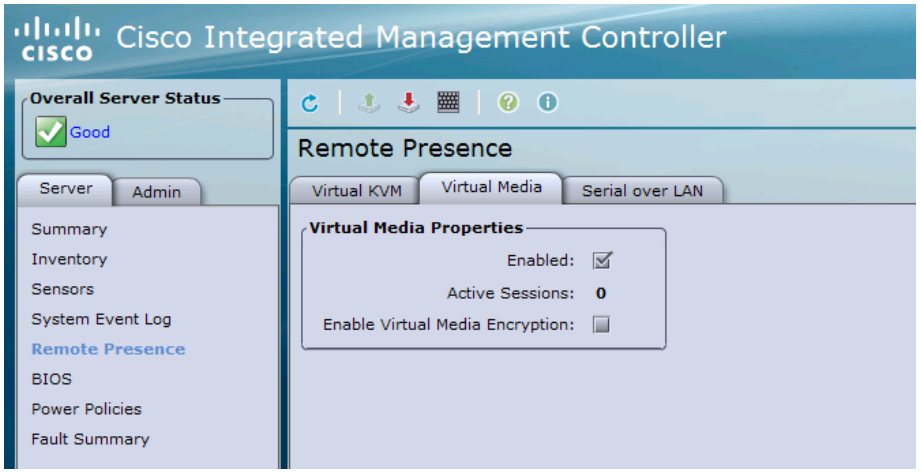


Tech Tip

You can launch the Cisco IMC 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.

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

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



Tech Tip

If you do not select **Enabled**, you will receive the error "Either Virtual Media is detached or ..." when you try to map a remote disk.

Step 6: Click **Save Changes**.

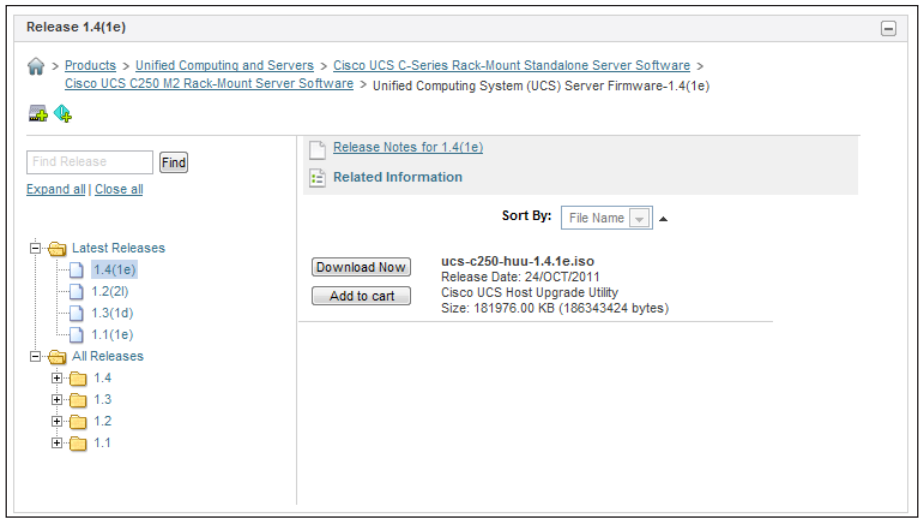
Procedure 2 Upgrade UCS C-Series server firmware

Step 1: You can use the Cisco Host Upgrade utility to upgrade the following firmware:

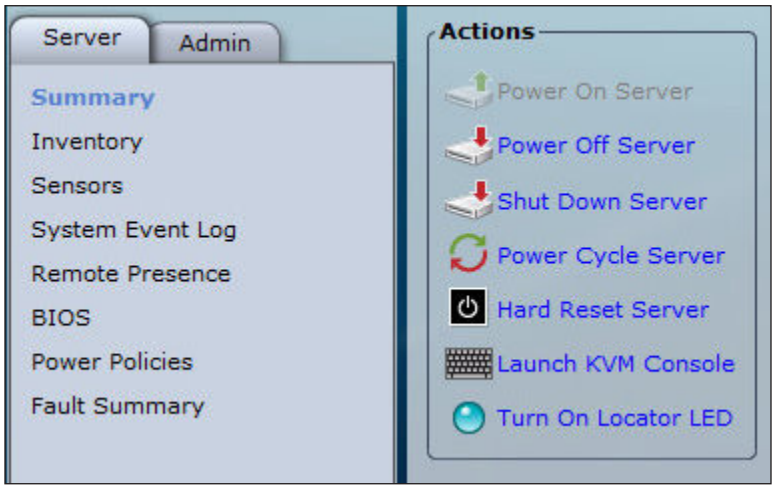
- Cisco IMC
- System BIOS
- LAN on motherboard
- LSI
- Cisco UCS P81E Virtual Interface Card

Download the Cisco UCS Host Upgrade utility ISO file from www.cisco.com. The version of Cisco UCS used in this guide is Server Firmware version 1.4(1e).

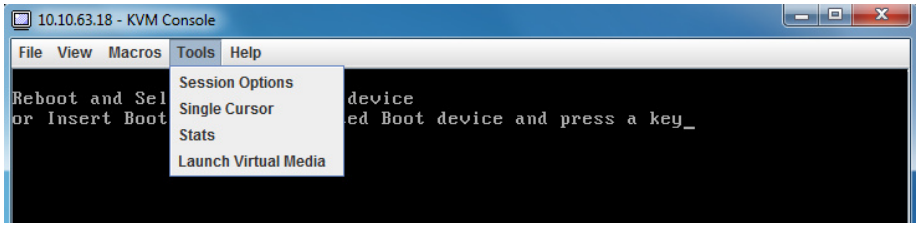
Step 2: Locate the ISO file corresponding to the model of your server, download the file, and store it locally on your hard disk.



Step 3: In the Cisco IMC Console, on the Server tab, click **Summary**, and then click **Launch KVM Console**.



Step 4: In the KVM Console dialog box, from the **Tools** menu, choose **Launch Virtual Media**. The virtual media feature allows for media on your desktop to be available to the remote host.

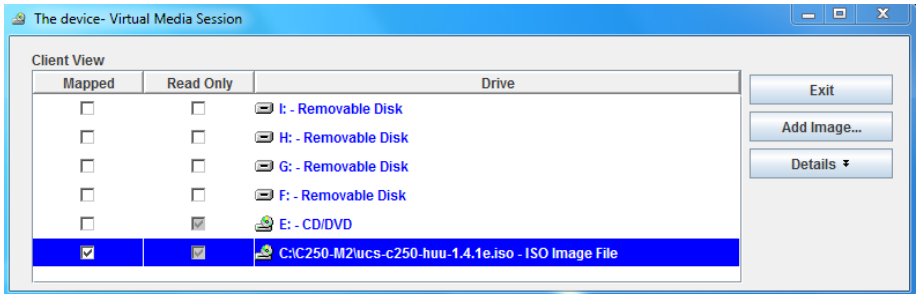


Reader Tip

If your Management Controller Firmware version is later than 1.3(1), you will see a KVM tab and VM tab. The KVM tab provides CLI access to the server. The VM tab allows you to map your disk drive or disk image files to virtual CD/DVD or floppy drives on the server.

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

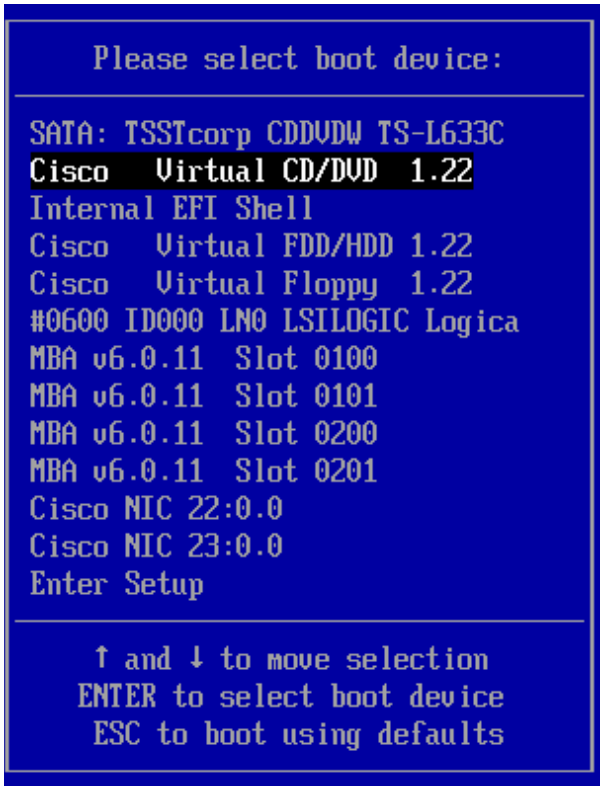
Step 6: Select the check box in the **Mapped** column for the ISO file. Do not click Exit when complete, proceed to the next step.



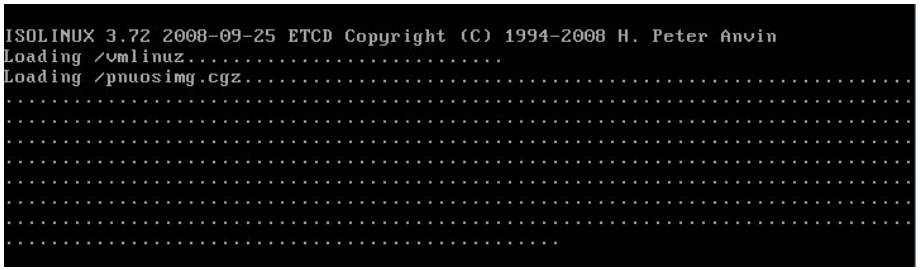
Step 7: In the KVM console, click the Macros tab; and then press **Ctrl-Alt-Del**. The server reboots.

If you are using a new server that has had no BIOS changes, skip the next step, because it is the default to boot from the Cisco Virtual CD/DVD. If server boot BIOS changes may have been made, follow the next step to ensure that the server will boot from the Virtual CD/DVD so you can load the upgrade files from the ISO image mounted earlier.

Step 8: (Optional) During the server's power-on self-test, press **F6**. Use the arrow key to select **Cisco Virtual CD/DVD**, and then press **Enter**. Do not close the virtual media screen while it is in use.



Step 9: 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 10: After the server loads the upgrade utility and displays the screen below, press **n** to read the Cisco EULA, and then press **y** to accept the EULA.

```
C-Series Host Based Upgrade v1.4(1e)
(c) 2011 Cisco Systems, Inc. All rights reserved.

C250M2 Server
------------
CIMC ............... 1.2(1a)
BIOS ............... C250.1.2.1b.0.080920102215
LOM1 BCM5709  ...... Version not available
LOM2 BCM5709  ...... Version not available
LSI 3081  .......... 01.30.00.00
UCS P81E Slot 4 .... 1.5(0.11)
Broadcom PCI Devices :
No Devices Found
Intel PCI Devices :
No Devices Found

This tool supports updating of CIMC/BIOS/LOM/LSI/UCS-P81E/Broadcom/Intel images
.
Once the update starts it cannot be stopped. After updating the
system will be rebooted when exited.


Have you read Cisco EULA?
Press 'y' to continue , 'n' to read EULA, 'q' to exit(reboot)
```

Step 11: In the Host upgrade utility screen, at the Enter Choice prompt, enter **8**. This choice upgrades Cisco IMC, BIOS, LAN on motherboard (LOM), LSI, P81E VIC firmware, and PCI adapters.

```
C-Series Host Based Upgrade v1.4(1e)
(c) 2011 Cisco Systems, Inc. All rights reserved.

C250M2 Server
----------------------

0) Inventory
1) Update CIMC Firmware  - 1.4(1d)
2) Update BIOS           - C250.1.4.1c.0
3) Update LOM Firmware   - C250T6045-2.0
4) Update LSI Firmware   - 3081(1.32.04.00)
5) Update UCS P81E VIC   - 1.6(1c)
6) Update BCM 5709(Dual Port)    - No Device
          BCM 5709(Quad Port)    - No Device
          BCM 57711(Dual Port)   - No Device
          BCM 57712(Dual Port)   - No Device
7) Update INTEL 82576(Quad Port)  - No Device
8) All the above
9) Save logs into USB
10) Reboot (Retains current settings of CIMC)
11) Reboot (Restore factory default settings)

Enter Choice : _
```

The firmware upgrade begins and status can be monitored as in the following figure.

```
Updating CIMC firmware from 1.2(1a) to 1.4(1d)
------------------------------------------------------------------
[Approx Time : 13-15 min]


Firmware Update Utility v1.1 Build 6
Copyright (c) 2010 Cisco Systems Inc.
All rights reserved.


Locked the front panel.


Current Firmware Version
------------------------
Running Version    : 1.2(1a)
Backup Version     : 1.2(1a)

Transferring Image
------------------
Host to CIMC FileSystem...51%
```

Step 12: After the upgrade is completed, at the Enter Choice prompt, enter **10**. The server will reboot with your existing Cisco IMC settings.

```
C-Series Host Based Upgrade v1.4(1e)
(c) 2011 Cisco Systems, Inc. All rights reserved.

C250M2 Server
----------------------

0) Inventory
1) Update CIMC Firmware  - 1.4(1d)              [ Success ]
2) Update BIOS           - C250.1.4.1c.0        [ Success ]
3) Update LOM Firmware   - C250T6045-2.0        [ LOM1-Success LOM2-Success ]
4) Update LSI Firmware   - 3081(1.32.04.00)     [ LSI_3081-Success ]
5) Update UCS P81E VIC   - 1.6(1c)               [ Slot4-Success ]
6) Update BCM 5709(Dual Port)    - No Device
          BCM 5709(Quad Port)    - No Device
          BCM 57711(Dual Port)   - No Device
          BCM 57712(Dual Port)   - No Device
7) Update INTEL 82576(Quad Port)  - No Device
8) All the above
9) Save logs into USB
10) Reboot (Retains current settings of CIMC)
11) Reboot (Restore factory default settings)

Enter Choice : 10
```

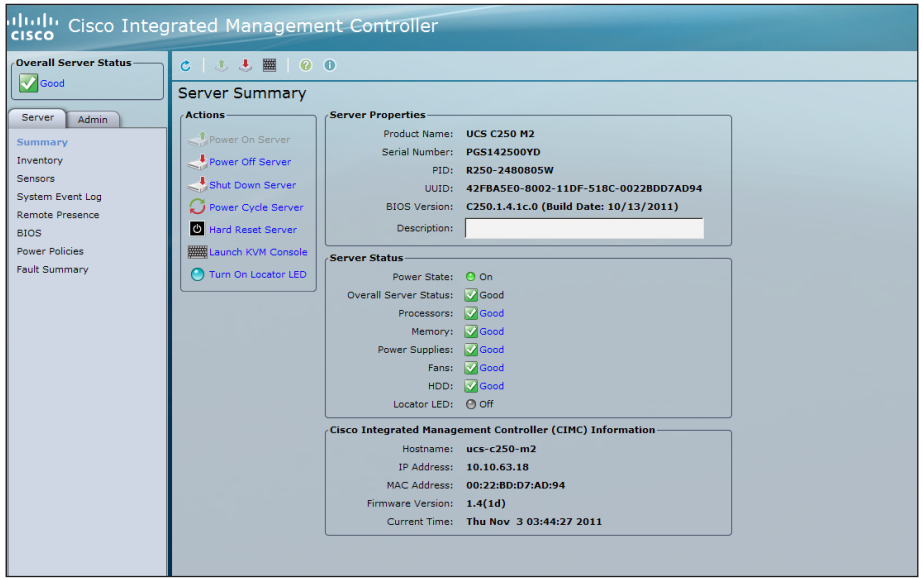
Step 13: To complete LAN on Motherboard (LOM) firmware update, you will be prompted to fully cycle the server power, unplug the power cords from all power supplies, and then reconnect them.

```
Please do A/C power cycle for LOM upgrade to be effective


As firmware has been updated, activating the firmware
Success in activating the image (CIMC will reset)

Waiting for CIMC to boot (Approx time taken is 1 min) .....
```

Step 14: After you cycle power and boot the server, log in to Cisco IMC to reestablish the connection. Verify under **Server Properties** that the **BIOS Version** has been updated, and under **Cisco IMC** that the **Firmware Version** has been updated.



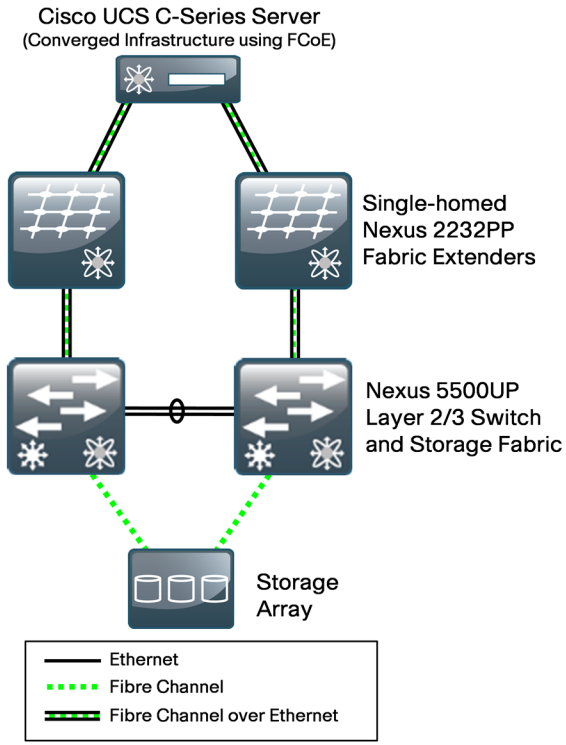
Process

Configuring Ethernet and FCoE Connectivity

1. Configure vNICs
2. Configure vHBAs

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.

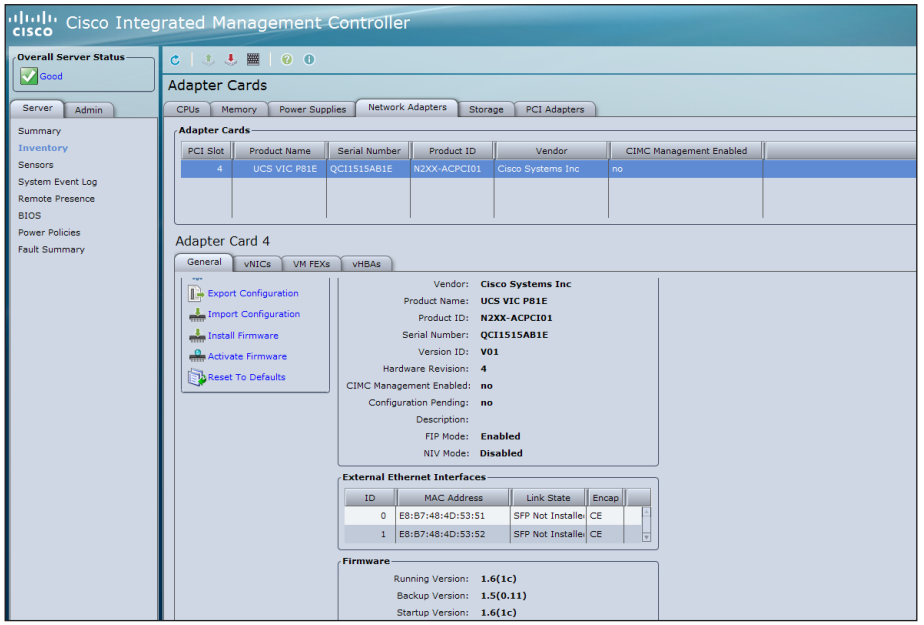
The FCoE-connected server is controlled by two drivers for Fibre Channel and Ethernet, respectively. Fibre Channel traffic over Ethernet is transparent to the operating system of the server. It operates as a Small Computer System Interface (SCSI) Initiator running over FCoE acting as if the server were 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 (PCIe) virtualization, the adapter will show 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

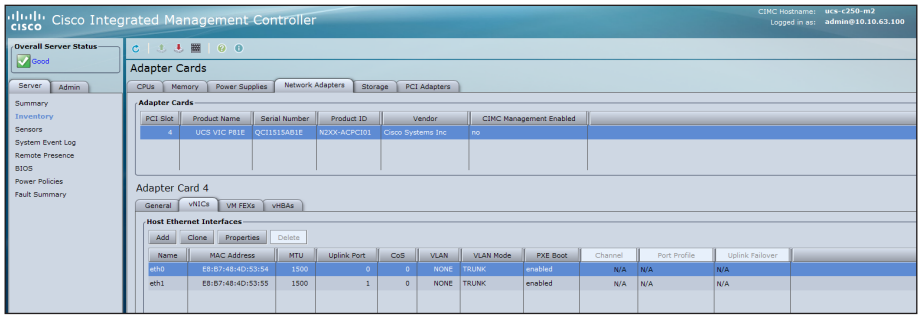
Step 1: In the Cisco IMC console navigation pane, click the **Server** tab, and then click **Inventory**.

Step 2: On the **Network Adapters** tab, click the adapter.

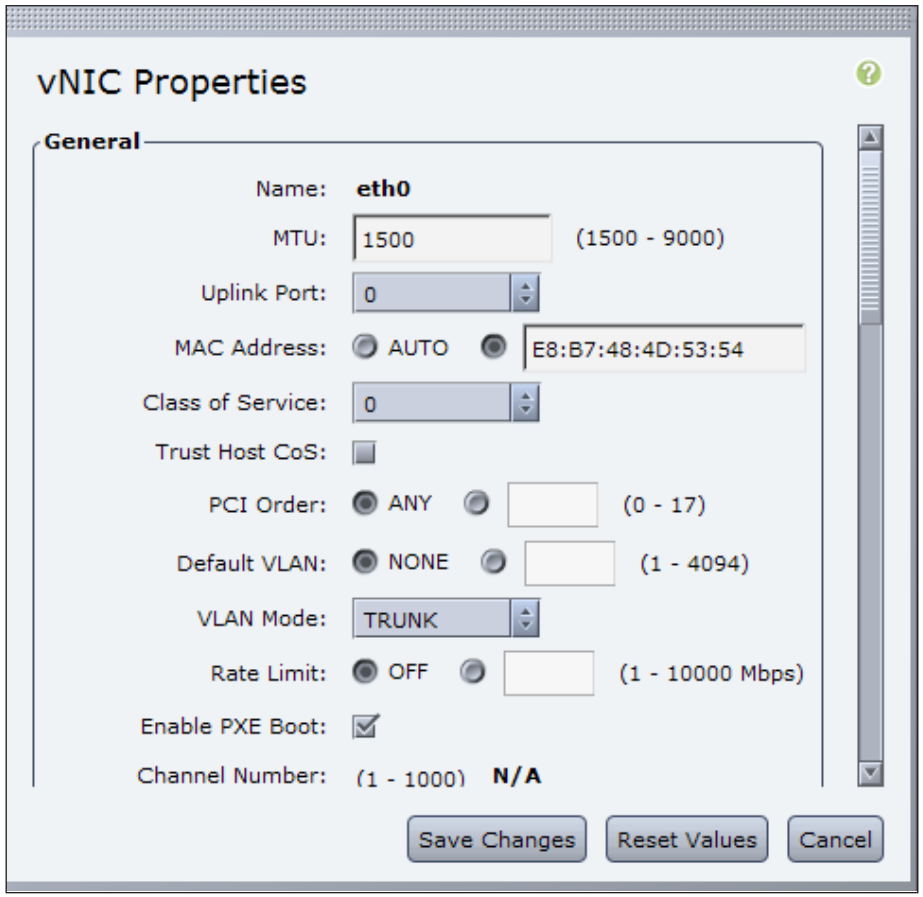


Step 3: On the General tab in the tabbed menu below the Adapter Cards area, verify that **FIP Mode** is set to **Enabled**. If the FIP mode is not enabled, click **Modify Adapter Properties**, select the **Enable FIP Mode** check box, and then click **Save Changes**. FIP mode ensures that the adapter 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.



Step 5: Click **Properties**.



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 will 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 on the Cisco P81E 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 will typically have 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 for the second vNIC, and ensure that the vNIC properties are the same as you set in Step 6 and Step 7.

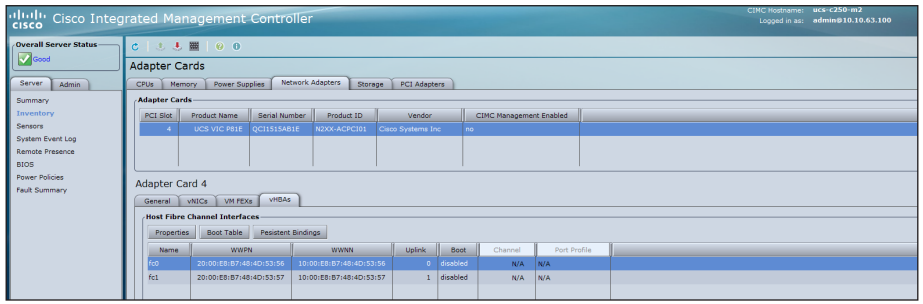
Procedure 2 Configure vHBAs

The Cisco P81E converged network adapter includes two physical 10–Gigabit Ethernet ports and has two vHBAs created by default. The two vHBAs labeled as **fc0** and **fc1** are connected to the upstream data-center core switches Nexus 5548-1 and Nexus 5548-2, respectively, as configured in the *Cisco SBA for Midsize Organizations—Data Center Deployment Guide* . VSAN allows logical partitioning of the physical SAN infrastructure. Cisco recommends dedicating 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 Deployment Guide*.

Data Center Core Switch	VSAN	FCoE VLAN
Nexus 5548-1	4	304
Nexus 5548-2	5	305

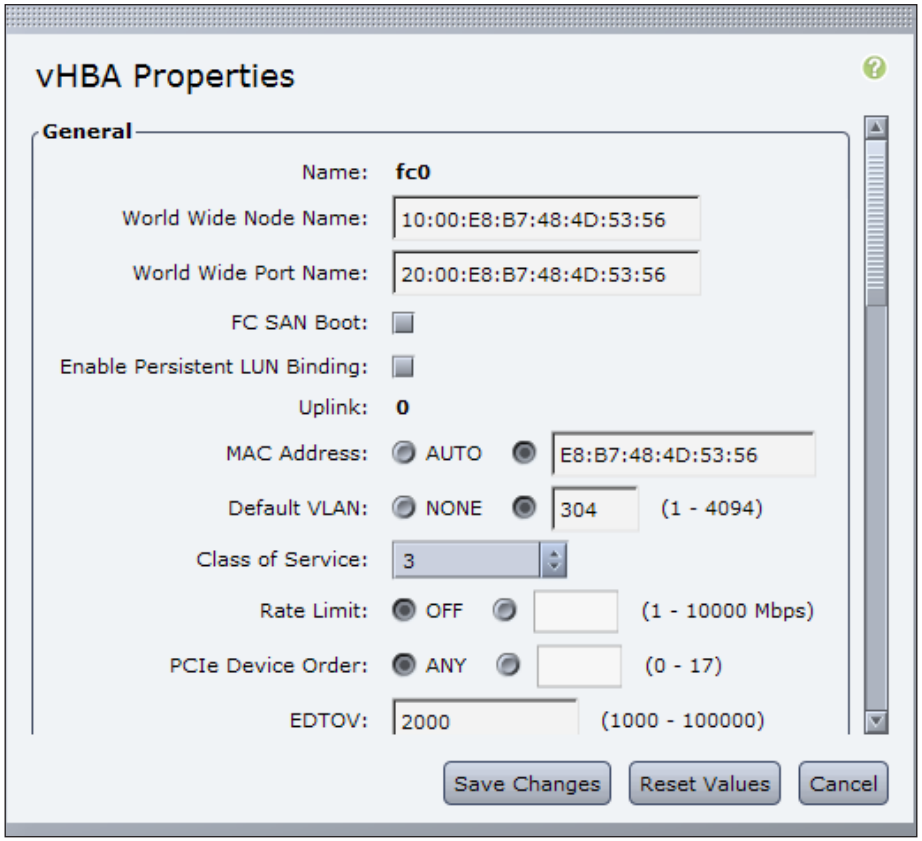
FCoE Initialization Protocol (FIP) is the control plane protocol used to establish the FCoE virtual link between the Ethernet-attached Fibre Channel node and the FCoE switch. FIP performs FCoE VLAN discovery by sending untagged frames to its neighbor. It provides a way for the host to log into and log 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 Cisco IMC console. More details about the Fibre Channel and FCoE setup can be found in the *Cisco SBA for Midsize Organizations—Data Center Deployment Guide*.

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



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**.

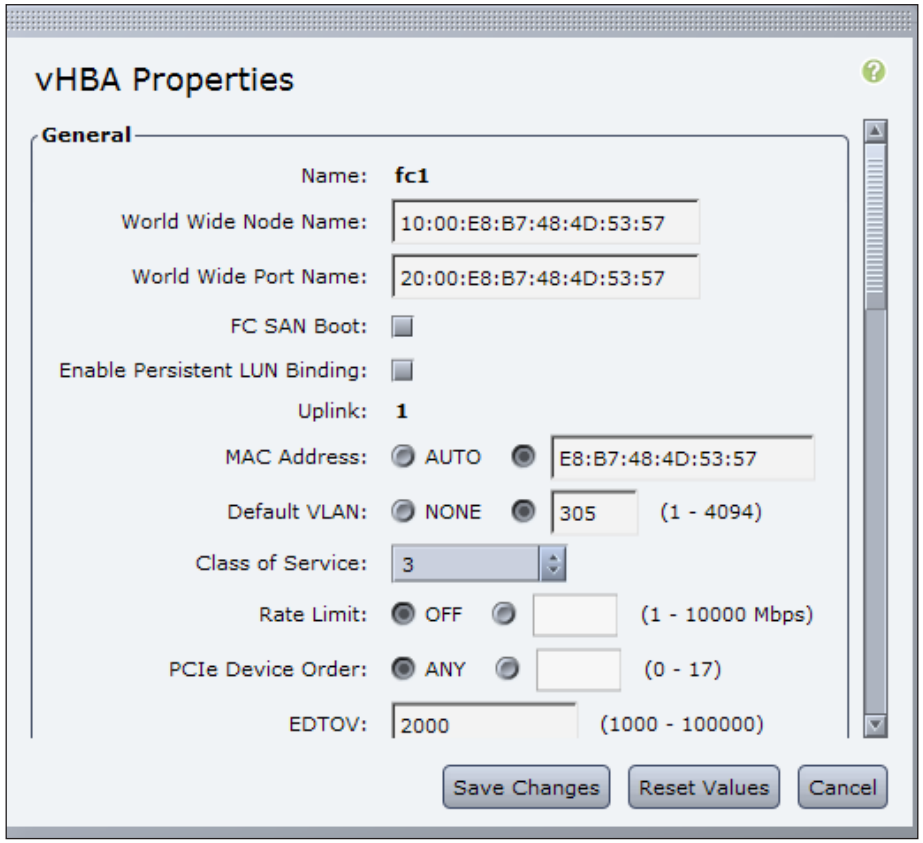
Step 3: In the **Default VLAN** field, select the second radio button, and then enter the FCoE VLAN which in this case is VLAN 304 (as shown in the VSAN to FCoE VLAN table earlier in this procedure).



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**.

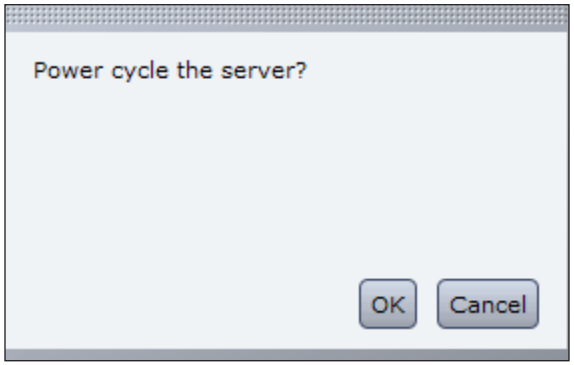
Step 6: In the **Default VLAN** field, select the second radio button, and then enter FCoE VLAN, which in this case is VLAN 305. This value must match with the FCoE VLAN configured in the upstream connected switch.



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: In the Power cycle the server? dialog box, click **OK**.



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

Details on how to configure a VMware environment is explained in detail in the *Cisco SBA for Midsize Organizations—Data Center Virtualization with UCS, Nexus 1000v and VMware Deployment Guide*.

Appendix A: Product List

The following products and software version have been validated for the Cisco Smart Business Architecture:

Functional Area	Product	Part Numbers	Software Version
Ethernet Infrastructure	Nexus 5548UP	N5K-C5548UP-FA	NX-OS 5.1(3)N1(1)
	Nexus 2248TP	N2K-C2248TP-1GE	
	Nexus 2232PP	N2K-C2232PP-10GE	
Storage Infrastructure	MDS 9148	DS-C9148D-8G16P-K9	NX-OS 5.0(7)
	MDS 9124	DS-C9124-K9	
Computing Resources	UCS 6120XP 20-port Fabric Interconnect	N10-S6100	Cisco UCS Release version 2.0t
	6-port 8Gb FC/Expansion module/UCS 6100 Series	N10-E0060	
	UCS 5108 Blade Server Chassis	N20-C6508	
	UCS 2104XP Fabric Extender	N20-I6584	
	UCS B200 M2 Blade Server	N20-B6625-1	
	UCS B250 M2 Blade Server	N20-B6625-2	
	UCS M81KR Virtual Interface Card	N20-AC0002	
	UCS C200 M2 Server	R200-1120402W	
	UCS C210 M2 Server	R210-2121605W	
	UCS C250 M2 Server	R250-2480805W	

Appendix B: Changes

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

- Combined the Ethernet Infrastructure and Fibre Channel Network Infrastructure modules into a module named "Data Center Core Network Infrastructure."
- Added more detail to the UCS C-Series deployment module to describe how to use Cisco IMC to upgrade firmware and program vNICs and vHBAs to prepare a server for operating system installation.
- Integrated the Advanced Configurations module into the main Cisco UCS B-Series and C-Series modules, and moved hypervisor information to the *Cisco SBA for Midsize Organizations—Data Center Virtualization with UCS, Nexus 1000v and VMware Deployment Guide*.

Notes

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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

B-0000597-1 2/12