Cisco UCS Manager GUI Configuration Guide, Release 1.4(1)

First Published: December 07, 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-24087-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at http://cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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

© 2010 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

This preface includes the following sections:

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security

New and Changed Information for this Release

The following table provides an overview of the significant changes to this guide for this current release. The table does not provide an exhaustive list of all changes made to the configuration guides or of the new features in this release. For information about new supported hardware in this release, see the *Release Notes for Cisco UCS Manager* available through the Cisco UCS B-Series Servers Documentation Roadmap.

Table 1: New Features

Feature	Description	Where Documented
Server BIOS setting enhancements	Enables you to configure additional BIOS settings.	Configuring Server-Related Policies, page 301
Chassis level power capping	Enables you to set power capping at the chassis level.	Managing Power in Cisco UCS, page 431
Deferred deployment of service profile changes	Enables you to schedule the deployment of service profile changes that cause the associated server to reboot.	Deferring Deployment of Service Profile Updates, page 347
Fibre Channel switching support	Enables you to configure the Fibre Channel switching mode for the fabric interconnects.	Configuring the Fabric Interconnects, page 53
Firmware upgrade enhancements	Adds support for the new method of releasing firmware bundles.	Managing Firmware, page 147
LDAP enhancements	Provides enhancements to the LDAP integration, including support for LDAP groups.	Configuring Authentication, page 105
MAC address synchronization	Enhances failover in a cluster configuration by replicating MAC addresses on both the primary and the secondary fabric interconnects.	System Configuration Type, page 54
Management IP address enhancements	Enables you to configure a static or pooled management IP address on a server and in the service profile associated with a server.	Setting the Management IP Address, page 295
Multiple simultaneous authorizations	Enables you to configure Cisco UCS Manager to use more than one primary authentication database to authorize remote user logins.	Configuring Authentication, page 105
Port and port channel types	Adds support for additional types of ports and port channels, including Fibre Channel storage ports, Fibre Channel over Ethernet storage ports, appliance ports for network-attached storage, and Fibre Channel port channels.	Configuring Ports, page 65
Private VLAN	Enables you to configure private VLANs in the Cisco UCS instance.	Configuring Named VLANs, page 223

Feature	Description	Where Documented
Rack-mount server integration	Enables you to integrate and manage Cisco UCS C-series rack-mount servers with Cisco UCS Manager.	Managing Rack-Mount Servers, page 515 Information about how to integrate these servers is available in the hardware installation guide for each server.
SNMP enhancements	Enhances support for SNMP monitoring.	Configuring Communication Services, page 89
System monitoring documentation enhancements	Enables you to find all documentation related to system monitoring in one part of the configuration guide.	System Monitoring, page 553
Traffic Monitoring	Provides support for traffic monitoring through SPAN functionality.	Monitoring Traffic, page 555

Organization

This document includes the following parts:

Part	Title	Description
Part 1	Introduction	Contains chapters that provide an overview of Cisco Unified Computing System (Cisco UCS) and Cisco UCS Manager.
Part 2	System Configuration	Contains chapters that describe how to configure fabric interconnects, ports, communication services, primary authentication, and role-based access control configuration, and how to manage firmware and the capability catalog on a system.
Part 3	Network Configuration	Contains chapters that describe how to configure named VLANs, LAN pin groups, MAC pools, and Quality of Service (QoS).
Part 4	Storage Configuration	Contains chapters that describe how to configure named VSANs, SAN pin groups, and WWN pools.
Part 5	Server Configuration	Contains chapters that describe how to configure server-related policies, server-related pools, service profiles, and server power usage.
Part 6	System Management	Contains chapters that describe how to manage a Cisco UCS instance, including managing the chassis, servers, and I/O modules, and how to back up and restore the configuration.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands, keywords, GUI elements, and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information that the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem*.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver	Means *the described action saves time*. You can save time by performing the action described in the paragraph.
Warning	Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.

Related Documentation

A roadmap that lists all documentation for Cisco Unified Computing System (Cisco UCS) is available at the following URL:

http://www.cisco.com/go/unifiedcomputing/b-series-doc

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

PART I

Introduction

CHAPTER 1

Overview of Cisco Unified Computing System

This chapter includes the following sections:

About Cisco Unified Computing System

Cisco Unified Computing System (Cisco UCS) fuses access layer networking and servers. This high-performance, next-generation server system provides a data center with a high degree of workload agility and scalability.

The hardware and software components support Cisco's unified fabric, which runs multiple types of data center traffic over a single converged network adapter.

Architectural Simplification

The simplified architecture of Cisco UCS reduces the number of required devices and centralizes switching resources. By eliminating switching inside a chassis, network access-layer fragmentation is significantly reduced.

Cisco UCS implements Cisco unified fabric within racks and groups of racks, supporting Ethernet and Fibre Channel protocols over 10 Gigabit Cisco Data Center Ethernet and Fibre Channel over Ethernet (FCoE) links.

This radical simplification reduces the number of switches, cables, adapters, and management points by up to two-thirds. All devices in a Cisco UCS instance remain under a single management domain, which remains highly available through the use of redundant components.

High Availability

The management and data plane of Cisco UCS is designed for high availability and redundant access layer fabric interconnects. In addition, Cisco UCS supports existing high availability and disaster recovery solutions for the data center, such as data replication and application-level clustering technologies.

Scalability

A single Cisco UCS instance supports multiple chassis and their servers, all of which are administered through one Cisco UCS Manager. For more detailed information about the scalability, speak to your Cisco representative.

Flexibility

A Cisco UCS instance allows you to quickly align computing resources in the data center with rapidly changing business requirements. This built-in flexibility is determined by whether you choose to fully implement the stateless computing feature.

Pools of servers and other system resources can be applied as necessary to respond to workload fluctuations, support new applications, scale existing software and business services, and accommodate both scheduled and unscheduled downtime. Server identity can be abstracted into a mobile service profile that can be moved from server to server with minimal downtime and no need for additional network configuration.

With this level of flexibility, you can quickly and easily scale server capacity without having to change the server identity or reconfigure the server, LAN, or SAN. During a maintenance window, you can quickly do the following:

- Deploy new servers to meet unexpected workload demand and rebalance resources and traffic.
- Shut down an application, such as a database management system, on one server and then boot it up again on another server with increased I/O capacity and memory resources.

Optimized for Server Virtualization

Cisco UCS has been optimized to implement VN-Link technology. This technology provides improved support for server virtualization, including better policy-based configuration and security, conformance with a company's operational model, and accommodation for VMware's VMotion.

Unified Fabric

With unified fabric, multiple types of data center traffic can run over a single Data Center Ethernet (DCE) network. Instead of having a series of different host bus adapters (HBAs) and network interface cards (NICs) present in a server, unified fabric uses a single converged network adapter. This type of adapter can carry LAN and SAN traffic on the same cable.

Cisco UCS uses Fibre Channel over Ethernet (FCoE) to carry Fibre Channel and Ethernet traffic on the same physical Ethernet connection between the fabric interconnect and the server. This connection terminates at a converged network adapter on the server, and the unified fabric terminates on the uplink ports of the fabric interconnect. On the core network, the LAN and SAN traffic remains separated. Cisco UCS does not require that you implement unified fabric across the data center.

The converged network adapter presents an Ethernet interface and Fibre Channel interface to the operating system. At the server, the operating system is not aware of the FCoE encapsulation because it sees a standard Fibre Channel HBA.

At the fabric interconnect, the server-facing Ethernet port receives the Ethernet and Fibre Channel traffic. The fabric interconnect (using Ethertype to differentiate the frames) separates the two traffic types. Ethernet frames and Fibre Channel frames are switched to their respective uplink interfaces.

Fibre Channel over Ethernet

Cisco UCS leverages Fibre Channel over Ethernet (FCoE) standard protocol to deliver Fibre Channel. The upper Fibre Channel layers are unchanged, so the Fibre Channel operational model is maintained. FCoE network management and configuration is similar to a native Fibre Channel network.

FCoE encapsulates Fibre Channel traffic over a physical Ethernet link. FCoE is encapsulated over Ethernet with the use of a dedicated Ethertype, 0x8906, so that FCoE traffic and standard Ethernet traffic can be carried on the same link. FCoE has been standardized by the ANSI T11 Standards Committee.

Fibre Channel traffic requires a lossless transport layer. Instead of the buffer-to-buffer credit system used by native Fibre Channel, FCoE depends upon the Ethernet link to implement lossless service.

Ethernet links on the fabric interconnect provide two mechanisms to ensure lossless transport for FCoE traffic:

- Link-level flow control
- Priority flow control

Link-Level Flow Control

IEEE 802.3x link-level flow control allows a congested receiver to signal the endpoint to pause data transmission for a short time. This link-level flow control pauses all traffic on the link.

The transmit and receive directions are separately configurable. By default, link-level flow control is disabled for both directions.

On each Ethernet interface, the fabric interconnect can enable either priority flow control or link-level flow control (but not both).

Priority Flow Control

The priority flow control (PFC) feature applies pause functionality to specific classes of traffic on the Ethernet link. For example, PFC can provide lossless service for the FCoE traffic, and best-effort service for the standard Ethernet traffic. PFC can provide different levels of service to specific classes of Ethernet traffic (using IEEE 802.1p traffic classes).

PFC decides whether to apply pause based on the IEEE 802.1p CoS value. When the fabric interconnect enables PFC, it configures the connected adapter to apply the pause functionality to packets with specific CoS values.

By default, the fabric interconnect negotiates to enable the PFC capability. If the negotiation succeeds, PFC is enabled and link-level flow control remains disabled (regardless of its configuration settings). If the PFC negotiation fails, you can either force PFC to be enabled on the interface or you can enable IEEE 802.x link-level flow control.

Server Architecture and Connectivity

Overview of Service Profiles

Service profiles are the central concept of Cisco UCS. Each service profile serves a specific purpose: ensuring that the associated server hardware has the configuration required to support the applications it will host.

The service profile maintains configuration information about the server hardware, interfaces, fabric connectivity, and server and network identity. This information is stored in a format that you can manage through Cisco UCS Manager. All service profiles are centrally managed and stored in a database on the fabric interconnect.

Every server must be associated with a service profile.

Important At any given time, each server can be associated with only one service profile. Similarly, each service profile can be associated with only one server at a time.

After you associate a service profile with a server, the server is ready to have an operating system and applications installed, and you can use the service profile to review the configuration of the server. If the server associated with a service profile fails, the service profile does not automatically fail over to another server.

When a service profile is disassociated from a server, the identity and connectivity information for the server is reset to factory defaults.

Network Connectivity through Service Profiles

Each service profile specifies the LAN and SAN network connections for the server through the Cisco UCS infrastructure and out to the external network. You do not need to manually configure the network connections for Cisco UCS servers and other components. All network configuration is performed through the service profile.

When you associate a service profile with a server, the Cisco UCS internal fabric is configured with the information in the service profile. If the profile was previously associated with a different server, the network infrastructure reconfigures to support identical network connectivity to the new server.

Configuration through Service Profiles

A service profile can take advantage of resource pools and policies to handle server and connectivity configuration.

Hardware Components Configured by Service Profiles

When a service profile is associated with a server, the following components are configured according to the data in the profile:

- Server, including BIOS and CIMC
- Adapters
- Fabric interconnects

You do not need to configure these hardware components directly.

Server Identity Management through Service Profiles

You can use the network and device identities burned into the server hardware at manufacture or you can use identities that you specify in the associated service profile either directly or through identity pools, such as MAC, WWN, and UUID.

The following are examples of configuration information that you can include in a service profile:

- Profile name and description
- Unique server identity (UUID)
- LAN connectivity attributes, such as the MAC address
- SAN connectivity attributes, such as the WWN

Operational Aspects configured by Service Profiles

You can configure some of the operational functions for a server in a service profile, such as the following:

- Firmware packages and versions
- Operating system boot order and configuration
- IPMI and KVM access

vNIC Configuration by Service Profiles

A vNIC is a virtualized network interface that is configured on a physical network adapter and appears to be a physical NIC to the operating system of the server. The type of adapter in the system determines how many vNICs you can create. For example, a converged network adapter has two NICs, which means you can create a maximum of two vNICs for each adapter.

A vNIC communicates over Ethernet and handles LAN traffic. At a minimum, each vNIC must be configured with a name and with fabric and network connectivity.

vHBA Configuration by Service Profiles

A vHBA is a virtualized host bus adapter that is configured on a physical network adapter and appears to be a physical HBA to the operating system of the server. The type of adapter in the system determines how many vHBAs you can create. For example, a converged network adapter has two HBAs, which means you can create a maximum of two vHBAs for each of those adapters. In contrast, a network interface card does not have any HBAs, which means you cannot create any vHBAs for those adapters.

A vHBA communicates over FCoE and handles SAN traffic. At a minimum, each vHBA must be configured with a name and fabric connectivity.

Service Profiles that Override Server Identity

This type of service profile provides the maximum amount of flexibility and control. This profile allows you to override the identity values that are on the server at the time of association and use the resource pools and policies set up in Cisco UCS Manager to automate some administration tasks.

You can disassociate this service profile from one server and then associate it with another server. This re-association can be done either manually or through an automated server pool policy. The burned-in settings,

such as UUID and MAC address, on the new server are overwritten with the configuration in the service profile. As a result, the change in server is transparent to your network. You do not need to reconfigure any component or application on your network to begin using the new server.

This profile allows you to take advantage of and manage system resources through resource pools and policies, such as the following:

- Virtualized identity information, including pools of MAC addresses, WWN addresses, and UUIDs
- Ethernet and Fibre Channel adapter profile policies
- Firmware package policies
- Operating system boot order policies

Unless the service profile contains power management policies, a server pool qualification policy, or another policy that requires a specific hardware configuration, the profile can be used for any type of server in the Cisco UCS instance.

You can associate these service profiles with either a rack-mount server or a blade server. The ability to migrate the service profile depends upon whether you choose to restrict migration of the service profile.

Service Profiles that Inherit Server Identity

This hardware-based service profile is the simplest to use and create. This profile uses the default values in the server and mimics the management of a rack-mounted server. It is tied to a specific server and cannot be moved or migrated to another server.

You do not need to create pools or configuration policies to use this service profile.

This service profile inherits and applies the identity and configuration information that is present at the time of association, such as the following:

- MAC addresses for the two NICs
- For a converged network adapter or a virtual interface card, the WWN addresses for the two HBAs
- BIOS versions
- Server UUID

Important The server identity and configuration information inherited through this service profile may not be the values burned into the server hardware at manufacture if those values were changed before this profile is associated with the server.

Service Profile Templates

With a service profile template, you can quickly create several service profiles with the same basic parameters, such as the number of vNICs and vHBAs, and with identity information drawn from the same pools.

Tip If you need only one service profile with similar values to an existing service profile, you can clone a service profile in the Cisco UCS Manager GUI.

For example, if you need several service profiles with similar values to configure servers to host database software, you can create a service profile template, either manually or from an existing service profile. You then use the template to create the service profiles.

Cisco UCS supports the following types of service profile templates:

Initial template	Service profiles created from an initial template inherit all the properties of the template. However, after you create the profile, it is no longer connected to the template. If you need to make changes to one or more profiles created from this template, you must change each profile individually.
Updating template	Service profiles created from an updating template inherit all the properties of the template and remain connected to the template. Any changes to the template automatically update the service profiles created from the template.

Policies

Policies determine how Cisco UCS components will act in specific circumstances. You can create multiple instances of most policies. For example, you might want different boot policies, so that some servers can PXE boot, some can SAN boot, and others can boot from local storage.

Policies allow separation of functions within the system. A subject matter expert can define policies that are used in a service profile, which is created by someone without that subject matter expertise. For example, a LAN administrator can create adapter policies and quality of service policies for the system. These policies can then be used in a service profile that is created by someone who has limited or no subject matter expertise with LAN administration.

You can create and use two types of policies in Cisco UCS Manager:

- Configuration policies that configure the servers and other components
- Operational policies that control certain management, monitoring, and access control functions

Configuration Policies

Boot Policy

The boot policy determines the following:

- Configuration of the boot device
- Location from which the server boots
- Order in which boot devices are invoked

For example, you can choose to have associated servers boot from a local device, such as a local disk or CD-ROM (VMedia), or you can select a SAN boot or a LAN (PXE) boot.

You must include this policy in a service profile, and that service profile must be associated with a server for it to take effect. If you do not include a boot policy in a service profile, the server uses the default settings in the BIOS to determine the boot order.

Important Changes to a boot policy may be propagated to all servers created with an updating service profile template that includes that boot policy. Reassociation of the service profile with the server to rewrite the boot order information in the BIOS is auto-triggered.

Guidelines

When you create a boot policy, you can add one or more of the following to the boot policy and specify their boot order:

Boot type	Description
SAN boot	Boots from an operating system image on the SAN. You can specify a primary and a secondary SAN boot. If the primary boot fails, the server attempts to boot from the secondary. We recommend that you use a SAN boot, because it offers the most service profile mobility within the system. If you boot from the SAN when you move a service profile from one server to another, the new server boots from the exact same operating system image. Therefore, the new server appears to be the exact same server to the network.
LAN boot	Boots from a centralized provisioning server. It is frequently used to install operating systems on a server from that server.
Local disk boot	If the server has a local drive, boots from that drive. **Note** Cisco UCS Manager does not differentiate between the types of local drives. If an operating system has been installed on more than one local drive or on an internal USB drive (eUSB), you cannot specify which of these local drives the server should use as the boot drive.
Virtual media boot	Mimics the insertion of a physical CD-ROM disk (read-only) or floppy disk (read-write) into a server. It is typically used to manually install operating systems on a server.

Note The default boot order is as follows:

1. Local disk boot
2. LAN boot
3. Virtual media read-only boot
4. Virtual media read-write boot

Chassis Discovery Policy

The chassis discovery policy determines how the system reacts when you add a new chassis. Cisco UCS Manager uses the settings in the chassis discovery policy to determine the minimum threshold for the number of links between the chassis and the fabric interconnect. However, the configuration in the chassis discovery policy does not prevent you from connecting multiple chassis to the fabric interconnects in a Cisco UCS instance and wiring those chassis with a different number of links.

If you have a Cisco UCS instance that has some chassis wired with 1 link, some with 2 links, and some with 4 links, we recommend that you configure the chassis discovery policy for the minimum number links in the instance so that Cisco UCS Manager can discover all chassis. After the initial discovery, you must reacknowledge the chassis that are wired for a greater number of links and Cisco UCS Manager configures the chassis to use all available links.

Cisco UCS Manager cannot discover any chassis that is wired for fewer links than are configured in the chassis discovery policy. For example, if the chassis discovery policy is configured for 4 links, Cisco UCS Manager cannot discover any chassis that is wired for 1 link or 2 links. Reacknowledgement of the chassis does not resolve this issue.

The following table provides an overview of how the chassis discovery policy works in a multi-chassis Cisco UCS instance:

Table 2: Chassis Discovery Policy and Chassis Links

Number of Links Wired for the Chassis	1-Link Chassis Discovery Policy	2-Link Chassis Discovery Policy	4-Link Chassis Discovery Policy
1 link between IOM and fabric interconnects	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS instance as a chassis wired with 1 link.	Chassis cannot be discovered by Cisco UCS Manager and is not added to the Cisco UCS instance.	Chassis cannot be discovered by Cisco UCS Manager and is not added to the Cisco UCS instance.
2 links between IOM and fabric interconnects	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS instance as a chassis wired with 1 link. After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS instance as a chassis wired with 2 link.	Chassis cannot be discovered by Cisco UCS Manager and is not added to the Cisco UCS instance.
4 links between IOM and fabric interconnects	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS instance as a chassis wired with 1 link. After initial discovery, reacknowledge the chassis and Cisco UCS	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS instance as a chassis wired with 2 links. After initial discovery, reacknowledge the chassis and Cisco UCS	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS instance as a chassis wired with 4 link.

Number of Links Wired for the Chassis	1-Link Chassis Discovery Policy	2-Link Chassis Discovery Policy	4-Link Chassis Discovery Policy
	Manager recognizes and uses the additional links.	Manager recognizes and uses the additional links.	

Dynamic vNIC Connection Policy

This policy determines how the VN-link connectivity between VMs and dynamic vNICs is configured. This policy is required for Cisco UCS instances that include servers with virtual interface card adapters on which you have installed VMs and configured dynamic vNICs.

Note If you Vmotion a server that is configured with dynamic vNICs, the dynamic interface used by the vNICs fails and Cisco UCS Manager raises a fault to notify you of that failure.

When the server comes back up, Cisco UCS Manager assigns new dynamic vNICs to the server. If you are monitoring traffic on the dynamic vNIC, you must reconfigure the monitoring source.

Each Dynamic vNIC connection policy must include an adapter policy and designate the number of vNICs that can be configured for any server associated with a service profile that includes the policy.

Ethernet and Fibre Channel Adapter Policies

These policies govern the host-side behavior of the adapter, including how the adapter handles traffic. For example, you can use these policies to change default settings for the following:

- Queues
- Interrupt handling
- Performance enhancement
- RSS hash
- Failover in an cluster configuration with two fabric interconnects

Note For Fibre Channel adapter policies, the values displayed by Cisco UCS Manager may not match those displayed by applications such as QLogic SANsurfer. For example, the following values may result in an apparent mismatch between SANsurfer and Cisco UCS Manager:

- Max LUNs Per Target—SANsurfer has a maximum of 256 LUNs and does not display more than that number. Cisco UCS Manager supports a higher maximum number of LUNs.
- Link Down Timeout—In SANsurfer, you configure the timeout threshold for link down in seconds. In Cisco UCS Manager, you configure this value in milliseconds. Therefore, a value of 5500 ms in Cisco UCS Manager displays as 5s in SANsurfer.
- Max Data Field Size—SANsurfer has allowed values of 512, 1024, and 2048. Cisco UCS Manager allows you to set values of any size. Therefore, a value of 900 in Cisco UCS Manager displays as 512 in SANsurfer.

Operating System Specific Adapter Policies

By default, Cisco UCS provides a set of Ethernet adapter policies and Fibre Channel adapter policies. These policies include the recommended settings for each supported server operating system. Operating systems are sensitive to the settings in these policies. Storage vendors typically require non-default adapter settings. You can find the details of these required settings on the support list provided by those vendors.

Important We recommend that you use the values in these policies for the applicable operating system. Do not modify any of the values in the default policies unless directed to do so by Cisco Technical Support.

However, if you are creating an Ethernet adapter policy for a Windows OS (instead of using the default Windows adapter policy), you must use the following formulas to calculate values that work with Windows:

Completion Queues = Transmit Queues + Receive Queues
Interrupt Count = (Completion Queues + 2) rounded up to nearest power of 2

For example, if Transmit Queues = 1 and Receive Queues = 8 then:

Completion Queues = 1 + 8 = 9
Interrupt Count = (9 + 2) rounded up to the nearest power of 2 = 16

Global Cap Policy

The global cap policy is a global policy that specifies whether policy-driven chassis group power capping or manual blade-level power capping will be applied to all servers in a chassis.

We recommend that you use the default power capping method: policy-driven chassis group power capping.

Important Any change to the manual blade-level power cap configuration will result in the loss of any groups or configuration options set for policy-driven chassis group power capping.

Host Firmware Package

This policy enables you to specify a set of firmware versions that make up the host firmware package (also known as the host firmware pack). The host firmware includes the following firmware for server and adapter endpoints:

- **Adapter**
- **BIOS**
- **Board Controller**
- **FC Adapters**
- **HBA Option ROM**
- **Storage Controller**

Tip You can include more than one type of firmware in the same host firmware package. For example, a host firmware package can include both BIOS firmware and storage controller firmware or adapter firmware for two different models of adapters. However, you can only have one firmware version with the same type, vendor, and model number. The system recognizes which firmware version is required for an endpoint and ignores all other firmware versions.

The firmware package is pushed to all servers associated with service profiles that include this policy.

This policy ensures that the host firmware is identical on all servers associated with service profiles which use the same policy. Therefore, if you move the service profile from one server to another, the firmware versions are maintained. Also, if you change the firmware version for an endpoint in the firmware package, new versions are applied to all the affected service profiles immediately, which could cause server reboots.

You must include this policy in a service profile, and that service profile must be associated with a server for it to take effect.

Prerequisites

This policy is not dependent upon any other policies. However, you must ensure that the appropriate firmware has been downloaded to the fabric interconnect. If the firmware image is not available when Cisco UCS Manager is associating a server with a service profile, Cisco UCS Manager ignores the firmware upgrade and completes the association.

IPMI Access Profile

This policy allows you to determine whether IPMI commands can be sent directly to the server, using the IP address. For example, you can send commands to retrieve sensor data from the CIMC. This policy defines the IPMI access, including a username and password that can be authenticated locally on the server, and whether the access is read-only or read-write.

You must include this policy in a service profile and that service profile must be associated with a server for it to take effect.

Local Disk Configuration Policy

This policy configures any optional SAS local drives that have been installed on a server through the onboard RAID controller of the local drive. This policy enables you to set a local disk mode for all servers that are associated with a service profile that includes the local disk configuration policy.

The local disk modes include the following:

- **No Local Storage**—For a diskless server or a SAN only configuration. If you select this option, you cannot associate any service profile which uses this policy with a server that has a local disk.
- **RAID 0 Stripes**—Data is striped across all disks in the array, providing fast throughput. There is no data redundancy, and all data is lost if any disk fails.
- **RAID 1 Mirrored**—Data is written to two disks, providing complete data redundancy if one disk fails. The maximum array size is equal to the available space on the smaller of the two drives.
- **Any Configuration**—For a server configuration that carries forward the local disk configuration without any changes.
- **No RAID**—For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered.

- **RAID 6 Stripes Dual Parity**—Data is striped across all disks in the array and two parity disks are used to provide protection against the failure of up to two physical disks. In each row of data blocks, two sets of parity data are stored.
- **RAID 5 Striped Parity**—Data is striped across all disks in the array. Part of the capacity of each disk stores parity information that can be used to reconstruct data if a disk fails. RAID 5 provides good data throughput for applications with high read request rates.
- **RAID10 Mirrored and Striped**— RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates.

You must include this policy in a service profile, and that service profile must be associated with a server for the policy to take effect.

Management Firmware Package

This policy enables you to specify a set of firmware versions that make up the management firmware package (also known as a management firmware pack). The management firmware package includes the Cisco Integrated Management Controller (CIMC) on the server. You do not need to use this package if you upgrade the CIMC directly.

The firmware package is pushed to all servers associated with service profiles that include this policy. This policy ensures that the CIMC firmware is identical on all servers associated with service profiles which use the same policy. Therefore, if you move the service profile from one server to another, the firmware versions are maintained.

You must include this policy in a service profile, and that service profile must be associated with a server for it to take effect.

This policy is not dependent upon any other policies. However, you must ensure that the appropriate firmware has been downloaded to the fabric interconnect.

Management Interfaces Monitoring Policy

This policy defines how the mgmt0 Ethernet interface on the fabric interconnect should be monitored. If Cisco UCS detects a management interface failure, a failure report is generated. If the configured number of failure reports is reached, the system assumes that the management interface is unavailable and generates a fault. By default, the management interfaces monitoring policy is disabled.

If the affected management interface belongs to a fabric interconnect which is the managing instance, Cisco UCS confirms that the subordinate fabric interconnect's status is up, that there are no current failure reports logged against it, and then modifies the managing instance for the end-points.

If the affected fabric interconnect is currently the primary inside of a high availability setup, a failover of the management plane is triggered. The data plane is not affected by this failover.

You can set the following properties related to monitoring the management interface:

- Type of mechanism used to monitor the management interface.
- Interval at which the management interface's status is monitored.
- Maximum number of monitoring attempts that can fail before the system assumes that the management is unavailable and generates a fault message.

Important In the event of a management interface failure on a fabric interconnect, the managing instance may not change if one of the following occurs:

- A path to the end-point through the subordinate fabric interconnect does not exist.
- The management interface for the subordinate fabric interconnect has failed.
- The path to the end-point through the subordinate fabric interconnect has failed.

Network Control Policy

This policy configures the network control settings for the Cisco UCS instance, including the following:

- Whether the Cisco Discovery Protocol (CDP) is enabled or disabled
- How the VIF behaves if no uplink port is available in end-host mode
- Whether the server can use different MAC addresses when sending packets to the fabric interconnect

The network control policy also determines the action that Cisco UCS Manager takes on the remote Ethernet port or the vEthernet interface when the associated border port fails. By default, the **Action on Uplink Fail** property in the network control policy is configured with a value of link-down. This default behavior directs Cisco UCS Manager to bring the remote Ethernet or vEthernet port down if the border port fails.

Note The default behaviour of the **Action on Uplink Fail** property is optimal for most Cisco UCS that support link failover at the adapter level or only carry Ethernet traffic. However, for those converged network adapters that support both Ethernet and Fibre Channel traffic, such as the Cisco UCS CNA M72KR-Q and the Cisco UCS CNA M72KR-E, the default behavior can affect and interrupt Fibre Channel traffic as well. Therefore, if the server includes one of those converged network adapters and the the adapter is expected to handle both Ethernet and Fibre Channel traffic, we recommend that you configure the **Action on Uplink Fail** property with a value of warning. Please note that this configuration may result in an Ethernet teaming driver not being able to detect a link failure when the border port goes down.

Power Control Policy

Cisco UCS uses the priority set in the power control policy, along with the blade type and configuration, to calculate the initial power allocation for each blade within a chassis. During normal operation, the active blades within a chassis can borrow power from idle blades within the same chassis. If all blades are active and reach the power cap, service profiles with higher priority power control policies take precedence over service profiles with lower priority power control policies.

Priority is ranked on a scale of 1-10, where 1 indicates the highest priority and 10 indicates lowest priority. The default priority is 5.

For mission-critical application a special priority called no-cap is also available. Setting the priority to no-cap prevents Cisco UCS from leveraging unused power from that particular blade server. The server is allocated the maximum amount of power that that blade can reach.

Note You must include this policy in a service profile and that service profile must be associated with a server for it to take effect.

Power Policy

The power policy is a global policy that specifies the redundancy for power supplies in all chassis in the Cisco UCS instance. This policy is also known as the PSU policy.

For more information about power supply redundancy, see *Cisco UCS 5108 Server Chassis Hardware Installation Guide*.

Quality of Service Policy

A quality of service (QoS) policy assigns a system class to the outgoing traffic for a vNIC or vHBA. This system class determines the quality of service for that traffic. For certain adapters you can also specify additional controls on the outgoing traffic, such as burst and rate.

You must include a QoS policy in a vNIC policy or vHBA policy and then include that policy in a service profile to configure the vNIC or vHBA.

Rack Server Discovery Policy

The rack server discovery policy determines how the system reacts when you add a new rack-mount server. Cisco UCS Manager uses the settings in the rack server discovery policy to determine whether any data on the hard disks are scrubbed and whether server discovery occurs immediately or needs to wait for explicit user acknowledgement.

Cisco UCS Manager cannot discover any rack-mount server that has not been correctly cabled and connected to the fabric interconnects. For information about how to integrate a supported Cisco UCS rack-mount server with Cisco UCS Manager, see the hardware installation guide for that server.

Server Autoconfiguration Policy

Cisco UCS Manager uses this policy to determine how to configure a new server. If you create a server autoconfiguration policy, the following occurs when a new server starts:

1. The qualification in the server autoconfiguration policy is executed against the server.
2. If the server meets the required qualifications, the server is associated with a service profile created from the service profile template configured in the server autoconfiguration policy. The name of that service profile is based on the name given to the server by Cisco UCS Manager.
3. The service profile is assigned to the organization configured in the server autoconfiguration policy.

Server Discovery Policy

This discovery policy determines how the system reacts when you add a new server. If you create a server discovery policy, you can control whether the system conducts a deep discovery when a server is added to a chassis, or whether a user must first acknowledge the new server. By default, the system conducts a full discovery.

If you create a server discovery policy, the following occurs when a new server starts:

1. The qualification in the server discovery policy is executed against the server.
2. If the server meets the required qualifications, Cisco UCS Manager applies the following to the server:
   - Depending upon the option selected for the action, either discovers the new server immediately or waits for a user to acknowledge the new server
   - Applies the scrub policy to the server

Server Inheritance Policy

This policy is invoked during the server discovery process to create a service profile for the server. All service profiles created from this policy use the values burned into the blade at manufacture. The policy performs the following:

- Analyzes the inventory of the server
- If configured, assigns the server to the selected organization
- Creates a service profile for the server with the identity burned into the server at manufacture

You cannot migrate a service profile created with this policy to another server.

Server Pool Policy

This policy is invoked during the server discovery process. It determines what happens if server pool policy qualifications match a server to the target pool specified in the policy.

If a server qualifies for more than one pool and those pools have server pool policies, the server is added to all those pools.

Server Pool Policy Qualifications

This policy qualifies servers based on the inventory of a server conducted during the discovery process. The qualifications are individual rules that you configure in the policy to determine whether a server meets the selection criteria. For example, you can create a rule that specifies the minimum memory capacity for servers in a data center pool.

Qualifications are used in other policies to place servers, not just by the server pool policies. For example, if a server meets the criteria in a qualification policy, it can be added to one or more server pools or have a service profile automatically associated with it.

You can use the server pool policy qualifications to qualify servers according to the following criteria:

- Adapter type
- Chassis location
- Memory type and configuration
- Power group
- CPU cores, type, and configuration
- Storage configuration and capacity
- Server model

Depending upon the implementation, you may configure several policies with server pool policy qualifications including the following:

- Autoconfiguration policy
- Chassis discovery policy
- Server discovery policy
- Server inheritance policy
- Server pool policy

vHBA Template

This template is a policy that defines how a vHBA on a server connects to the SAN. It is also referred to as a vHBA SAN connectivity template.

You need to include this policy in a service profile for it to take effect.

VM Lifecycle Policy

The VM lifecycle policy determines how long Cisco UCS Manager retains offline VMs and offline dynamic vNICs in its database. If a VM or dynamic vNIC remains offline after that period, Cisco UCS Manager deletes the object from its database.

All virtual machines (VMs) on Cisco UCS servers are managed by vCenter. Cisco UCS Manager cannot determine whether an inactive VM is temporarily shutdown, has been deleted, or is in some other state that renders it inaccessible. Therefore, Cisco UCS Manager considers all inactive VMs to be in an offline state.

Cisco UCS Manager considers a dynamic vNIC to be offline when the associated VM is shutdown, or the link between the fabric interconnect and the I/O module fails. On rare occasions, an internal error can also cause Cisco UCS Manager to consider a dynamic vNIC to be offline.

The default VM and dynamic vNIC retention period is 15 minutes. You can set that for any period of time between 1 minute and 7200 minutes (or 5 days).

Note The VMs that Cisco UCS Manager displays are for information and monitoring only. You cannot manage VMs through Cisco UCS Manager. Therefore, when you delete a VM from the Cisco UCS Manager database, you do not delete the VM from the server or from vCenter.

vNIC Template

This policy defines how a vNIC on a server connects to the LAN. This policy is also referred to as a vNIC LAN connectivity policy.

You need to include this policy in a service profile for it to take effect.

vNIC/vHBA Placement Policies

vNIC/vHBA placement policies are used to assign vNICs or vHBAs to the physical adapters on a server. Each vNIC/vHBA placement policy contains two virtual network interface connections (vCons) that are virtual representations of the physical adapters. When a vNIC/vHBA placement policy is assigned to a service profile, and the service profile is associated to a server, the vCons in the vNIC/vHBA placement policy are assigned

to the physical adapters. For servers with only one adapter, both vCons are assigned to the adapter; for servers with two adapters, one vCon is assigned to each adapter.

You can assign vNICs or vHBAs to either of the two vCons, and they are then assigned to the physical adapters based on the vCon assignment during server association. Additionally, vCons use the following selection preference criteria to assign vHBAs and vNICs:

All	The vCon is used for vNICs or vHBAs assigned to it, vNICs or vHBAs not assigned to either vCon, and dynamic vNICs or vHBAs.
Assigned-Only	The vCon is reserved for only vNICs or vHBAs assigned to it.
Exclude-Dynamic	The vCon is not used for dynamic vNICs or vHBAs.
Exclude-Unassigned	The vCon is not used for vNICs or vHBAs not assigned to the vCon. The vCon is used for dynamic vNICs and vHBAs.

For servers with two adapters, if you do not include a vNIC/vHBA placement policy in a service profile, or you do not configure vCons for a service profile, Cisco UCS equally distributes the vNICs and vHBAs between the two adapters.

Operational Policies

Fault Collection Policy

The fault collection policy controls the lifecycle of a fault in a Cisco UCS instance, including when faults are cleared, the flapping interval (the length of time between the fault being raised and the condition being cleared), and the retention interval (the length of time a fault is retained in the system).

A fault in Cisco UCS has the following lifecycle:

1. A condition occurs in the system and Cisco UCS Manager raises a fault. This is the active state.
2. When the fault is alleviated, it is cleared if the time between the fault being raised and the condition being cleared is greater than the flapping interval, otherwise, the fault remains raised but its status changes to soaking-clear. Flapping occurs when a fault is raised and cleared several times in rapid succession. During the flapping interval the fault retains its severity for the length of time specified in the fault collection policy.
3. If the condition reoccurs during the flapping interval, the fault remains raised and its status changes to flapping. If the condition does not reoccur during the flapping interval, the fault is cleared.
4. When a fault is cleared, it is deleted if the clear action is set to delete, or if the fault was previously acknowledged; otherwise, it is retained until either the retention interval expires, or if the fault is acknowledged.
5. If the condition reoccurs during the retention interval, the fault returns to the active state. If the condition does not reoccur, the fault is deleted.

Flow Control Policy

Flow control policies determine whether the uplink Ethernet ports in a Cisco UCS instance send and receive IEEE 802.3x pause frames when the receive buffer for a port fills. These pause frames request that the transmitting port stop sending data for a few milliseconds until the buffer clears.

For flow control to work between a LAN port and an uplink Ethernet port, you must enable the corresponding receive and send flow control parameters for both ports. For Cisco UCS, the flow control policies configure these parameters.

When you enable the send function, the uplink Ethernet port sends a pause request to the network port if the incoming packet rate becomes too high. The pause remains in effect for a few milliseconds before traffic is reset to normal levels. If you enable the receive function, the uplink Ethernet port honors all pause requests from the network port. All traffic is halted on that uplink port until the network port cancels the pause request.

Because you assign the flow control policy to the port, changes to the policy have an immediate effect on how the port reacts to a pause frame or a full receive buffer.

Maintenance Policy

A maintenance policy determines how Cisco UCS Manager reacts when a change that requires a server reboot is made to a service profile associated with a server or to an updating service profile bound to one or more service profiles.

The maintenance policy specifies how Cisco UCS Manager deploys the service profile changes. The deployment can occur in one of the following ways:

- Immediately
- When acknowledged by a user with admin privileges
- Automatically at the time specified in the schedule

If the maintenance policy is configured to deploy the change during a scheduled maintenance window, the policy must include a valid schedule. The schedule deploys the changes in the first available maintenance window.

Scrub Policy

This policy determines what happens to local data and to the BIOS settings on a server during the discovery process and when the server is disassociated from a service profile. Depending upon how you configure a scrub policy, the following can occur at those times:

Disk Scrub — One of the following occurs to the data on any local drives on disassociation:

- If enabled, destroys all data on any local drives
- If disabled, preserves all data on any local drives, including local storage configuration

BIOS Settings Scrub — One of the following occurs to the BIOS settings when a service profile containing the scrub policy is disassociated from a server:

- If enabled, erases all BIOS settings for the server and and resets them to the BIOS defaults for that server type and vendor

- If disabled, preserves the existing BIOS settings on the server

Serial over LAN Policy

This policy sets the configuration for the serial over LAN connection for all servers associated with service profiles that use the policy. By default, the serial over LAN connection is disabled.

If you implement a serial over LAN policy, we recommend that you also create an IPMI profile.

You must include this policy in a service profile and that service profile must be associated with a server for it to take effect.

Statistics Collection Policy

A statistics collection policy defines how frequently statistics are to be collected (collection interval) and how frequently the statistics are to be reported (reporting interval). Reporting intervals are longer than collection intervals so that multiple statistical data points can be collected during the reporting interval, which provides Cisco UCS Manager with sufficient data to calculate and report minimum, maximum, and average values.

For NIC statistics, Cisco UCS Manager displays the average, minimum, and maximum of the change since the last collection of statistics. If the values are 0, there has been no change since the last collection.

Statistics can be collected and reported for the following five functional areas of the Cisco UCS system:

- Adapter—statistics related to the adapters
- Chassis—statistics related to the blade chassis
- Host—this policy is a placeholder for future support
- Port—statistics related to the ports, including server ports, uplink Ethernet ports, and uplink Fibre Channel ports
- Server—statistics related to servers

Note Cisco UCS Manager has one default statistics collection policy for each of the five functional areas. You cannot create additional statistics collection policies and you cannot delete the existing default policies. You can only modify the default policies.

Statistics Threshold Policy

A statistics threshold policy monitors statistics about certain aspects of the system and generates an event if the threshold is crossed. You can set both minimum and maximum thresholds. For example, you can configure the policy to raise an alarm if the CPU temperature exceeds a certain value, or if a server is overutilized or underutilized.

These threshold policies do not control the hardware or device-level thresholds enforced by endpoints, such as the CIMC. Those thresholds are burned in to the hardware components at manufacture.

Cisco UCS enables you to configure statistics threshold policies for the following components:

- Servers and server components
- Uplink Ethernet ports

- Ethernet server ports, chassis, and fabric interconnects
- Fibre Channel port

Note You cannot create or delete a statistics threshold policy for Ethernet server ports, uplink Ethernet ports, or uplink Fibre Channel ports. You can only configure the existing default policy.

Pools

Pools are collections of identities, or physical or logical resources, that are available in the system. All pools increase the flexibility of service profiles and allow you to centrally manage your system resources.

You can use pools to segment unconfigured servers or available ranges of server identity information into groupings that make sense for the data center. For example, if you create a pool of unconfigured servers with similar characteristics and include that pool in a service profile, you can use a policy to associate that service profile with an available, unconfigured server.

If you pool identifying information, such as MAC addresses, you can pre-assign ranges for servers that will host specific applications. For example, all database servers could be configured within the same range of MAC addresses, UUIDs, and WWNs.

Server Pools

A server pool contains a set of servers. These servers typically share the same characteristics. Those characteristics can be their location in the chassis, or an attribute such as server type, amount of memory, local storage, type of CPU, or local drive configuration. You can manually assign a server to a server pool, or use server pool policies and server pool policy qualifications to automate the assignment.

If your system implements multi-tenancy through organizations, you can designate one or more server pools to be used by a specific organization. For example, a pool that includes all servers with two CPUs could be assigned to the Marketing organization, while all servers with 64 GB memory could be assigned to the Finance organization.

A server pool can include servers from any chassis in the system. A given server can belong to multiple server pools.

MAC Pools

A MAC pool is a collection of network identities, or MAC addresses, that are unique in their layer 2 environment and are available to be assigned to vNICs on a server. If you use MAC pools in service profiles, you do not have to manually configure the MAC addresses to be used by the server associated with the service profile.

In a system that implements multi-tenancy, you can use the organizational hierarchy to ensure that MAC pools can only be used by specific applications or business services. Cisco UCS Manager uses the name resolution policy to assign MAC addresses from the pool.

To assign a MAC address to a server, you must include the MAC pool in a vNIC policy. The vNIC policy is then included in the service profile assigned to that server.

You can specify your own MAC addresses or use a group of MAC addresses provided by Cisco.

UUID Suffix Pools

A 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 ensures that these variable values are unique for each server associated with a service profile which uses that particular pool to avoid conflicts.

If you use UUID suffix pools in service profiles, you do not have to manually configure the UUID of the server associated with the service profile.

WWN Pools

A WWN pool is a collection of WWNs for use by the Fibre Channel vHBAs in a Cisco UCS instance. You create separate pools for the following:

- WW node names assigned to the server
- WW port names assigned to the vHBA

Important A WWN pool can include only WWNNs or WWPNs in the ranges from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF. All other WWN ranges are reserved. To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, we recommend that you use the following WWN prefix for all blocks in a pool: 20:00:00:25:B5:XX:XX:XX

If you use WWN pools in service profiles, you do not have to manually configure the WWNs that will be used by the server associated with the service profile. In a system that implements multi-tenancy, you can use a WWN pool to control the WWNs used by each organization.

You assign WWNs to pools in blocks. For each block or individual WWN, you can assign a boot target.

WWNN Pools

A WWNN pool is a WWN pool that contains only WW node names. If you include a pool of WWNNs in a service profile, the associated server is assigned a WWNN from that pool.

WWPN Pools

A WWPN pool is a WWN pool that contains only WW port names. If you include a pool of WWPNs in a service profile, the port on each vHBA of the associated server is assigned a WWPN from that pool.

Management IP Pool

The management IP pool is a collection of external IP addresses. Cisco UCS Manager reserves each block of IP addresses in the management IP pool for external access that terminates in the CIMC on a server.

You can configure service profiles and service profile templates to use IP addresses from the management IP pool. You cannot configure servers to use the management IP pool.

Note The management IP pool must not contain any IP addresses that have been assigned as static IP addresses for a server or service profile.

Traffic Management

Oversubscription

Oversubscription occurs when multiple network devices are connected to the same fabric interconnect port. This practice optimizes fabric interconnect use, since ports rarely run at maximum speed for any length of time. As a result, when configured correctly, oversubscription allows you to take advantage of unused bandwidth. However, incorrectly configured oversubscription can result in contention for bandwidth and a lower quality of service to all services that use the oversubscribed port.

For example, oversubscription can occur if four servers share a single uplink port, and all four servers attempt to send data at a cumulative rate higher than available bandwidth of uplink port.

Oversubscription Considerations

The following elements can impact how you configure oversubscription in a Cisco UCS instance:

Ratio of Server-Facing Ports to Uplink Ports

You need to know what how many server-facing ports and uplink ports are in the system, because that ratio can impact performance. For example, if your system has twenty ports that can communicate down to the servers and only two ports that can communicate up to the network, your uplink ports will be oversubscribed. In this situation, the amount of traffic created by the servers can also affect performance.

Number of Uplink Ports from Fabric Interconnect to Network

You can choose to add more uplink ports between the Cisco UCS fabric interconnect and the upper layers of the LAN to increase bandwidth. In Cisco UCS, you must have at least one uplink port per fabric interconnect to ensure that all servers and NICs to have access to the LAN. The number of LAN uplinks should be determined by the aggregate bandwidth needed by all Cisco UCS servers.

FC uplink ports are available on the expansion slots only. You must add more expansion slots to increase number of available FC uplinks. Ethernet uplink ports can exist on the fixed slot and on expansion slots.

For example, if you have two Cisco UCS 5100 series chassis that are fully populated with half width Cisco UCS B200-M1 servers, you have 16 servers. In a cluster configuration, with one LAN uplink per fabric interconnect, these 16 servers share 20GbE of LAN bandwidth. If more capacity is needed, more uplinks from the fabric interconnect should be added. We recommend that you have symmetric configuration of the uplink in cluster configurations. In the same example, if 4 uplinks are used in each fabric interconnect, the 16 servers are sharing 80 GB of bandwidth, so each has approximately 5 GB of capacity. When multiple uplinks are used on a Cisco UCS fabric interconnect the network design team should consider using a port channel to make best use of the capacity.

Number of Uplink Ports from I/O Module to Fabric Interconnect

You can choose to add more bandwidth between I/O module and fabric interconnect by using more uplink ports and increasing the number of cables. In Cisco UCS, you can have one, two, or four cables connecting

a I/O module to a Cisco UCS fabric interconnect. The number of cables determines the number of active uplink ports and the oversubscription ratio. For example, one cable results in 8:1 oversubscription for one I/O module. If two I/O modules are in place, each with one cable, and you have 8 half-width blades, the 8 blades will be sharing two uplinks (one left IOM and one right IOM). This results in 8 blades sharing an aggregate bandwidth of 20 GB of Unified Fabric capacity. If two cables are used, this results in 4:1 oversubscription per IOM (assuming all slots populated with half width blades), and four cables result in 2:1 oversubscription. The lower oversubscription ratio gives you higher performance, but is also more costly as you consume more fabric interconnect ports.

Number of Active Links from Server to Fabric Interconnect

The amount of non-oversubscribed bandwidth available to each server depends on the number of I/O modules used and the number of cables used to connect those I/O modules to the fabric interconnects. Having a second I/O module in place provides additional bandwidth and redundancy to the servers. This level of flexibility in design ensures that you can provide anywhere from 80 Gbps (two I/O modules with four links each) to 10 Gbps (one I/O module with one link) to the chassis.

With 80 Gbps to the chassis, each half-width server in the Cisco UCS instance can get up to 10 Gbps in a non-oversubscribed configuration, with an ability to use up to 20 Gbps with 2:1 oversubscription.

Guidelines for Estimating Oversubscription

When you estimate the optimal oversubscription ratio for a fabric interconnect port, consider the following guidelines:

Cost/Performance Slider

The prioritization of cost and performance is different for each data center and has a direct impact on the configuration of oversubscription. When you plan hardware usage for oversubscription, you need to know where the data center is located on this slider. For example, oversubscription can be minimized if the data center is more concerned with performance than cost. However, cost is a significant factor in most data centers, and oversubscription requires careful planning.

Bandwidth Usage

The estimated bandwidth that you expect each server to actually use is important when you determine the assignment of each server to a fabric interconnect port and, as a result, the oversubscription ratio of the ports. For oversubscription, you must consider how many GBs of traffic the server will consume on average, the ratio of configured bandwidth to used bandwidth, and the times when high bandwidth use will occur.

Network Type

The network type is only relevant to traffic on uplink ports, because FCoE does not exist outside Cisco UCS. The rest of the data center network only differentiates between LAN and SAN traffic. Therefore, you do not need to take the network type into consideration when you estimate oversubscription of a fabric interconnect port.

Pinning

Pinning in Cisco UCS is only relevant to uplink ports. You can pin Ethernet or FCoE traffic from a given server to a specific uplink Ethernet port or uplink FC port.

When you pin the NIC and HBA of both physical and virtual servers to uplink ports, you give the fabric interconnect greater control over the unified fabric. This control ensures more optimal utilization of uplink port bandwidth.

Cisco UCS uses pin groups to manage which NICs, vNICs, HBAs, and vHBAs are pinned to an uplink port. To configure pinning for a server, you can either assign a pin group directly, or include a pin group in a vNIC policy, and then add that vNIC policy to the service profile assigned to that server. All traffic from the vNIC or vHBA on the server travels through the I/O module to the same uplink port.

Pinning Server Traffic to Server Ports

All server traffic travels through the I/O module to server ports on the fabric interconnect. The number of links for which the chassis is configured determines how this traffic is pinned.

The pinning determines which server traffic goes to which server port on the fabric interconnect.This pinning is fixed. You cannot modify it. As a result, you must consider the server location when you determine the appropriate allocation of bandwidth for a chassis.

Note You must review the allocation of ports to links before you allocate servers to slots. The cabled ports are not necessarily port 1 and port 2 on the I/O module. If you change the number of links between the fabric interconnect and the I/O module, you must reacknowledge the chassis to have the traffic rerouted.

All port numbers refer to the fabric interconnect-side ports on the I/O module.

Chassis with One I/O Module

Links on Chassis	Servers Pinned to Link 1	Servers Pinned to Link 2	Servers Pinned to Link 3	Servers Pinned to Link 4
1 link	All server slots	None	None	None
2 links	Slots 1, 3, 5, and 7	Slots 2, 4, 6, and 8	None	None
4 links	Slots 1 and 5	Slots 2 and 6	Slots 3 and 7	Slots 4 and 8

Chassis with Two I/O Modules

If a chassis has two I/O modules, traffic from one I/O module goes to one of the fabric interconnects and traffic from the other I/O module goes to the second fabric interconnect. You cannot connect two I/O modules to a single fabric interconnect.

Fabric Interconnect Configured in vNIC	Server Traffic Path
A	Server traffic goes to fabric interconnect A. If A fails, the server traffic does not fail over to B.
B	All server traffic goes to fabric interconnect B. If B fails, the server traffic does not fail over to A.
A-B	All server traffic goes to fabric interconnect A. If A fails, the server traffic fails over to B.

Fabric Interconnect Configured in vNIC	Server Traffic Path
B-A	All server traffic goes to fabric interconnect B. If B fails, the server traffic fails over to A.

Guidelines for Pinning

When you determine the optimal configuration for pin groups and pinning for an uplink port, consider the estimated bandwidth usage for the servers. If you know that some servers in the system will use a lot of bandwidth, ensure that you pin these servers to different uplink ports.

Quality of Service

Cisco UCS provides the following methods to implement quality of service:

- System classes that specify the global configuration for certain types of traffic across the entire system
- QoS policies that assign system classes for individual vNICs
- Flow control policies that determine how uplink Ethernet ports handle pause frames

System Classes

Cisco UCS uses Data Center Ethernet (DCE) to handle all traffic inside a Cisco UCS instance. This industry standard enhancement to Ethernet divides the bandwidth of the Ethernet pipe into eight virtual lanes. Two virtual lanes are reserved for internal system and management traffic. You can configure quality of service for the other six virtual lanes. System classes determine how the DCE bandwidth in these six virtual lanes is allocated across the entire Cisco UCS instance.

Each system class reserves a specific segment of the bandwidth for a specific type of traffic. This provides a level of traffic management, even in an oversubscribed system. For example, you can configure the Fibre Channel Priority system class to determine the percentage of DCE bandwidth allocated to FCoE traffic.

The following table describes the system classes that you can configure:

Table 3: System Classes

System Class	Description
Platinum Gold Silver Bronze	A configurable set of system classes that you can include in the QoS policy for a service profile. Each system class manages one lane of traffic. All properties of these system classes are available for you to assign custom settings and policies.
Best Effort	A system class that sets the quality of service for the lane reserved for Basic Ethernet traffic. Some properties of this system class are preset and cannot be modified. For example, this class has a drop policy that allows it to drop data packets if required. You cannot disable this system class.

System Class	Description
Fibre Channel	A system class that sets the quality of service for the lane reserved for Fibre Channel over Ethernet traffic. Some properties of this system class are preset and cannot be modified. For example, this class has a no-drop policy that ensures it never drops data packets. You cannot disable this system class.

Quality of Service Policy

A quality of service (QoS) policy assigns a system class to the outgoing traffic for a vNIC or vHBA. This system class determines the quality of service for that traffic. For certain adapters you can also specify additional controls on the outgoing traffic, such as burst and rate.

You must include a QoS policy in a vNIC policy or vHBA policy and then include that policy in a service profile to configure the vNIC or vHBA.

Flow Control Policy

Flow control policies determine whether the uplink Ethernet ports in a Cisco UCS instance send and receive IEEE 802.3x pause frames when the receive buffer for a port fills. These pause frames request that the transmitting port stop sending data for a few milliseconds until the buffer clears.

For flow control to work between a LAN port and an uplink Ethernet port, you must enable the corresponding receive and send flow control parameters for both ports. For Cisco UCS, the flow control policies configure these parameters.

When you enable the send function, the uplink Ethernet port sends a pause request to the network port if the incoming packet rate becomes too high. The pause remains in effect for a few milliseconds before traffic is reset to normal levels. If you enable the receive function, the uplink Ethernet port honors all pause requests from the network port. All traffic is halted on that uplink port until the network port cancels the pause request.

Because you assign the flow control policy to the port, changes to the policy have an immediate effect on how the port reacts to a pause frame or a full receive buffer.

Opt-In Features

Each Cisco UCS instance is licensed for all functionality. Depending upon how the system is configured, you can decide to opt in to some features or opt out of them for easier integration into existing environment. If a process change happens, you can change your system configuration and include one or both of the opt-in features.

The opt-in features are as follows:

- Stateless computing, which takes advantage of mobile service profiles with pools and policies where each component, such as a server or an adapter, is stateless.
- Multi-tenancy, which uses organizations and role-based access control to divide the system into smaller logical segments.

Stateless Computing

Stateless computing allows you to use a service profile to apply the personality of one server to a different server in the same Cisco UCS instance. The personality of the server includes the elements that identify that server and make it unique in the instance. If you change any of these elements, the server could lose its ability to access, use, or even achieve booted status.

The elements that make up a server's personality include the following:

- Firmware versions
- UUID (used for server identification)
- MAC address (used for LAN connectivity)
- World Wide Names (used for SAN connectivity)
- Boot settings

Stateless computing creates a dynamic server environment with highly flexible servers. Every physical server in a Cisco UCS instance remains anonymous until you associate a service profile with it, then the server gets the identity configured in the service profile. If you no longer need a business service on that server, you can shut it down, disassociate the service profile, and then associate another service profile to create a different identity for the same physical server. The "new" server can then host another business service.

To take full advantage of the flexibility of statelessness, the optional local disks on the servers should only be used for swap or temp space and not to store operating system or application data.

You can choose to fully implement stateless computing for all physical servers in a Cisco UCS instance, to not have any stateless servers, or to have a mix of the two types.

If You Opt In to Stateless Computing

Each physical server in the Cisco UCS instance is defined through a service profile. Any server can be used to host one set of applications, then reassigned to another set of applications or business services, if required by the needs of the data center.

You create service profiles that point to policies and pools of resources that are defined in the instance. The server pools, WWN pools, and MAC pools ensure that all unassigned resources are available on an as-needed basis. For example, if a physical server fails, you can immediately assign the service profile to another server. Because the service profile provides the new server with the same identity as the original server, including WWN and MAC address, the rest of the data center infrastructure sees it as the same server and you do not need to make any configuration changes in the LAN or SAN.

If You Opt Out of Stateless Computing

Each server in the Cisco UCS instance is treated as a traditional rack mount server.

You create service profiles that inherit the identify information burned into the hardware and use these profiles to configure LAN or SAN connectivity for the server. However, if the server hardware fails, you cannot reassign the service profile to a new server.

Multi-Tenancy

Multi-tenancy allows you to divide up the large physical infrastructure of an instance into logical entities known as organizations. As a result, you can achieve a logical isolation between organizations without providing a dedicated physical infrastructure for each organization.

You can assign unique resources to each tenant through the related organization, in the multi-tenant environment. These resources can include different policies, pools, and quality of service definitions. You can also implement locales to assign or restrict user privileges and roles by organization, if you do not want all users to have access to all organizations.

If you set up a multi-tenant environment, all organizations are hierarchical. The top-level organization is always root. The policies and pools that you create in root are system-wide and are available to all organizations in the system. However, any policies and pools created in other organizations are only available to organizations that are above it in the same hierarchy. For example, if a system has organizations named Finance and HR that are not in the same hierarchy, Finance cannot use any policies in the HR organization, and HR cannot access any policies in the Finance organization. However, both Finance and HR can use policies and pools in the root organization.

If you create organizations in a multi-tenant environment, you can also set up one or more of the following for each organization or for a sub-organization in the same hierarchy:

- Resource pools
- Policies
- Service profiles
- Service profile templates

If You Opt In to Multi-Tenancy

Each Cisco UCS instance is divided into several distinct organizations. The types of organizations you create in a multi-tenancy implementation depends upon the business needs of the company. Examples include organizations that represent the following:

- Enterprise groups or divisions within a company, such as marketing, finance, engineering, or human resources
- Different customers or name service domains, for service providers

You can create locales to ensure that users have access only to those organizations that they are authorized to administer.

If You Opt Out of Multi-Tenancy

The Cisco UCS instance remains a single logical entity with everything in the root organization. All policies and resource pools can be assigned to any server in the instance.

Virtualization in Cisco UCS

Overview of Virtualization

Virtualization allows the creation of multiple virtual machines to run in isolation, side-by-side on the same physical machine.

Each virtual machine has its own set of virtual hardware (RAM, CPU, NIC) upon which an operating system and fully configured applications are loaded. The operating system sees a consistent, normalized set of hardware regardless of the actual physical hardware components.

In a virtual machine, both hardware and software are encapsulated in a single file for rapid copying, provisioning, and moving between physical servers. You can move a virtual machine, within seconds, from one physical server to another for zero-downtime maintenance and continuous workload consolidation.

The virtual hardware makes it possible for many servers, each running in an independent virtual machine, to run on a single physical server. The advantages of virtualization include better use of computing resources, greater server density, and seamless server migration.

Virtualization in Cisco UCS

Cisco UCS provides hardware-level server virtualization. Hardware-level server virtualization allows a server to be simulated at the physical level and cannot be detected by existing software, including the operating system, drivers, and management tools. If underlying hardware faults require you to recreate the virtual server in another location, the network and existing software remain unaware that the physical server has changed.

Server virtualization allows networks to rapidly adapt to changing business and technical conditions. The lower level integration with the virtualized environment in Cisco UCS improves visibility and control of the virtual machine environment, and enhances the overall agility of the system. In addition, this virtualization ensures that there is no performance penalty or overhead for applications while running.

The virtualized environment available in a Cisco UCS server depends upon the type of adapter installed in the server. For example, a virtual interface card (VIC) adapter provides a unique and flexible virtualized environment and support for virtual machines. The other adapters support the standard integration and virtualized environment with VMware.

Virtualization with Network Interface Cards and Converged Network Adapters

Network interface card (NIC) and converged network adapters support virtualized environments with the standard VMware integration with ESX installed on the server and all virtual machine management performed through the VC.

Portability of Virtual Machines

If you implement service profiles you retain the ability to easily move a server identity from one server to another. After you image the new server, the ESX treats that server as if it were the original.

Communication between Virtual Machines on the Same Server

These adapters implement the standard communications between virtual machines on the same server. If an ESX host includes multiple virtual machines, all communications must go through the virtual switch on the server.

If the system uses the native VMware drivers, the virtual switch is out of the network administrator's domain and is not subject to any network policies. As a result, for example, QoS policies on the network are not applied to any data packets traveling from VM1 to VM2 through the virtual switch.

If the system includes another virtual switch, such as the Nexus 1000, that virtual switch is subject to the network policies configured on that switch by the network administrator.

Virtualization with a Virtual Interface Card Adapter

Virtual interface card (VIC) adapters support virtualized environments with VMware. These environments support the standard VMware integration with ESX installed on the server and all virtual machine management performed through the VMware vCenter.

This virtualized adapter supports the following:

- Dynamic vNICs in a virtualized environment with VM software, such as vSphere. This solution enables you to divide a single physical blade server into multiple logical PCIE instances.
- Static vNICs in a single operating system installed on a server.

With a VIC adapter, the solution you choose determines how communication works. This type of adapter supports the following communication solutions:

- Cisco VN-Link in hardware, which is a hardware-based method of handling traffic to and from a virtual machine. Details of how to configure this solution are available in this document.
- Cisco VN-Link in software, which is a software-based method of handling traffic to and from a virtual machine and uses the Nexus 1000v virtual switch. Details of how to configure this solution are available in the Nexus 1000v documentation.
- Single operating system installed on the server without virtualization, which uses the same methods of handling traffic as the other Cisco UCS adapters.

Cisco VN-Link

Cisco Virtual Network Link (VN-Link) is a set of features and capabilities that enable you to individually identify, configure, monitor, migrate, and diagnose virtual machine interfaces in a way that is consistent with the current network operation models for physical servers. VN-Link literally indicates the creation of a logical link between a vNIC on a virtual machine and a Cisco UCS fabric interconnect. This mapping is the logical equivalent of using a cable to connect a NIC with a network port on an access-layer switch.

VN-Link in Hardware

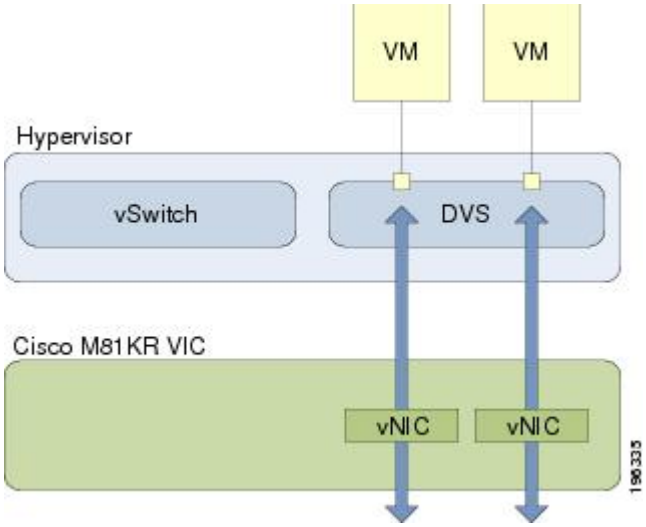
Cisco VN-Link in hardware is a hardware-based method of handling traffic to and from a virtual machine on a server with a VIC adapter. This method is sometimes referred to as pass-through switching. This solution replaces software-based switching with ASIC-based hardware switching and improves performance.

The distributed virtual switch (DVS) framework delivers VN-Link in hardware features and capabilities for virtual machines on Cisco UCS servers with VIC adapters. This approach provides an end-to-end network solution to meet the new requirements created by server virtualization.

With VN-Link in hardware, all traffic to and from a virtual machine passes through the DVS and the hypervisor. and then returns to the virtual machine on the server. Switching occurs in the fabric interconnect (hardware). As a result, network policies can be applied to traffic between virtual machines. This capability provides consistency between physical and virtual servers.

The following figure shows the traffic paths taken by VM traffic on a Cisco UCS server with a VIC adapter:

Figure 1: Traffic Paths for VM traffic with VN-Link in Hardware



Extension File for Communication with VMware vCenter

For Cisco UCS instances that use VIC adapters to implement VN-Link in hardware, you must create and install an extension file to establish the relationship and communications between Cisco UCS Manager and the VMware vCenter. This extension file is an XML file that contains vital information, including the following:

- Extension key
- Public SSL certificate

If you need to have two Cisco UCS instances share the same set of distributed virtual switches in a vCenter, you can create a custom extension key and import the same SSL certificate in the Cisco UCS Manager for each Cisco UCS instance.

Extension Key

The extension key includes the identity of the Cisco UCS instance. By default, this key has the value Cisco UCS GUID, as this value is identical across both fabric interconnects in a cluster configuration.

When you install the extension, vCenter uses the extension key to create a distributed virtual switch (DVS).

Public SSL Certificate

Cisco UCS Manager generates a default, self-signed SSL certificate to support communication with vCenter. You can also provide your own custom certificate.

Custom Extension Files

You can create a custom extension file for a Cisco UCS instance that does not use either or both of the default extension key or SSL certificate. For example, you can create the same custom key in two different Cisco UCS instances when they are managed by the same VMware vCenter instance.

Important You cannot change an extension key that is being used by a DVS or vCenter. If you want to use a custom extension key, we recommend that you create and register the custom key before you create the DVS in Cisco UCS Manager to avoid any possibility of having to delete and recreate the associated DVS.

Distributed Virtual Switches

Each VMware ESX host has its own software-based virtual switch (vSwitch) in its hypervisor that performs the switching operations between its virtual machines (VMs). The Cisco UCS distributed virtual switch (DVS) is a software-based virtual switch that runs alongside the vSwitch in the ESX hypervisor, and can be distributed across multiple ESX hosts. Unlike vSwitch, which uses its own local port configuration, a DVS associated with multiple ESX hosts uses the same port configuration across all ESX hosts.

After associating an ESX host to a DVS, you can migrate existing VMs from the vSwitch to the DVS, and you can create VMs to use the DVS instead of the vSwitch. With the hardware-based VN-Link implementation, when a VM uses the DVS, all VM traffic passes through the DVS and ASIC-based switching is performed by the fabric interconnect.

In Cisco UCS Manager, DVSes are organized in the following hierarchy:

```
vCenter
    Folder (optional)
        Datacenter
            Folder (required)
                DVS
```

At the top of the hierarchy is the vCenter, which represents a VMware vCenter instance. Each vCenter contains one or more datacenters, and optionally vCenter folders with which you can organize the datacenters. Each datacenter contains one or more required datacenter folders. Datacenter folders contain the DVSes.

Port Profiles

Port profiles contain the properties and settings used to configure virtual interfaces in Cisco UCS for VN-Link in hardware. The port profiles are created and administered in Cisco UCS Manager. There is no clear visibility into the properties of a port profile from VMware vCenter.

In VMware vCenter, a port profile is represented as a port group. Cisco UCS Manager pushes the port profile names to vCenter, which displays the names as port groups. None of the specific networking properties or settings in the port profile are visible in VMware vCenter.

After a port profile is created, assigned to, and actively used by one or more DVSes, any changes made to the networking properties of the port profile in Cisco UCS Manager are immediately applied to those DVSes.

You must configure at least one port profile client for a port profile, if you want Cisco UCS Manager to push the port profile to VMware vCenter.

Port Profile Clients

The port profile client determines the DVSes to which a port profile is applied. By default, the port profile client specifies that the associated port profile applies to all DVSes in the vCenter. However, you can configure the client to apply the port profile to all DVSes in a specific datacenter or datacenter folder, or only to one DVS.

VN-Link in Hardware Considerations

How you configure a Cisco UCS instance for VN-Link in hardware has several dependencies. The information you need to consider before you configure VN-Link in hardware includes the following:

- A Cisco UCS instance can have a maximum of 4 vCenters

- Each vCenter can have a maximum of 8 distributed virtual switches
- Each distributed virtual switch can have a maximum of 4096 ports
- Each port profile can have a maximum of 4096 ports
- Each Cisco UCS instance can have a maximum of 256 port profiles

CHAPTER 2

Overview of Cisco UCS Manager

This chapter includes the following sections:

About Cisco UCS Manager

Cisco UCS Manager is the management system for all components in a Cisco UCS instance. Cisco UCS Manager runs within the fabric interconnect. You can use any of the interfaces available with this management service to access, configure, administer, and monitor the network and server resources for all chassis connected to the fabric interconnect.

Multiple Management Interfaces

Cisco UCS Manager includes the following interfaces you can use to manage a Cisco UCS instance:

- Cisco UCS Manager GUI
- Cisco UCS Manager CLI
- XML API
- KVM
- IPMI

Almost all tasks can be performed in any of the interfaces, and the results of tasks performed in one interface are automatically displayed in another.

However, you cannot do the following:

- Use Cisco UCS Manager GUI to invoke Cisco UCS Manager CLI.
- View the results of a command invoked through Cisco UCS Manager CLI in Cisco UCS Manager GUI.
- Generate CLI output from Cisco UCS Manager GUI.

Centralized Management

Cisco UCS Manager centralizes the management of resources and devices, rather than using multiple management points. This centralized management includes management of the following devices in a Cisco UCS instance:

- Fabric interconnects.
- Software switches for virtual servers.
- Power and environmental management for chassis and servers.
- Configuration and firmware updates for server network interfaces (Ethernet NICs and converged network adapters).
- Firmware and BIOS settings for servers.

Support for Virtual and Physical Servers

Cisco UCS Manager abstracts server state information—including server identity, I/O configuration, MAC addresses and World Wide Names, firmware revision, and network profiles—into a service profile. You can apply the service profile to any server resource in the system, providing the same flexibility and support to physical servers, virtual servers, and virtual machines connected to a virtual device provided by a VIC adapter.

Role-Based Administration and Multi-Tenancy Support

Cisco UCS Manager supports flexibly defined roles so that data centers can use the same best practices with which they manage discrete servers, storage, and networks to operate a Cisco UCS instance. You can create user roles with privileges that reflect user responsibilities in the data center. For example, you can create the following:

- Server administrator roles with control over server-related configurations.
- Storage administrator roles with control over tasks related to the SAN.
- Network administrator roles with control over tasks related to the LAN.

Cisco UCS is multi-tenancy ready, exposing primitives that allow systems management software using the API to get controlled access to Cisco UCS resources. In a multi-tenancy environment, Cisco UCS Manager enables you to create locales for user roles that can limit the scope of a user to a particular organization.

Tasks You Can Perform in Cisco UCS Manager

You can use Cisco UCS Manager to perform management tasks for all physical and virtual devices within a Cisco UCS instance.

Cisco UCS Hardware Management

You can use Cisco UCS Manager to manage all hardware within a Cisco UCS instance, including the following:

- Chassis
- Servers
- Fabric interconnects
- Fans

- Ports
- Interface cards
- I/O modules

Cisco UCS Resource Management

You can use Cisco UCS Manager to create and manage all resources within a Cisco UCS instance, including the following:

- Servers
- WWN addresses
- MAC addresses
- UUIDs
- Bandwidth

Server Administration in a Cisco UCS Instance

A server administrator can use Cisco UCS Manager to perform server management tasks within a Cisco UCS instance, including the following:

- Create server pools and policies related to those pools, such as qualification policies
- Create policies for the servers, such as discovery policies, scrub policies, and IPMI policies
- Create service profiles and, if desired, service profile templates
- Apply service profiles to servers
- Monitor faults, alarms, and the status of equipment

Network Administration in a Cisco UCS Instance

A network administrator can use Cisco UCS Manager to perform tasks required to create LAN configuration for a Cisco UCS instance, including the following:

- Configure uplink ports, port channels, and LAN PIN groups
- Create VLANs
- Configure the quality of service classes and definitions
- Create the pools and policies related to network configuration, such as MAC address pools and Ethernet adapter profiles

Storage Administration in a Cisco UCS Instance

A storage administrator can use Cisco UCS Manager to perform tasks required to create SAN configuration for a Cisco UCS instance, including the following:

- Configure ports, port channels, and SAN PIN groups
- Create VSANs
- Configure the quality of service classes and definitions

- Create the pools and policies related to the network configuration, such as WWN pools and Fibre Channel adapter profiles

Tasks You Cannot Perform in Cisco UCS Manager

You cannot use Cisco UCS Manager to perform certain system management tasks that are not specifically related to device management within a Cisco UCS instance

No Cross-System Management

You cannot use Cisco UCS Manager to manage systems or devices that are outside the Cisco UCS instance where Cisco UCS Manager is located. For example, you cannot manage heterogeneous environments, such as non-Cisco UCS x86 systems, SPARC systems, or PowerPC systems.

No Operating System or Application Provisioning or Management

Cisco UCS Manager provisions servers and, as a result, exists below the operating system on a server. Therefore, you cannot use it to provision or manage operating systems or applications on servers. For example, you cannot do the following:

- Deploy an OS, such as Windows or Linux
- Deploy patches for software, such as an OS or an application
- Install base software components, such as anti-virus software, monitoring agents, or backup clients
- Install software applications, such as databases, application server software, or web servers
- Perform operator actions, including restarting an Oracle database, restarting printer queues, or handling non-Cisco UCS user accounts
- Configure or manage external storage on the SAN or NAS storage

Cisco UCS Manager in a High Availability Environment

In a high availability environment with two fabric interconnects, you can run a separate instance of Cisco UCS Manager on each fabric interconnect. The Cisco UCS Manager on the primary fabric interconnect acts as the primary management instance, and the Cisco UCS Manager on the other fabric interconnect is the subordinate management instance.

The two instances of Cisco UCS Manager communicate across a private network between the L1 and L2 Ethernet ports on the fabric interconnects. Configuration and status information is communicated across this private network to ensure that all management information is replicated. This ongoing communication ensures that the management information for Cisco UCS persists even if the primary fabric interconnect fails. In addition, the "floating" management IP address that runs on the primary Cisco UCS Manager ensures a smooth transition in the event of a failover to the subordinate fabric interconnect.

CHAPTER 3

Overview of Cisco UCS Manager GUI

This chapter includes the following sections:

Overview of Cisco UCS Manager GUI

Cisco UCS Manager GUI is the Java application that provides a GUI interface to Cisco UCS Manager. You can start and access Cisco UCS Manager GUI from any computer that meets the following requirements:

- Has Java 1.6 or higher installed
- Runs a supported operating system
- Has HTTP or HTTPS access to the fabric interconnect

Each time you start Cisco UCS Manager GUI, Cisco UCS Manager uses Java Web Start technology to cache the current version of the application on your computer. As a result, you do not have to download the application every time you log in. You only have to download the application the first time that you log in from a computer after the Cisco UCS Manager software has been updated on a system.

Tip The title bar displays the name of the Cisco UCS instance to which you are connected.

Fault Summary Area

The **Fault Summary** area displays in the upper left of Cisco UCS Manager GUI. This area displays a summary of all faults that have occurred in the Cisco UCS instance.

Each type of fault is represented by a different icon. The number below each icon indicates how many faults of that type have occurred in the system. If you click an icon, Cisco UCS Manager GUI opens the **Faults** tab in the **Work** area and displays the details of all faults of that type.

The following table describes the types of faults each icon in the **Fault Summary** area represents:

Fault Type	Description
Critical Alarms	Critical problems exist with one or more components. These issues should be researched and fixed immediately.
Major Alarms	Serious problems exist with one or more components. These issues should be researched and fixed immediately.
Minor Alarms	Problems exist with one or more components that may adversely affect system performance. These issues should be researched and fixed as soon as possible before they become major or critical issues.
Warning Alarms	Potential problems exist with one or more components that may adversely affect system performance if they are allowed to continue. These issues should be researched and fixed as soon as possible before the problem grows worse.

Tip If you only want to see faults for a specific object, navigate to that object and then review the **Faults** tab for that object.

Navigation Pane

The **Navigation** pane displays on the left side of Cisco UCS Manager GUI below the **Fault Summary** area. This pane provides centralized navigation to all equipment and other components in the Cisco UCS instance. When you select a component in the **Navigation** pane, the object displays in the **Work** area.

The **Navigation** pane has five tabs. Each tab includes the following elements:

- A **Filter** combo box that you can use to filter the navigation tree to view all nodes or only one node.
- An expandable navigation tree that you can use to access all components on that tab. An icon next to an folder indicates that the node or folder has subcomponents.

Equipment Tab

This tab contains a basic inventory of the equipment in the Cisco UCS instance. A system or server administrator can use this tab to access and manage the chassis, fabric interconnects, servers, and other hardware. A red, orange, or yellow rectangle around a device name indicate that the device has a fault.

The major nodes below the **Equipment** node in this tab are the following:

- **Chassis**
- **Fabric Interconnects**

Servers Tab

This tab contains the server-related components, such as service profiles, polices, and pools. A server administrator typically accesses and manages the components on this tab.

The major nodes below the **Servers** node in this tab are the following:

- **Service Profiles**
- **Service Profile Templates**
- **Policies**
- **Pools**

LAN Tab

This tab contains the components related to LAN configuration, such as LAN pin groups, quality of service classes, VLANs, policies, pools, and the internal domain. A network administrator typically accesses and manages the components on this tab.

The major nodes below the **LAN** node in this tab are the following:

- **LAN Cloud**
- **Policies**
- **Pools**
- **Internal LAN Domains**

SAN Tab

This tab contains the components related to SAN configuration, such as pin groups, VSANs, policies, and pools. A storage administrator typically accesses and manages the components on this tab.

The major nodes below the **SAN** node in this tab are the following:

- **SAN Cloud**
- **Policies**
- **Pools**

VM Tab

This tab contains the components required to configure VN-Link in Hardware for servers with a VIC adapter. For example, you use components on this tab to configure the connection between Cisco UCS Manager and VMware vCenter, to configure distributed virtual switches, port profiles, and to view the virtual machines hosted on servers in the Cisco UCS instance.

The major node below the **All** node in this tab is the **VMware** node.

Admin Tab

This tab contains system-wide settings, such as user manager and communication services, and troubleshooting components, such as faults and events. The system administrator typically accesses and manages the components on this tab.

The major nodes below the **All** node in this tab are the following:

- **Faults, Events and Audit Log**
- **User Management**
- **Key Management**
- **Communication Management**
- **Stats Management**
- **Timezone Management**
- **Capability Catalog**

Toolbar

The toolbar displays on the right side of Cisco UCS Manager GUI above the **Work** pane. You can use the menu buttons in the toolbar to perform common actions, including the following actions:

- Navigate between previously viewed items in the **Work** pane
- Create elements for the Cisco UCS instance
- Set options for Cisco UCS Manager GUI
- Access online help for Cisco UCS Manager GUI

Work Pane

The **Work** pane displays on the right side of Cisco UCS Manager GUI. This pane displays details about the component selected in the **Navigation** pane.

The **Work** pane includes the following elements:

- A navigation bar that displays the path from the main node of the tab in the **Navigation** pane to the selected element. You can click any component in this path to display that component in the **Work** pane.
- A content area that displays tabs with information related to the component selected in the **Navigation** pane. The tabs displayed in the content area depends upon the selected component. You can use these tabs to view information about the component, create components, modify properties of the component, and examine a selected object.

Status Bar

The status bar displays across the bottom of Cisco UCS Manager GUI. The status bar provides information about the state of the application.

On the left, the status bar displays the following information about your current session in Cisco UCS Manager GUI:

- A lock icon that indicates the protocol you used to log in. If the icon is locked, you connected with HTTPS and if the icon is unlocked, you connected with HTTP.
- The username you used to log in.
- The IP address of the server where you logged in.

On the right, the status bar displays the system time.

Table Customization

Cisco UCS Manager GUI enables you to customize the tables on each tab. You can change the type of content that you view and filter the content.

Table Customization Menu Button

This menu button in the upper right of every table enables you to control and customize your view of the table. The drop-down menu for this button includes the following options:

Menu Item	Description
Column Name	The menu contains an entry for each column in the table. Click a column name to display or hide the column.
Horizontal Scroll	If selected, adds a horizontal scroll bar to the table. If not selected, when you widen one of the columns, all columns to the right narrow and do not scroll.
Pack All Columns	Resizes all columns to their default width.
Pack Selected Column	Resizes only the selected column to its default width.

Table Content Filtering

The **Filter** button above each table enables you to filter the content in the table according to the criteria that you set in the **Filter** dialog box. The dialog box includes the following filtering options:

Name	Description
Disable option	No filtering criteria is used on the content of the column. This is the default setting.
Equal option	Displays only that content in the column which exactly matches the value specified.
Not Equal option	Displays only that content in the column which does not exactly match the value specified.
Wildcard option	The criteria you enter can include one of the following wildcards: • _ (underscore) or ? (question mark)—replaces a single character • % (percent sign) or * (asterisk)—replaces any sequence of characters
Less Than option	Displays only that content in the column which is less than the value specified.

Name	Description
Less Than Or Equal option	Displays only that content in the column which is less than or equal to the value specified.
Greater Than option	Displays only that content in the column which is greater than the value specified.
Greater Than Or Equal option	Displays only that content in the column which is greater than or equal to the value specified.

LAN Uplinks Manager

The LAN Uplinks Manager provides a single interface where you can configure the connections between Cisco UCS and the LAN. You can use the LAN Uplinks Manager to create and configure the following:

- Ethernet switching mode
- Uplink Ethernet ports
- Port channels
- LAN pin groups
- Named VLANs
- Server ports
- QoS system classes

Some of the configuration that you can do in the LAN Uplinks Manager can also be done in nodes on other tabs, such as the **Equipment** tab or the **LAN** tab.

Internal Fabric Manager

The Internal Fabric Manager provides a single interface where you can configure server ports for a fabric interconnect in a Cisco UCS instance. The Internal Fabric Manager is accessible from the **General** tab for that fabric interconnect.

Some of the configuration that you can do in the Internal Fabric Manager can also be done in nodes on the **Equipment** tab, on the **LAN** tab, or in the LAN Uplinks Manager.

Hybrid Display

For each chassis in a Cisco UCS instance, Cisco UCS Manager GUI provides a hybrid display that includes both physical components and connections between the chassis and the fabric interconnects.

This tab displays detailed information about the connections between the selected chassis and the fabric interconnects. It has an icon for the following:

- Each fabric interconnect in the system
- The I/O module (IOM) in the selected component, which is shown as an independent unit to make the connection paths easier to see

- The selected chassis showing the servers and PSUs

The lines between the icons represent the connections between the following:

- DCE interface on each server and the associated server port on the IOM. These connections are created by Cisco and cannot be changed.
- Server port on the IOM and the associated port on the fabric interconnect. You can change these connections if desired.

You can mouse over the icons and lines to view tooltips identifying each component or connection, and you can double-click any component to view properties for that component.

If there is a fault associated with the component or any of its subcomponents, Cisco UCS Manager GUI displays a fault icon on top of the appropriate component. If there are multiple fault messages, Cisco UCS Manager GUI displays the icon associated with the most serious fault message in the system.

Logging in to Cisco UCS Manager GUI through HTTPS

The default HTTPS web link for Cisco UCS Manager GUI is `https://UCSManager_IP`, where *UCSManager_IP* represents the IP address assigned to Cisco UCS Manager. This IP address can be one of the following:

- Cluster configuration: *UCSManager_IP* represents the virtual or cluster IP address assigned to Cisco UCS Manager. Do not use the IP addresses assigned to the management port on the fabric interconnects.
- Standalone configuration: *UCSManager_IP* represents the IP address for the management port on the fabric interconnect

Procedure

Step 1 In your web browser, type the Cisco UCS Manager GUI web link or select the bookmark in your browser.

Step 2 If a **Security Alert** dialog box appears, click **Yes** to accept the security certificate and continue.

Step 3 In the Cisco UCS Manager page, click **Launch**.
Depending upon the web browser you use to log in, you may be prompted to download or save the .JNLP file.

Step 4 If a **Security** dialog box displays, do the following:

a) (Optional) Check the check box to accept all content from Cisco.
b) Click **Yes** to accept the certificate and continue.

Step 5 In the **Login** dialog box, do the following:

a) Enter your username and password.
b) If the Cisco UCS instance implements domains, select the appropriate domain from the **Domain** drop-down list.
c) Click **Login**.

Logging in to Cisco UCS Manager GUI through HTTP

The default HTTP web link for Cisco UCS Manager GUI is `http://UCSManager_IP`, where *UCSManager_IP* represents the IP address assigned to Cisco UCS Manager. This IP address can be one of the following:

- Cluster configuration: *UCSManager_IP* represents the virtual or cluster IP address assigned to Cisco UCS Manager. Do not use the IP addresses assigned to the management port on the fabric interconnects.
- Standalone configuration: *UCSManager_IP* represents the IP address for the management port on the fabric interconnect

Procedure

Step 1 In your web browser, type the Cisco UCS Manager GUI web link or select the bookmark in your browser.

Step 2 In the Cisco UCS Manager page, click **Launch**.
Depending upon the web browser you use to log in, you may be prompted to download or save the .JNLP file.

Step 3 In the **Login** dialog box, do the following:

a) Enter your username and password.
b) If the Cisco UCS instance implements domains, select the appropriate domain from the **Domain** drop-down list.
c) Click **Login**.

Logging Off Cisco UCS Manager GUI

Procedure

Step 1 In Cisco UCS Manager GUI, click **Exit** in the upper right.
Cisco UCS Manager GUI blurs on your screen to indicate that you cannot use it and displays the **Exit** dialog box.

Step 2 From the drop-down list, select one of the following:

- **Exit** to log out and shut down Cisco UCS Manager GUI.
- **Log Off** to log out of Cisco UCS Manager GUI and log in a different user.

Step 3 Click **OK**.

Changing the Cisco UCS Manager GUI Properties

Procedure

Step 1 In the toolbar, click **Options** to open the **Properties** dialog box.

Step 2 (Optional) To specify if Cisco UCS Manager GUI will require confirmation for certain procedures, do the following:

a) In the right pane, click **Confirmation Messages**.

b) In the left pane, complete the following fields:

Name	Description
Confirm Deletion check box	If checked, Cisco UCS Manager GUI requires that you confirm all delete operations.
Confirm Discard Changes check box	If checked, Cisco UCS Manager GUI requires that you confirm before the system discards any changes.
Confirm Modification/Creation check box	If checked, Cisco UCS Manager GUI requires that you confirm before the system modifies or creates objects.
Confirm Successful Operations check box	If checked, Cisco UCS Manager GUI displays a confirmation when operations are successful.

Step 3 (Optional) To configure SSH external applications, do the following:

a) In the right pane, click **External Applications**.

b) In the left pane, complete the following fields:

Name	Description
SSH field	The application to use for SSH processing.
SSH Parameters field	Any parameters to include in all SSH commands.

Step 4 (Optional) To change the session properties, do the following:

a) In the right pane, click **Session**.

b) In the **Session** page, update one or more of the following fields:

Name	Description
Automatically Reconnect check box	If checked, the system tries to reconnect if communication between the GUI and the fabric interconnect is interrupted.
GUI Inactivity Time Out drop-down list	The number of minutes the system should wait before ending an inactive session. To specify that the session should not time out regardless of the length of inactivity, choose **NEVER**.

Name	Description
Reconnection Interval field	If the **Automatically Reconnect** check box is checked, this is the number of seconds the system waits before trying to reconnect.

Step 5 (Optional) To change the look of Cisco UCS Manager GUI, do the following:

a) In the right pane, click **Visual Enhancements**.

b) In the **Visual Enhancements** page, update one or more of the following fields:

Name	Description
Max History Size field	The number of tabs the system should store in memory for use with the Forward and Back toolbar buttons.
Right Aligned Labels check box	If checked, all labels are right-aligned with respect to one another. Otherwise all labels are left-aligned.
Show Image while Dragging check box	If checked, when you drag an object from one place to another, the GUI displays a transparent version of that object until you drop the object in its new location.
Wizard Transition Effects check box	If checked, when you go to a new page in a wizard the first page fades out and the new page fades in. Otherwise the page changes without a visible transition.

Step 6 Click **OK**.

Copying the XML

To assist you in developing scripts or creating applications with the XML API for Cisco UCS, Cisco UCS Manager GUI includes an option to copy the XML used to create an object in Cisco UCS Manager. This option is available on the right-click menu for most object nodes in the **Navigation** pane, such as the **Port Profiles** node or the node for a specific service profile.

Procedure

Step 1 In the **Navigation** pane, navigate to the object for which you want to copy the XML.

Step 2 Right-click on that object and choose **Copy XML**.

Step 3 Paste the XML into an XML editor, Notepad, or another application.

PART II

System Configuration

CHAPTER 4

Configuring the Fabric Interconnects

This chapter includes the following sections:

Initial System Setup

The first time that you access a fabric interconnect in a Cisco UCS instance, a setup wizard prompts you for the following information required to configure the system:

- Installation method (GUI or CLI)
- Setup mode (restore from full system backup or initial setup)
- System configuration type (standalone or cluster configuration)
- System name
- Admin password
- Management port IP address and subnet mask
- Default gateway IP address
- DNS Server IP address

- Default domain name

Setup Mode

You can choose to either restore the system configuration from an existing backup file, or manually set up the system by going through the Setup wizard. If you choose to restore the system, the backup file must be reachable from the management network.

System Configuration Type

You can configure a Cisco UCS instance to use a single fabric interconnect in a standalone configuration or to use a redundant pair of fabric interconnects in a cluster configuration.

A cluster configuration provides high availability. If one fabric interconnect becomes unavailable, the other takes over. Only one management port (Mgmt0) connection is required to support a cluster configuration; however, both Mgmt0 ports should be connected to provide link-level redundancy.

In addition, a cluster configuration actively enhances failover recovery time for redundant virtual interface (VIF) connections. When an adapter has an active VIF connection to one fabric interconnect and a standby VIF connection to the second, the learned MAC addresses of the active VIF are replicated but not installed on the second fabric interconnect. If the active VIF fails, the second fabric interconnect installs the replicated MAC addresses and broadcasts them to the network through gratuitous ARP messages, shortening the switchover time.

Note The cluster configuration provides redundancy only for the management plane. Data redundancy is dependent on the user configuration and may require a third-party tool to support data redundancy.

To use the cluster configuration, the two fabric interconnects must be directly connected together using Ethernet cables between the L1 (L1-to-L1) and L2 (L2-to-L2) high availability ports, with no other fabric interconnects in between. This allows the two fabric interconnects to continuously monitor the status of each other and quickly know when one has failed.

Both fabric interconnects in a cluster configuration must go through the initial setup process. The first fabric interconnect to be set up must be enabled for a cluster configuration. Then, when the second fabric interconnect is set up, it detects the first fabric interconnect as a peer fabric interconnect in the cluster.

For more information, refer to the *Cisco UCS 6100 Series Fabric Interconnect Hardware Installation Guide*.

Management Port IP Address

In a standalone configuration, you must specify only one IP address and the subnet mask for the single management port on the fabric interconnect.

In a cluster configuration, you must specify the following three IP addresses in the same subnet:

- Management port IP address for fabric interconnect A
- Management port IP address for fabric interconnect B
- Cluster IP address

Performing an Initial System Setup for a Standalone Configuration

Before You Begin

1 Verify the following physical connections on the fabric interconnect:

- The console port is physically connected to a computer terminal or console server
- The management Ethernet port (mgmt0) is connected to an external hub, switch, or router

For more information, refer to the *Cisco UCS Hardware Installation Guide* for your fabric interconnect.

2 Verify that the console port parameters on the computer terminal (or console server) attached to the console port are as follows:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit

3 Collect the following information that you will need to supply during the initial setup:

- System name.
- Password for the admin account. Choose a strong password that meets the guidelines for Cisco UCS Manager passwords. This password cannot be blank.
- Management port IP address and subnet mask.
- Default gateway IP address.
- DNS server IP address (optional).
- Domain name for the system (optional).

Procedure

Step 1 Connect to the console port.

Step 2 Power on the fabric interconnect.
You will see the power on self-test messages as the fabric interconnect boots.

Step 3 At the installation method prompt, enter gui.

Step 4 If the system cannot access a DHCP server, you are prompted to enter the following information:

- IP address for the management port on the fabric interconnect
- Subnet mask for the management port on the fabric interconnect
- IP address for the default gateway assigned to the fabric interconnect

Step 5 Copy the web link from the prompt into a supported web browser and go to the Cisco UCS Manager GUI launch page.

Step 6 On the Cisco UCS Manager GUI launch page, select **Express Setup**.

Step 7 On the **Express Setup** page, select **Initial Setup** and click **Submit**.

Step 8 In the **Cluster and Fabric Setup** Area, select the **Standalone Mode** option.

Step 9 In the **System Setup** Area, complete the following fields:

Field	Description
System Name field	The name assigned to the Cisco UCS instance In a standalone configuration, the system adds "-A" to the system name. In a cluster configuration, the system adds "-A" to the fabric interconnect assigned to fabric A, and "-B" to the fabric interconnect assigned to fabric B.
Admin Password field	The password used for the Admin account on the fabric interconnect. Choose a strong password that meets the guidelines for Cisco UCS Manager passwords. This password cannot be blank.
Confirm Admin Password field	The password used for the Admin account on the fabric interconnect.
Mgmt IP Address field	The static IP address for the management port on the fabric interconnect.
Mgmt IP Netmask field	The subnet mask for the management port on the fabric interconnect.
Default Gateway field	The IP address for the default gateway assigned to the management port on the fabric interconnect.
DNS Server IP field	The IP address for the DNS server assigned to the fabric interconnect.
Domain Name field	The name of the domain in which the fabric interconnect resides.

Step 10 Click **Submit.**
A page displays the results of your setup operation.

Initial System Setup for a Cluster Configuration

Performing an Initial System Setup on the First Fabric Interconnect

Before You Begin

1 Verify the following physical connections on the fabric interconnect:

- A console port on the first fabric interconnect is physically connected to a computer terminal or console server
- The management Ethernet port (mgmt0) is connected to an external hub, switch, or router
- The L1 ports on both fabric interconnects are directly connected to each other
- The L2 ports on both fabric interconnects are directly connected to each other

For more information, refer to the *Cisco UCS Hardware Installation Guide* for your fabric interconnect.

2 Verify that the console port parameters on the computer terminal (or console server) attached to the console port are as follows:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit

3 Collect the following information that you will need to supply during the initial setup:

- System name.
- Password for the admin account. Choose a strong password that meets the guidelines for Cisco UCS Manager passwords. This password cannot be blank.
- Three static IP addresses: two for the management port on both fabric interconnects (one per fabric interconnect) and one for the cluster IP address used by Cisco UCS Manager.
- Subnet mask for the three static IP addresses.
- Default gateway IP address.
- DNS server IP address (optional).
- Domain name for the system (optional).

Procedure

Step 1 Connect to the console port.

Step 2 Power on the fabric interconnect.

You will see the power on self-test messages as the fabric interconnect boots.

Step 3 At the installation method prompt, enter gui.

Step 4 If the system cannot access a DHCP server, you are prompted to enter the following information:

- IP address for the management port on the fabric interconnect
- Subnet mask for the management port on the fabric interconnect
- IP address for the default gateway assigned to the fabric interconnect

Step 5 Copy the web link from the prompt into a web browser and go to the Cisco UCS Manager GUI launch page.

Step 6 On the Cisco UCS Manager GUI launch page, select **Express Setup**.

Step 7 On the **Express Setup** page, select **Initial Setup** and click **Submit**.

Step 8 In the **Cluster and Fabric Setup** Area:

a) Click the **Enable Clustering** option.
b) For the **Fabric Setup** option, select **Fabric A**.
c) In the **Cluster IP Address** field, enter the IP address that Cisco UCS Manager will use.

Step 9 In the **System Setup** Area, complete the following fields:

Field	Description
System Name field	The name assigned to the Cisco UCS instance In a standalone configuration, the system adds "-A" to the system name. In a cluster configuration, the system adds "-A" to the fabric interconnect assigned to fabric A, and "-B" to the fabric interconnect assigned to fabric B.
Admin Password field	The password used for the Admin account on the fabric interconnect. Choose a strong password that meets the guidelines for Cisco UCS Manager passwords. This password cannot be blank.
Confirm Admin Password field	The password used for the Admin account on the fabric interconnect.
Mgmt IP Address field	The static IP address for the management port on the fabric interconnect.
Mgmt IP Netmask field	The subnet mask for the management port on the fabric interconnect.
Default Gateway field	The IP address for the default gateway assigned to the management port on the fabric interconnect.
DNS Server IP field	The IP address for the DNS server assigned to the fabric interconnect.

Field	Description
Domain Name field	The name of the domain in which the fabric interconnect resides.

Step 10 Click **Submit**.
A page displays the results of your setup operation.

Performing an Initial System Setup on the Second Fabric Interconnect

Before You Begin

You must ensure the following:

- A console port on the second fabric interconnect is physically connected to a computer terminal or console server
- You know the password for the admin account on the first fabric interconnect that you configured.

Procedure

Step 1 Connect to the console port.

Step 2 Power on the fabric interconnect.
You will see the power on self-test messages as the fabric interconnect boots.

Step 3 At the installation method prompt, enter gui.

Step 4 If the system cannot access a DHCP server, you are prompted to enter the following information:

- IP address for the management port on the fabric interconnect
- Subnet mask for the management port on the fabric interconnect
- IP address for the default gateway assigned to the fabric interconnect

Step 5 Copy the web link from the prompt into a web browser and go to the Cisco UCS Manager GUI launch page.

Step 6 On the Cisco UCS Manager GUI launch page, select **Express Setup**.

Step 7 On the **Express Setup** page, select **Initial Setup** and click **Submit**.
The fabric interconnect should detect the configuration information for the first fabric interconnect.

Step 8 In the **Cluster and Fabric Setup** Area:

a) Select the **Enable Clustering** option.

b) For the **Fabric Setup** option, make sure **Fabric B** is selected.

Step 9 In the **System Setup** Area, enter the password for the Admin account into the **Admin Password of Master** field.

Step 10 Click **Submit**.
A page displays the results of your setup operation.

Enabling a Standalone Fabric Interconnect for Cluster Configuration

You can add a second fabric interconnect to an existing Cisco UCS instance that uses a single standalone fabric interconnect. To do this, you must enable the standalone fabric interconnect for cluster operation, and then add the second fabric interconnect to the cluster.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **connect local-mgmt**	Enters local management mode.
Step 2	UCS-A(local-mgmt) # **enable cluster** *ip-addr*	Enables cluster operation on the standalone fabric interconnect with the specified IP address. When you enter this command, you are prompted to confirm that you want to enable cluster operation. Type **yes** to confirm.

The following example enables a standalone fabric interconnect with IP address 192.168.1.101 for cluster operation:

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# enable cluster 192.168.1.101
This command will enable cluster mode on this setup. You cannot change it
back to stand-alone. Are you sure you want to continue? (yes/no): yes
UCS-A(local-mgmt)#
```

What to Do Next

Add the second fabric interconnect to the cluster.

Ethernet Switching Mode

The Ethernet switching mode determines how the fabric interconnect behaves as a switching device between the servers and the network. The fabric interconnect operates in either of the following Ethernet switching modes:

End-Host Mode

End-host mode allows the fabric interconnect to act as an end host to the network, representing all server (hosts) connected to it through vNICs. This is achieved by pinning (either dynamically pinned or hard pinned) vNICs to uplink ports, which provides redundancy toward the network, and makes the uplink ports appear as server ports to the rest of the fabric. When in end-host mode, the fabric interconnect does not run the Spanning Tree Protocol (STP) and avoids loops by denying uplink ports from forwarding traffic to each other, and by denying egress server traffic on more than one uplink port at a time. End-host mode is the default Ethernet switching mode and should be used if either of the following are used upstream:

- Layer 2 switching for L2 aggregation
- Virtual Switching System (VSS) aggregation layer

Note When end-host mode is enabled, if a vNIC is hard pinned to an uplink port and this uplink port goes down, the system cannot re-pin the vNIC, and the vNIC remains down.

Switch Mode

Switch mode is the traditional Ethernet switching mode. The fabric interconnect runs STP to avoid loops, and broadcast and multicast packets are handled in the traditional way. Switch mode is not the default Ethernet switching mode, and should be used only if the fabric interconnect is directly connected to a router, or if either of the following are used upstream:

- Layer 3 aggregation
- VLAN in a box

Note For both Ethernet switching modes, even when vNICs are hard pinned to uplink ports, all server-to-server unicast traffic in the server array is sent only through the fabric interconnect and is never sent through uplink ports. Server-to-server multicast and broadcast traffic is sent through all uplink ports in the same VLAN.

Configuring Ethernet Switching Mode

Important When you change the Ethernet switching mode, Cisco UCS Manager logs you out and restarts the fabric interconnect. For a cluster configuration, Cisco UCS Manager restarts both fabric interconnects sequentially. The second fabric interconnect can take several minutes to complete the change in Ethernet switching mode and become system ready.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Fabric Interconnects ➤** ***Fabric_Interconnect_Name***.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area of the **General** tab, click one of the following links:

- **Set Ethernet Switching Mode**
- **Set Ethernet End-Host Mode**

The link for the current mode is dimmed.

Step 5 In the dialog box, click **Yes**.
Cisco UCS Manager restarts the fabric interconnect, logs you out, and disconnects Cisco UCS Manager GUI.

Fibre Channel Switching Mode

The Fibre Channel switching mode determines how the fabric interconnect behaves as a switching device between the servers and storage devices. The fabric interconnect operates in either of the following Fibre Channel switching modes:

End-Host Mode

End-host mode allows the fabric interconnect to act as an end host to the connected fibre channel networks, representing all server (hosts) connected to it through vHBAs. This is achieved by pinning (either dynamically pinned or hard pinned) vHBAs to Fibre Channel uplink ports, which makes the Fibre Channel ports appear as server ports (N-ports) to the rest of the fabric. When in end-host mode, the fabric interconnect avoids loops by denying uplink ports from receiving traffic from one another.

End-host mode is synonymous with NPV mode. This is the default Fibre Channel Switching mode.

Note When end-host mode is enabled, if a vHBA is hard pinned to a uplink Fibre Channel port and this uplink port goes down, the system cannot re-pin the vHBA, and the vHBA remains down.

Switch Mode

Switch mode is the traditional Fibre Channel switching mode. Switch mode allows the fabric interconnect to connect directly to a storage device. Enabling Fibre Channel switch mode is useful in POD models where there is no SAN (for example, a single Cisco UCS system connected directly to storage), or where a SAN exists (with an upstream MDS).

Note In Fibre Channel switch mode, SAN pin groups are irrelevant. Any existing SAN pin groups will be ignored.

Switch mode is not the default Fibre Channel switching mode. Enabling Fibre Channel switching mode requires a license.

Configuring Fibre Channel Switching Mode

Important When you change the Fibre Channel switching mode, Cisco UCS Manager logs you out and restarts the fabric interconnect. For a cluster configuration, Cisco UCS Manager restarts both fabric interconnects sequentially. The second fabric interconnect can take several minutes to complete the change in Fibre Channel switching mode and become system ready.

Before You Begin

Enabling Fibre Channel Switching requires a license. Ensure that the proper license has been installed before proceeding with your configuration.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Fabric Interconnects ➤** ***Fabric_Interconnect_Name***.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area of the **General** tab, click one of the following links:

- **Set Fibre Channel Switching Mode**
- **Set Fibre Channel End-Host Mode**

The link for the current mode is dimmed.

Step 5 In the dialog box, click **Yes**.
Cisco UCS Manager restarts the fabric interconnect, logs you out, and disconnects Cisco UCS Manager GUI.

Changing the Properties of the Fabric Interconnects

Note To change the subnet for a Cisco UCS instance, you must simultaneously change all subnets, the virtual IP address used to access Cisco UCS Manager, and the IP addresses for all fabric interconnects.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **All**.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area, click **Management Interfaces** to open the **Management Interfaces** dialog box.

Step 5 To change only the virtual IP address that you use to access Cisco UCS Manager, enter the desired IP address in the **IP Address** field in the **Virtual IP** area.

Step 6 To change only the name assigned to the Cisco UCS instance, enter the desired name in the **Name** field in the **Virtual IP** area.

Step 7 To change the subnet, IP address, and default gateway assigned to the fabric interconnects, update the following fields:

a) In the **Virtual IP** area, change the IP address used to access Cisco UCS Manager in the **IP Address** field.

b) In the **Fabric Interconnect** area for each fabric interconnect, update the following fields:

Name	Description
IP Address field	The IP address to use when communicating with the fabric interconnect.
Subnet Mask field	The associated subnet mask.

Name	Description
Default Gateway field	The associated gateway.

Step 8 Click **OK**.

Step 9 Log out of Cisco UCS Manager GUI and log back in again to see your changes.

Determining the Leadership Role of a Fabric Interconnect

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 In the **Equipment** tab, expand **Equipment ➤ Fabric Interconnects**.

Step 3 Click the fabric interconnect for which you want to identify the role.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **General** tab, click the down arrows on the **High Availability Details** bar to expand that area.

Step 6 View the **Leadership** field to determine whether the fabric interconnect is the primary or subordinate.

CHAPTER 5

Configuring Ports

This chapter includes the following sections:

Server and Uplink Ports on the Fabric Interconnect

Each fabric interconnect has a set of ports in a fixed port module that you can configure as either server ports or uplink Ethernet ports. These ports are not reserved. They cannot be used by a Cisco UCS instance until you configure them. You can add expansion modules to increase the number of uplink ports on the fabric interconnect or to add uplink Fibre Channel ports to the fabric interconnect.

You need to create LAN pin groups and SAN pin groups to pin traffic from servers to an uplink port.

Each fabric interconnect can include the following types of ports:

Server Ports	Server ports handle data traffic between the fabric interconnect and the adapter cards on the servers. You can only configure server ports on the fixed port module. Expansion modules do not include server ports.
Uplink Ethernet Ports	Uplink Ethernet ports handle Ethernet traffic between the fabric interconnect and the next layer of the network. All network-bound Ethernet traffic is pinned to one of these ports. By default, Ethernet ports are unconfigured. However, you can configure them to function in the following ways: • Server • Uplink • FCoE • Appliance You can configure uplink Ethernet ports on either the fixed module or an expansion module.
Uplink Fibre Channel Ports	Uplink Fibre Channel ports handle FCoE traffic between the fabric interconnect and the next layer of the network. All network-bound FCoE traffic is pinned to one of these ports. By default, Fibre Channel ports are uplink. However, you can configure them to function as Fibre Channel storage ports. This is useful in cases where a Cisco UCS requires a connection to a Direct-Attached Storage (DAS) device. You can only configure uplink Fibre Channel ports on an expansion module. The fixed module does not include uplink Fibre Channel ports.

Configuring Server Ports

You can only configure server ports on the fixed port module. Expansion modules do not include server ports.

This task describes only one method of configuring ports. You can also configure ports from a right-click menu, from the **General** tab for the port, or in the LAN Uplinks Manager.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 In the **Equipment** tab, expand **Fabric Interconnects** ➤ ***Fabric_Interconnect_Name*** ➤ **Fixed Module** ➤ **Unconfigured Ports**.

Step 3 Click one or more ports under the **Unconfigured Ports** node.

Step 4 Drag the selected port or ports and drop them in the **Server Ports** node.
The port or ports are configured as server ports, removed from the list of unconfigured ports, and added to the **Server Ports** node.

Configuring Uplink Ethernet Ports

You can configure uplink Ethernet ports on either the fixed module or an expansion module.

This task describes only one method of configuring uplink Ethernet ports. You can also configure uplink Ethernet ports from a right-click menu or from the **General** tab for the port.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Fabric Interconnects ➤** ***Fabric_Interconnect_Name***.

Step 3 Depending upon the location of the ports you want to configure, expand one of the following:

- **Fixed Module**
- **Expansion Module**

Step 4 Click one or more of the ports under the **Unconfigured Ethernet Ports** node.
If you want to reconfigure a server port, appliance port, or FCoE storage port, expand the appropriate node.

Step 5 Drag the selected port or ports and drop them in the **Uplink Ethernet Ports** node.
The port or ports are configured as uplink Ethernet ports, removed from the list of unconfigured ports, and added to the **Uplink Ethernet Ports** node.

What to Do Next

If desired, change the properties for the default flow control policy and admin speed of the uplink Ethernet port.

Changing the Properties of an Uplink Ethernet Port

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Fabric Interconnects ➤** ***Fabric_Interconnect_Name***.

Step 3 Depending upon the location of the ports you want to configure, expand one of the following:

- **Fixed Module**
- **Expansion Module**

Step 4 In the **Uplink Ethernet Ports** node, click the uplink Ethernet port that you want to change.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Actions** area, click **Show Interface**.

Step 7 In the **Properties** dialog box, complete the following fields:

a) (Optional) In the **User Label** field, enter a label to identify the port.

b) From the **Flow Control Policy** drop-down list, select a flow control policy to determine how the port sends and receives IEEE 802.3x pause frames when the receive buffer fills.

c) In the **Admin Speed** field, click one of the following radio buttons:

- 1Gbps
- 10Gbps

Step 8 Click **OK**.

Configuring an FCoE Storage Port

You can configure FCoE storage ports on either the fixed module or an expansion module.

This task describes only one method of configuring FCoE storage ports. You can also configure FCoE storage ports from the **General** tab for the port.

Before You Begin

The Fibre Channel switching mode must be set to Switching for these ports to be valid. The storage ports cannot function in end-host mode.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Fabric Interconnects ➤** ***Fabric_Interconnect_Name***.

Step 3 Depending upon the location of the ports you want to configure, expand one of the following:

- **Fixed Module**
- **Expansion Module**

Step 4 Click one or more of the ports under the **Unconfigured Ethernet Ports** node.
If you want to reconfigure an uplink Ethernet port, server port, or appliance port, expand the appropriate node.

Step 5 Right-click the selected port or ports and choose **Configure as FCoE Storage Port**.

Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 7 Click **OK**.
The port or ports are configured as FCoE storage ports, removed from the list of unconfigured ports, and added to the **Storage Ethernet Ports** node.

Reconfiguring a Port on a Fabric Interconnect

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Fabric Interconnects ➤** ***Fabric_Interconnect_Name***.

Step 3 Depending upon the location of the ports you want to reconfigure, expand one of the following:

- **Fixed Module**
- **Expansion Module**

Step 4 Click the port or ports you want to reconfigure.

Step 5 Drag the selected port or ports and drop them in the appropriate node.
The port or ports are reconfigured as the appropriate type of port, removed from the original node, and added to the new node.

Example: Reconfiguring an Uplink Ethernet Port as a Server Port

1 Expand the **Uplink Ethernet Ports** node and select the port you want to reconfigure.

2 Drag the port and drop it into the **Server Ports** node.

Enabling a Port on a Fabric Interconnect

After you enable or disable a port on a fabric interconnect, wait for at least 1 minute before you reacknowledge the chassis. If you reacknowledge the chassis too soon, the pinning of server traffic from the chassis may not be updated with the changes to the port that you enabled or disabled.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN ➤ LAN Cloud**.

Step 3 Expand ***Fabric_Interconnect_Name*** **➤ Ports**.

Step 4 Right-click the port that you want to enable and choose **Enable Port**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Disabling a Port on a Fabric Interconnect

After you enable or disable a port on a fabric interconnect, wait for at least 1 minute before you reacknowledge the chassis. If you reacknowledge the chassis too soon, the pinning of server traffic from the chassis may not be updated with the changes to the port that you enabled or disabled.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN ➤ LAN Cloud**.

Step 3 Expand ***Fabric_Interconnect_Name*** **➤ Ports**.

Step 4 Right-click the port that you want to disable and choose **Disable Port**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Unconfiguring a Port on a Fabric Interconnect

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Fabric Interconnects ➤** ***Fabric_Interconnect_Name***.

Step 3 Depending upon the location of the ports you want to unconfigure, expand one of the following:

- **Fixed Module**
- **Expansion Module**

Step 4 Click the port or ports you want to unconfigure.

Step 5 Drag the selected port or ports and drop them in the **Unconfigured Ports** node.
The port or ports are unconfigured, removed from the original node, and added to the new node.

Appliance Ports

Configuring an Appliance Port

You can configure Appliance ports on either the fixed module or an expansion module.

This task describes only one method of configuring appl ports. You can also configure appliance ports from the **General** tab for the port.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Fabric Interconnects ➤** ***Fabric_Interconnect_Name***.

Step 3 Depending upon the location of the ports you want to configure, expand one of the following:

- **Fixed Module**
- **Expansion Module**

Step 4 Click one or more of the ports under the **Unconfigured Ethernet Ports** node.
If you want to reconfigure a server port, uplink Ethernet port, or FCoE storage port, expand the appropriate node.

Step 5 Right-click the selected port or ports and choose **Configure as Appliance Port**.

Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 7 In the **Configure as Appliance Port** dialog box, complete the following fields:

Name	Description
Priority drop-down list	The QoS priority assigned to this port. This can be: • **best-effort**—This priority is reserved for the Basic Ethernet traffic lane. • **bronze**—Use this priority for vNIC traffic only. • **fc**—Use this priority for vHBA traffic only. • **gold**—Use this priority for vNIC traffic only. • **platinum**—Use this priority for vNIC traffic only. • **silver**—Use this priority for vNIC traffic only.
Pin Group drop-down list	The LAN pin group that you want to use as the appliance pin target to the specified fabric and port, or fabric and port channel
Create LAN Pin Group link	Click this link if you want to create a LAN pin group.
Admin Speed field	The data transfer rate for this port. Select the value that matches the destination to which the port is linked. This can be: • **1Gbps** • **10Gbps** **Note** The admin speed can only be changed for certain ports. For more information, see the *Hardware Installation Guide* for your fabric interconnect.
Port Mode field	The port mode used for the appliance port. By default, the mode is set to trunk. This can be:

Name	Description
	• **trunk**—If you click this radio button, check one or more check boxes in the table to assign VLANs to the appliance port. • **access**—If you click this radio button, choose a VLAN from the **Select VLAN** drop-down list to assign it to the appliance port. You can also assign an Ethernet target endpoint to the appliance port if you choose this mode. You can also click **Create VLAN** to create a VLAN to assign to the appliance port.
Ethernet Target Endpoint check box	Check this check box if you want to assign a VLAN or target MAC address to the appliance port. This option is only available if you configure the appliance port to use the access port mode.
Name field	A user-defined name for the endpoint. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
MAC Address field	The MAC address for the endpoint in nn:nn:nn:nn:nn:nn format.

Step 8 Click **OK**.
The port or ports are configured as Appliance ports, removed from the list of unconfigured ports, and added to the **Storage Ethernet Ports** node.

Modifying the Properties of an Appliance Port

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, expand **Equipment ➤ Fabric Interconnects ➤** ***Fabric_Interconnect_Name***.
Step 3 Depending upon the location of the appliance port you want to modify, expand one of the following:

- **Fixed Module**
- **Expansion Module**

Step 4 Expand **Appliance Ports**.
Step 5 Click the appliance port for which you want to modify the properties.
Step 6 In the **Work** pane, click the **General** tab.
Step 7 In the **Actions** area, click **Show Interface**.
You may need to expand or use the scroll bars in the **Properties** dialog box to see all the fields.

Step 8 In the **Properties** dialog box, modify the values in one or more of the following fields:

Name	Description
User Label field	A user-defined name that can be used for internal tracking or customized identification. Enter up to 32 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Admin Speed field	The data transfer rate for this port. Select the value that matches the destination to which the port is linked. This can be: • **1Gbps** • **10Gbps** **Note** The admin speed can only be changed for certain ports. For more information, see the *Hardware Installation Guide* for your fabric interconnect.
Priority drop-down list	• **best-effort**—This priority is reserved for the Basic Ethernet traffic lane. • **bronze**—Use this priority for vNIC traffic only. • **fc**—Use this priority for vHBA traffic only. • **gold**—Use this priority for vNIC traffic only. • **platinum**—Use this priority for vNIC traffic only. • **silver**—Use this priority for vNIC traffic only.
Pin Group drop-down list	The LAN pin group that you want to use as the appliance pin target to the specified fabric and port, or fabric and port channel
MAC Address field	The MAC address for the endpoint in nn:nn:nn:nn:nn:nn format. If you do not see this field, the port does not have an Ethernet target endpoint set. Click **Add Ethernet Target Endpoint** in the **Actions** area to add an endpoint.
Port Mode field	The port mode used for the appliance port. By default, the mode is set to trunk. This can be: • **trunk**—If you click this radio button, check one or more check boxes in the table to assign VLANs to the appliance port. • **access**—If you click this radio button, choose a VLAN from the **Select VLAN** drop-down list to assign it to the

Name	Description
	appliance port. You can also assign an Ethernet target endpoint to the appliance port if you choose this mode.

Step 9 Click **OK**.

Fibre Channel Storage Ports

Configuring a Fibre Channel Storage Port

This task describes only one method of configuring FC storage ports. You can also configure FC storage ports from the **General** tab for the port.

Before You Begin

The Fibre Channel switching mode must be set to Switching for these ports to be valid. The storage ports cannot function in end-host mode.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Fabric Interconnects ➤** ***Fabric_Interconnect_Name***.

Step 3 Expand the **Expansion Module** node.

Step 4 Click one or more of the ports under the **Uplink FC Ports** node.

Step 5 Right-click the selected port or ports and choose **Configure as FC Storage Port**.

Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 7 Click **OK**.
The port or ports are configured as FC storage ports, removed from the list of uplink FC ports, and added to the **Storage FC Ports** node.

Restoring an Uplink Fibre Channel Port

This task describes only one method of restoring an FC storage port to function as an uplink FC port. You can also reconfigure FC storage ports from the **General** tab for the port.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Fabric Interconnects ➤** ***Fabric_Interconnect_Name***.

Step 3 Expand the **Expansion Module** node.

Step 4 Click one or more of the ports under the **Storage FC Ports** node.

Step 5 Right-click the selected port or ports and choose **Configure as FC Uplink Port**.

Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 7 Click **OK**.
The port or ports are configured as uplink FC ports, removed from the list of FC storage ports, and added to the **Uplink FC Ports** node.

Default Zoning

Zoning allows you to set up access control between hosts and storage devices. When a zone is configured or the configuration is updated, this information is propagated to all the other switches in the fabric.

In Cisco UCS, the zoning configuration is inherited from an upstream switch. You cannot configure zoning or view information about your zoning configuration through Cisco UCS Manager. The only configurable zoning option in Cisco UCS Manager is whether default zoning is enabled or disabled for a specific VSAN.

Note Default zoning is applied on a per-VSAN basis. You cannot enable default zoning at the fabric level.

Enabling Default Zoning

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 In the **SAN** tab, click the **SAN** node.

Step 3 In the **Work** pane, click the **VSANs** tab.

Step 4 Click one of the following subtabs, depending upon the type of VSAN for which you want to enable default zoning:

Subtab	Description
All	Displays all VSANs in the Cisco UCS instance.
Dual Mode	Displays the VSANs that are accessible to both fabric interconnects.
Switch A	Displays the VSANs that are accessible to only fabric interconnect A.

Subtab	Description
Switch B	Displays the VSANs that are accessible to only fabric interconnect B.

Step 5 In the table, double-click the VSAN.
Cisco UCS Manager GUI displays the **General** tab for the VSAN.

Step 6 In the **Actions** area, click **Enable Default Zoning**.

Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Disabling Default Zoning

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 In the **SAN** tab, click the **SAN** node.

Step 3 In the **Work** pane, click the **VSANs** tab.

Step 4 Click one of the following subtabs, depending upon the type of VSAN for which you want to disable default zoning:

Subtab	Description
All	Displays all VSANs in the Cisco UCS instance.
Dual Mode	Displays the VSANs that are accessible to both fabric interconnects.
Switch A	Displays the VSANs that are accessible to only fabric interconnect A.
Switch B	Displays the VSANs that are accessible to only fabric interconnect B.

Step 5 In the table, double-click the VSAN.
Cisco UCS Manager GUI displays the **General** tab for the VSAN.

Step 6 In the **Actions** area, click **Disable Default Zoning**.

Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Uplink Ethernet Port Channels

An uplink Ethernet port channel allows you to group several physical uplink Ethernet ports (link aggregation) to create one logical Ethernet link to provide fault-tolerance and high-speed connectivity. In Cisco UCS Manager, you create a port channel first and then add uplink Ethernet ports to the port channel. You can add up to eight uplink Ethernet ports to a port channel.

Note Cisco UCS uses Link Aggregation Control Protocol (LACP), not Port Aggregation Protocol (PAgP), to group the uplink Ethernet ports into a port channel.

Creating an Uplink Ethernet Port Channel

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN ➤ LAN Cloud**.

Step 3 Expand the node for the fabric interconnect where you want to add the port channel.

Step 4 Right-click the **Port Channels** node and choose **Create Port Channel**.

Step 5 In the **Set Port Channel Name** page of the **Create Port Channel** wizard, do the following:

a) Complete the following fields:

Name	Description
ID field	The identifier for the port channel. Enter an integer between 1 and 256. This ID cannot be changed after the port channel has been saved.
Name field	A user-defined name for the port channel. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

b) Click **Next**.

Step 6 In the **Add Ports** page of the **Create Port Channel** wizard, do the following:

a) In the **Ports** table, choose one or more ports to include in the port channel.

b) Click the >> button to add the ports to the **Ports in the port channel** table.
You can use the << button to remove ports from the port channel.

Note Cisco UCS Manager warns you if you select a port that has been configured as a server port. You can click **Yes** in the dialog box to reconfigure that port as an uplink Ethernet port and include it in the port channel.

Step 7 Click **Finish**.

Enabling an Uplink Ethernet Port Channel

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.
Step 2 On the **LAN** tab, expand **LAN ➤ LAN Cloud**.
Step 3 Expand the node for the fabric interconnect that includes the port channel you want to enable.
Step 4 Expand the **Port Channels** node.
Step 5 Right-click the port channel you want to enable and choose **Enable Port Channel**.
Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Disabling an Uplink Ethernet Port Channel

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.
Step 2 On the **LAN** tab, expand **LAN ➤ LAN Cloud**.
Step 3 Expand the node for the fabric interconnect that includes the port channel you want to disable.
Step 4 Expand the **Port Channels** node.
Step 5 Right-click the port channel you want to disable and choose **Enable Port Channel**.

Adding Ports to and Removing Ports from an Uplink Ethernet Port Channel

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.
Step 2 On the **LAN** tab, expand **LAN ➤ LAN Cloud ➤** ***Fabric*** **➤ Port Channels**.
Step 3 Click the port channel to which you want to add or remove ports.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Actions** area, click **Add Ports**.
Step 6 In the **Add Ports** dialog box, do one of the following:

- To add ports, choose one or more ports in the **Ports** table, and then click the >> button to add the ports to the **Ports in the port channel** table.

- To remove ports, choose one or more ports in the **Ports in the port channel** table, and then click the << button to remove the ports from the port channel and add them to the **Ports** table.

Step 7 Click **OK**.

Deleting an Uplink Ethernet Port Channel

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.
Step 2 On the **LAN** tab, expand **LAN ➤ LAN Cloud**.
Step 3 Expand the node for the fabric interconnect where you want to delete the port channel.
Step 4 Click the **Port Channels** node.
Step 5 In the **General** tab for the **Port Channels** node, choose the port channel you want to delete.
Step 6 Right-click the port channel and choose **Delete**.

Appliance Port Channels

An appliance port channel allows you to group several physical appliance ports (link aggregation) to create one logical Ethernet storage link for the purpose of providing fault-tolerance and high-speed connectivity. In Cisco UCS Manager, you create a port channel first and then add appliance ports to the port channel. You can add up to eight appliance ports to a port channel.

Note Cisco UCS uses Link Aggregation Control Protocol (LACP), not Port Aggregation Protocol (PAgP), to group the appliance ports into a port channel.

Creating an Appliance Port Channel

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.
Step 2 On the **LAN** tab, expand **LAN ➤ Appliances**.
Step 3 Expand the node for the fabric interconnect where you want to add the port channel.
Step 4 Right-click the **Port Channels** node and choose **Create Port Channel**.
Step 5 In the **Set Port Channel Name** page of the **Create Port Channel** wizard, complete the following fields to specify the identity and other properties of the port channel:

Name	Description
ID field	The unique identifier of the port channel. Enter an integer between 1 and 256. This ID cannot be changed after the port channel has been saved.
Name field	A user-defined name for the port channel. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters.
Priority drop-down list	The quality of service setting associated with this port channel. This can be: • **fc**—Use this priority for QoS policies that control vHBA traffic only. • **platinum**—Use this priority for QoS policies that control vNIC traffic only. • **gold**—Use this priority for QoS policies that control vNIC traffic only. • **silver**—Use this priority for QoS policies that control vNIC traffic only. • **bronze**—Use this priority for QoS policies that control vNIC traffic only. • **best-effort**—Do not use this priority. It is reserved for the Basic Ethernet traffic lane. If you assign this priority to a QoS policy and configure another system class as CoS 0, Cisco UCS Manager does not default to this system class. It defaults to the priority with CoS 0 for that traffic.
Pin Group drop-down list	The pin group associated with this port channel.

Step 6 In the **VLANs** area, do the following:

a) In the **Port Mode** field, click one of the following radio buttons to select the mode you want to use for the port channel:

- **trunk**
- **access**

With either mode selected, you can click the **Create VLAN** link to create a new VLAN.

b) If you clicked the **trunk** radio button, complete the following fields:

Name	Description
Select column	Check the check box in this column for each VLAN you want to use.

Name	Description
Native VLAN column	To designate one of the VLANs as the native VLAN, click the radio button in this column.

c) If you clicked the **access** radio button, choose a VLAN from the **Select VLAN** drop-down list.

Step 7 (Optional) If you want to add an endpoint, check the **Ethernet Target Endpoint** check box and complete the following fields:

Name	Description
Name field	The name of the endpoint. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
MAC Address field	The MAC address for the endpoint.

Step 8 Click **Next**.

Step 9 In the **Add Ports** page of the **Create Port Channel** wizard, do the following:

a) In the **Ports** table, choose one or more ports to include in the port channel.

b) Click the >> button to add the ports to the **Ports in the port channel** table.
You can use the << button to remove ports from the port channel.

Note Cisco UCS Manager warns you if your configuration could cause issues with service profiles or port configurations. You can click **Yes** in the dialog box if you want to create the port channel despite those potential issues.

Step 10 Click **Finish**.

Enabling an Appliance Port Channel

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN ➤ Appliances**.

Step 3 Expand the node for the fabric interconnect that includes the port channel you want to enable.

Step 4 Expand the **Port Channels** node.

Step 5 Right-click the port channel you want to enable and choose **Enable Port Channel**.

Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Disabling an Appliance Port Channel

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN ➤ Appliances**.

Step 3 Expand the node for the fabric interconnect that includes the port channel you want to disable.

Step 4 Expand the **Port Channels** node.

Step 5 Right-click the port channel you want to disable and choose **Disable Port Channel**.

Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Adding Ports to and Removing Ports from an Appliance Port Channel

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN ➤ Appliances ➤** ***Fabric*** **➤ Port Channels**.

Step 3 Click the port channel to which you want to add or remove ports.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Add Ports**.

Step 6 In the **Add Ports** dialog box, do one of the following:

- To add ports, choose one or more ports in the **Ports** table, and then click the >> button to add the ports to the **Ports in the port channel** table.
- To remove ports, choose one or more ports in the **Ports in the port channel** table, and then click the << button to remove the ports from the port channel and add them to the **Ports** table.

Step 7 Click **OK**.

Deleting an Appliance Port Channel

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN ➤ Appliances**.

Step 3 Expand the node for the fabric interconnect that includes the port channel you want to enable.

Step 4 Expand the **Port Channels** node.

Step 5 Right-click the port channel you want to enable and choose **Disable Port Channel**.

Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Fibre Channel Port Channels

A Fibre Channel port channel allows you to group several physical Fibre Channel ports (link aggregation) to create one logical Fibre Channel link to provide fault-tolerance and high-speed connectivity. In Cisco UCS Manager, you create a port channel first and then add Fibre Channel ports to the port channel.

You can create up to four Fibre Channel port channels in each Cisco UCS instance. Each Fibre Channel port channel can include a maximum of 16 uplink Fibre Channel ports.

Creating a Fibre Channel Port Channel

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 On the **SAN** tab, expand **SAN ➤ SAN Cloud**.

Step 3 Expand the node for the fabric where you want to create the port channel.

Step 4 Right-click the **FC Port Channels** node and choose **Create Port Channel**.

Step 5 In the **Set Port Channel Name** page of the **Create Port Channel** wizard, do the following:

a) Complete the following fields:

Name	Description
ID field	The identifier for the port channel. Enter an integer between 1 and 256. This ID cannot be changed after the port channel has been saved.
Name field	A user-defined name for the port channel. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

b) Click **Next**.

Step 6 In the **Add Ports** page of the **Create Port Channel** wizard, do the following:

a) From the **Port Channel Admin Speed** drop-down list, select the admin speed for traffic on the port channel.

b) In the **Ports** table, choose one or more ports to include in the port channel.

c) Click the >> button to add the ports to the **Ports in the port channel** table.
You can use the << button to remove ports from the port channel.

Step 7 Click **Finish**.

Enabling a Fibre Channel Port Channel

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 On the **SAN** tab, expand **SAN ➤ SAN Cloud ➤** ***Fabric*** **➤ FC Port Channels**.

Step 3 Click the port channel you want to enable.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Enable Port Channel**.

Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Disabling a Fibre Channel Port Channel

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 On the **SAN** tab, expand **SAN ➤ SAN Cloud ➤** ***Fabric*** **➤ FC Port Channels**.

Step 3 Click the port channel you want to disable.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Disable Port Channel**.

Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Adding Ports to and Removing Ports from a Fibre Channel Port Channel

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 On the **SAN** tab, expand **SAN ➤ SAN Cloud ➤** ***Fabric*** **➤ FC Port Channels**.

Step 3 Click the port channel to which you want to add or remove ports.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Add Ports**.

Step 6 In the **Add Ports** dialog box, do one of the following:

- To add ports, choose one or more ports in the **Ports** table, and then click the >> button to add the ports to the **Ports in the port channel** table.
- To remove ports, choose one or more ports in the **Ports in the port channel** table, and then click the << button to remove the ports from the port channel and add them to the **Ports** table.

Step 7 Click **OK**.

Modifying the Properties of a Fibre Channel Port Channel

Note If you are connecting two Fibre Channel port channels, the admin speed for both port channels must match for the link to operate. If the admin speed for one or both of the Fibre Channel port channels is set to auto, Cisco UCS adjusts the admin speed automatically.

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 On the **SAN** tab, expand **SAN ➤ SAN Cloud ➤** ***Fabric*** **➤ FC Port Channels**.

Step 3 Click the port channel that you want to modify.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, change the values in one or more of the following fields:

Name	Description
Name field	The user-defined name given to the port channel. This name can be between 1 and 16 alphanumeric characters.
VSAN drop-down list	The VSAN associated with the port channel.
Port Channel Admin Speed drop-down list	The admin speed of the port channel. This can be:

Name	Description
	• 1 Gbps • 2 Gbps • 4 Gbps • 8 Gbps • auto

Step 6 Click **Save Changes**.

Deleting a Fibre Channel Port Channel

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **SAN** tab, expand **SAN ➤ SAN Cloud ➤** ***Fabric*** **➤ FC Port Channels**.

Step 3 Right-click the port channel you want to delete and choose **Delete**.

Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring Server Ports with the Internal Fabric Manager

Internal Fabric Manager

The Internal Fabric Manager provides a single interface where you can configure server ports for a fabric interconnect in a Cisco UCS instance. The Internal Fabric Manager is accessible from the **General** tab for that fabric interconnect.

Some of the configuration that you can do in the Internal Fabric Manager can also be done in nodes on the **Equipment** tab, on the **LAN** tab, or in the LAN Uplinks Manager.

Launching the Internal Fabric Manager

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Fabric Interconnects ➤** ***Fabric_Interconnect_Name***.

Step 3 Click **Fixed Module**.

Step 4 In the **Work** pane, click **Internal Fabric Manager** in the **Actions** area.
The Internal Fabric Manager opens in a separate window.

Configuring a Server Port with the Internal Fabric Manager

Procedure

Step 1 In the Internal Fabric Manager, click the down arrows to expand the **Unconfigured Ports** area.

Step 2 Right-click the port that you want to configure and choose **Configure as Server Port**.

Step 3 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 4 If you have completed all tasks in the Internal Fabric Manager, click **OK**.

Unconfiguring a Server Port with the Internal Fabric Manager

Procedure

Step 1 In the Internal Fabric Manager, click the server port in the **Server Ports** table.

Step 2 Click **Unconfigure Port**.

Step 3 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 4 If you have completed all tasks in the Internal Fabric Manager, click **OK**.

Enabling a Server Port with the Internal Fabric Manager

Procedure

Step 1 In the Internal Fabric Manager, click the server port in the **Server Ports** table.
Step 2 Click **Enable Port**.
Step 3 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
Step 4 If you have completed all tasks in the Internal Fabric Manager, click **OK**.

Disabling a Server Port with the Internal Fabric Manager

Procedure

Step 1 In the Internal Fabric Manager, click the server port in the **Server Ports** table.
Step 2 Click **Disable Port**.
Step 3 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
Step 4 If you have completed all tasks in the Internal Fabric Manager, click **OK**.

CHAPTER 6

Configuring Communication Services

This chapter includes the following sections:

Communication Services

You can use the following communication services to interface third-party applications with Cisco UCS:

Communication Service	Description
CIM XML	This service is disabled by default and is only available in read-only mode. The default port is 5988. This common information model is one of the standards defined by the Distributed Management Task Force.
HTTP	This service is enabled on port 80 by default. You must enable either HTTP or HTTPS to run Cisco UCS Manager GUI. If you select HTTP, all data is exchanged in clear text mode. For security purposes, we recommend that you enable HTTPS and disable HTTP. By default, Cisco UCS redirects any attempt to communicate via HTTP to the HTTPS equivalent. We recommend that you do not change this behavior.

Communication Service	Description
	Note If you are upgrading to Cisco UCS, version 1.4(1), this does not happen by default. If you want to redirect any attempt to communicate via HTTP to an HTTPS equivalent, you should enable **Redirect HTTP to HTTPS** in Cisco UCS Manager.
HTTPS	This service is enabled on port 443 by default. With HTTPS, all data is exchanged in encrypted mode through a secure server. For security purposes, we recommend that you only use HTTPS and either disable or redirect HTTP communications.
SMASH CLP	This service is enabled for read-only access and supports a limited subset of the protocols, such as the **show** command. You cannot disable it. This shell service is one of the standards defined by the Distributed Management Task Force.
SNMP	This service is disabled by default. If enabled, the default port is 161. You must configure the community and at least one SNMP trap. Enable this service only if your system includes integration with an SNMP server.
SSH	This service is enabled on port 22. You cannot disable it, nor can you change the default port. This service provides access to the Cisco UCS Manager CLI.
Telnet	This service is disabled by default. This service provides access to the Cisco UCS Manager CLI.

Configuring CIM-XML

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.

Step 3 Select the **Communication Services** tab.

Step 4 In the **CIM-XML** area, click the **enabled** radio button.
The **CIM-XML** area expands to display the available configuration options.

Step 5 (Optional) In the **Port** field, change the default port that Cisco UCS Manager GUI will use for CIM-XML. The default port is 5988.

Step 6 Click **Save Changes**.

Configuring HTTP

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.

Step 3 Click the **Communication Services** tab.

Step 4 In the **HTTP** area, click the **enabled** radio button.
The **HTTP** area expands to display the available configuration options.

Step 5 (Optional) In the **Port** field, change the default port that Cisco UCS Manager GUI uses for HTTP.
The default port is 80.

Step 6 (Optional) In the **Redirect HTTP to HTTPS** field, click the **enabled** radio button.
You must also configure and enable HTTPS to enable redirection of HTTP logins to the HTTPS login. Once enabled, you cannot disable the redirection until you have disabled HTTPS.

Step 7 Click **Save Changes**.

Configuring HTTPS

Certificates, Key Rings, and Trusted Points

HTTPS uses components of the Public Key Infrastructure (PKI) to establish secure communications between two devices, such as a client's browser and Cisco UCS Manager.

Encryption Keys and Key Rings

Each PKI device holds a pair of asymmetric Rivest-Shamir-Adleman (RSA) encryption keys, one kept private and one made public, stored in an internal key ring. A message encrypted with either key can be decrypted with the other key. To send an encrypted message, the sender encrypts the message with the receiver's public key, and the receiver decrypts the message using its own private key. A sender can also prove its ownership of a public key by encrypting (also called 'signing') a known message with its own private key. If a receiver can successfully decrypt the message using the public key in question, the sender's possession of the corresponding private key is proven. Encryption keys can vary in length, with typical lengths from 512 bits to 2048 bits. In general, a longer key is more secure than a shorter key. Cisco UCS Manager provides a default key ring with an initial 1024-bit key pair, and allows you to create additional key rings.

Certificates

To prepare for secure communications, two devices first exchange their digital certificates. A certificate is a file containing a device's public key along with signed information about the device's identity. To merely support encrypted communications, a device can generate its own key pair and its own self-signed certificate. When a remote user connects to a device that presents a self-signed certificate, the user has no easy method to verify the identity of the device, and the user's browser will initially display an authentication warning. By

default, Cisco UCS Manager contains a built-in self-signed certificate containing the public key from the default key ring.

Trusted Points

To provide stronger authentication for Cisco UCS Manager, you can obtain and install a third-party certificate from a trusted source, or trusted point, that affirms the identity of your device. The third-party certificate is signed by the issuing trusted point, which can be a root certificate authority (CA) or an intermediate CA or trust anchor that is part of a trust chain that leads to a root CA. To obtain a new certificate, you must generate a certificate request through Cisco UCS Manager and submit the request to a trusted point.

Creating a Key Ring

Cisco UCS Manager supports a maximum of 8 key rings, including the default key ring.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All ➤ Key Management**.

Step 3 Right-click **Key Management** and choose **Create Key Ring**.

Step 4 In the **Create Key Ring** dialog box, do the following:

a) In the **Name** field, enter a unique name for the key ring.

b) In the **Modulus** field, select one of the following radio buttons to specify the SSL key length in bits:

- **mod512**
- **mod1024**
- **mod1536**
- **mod2048**

c) Click **OK**.

What to Do Next

Create a certificate request for this key ring.

Creating a Certificate Request for a Key Ring

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All ➤ Key Management**.

Step 3 Click the key ring for which you want to create a certificate request.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **General** tab, click **Create Certificate Request**.

Step 6 In the **Create Certificate Request** dialog box, complete the following fields:

Name	Description
Password field	An optional password for this request.
Confirm Password field	If you specified a password, enter it again for confirmation.
Subject field	The fully qualified domain name of the fabric interconnect.
IP Address field	The IP address of the fabric interconnect.

Step 7 Click **OK**.

Step 8 Copy the text of the certificate request out of the **Request** field and save in a file.

Step 9 Send the file with the certificate request to the trust anchor or certificate authority.

What to Do Next

Create a trusted point and set the certificate chain for the certificate of trust received from the trust anchor.

Creating a Trusted Point

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All ➤ Key Management**.

Step 3 Right-click **Key Management** and choose **Create Trusted Point**.

Step 4 In the **Create Trusted Point** dialog box, complete the following fields:

Name	Description
Name field	The name of the trusted point. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

Name	Description
Certificate Chain field	The certificate information for this trusted point.

Step 5 Click **OK**.

What to Do Next

When you receive the certificate from the trust anchor or certificate authority, import it into the key ring.

Importing a Certificate into a Key Ring

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All ➤ Key Management**.

Step 3 Click the key ring into which you want to import the certificate.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Certificate** area, complete the following fields:

a) From the **Trusted Point** drop-down list, select the trusted point for the trust anchor that granted this certificate.

b) In the **Certificate** field, paste the text from the certificate you received from the trust anchor or certificate authority.

Tip If the fields in an area are not displayed, click the **Expand** icon to the right of the heading.

Step 6 Click **Save Changes**.

What to Do Next

Configure your HTTPS service with the key ring.

Configuring HTTPS

Caution After you complete the HTTPS configuration, including changing the port and key ring to be used by HTTPS, all current HTTP and HTTPS sessions are closed without warning as soon as you save or commit the transaction.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.

Step 3 Select the **Communication Services** tab.

Step 4 In the **HTTPS** area, click the **enabled** radio button.
The **HTTPS** area expands to display the available configuration options.

Step 5 (Optional) In the **Port** field, change the default port that Cisco UCS Manager GUI uses for HTTPS.
The default port is 443.

Step 6 (Optional) From the **Key Ring** drop-down list, choose the key ring you created for HTTPS.

Step 7 Click **Save Changes**.

Deleting a Key Ring

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All ➤ Key Management**.

Step 3 Right-click the key ring you want to delete and choose **Delete**.

Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Deleting a Trusted Point

Before You Begin

Ensure that the trusted point is not used by a key ring.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All ➤ Key Management**.

Step 3 Right-click the trusted point you want to delete and choose **Delete**.

Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 5 Click **OK**.

Configuring SNMP

Information about SNMP

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.

SNMP Functional Overview

The SNMP framework consists of three parts:

- An SNMP manager—The system used to control and monitor the activities of network devices using SNMP.
- An SNMP agent—The software component within Cisco UCS, the managed device, that maintains the data for Cisco UCS and reports the data, as needed, to the SNMP manager. Cisco UCS includes the agent and a collection of MIBs. To enable the SNMP agent and create the relationship between the manager and agent, enable and configure SNMP in Cisco UCS Manager.
- A managed information base (MIB)—The collection of managed objects on the SNMP agent. Cisco UCS release 1.4(1) and higher support a larger number of MIBs than earlier releases.

Cisco UCS supports SNMPv1, SNMPv2c and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security. SNMP is defined in the following:

- RFC 3410 (http://tools.ietf.org/html/rfc3410)
- RFC 3411 (http://tools.ietf.org/html/rfc3411)
- RFC 3412 (http://tools.ietf.org/html/rfc3412)
- RFC 3413 (http://tools.ietf.org/html/rfc3413)
- RFC 3414 (http://tools.ietf.org/html/rfc3414)
- RFC 3415 (http://tools.ietf.org/html/rfc3415)
- RFC 3416 (http://tools.ietf.org/html/rfc3416)
- RFC 3417 (http://tools.ietf.org/html/rfc3417)
- RFC 3418 (http://tools.ietf.org/html/rfc3418)
- RFC 3584 (http://tools.ietf.org/html/rfc3584)

SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. These notifications do not require that requests be sent from the SNMP manager. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to a neighbor router, or other significant events.

Cisco UCS Manager generates SNMP notifications as either traps or informs. Traps are less reliable than informs because the SNMP manager does not send any acknowledgment when it receives a trap, and Cisco

UCS Manager cannot determine if the trap was received. An SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the Cisco UCS Manager does not receive the PDU, it can send the inform request again.

SNMP Security Levels and Privileges

SNMPv1, SNMPv2c, and SNMPv3 each represent a different security model. The security model combines with the selected security level to determine the security mechanism applied when the SNMP message is processed.

The security level determines the privileges required to view the message associated with an SNMP trap. The privilege level determines whether the message needs to be protected from disclosure or authenticated. The supported security level depends upon which security model is implemented. SNMP security levels support one or more of the following privileges:

- noAuthNoPriv—No authentication or encryption
- authNoPriv—Authentication but no encryption
- authPriv—Authentication and encryption

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

Supported Combinations of SNMP Security Models and Levels

The following table identifies what the combinations of security models and levels mean.

Table 4: SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	HMAC-MD5 or HMAC-SHA	No	Provides authentication based on the Hash-Based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm or the

Model	Level	Authentication	Encryption	What Happens
				HMAC Secure Hash Algorithm (SHA).
v3	authPriv	HMAC-MD5 or HMAC-SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.

SNMPv3 Security Features

SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. SNMPv3 authorizes management operations only by configured users and encrypts SNMP messages. The SNMPv3 User-Based Security Model (USM) refers to SNMP message-level security and offers the following services:

- Message integrity—Ensures that messages have not been altered or destroyed in an unauthorized manner and that data sequences have not been altered to an extent greater than can occur non-maliciously.
- Message origin authentication—Ensures that the claimed identity of the user on whose behalf received data was originated is confirmed.
- Message confidentiality and encryption—Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

SNMP Support in Cisco UCS

Cisco UCS provides the following support for SNMP:

Support for MIBs

Cisco UCS supports read-only access to MIBs.

For information about the specific MIBs available for Cisco UCS and where you can obtain them, see the MIB Quick Reference for Cisco UCS.

Authentication Protocols for SNMPv3 Users

Cisco UCS supports the following authentication protocols for SNMPv3 users:

- HMAC-MD5-96 (MD5)

- HMAC-SHA-96 (SHA)

AES Privacy Protocol for SNMPv3 Users

Cisco UCS uses Advanced Encryption Standard (AES) as one of the privacy protocols for SNMPv3 message encryption and conforms with RFC 3826.

The privacy password, or priv option, offers a choice of DES or 128-bit AES encryption for SNMP security encryption. If you enable AES-128 configuration and include a privacy password for an SNMPv3 user, Cisco UCS Manager uses the privacy password to generate a 128-bit AES key. The AES privacy password can have a minimum of eight characters. If the passphrases are specified in clear text, you can specify a maximum of 64 characters.

Enabling SNMP and Configuring SNMP Properties

SNMP messages from a Cisco UCS instance display the fabric interconnect name rather than the system name.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.

Step 3 Select the **Communication Services** tab.

Step 4 In the **SNMP** area, click the **enabled** radio button.
The **SNMP** area expands to display the available configuration options. You cannot change the port on which Cisco UCS Manager communicates with the SNMP host.

Step 5 Complete the following fields:

Name	Description
Community/Username field	The default SNMP v1 or v2c community name or SNMP v3 username Cisco UCS Manager includes on any trap messages it sends to the SNMP host. Enter an alphanumeric string between 1 and 32 characters. Do not use @ (at sign), \ (backslash), " (double quote), ? (question mark) or an empty space. The default is public.
System Contact field	The system contact person responsible for the SNMP implementation. Enter a string of up to 255 characters, such as an email address or a name and telephone number.
System Location field	The location of the host on which the SNMP agent (server) runs. Enter an alphanumeric string up to 512 characters.

Step 6 Click **Save Changes**.

What to Do Next

Create SNMP traps and users.

Creating an SNMP Trap

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.

Step 3 Select the **Communication Services** tab.

Step 4 In the **SNMP Traps** area, click +.

Step 5 In the **Create SNMP Trap** dialog box, complete the following fields:

Name	Description
IP Address field	The IP address of the SNMP host to which Cisco UCS Manager should send the trap.
Community/Username field	The SNMP v1 or v2c community name or the SNMP v3 username Cisco UCS Manager includes when it sends the trap to the SNMP host. This must be the same as the community or username that is configured for the SNMP service. Enter an alphanumeric string between 1 and 32 characters. Do not use @ (at sign), \ (backslash), " (double quote), ? (question mark) or an empty space.
Port field	The port on which Cisco UCS Manager communicates with the SNMP host for the trap. The default port is 162.
Version field	The SNMP version and model used for the trap. This can be: • **v1** • **v2c** • **v3**
Type field	If you select v2c or v3 for the version, the type of trap to send. This can be: • **traps** • **informs**
v3 Privilege field	If you select v3 for the version, the privilege associated with the trap. This can be:

Name	Description
	• **auth**—Authentication but no encryption • **noauth**—No authentication or encryption • **priv**—Authentication and encryption

Step 6 Click **OK**.

Step 7 Click **Save Changes**.

Deleting an SNMP Trap

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.

Step 3 Select the **Communication Services** tab.

Step 4 In the **SNMP Traps** area, click the row in the table that corresponds to the user you want to delete.

Step 5 Click the **Delete** icon to the right of the table.

Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 7 Click **Save Changes**.

Creating an SNMPv3 user

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.

Step 3 Select the **Communication Services** tab.

Step 4 In the **SNMP Users** area, click +.

Step 5 In the **Create SNMP User** dialog box, complete the following fields:

Name	Description
Name field	The username assigned to the SNMP user. An SNMP username cannot be the same as a local username. Choose an SNMP username that does not match a local username.
Auth Type field	The authorization type. This can be:

Name	Description
	• **MD5** • **SHA**
Use AES-128 check box	If checked, this user uses AES-128 encryption.
Password field	The password for this user.
Confirm Password field	The password again for confirmation purposes.
Privacy Password field	The privacy password for this user.
Confirm Privacy Password field	The privacy password again for confirmation purposes.

Step 6 Click **OK**.

Step 7 Click **Save Changes**.

Deleting an SNMPv3 User

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.

Step 3 Select the **Communication Services** tab.

Step 4 In the **SNMP Users** area, click the row in the table that corresponds to the user you want to delete.

Step 5 Click the **Delete** icon to the right of the table.

Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 7 Click **Save Changes**.

Enabling Telnet

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.
Step 3 Click the **Communication Services** tab.
Step 4 In the **Telnet** area, click the **enabled** radio button.
Step 5 Click **Save Changes**.

Disabling Communication Services

Note We recommend that you disable all communication services that are not required to interface with other network applications.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.
Step 3 On the **Communication Services** tab, click the **disable** radio button for each service that you want to disable.
Step 4 Click **Save Changes**.

CHAPTER 7

Configuring Authentication

This chapter includes the following sections:

Authentication Services

Cisco UCS supports two methods to authenticate user logins:

- Through user accounts local to Cisco UCS Manager
- Remotely through one of the following protocols:
  - LDAP
  - RADIUS
  - TACACS+

Guidelines and Recommendations for Remote Authentication Providers

If a system is configured for one of the supported remote authentication services, you must create a provider for that service to ensure that Cisco UCS Manager can communicate with it. In addition, you need to be aware of the following guidelines that impact user authorization:

User Accounts in Remote Authentication Services

User accounts can exist locally in Cisco UCS Manager or in the remote authentication server.

The temporary sessions for users who log in through remote authentication services can be viewed through Cisco UCS Manager GUI or Cisco UCS Manager CLI.

User Roles in Remote Authentication Services

If you create user accounts in the remote authentication server, you must ensure that the accounts include the roles those users require for working in Cisco UCS Manager and that the names of those roles match the names used in Cisco UCS Manager. Depending on the role policy, a user may not be allowed to log in or will be granted only read-only privileges.

User Attributes in Remote Authentication Providers

You must configure a user attribute for Cisco UCS in each remote authentication provider through which users log in to Cisco UCS Manager. This user attribute holds the roles and locales assigned to each user.

When a user logs in, Cisco UCS Manager does the following:

1. Queries the remote authentication service.
2. Validates the user.
3. If the user is validated, checks for the roles and locales assigned to that user.

The following table contains a comparison of the user attribute requirements for the remote authentication providers supported by Cisco UCS.

Table 5: Comparison of User Attributes by Remote Authentication Provider

Authentication Provider	Custom Attribute	Schema Extension	Attribute ID Requirements
LDAP	Optional	Optional. You can choose to do either of the following: • Do not extend the LDAP schema and configure an existing, unused attribute that meets the requirements. • Extend the LDAP schema and create a custom attribute with a unique name, such as CiscoAVPair.	The Cisco LDAP implementation requires a unicode type attribute. If you choose to create the CiscoAVPair custom attribute, use the following attribute ID: 1.3.6.1.4.1.9.287247.1 A sample OID is provided in the following section.
RADIUS	Optional	Optional. You can choose to do either of the following: • Do not extend the RADIUS schema and use an existing, unused attribute that meets the requirements.	The vendor ID for the Cisco RADIUS implementation is 009 and the vendor ID for the attribute is 001. The following syntax example shows how to specify multiples user

Authentication Provider	Custom Attribute	Schema Extension	Attribute ID Requirements
		• Extend the RADIUS schema and create a custom attribute with a unique name, such as cisco-avpair.	roles and locales if you choose to create the cisco-avpair attribute: `shell:roles="admin,aaa" shell:locales="L1,abc"`. Use a comma "," as the delimiter to separate multiple values.
TACACS+	Required	Required. You must extend the schema and create a custom attribute with the name cisco-av-pair.	The cisco-av-pair name is the string that provides the attribute ID for the TACACS+ provider. The following syntax example shows how to specify multiples user roles and locales when you create the cisco-av-pair attribute: `cisco-av-pair=shell:roles="admin aaa" shell:locales="L1 abc"`. Use a space as the delimiter to separate multiple values.

Sample OID for LDAP User Attribute

The following is a sample OID for a custom CiscoAVPair attribute:

```
CN=CiscoAVPair,CN=Schema,
CN=Configuration,CN=X
objectClass: top
objectClass: attributeSchema
cn: CiscoAVPair
distinguishedName: CN=CiscoAVPair,CN=Schema,CN=Configuration,CN=X
instanceType: 0x4
uSNCreated: 26318654
attributeID: 1.3.6.1.4.1.9.287247.1
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: TRUE
adminDisplayName: CiscoAVPair
adminDescription: UCS User Authorization Field
oMSyntax: 64
lDAPDisplayName: CiscoAVPair
name: CiscoAVPair
objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,CN=X
```

LDAP Group Rule

The LDAP group rule is used to determine whether Cisco UCS should use LDAP groups when assigning user roles and locales to a remote user.

Configuring LDAP Providers

Configuring Default Properties for LDAP Providers

The properties that you configure in this task are the default settings for all LDAP provider connections defined in Cisco UCS Manager. If an individual provider includes a setting for any of these properties, Cisco UCS uses that setting and ignores the default setting.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ User Management ➤ LDAP**.

Step 3 Complete the following fields in the **Properties** area:

Name	Description
Timeout field	The length of time in seconds the system should spend trying to contact the LDAP database before it times out. Enter an integer from 1 to 60 seconds. The default value is 30 seconds. This property is required.
Attribute field	An LDAP attribute that stores the values for the user roles and locales. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name. If you do not want to extend your LDAP schema, you can configure an existing, unused LDAP attribute with the Cisco UCS roles and locales. Alternatively, you can create an attribute named CiscoAVPair in the remote authentication service with the following attribute ID: 1.3.6.1.4.1.9.287247.1
Base DN field	The specific distinguished name in the LDAP hierarchy where the server should begin a search when a remote user logs in and the system attempts to get the user's DN based on their username. The maximum supported string length is 127 characters. This property is required. If you do not specify a base DN on this tab then you must specify one on the **General** tab for every LDAP provider defined in this Cisco UCS instance.
Filter field	The LDAP search is restricted to those usernames that match the defined filter. This property is required. If you do not specify a filter on this tab then you must specify one on the **General** tab for every LDAP provider defined in this Cisco UCS instance.

Step 4 Click **Save Changes**.

What to Do Next

Create an LDAP provider.

Creating an LDAP Provider

Cisco UCS Manager supports a maximum of 16 LDAP providers.

Before You Begin

- In the LDAP server, perform one of the following configurations:
  - Configure LDAP groups. LDAP groups contain user role and locale information.
  - Configure users with the attribute that holds the user role and locale information for Cisco UCS Manager. You can choose whether to extend the LDAP schema for this attribute. If you do not want to extend the schema, use an existing LDAP attribute to hold the Cisco UCS user roles and locales. If you prefer to extend the schema, create a custom attribute, such as the CiscoAVPair attribute.

    The Cisco LDAP implementation requires a unicode type attribute.

    If you choose to create the CiscoAVPair custom attribute, use the following attribute ID: 1.3.6.1.4.1.9.287247.1
  - For a cluster configuration, add the management port IP addresses for both fabric interconnects. This configuration ensures that remote users can continue to log in if the first fabric interconnect fails and the system fails over to the second fabric interconnect. All login requests are sourced from these IP addresses, not the virtual IP address used by Cisco UCS Manager.
- If you want to use secure communications, create a trusted point containing the certificate of the root certificate authority (CA) of the LDAP server in Cisco UCS Manager.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ User Management ➤ LDAP**.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area, click **Create LDAP Provider**.

Step 5 On the **Create LDAP Provider** page of the wizard, do the following:

a) Complete the following fields with information about the LDAP service you want to use:

Name	Description
Hostname field	The hostname or IP address on which the LDAP provider resides. If SSL is enabled, this field must exactly match a Common Name (CN) in the security certificate of the LDAP database. **Note** If you use a hostname rather than an IP address, you must configure a DNS server in Cisco UCS Manager.

Name	Description
Order field	The order in which Cisco UCS uses this provider to authenticate users. Enter an integer between 1 and 16, or enter lowest-available or 0 (zero) if you want Cisco UCS to assign the next available order based on the other providers defined in this Cisco UCS instance.
Bind DN field	The distinguished name (DN) for an LDAP database account that has read and search permissions for all objects under the base DN. The maximum supported string length is 127 characters.
Base DN field	The specific distinguished name in the LDAP hierarchy where the server should begin a search when a remote user logs in and the system attempts to get the user's DN based on their username. The maximum supported string length is 127 characters. This value is required unless a default base DN has been set on the LDAP **General** tab.
Port field	The port through which Cisco UCS communicates with the LDAP database. The standard port number is 389.
Enable SSL check box	If checked, encryption is required for communications with the LDAP database. If unchecked, authentication information will be sent as clear text. LDAP uses STARTTLS. This allows encrypted communication using port 389.
Filter field	The LDAP search is restricted to those usernames that match the defined filter. This value is required unless a default filter has been set on the LDAP **General** tab.
Attribute field	An LDAP attribute that stores the values for the user roles and locales. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name. If you do not want to extend your LDAP schema, you can configure an existing, unused LDAP attribute with the Cisco UCS roles and locales. Alternatively, you can create an attribute named CiscoAVPair in the remote authentication service with the following attribute ID: 1.3.6.1.4.1.9.287247.1 This value is required unless a default attribute has been set on the LDAP **General** tab.
Password field	The password for the LDAP database account specified in the **Bind DN** field.
Confirm Password field	The LDAP database password repeated for confirmation purposes.

Name	Description
Timeout field	The length of time in seconds the system should spend trying to contact the LDAP database before it times out. Enter an integer from 1 to 60 seconds, or enter 0 (zero) to use the global timeout value specified on the LDAP **General** tab. The default is 30 seconds.

b) Click **Next**.

Step 6 On the **LDAP Group Rule** page of the wizard, do the following:

a) Complete the following fields:

Name	Description
Group Authorization field	Whether Cisco UCS also searches LDAP groups when authenticating and assigning user roles and locales to remote users. This can be: • **disable**—Cisco UCS does not access any LDAP groups. • **enable**—Cisco UCS searches all LDAP groups mapped in this Cisco UCS instance. If the remote user is found, Cisco UCS assigns the user roles and locales defined for that LDAP group in the associated LDAP group map. **Note** Role and locale assignment is cumulative. If a user is included in multiple groups, or has a role or locale specified in the LDAP attribute, Cisco UCS assigns that user all the roles and locales mapped to any of those groups or attributes.
Group Recursion field	Whether Cisco UCS searches both the mapped groups and their parent groups. This can be: • **non-recursive**—Cisco UCS searches only the groups mapped in this Cisco UCS instance. If none of the groups containing the user explicitly set the user's authorization properties, Cisco UCS uses the default settings. • **recursive**—Cisco UCS searches each mapped grouped and all its parent groups for the user's authorization properties. These properties are cumulative, so for each group Cisco UCS finds with explicit authorization property settings, it applies those settings to the current user. Otherwise it uses the default settings.
Target Attribute field	The attribute Cisco UCS uses to determine group membership in the LDAP database. The supported string length is 63 characters. The default string is memberOf.

b) Click **Finish**.

What to Do Next

For implementations involving a single LDAP database, select LDAP as the authentication service.

For implementations involving multiple LDAP databases, configure an LDAP provider group.

Changing the LDAP Group Rule for an LDAP Provider

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ User Management ➤ LDAP**.

Step 3 Expand **LDAP Providers** and choose the LDAP provider for which you want to change the group rule.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **LDAP Group Rules** area, complete the following fields:

Name	Description
Group Authorization field	Whether Cisco UCS also searches LDAP groups when authenticating and assigning user roles and locales to remote users. This can be: • **disable**—Cisco UCS does not access any LDAP groups. • **enable**—Cisco UCS searches all LDAP groups mapped in this Cisco UCS instance. If the remote user is found, Cisco UCS assigns the user roles and locales defined for that LDAP group in the associated LDAP group map. **Note** Role and locale assignment is cumulative. If a user is included in multiple groups, or has a role or locale specified in the LDAP attribute, Cisco UCS assigns that user all the roles and locales mapped to any of those groups or attributes.
Group Recursion field	Whether Cisco UCS searches both the mapped groups and their parent groups. This can be: • **non-recursive**—Cisco UCS searches only the groups mapped in this Cisco UCS instance. If none of the groups containing the user explicitly set the user's authorization properties, Cisco UCS uses the default settings. • **recursive**—Cisco UCS searches each mapped grouped and all its parent groups for the user's authorization properties. These properties are cumulative, so for each group Cisco UCS finds with explicit authorization property settings, it applies those settings to the current user. Otherwise it uses the default settings.
Target Attribute field	The attribute Cisco UCS uses to determine group membership in the LDAP database.

Name	Description
	The supported string length is 63 characters. The default string is memberOf.

Step 6 Click **Save Changes**.

Deleting an LDAP Provider

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 In the **Admin** tab, expand **All ➤ User Management ➤ LDAP**.
Step 3 Expand **LDAP Providers**.
Step 4 Right-click the LDAP provider you want to delete and choose **Delete**.
Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

LDAP Group Mapping

For organizations that already use LDAP groups to restrict access to LDAP databases, group membership information can be used by UCSM to assign a role or locale to an LDAP user during login. This eliminates the need to define role or locale information in the LDAP user object when Cisco UCS Manager is deployed.

When a user logs in to Cisco UCS Manager, information about the user's role and locale are pulled from the LDAP group map. If the role and locale criteria match the information in the policy, access is granted.

Role and locale definitions are configured locally in UCSM and do not update automatically based on changes to an LDAP directory. When deleting or renaming LDAP groups in an LDAP directory, it is important that you update your Cisco UCS Manager instance with the change.

An LDAP group map can be configured to include any of the following combinations of roles and locales:

- Roles only
- Locales only
- Both roles and locales

For example, consider an LDAP group representing a group of server administrators at a specific location. The LDAP group map might be configured to include user roles like server-profile and server-equipment. To restrict access to server administrators at a specific location, the locale could be set to a particular site name.

Note Cisco UCS Manager includes many out-of-the-box user roles but does not include any locales. Mapping an LDAP provider group to a locale requires that you create a custom locale.

Creating an LDAP Group Map

Before You Begin

- Create an LDAP group in the LDAP server.
- Configure the distinguished name for the LDAP group in the LDAP server.
- Create locales in Cisco UCS Manager (optional).
- Create custom roles in Cisco UCS Manager (optional).

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ User Management ➤ LDAP**.

Step 3 Right-click **LDAP Group Maps** and choose **Create LDAP Group Map**.

Step 4 In the **Create LDAP Group Map** dialog box, do the following:

a) In the **LDAP Group DN** field, enter the distinguished name of the group in the LDAP database.

Important This name must match the name in the LDAP database exactly.

b) In the **Roles** table, check the check boxes for all roles that you want to assign to users who are included in the group map.

c) In the **Locales** table, check the check boxes for all locales that you want to assign to users who are included in the group map.

d) Click **OK**.

What to Do Next

Set the LDAP group rule.

Deleting an LDAP Group Map

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ User Management ➤ LDAP**.

Step 3 Expand **LDAP Group Maps**.

Step 4 Right-click the LDAP group map you want to delete and choose **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring RADIUS Providers

Configuring Default Properties for RADIUS Providers

The properties that you configure in this task are the default settings for all RADIUS provider connections defined in Cisco UCS Manager. If an individual provider includes a setting for any of these properties, Cisco UCS uses that setting and ignores the default setting.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **User Management ➤ RADIUS** .

Step 3 Complete the following fields in the **Properties** area:

Name	Description
Timeout field	The length of time in seconds the system should spend trying to contact the RADIUS database before it times out. Enter an integer from 1 to 60 seconds, or enter 0 (zero) to use the global timeout value specified on the RADIUS **General** tab. The default is 5 seconds.
Retries field	The number of times to retry the connection before the request is considered to have failed.

Step 4 Click **Save Changes**.

What to Do Next

Create a RADIUS provider.

Creating a RADIUS Provider

Cisco UCS Manager supports a maximum of 16 RADIUS providers.

Before You Begin

Perform the following configuration in the RADIUS server:

- Configure users with the attribute that holds the user role and locale information for Cisco UCS Manager. You can choose whether to extend the RADIUS schema for this attribute. If you do not want to extend the schema, use an existing RADIUS attribute to hold the Cisco UCS user roles and locales. If you prefer to extend the schema, create a custom attribute, such as the cisco-avpair attribute.

  The vendor ID for the Cisco RADIUS implementation is 009 and the vendor ID for the attribute is 001.

  The following syntax example shows how to specify multiples user roles and locales if you choose to create the cisco-avpair attribute: `shell:roles="admin,aaa" shell:locales="L1,abc"`. Use a comma "," as the delimiter to separate multiple values.

- For a cluster configuration, add the management port IP addresses for both fabric interconnects. This configuration ensures that remote users can continue to log in if the first fabric interconnect fails and the system fails over to the second fabric interconnect. All login requests are sourced from these IP addresses, not the virtual IP address used by Cisco UCS Manager.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ User Management ➤ RADIUS**.

Step 3 In the **Create RADIUS Provider** dialog box:

a) Complete the fields with the information about the RADIUS service you want to use.

Name	Description
Hostname field	The hostname or IP address on which the RADIUS provider resides. **Note** If you use a hostname rather than an IP address, you must configure a DNS server in Cisco UCS Manager.
Order field	The order in which Cisco UCS uses this provider to authenticate users. Enter an integer between 1 and 16, or enter lowest-available or 0 (zero) if you want Cisco UCS to assign the next available order based on the other providers defined in this Cisco UCS instance.
Key field	The SSL encryption key for the database.
Confirm Key field	The SSL encryption key repeated for confirmation purposes.
Authorization Port field	The port through which Cisco UCS communicates with the RADIUS database.
Timeout field	The length of time in seconds the system should spend trying to contact the RADIUS database before it times out. Enter an integer from 1 to 60 seconds, or enter 0 (zero) to use the global timeout value specified on the RADIUS **General** tab. The default is 5 seconds.
Retries field	The number of times to retry the connection before the request is considered to have failed. If you do not specify a value, Cisco UCS uses the value specified on the RADIUS **General** tab.

b) Click **OK**.

Step 4 Click **Save Changes**.

What to Do Next

For implementations involving a single RADIUS database, select RADIUS as the primary authentication service.

For implementations involving multiple RADIUS databases, configure a RADIUS provider group.

Deleting a RADIUS Provider

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **User Management ➤ RADIUS** .

Step 3 Right-click the RADIUS provider you want to delete and choose **Delete**.

Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring TACACS+ Providers

Configuring Default Properties for TACACS+ Providers

The properties that you configure in this task are the default settings for all TACACS+ provider connections defined in Cisco UCS Manager. If an individual provider includes a setting for any of these properties, Cisco UCS uses that setting and ignores the default setting.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **User Management ➤ TACACS+** .

Step 3 In the **Properties** area, complete the **Timeout** field:
The length of time in seconds the system should spend trying to contact the TACACS+ database before it times out.

Enter an integer from 1 to 60 seconds, or enter 0 (zero) to use the global timeout value specified on the TACACS+ **General** tab. The default is 5 seconds.

Step 4 Click **Save Changes**.

What to Do Next

Create an TACACS+ provider.

Creating a TACACS+ Provider

Cisco UCS Manager supports a maximum of 16 TACACS+ providers.

Before You Begin

Perform the following configuration in the TACACS+ server:

- Create the cisco-av-pair attribute. You cannot use an existing TACACS+ attribute.

  The cisco-av-pair name is the string that provides the attribute ID for the TACACS+ provider.

  The following syntax example shows how to specify multiples user roles and locales when you create the cisco-av-pair attribute: `cisco-av-pair=shell:roles="admin aaa" shell:locales="L1 abc"`. Use a space as the delimiter to separate multiple values.

- For a cluster configuration, add the management port IP addresses for both fabric interconnects. This configuration ensures that remote users can continue to log in if the first fabric interconnect fails and the system fails over to the second fabric interconnect. All login requests are sourced from these IP addresses, not the virtual IP address used by Cisco UCS Manager.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ User Management ➤ TACACS+**.

Step 3 In the **Actions** area of the **General** tab, click **Create TACACS+ Provider**.

Step 4 In the **Create TACACS+ Provider** dialog box:

a) Complete the fields with the information about the TACACS+ service you want to use.

Name	Description
Hostname field	The hostname or IP address on which the TACAS+ provider resides. **Note** If you use a hostname rather than an IP address, you must configure a DNS server in Cisco UCS Manager.
Order field	The order in which Cisco UCS uses this provider to authenticate users. Enter an integer between 1 and 16, or enter lowest-available or 0 (zero) if you want Cisco UCS to assign the next available order based on the other providers defined in this Cisco UCS instance.
Key field	The SSL encryption key for the database.
Confirm Key field	The SSL encryption key repeated for confirmation purposes.
Port field	The port through which Cisco UCS should communicate with the TACACS+ database.
Timeout field	The length of time in seconds the system should spend trying to contact the TACACS+ database before it times out. Enter an integer from 1 to 60 seconds, or enter 0 (zero) to use the global timeout value specified on the TACACS+ **General** tab. The default is 5 seconds.

b) Click **OK**.

Step 5 Click **Save Changes**.

What to Do Next

For implementations involving a single TACACS+ database, select TACACS+ as the primary authentication service.

For implementations involving multiple TACACS+ databases, configure a TACACS+ provider group.

Deleting a TACACS+ Provider

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **User Management ➤ TACACS+** .

Step 3 Right-click the TACACS+ provider you want to delete and choose **Delete**.

Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring Multiple Authentication Systems

Multiple Authentication Systems

You can configure Cisco UCS to use multiple authentication systems by configuring the following features:

- Provider groups
- Authentication domains

Provider Groups

A provider group is a set of providers that will be used by Cisco UCS during the authentication process. Cisco UCS Manager allows you to create a maximum of 16 provider groups, with a maximum of eight providers allowed per group.

During authentication, all the providers within a provider group are tried in order. When a provider successfully responds to the authentication request the authentication process ends.

Creating an LDAP Provider Group

Creating an LDAP provider group allows you to authenticate using multiple LDAP databases.

Note Authenticating with a single LDAP database does not require you to set up an LDAP provider group.

Before You Begin

Create one or more LDAP providers.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ User Management ➤ LDAP**.

Step 3 Right-click **LDAP Provider Groups** and choose **Create LDAP Provider Group**.

Step 4 In the **Create LDAP Provider Group** dialog box, do the following:

a) In the **Name** field, enter a unique name for the group.
This name can be between 1 and 127 characters. You cannot use . (period), _ (underscore), or - (hyphen).

b) In the **LDAP Providers** table, choose one or more providers to include in the group.

c) Click the >> button to add the providers to the **Included Providers** table.
You can use the << button to remove providers from the group.

d) After you have added all desired providers to the provider group, click **OK**.

What to Do Next

Configure an authentication domain or select a default authentication service.

Deleting an LDAP Provider Group

Before You Begin

Remove the provider group from an authentication configuration.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ User Management ➤ LDAP**.

Step 3 Expand **LDAP Provider Groups**.

Step 4 Right-click the LDAP provider group you want to delete and choose **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Creating a RADIUS Provider Group

Creating a RADIUS provider group allows you to authenticate using multiple RADIUS databases.

Note Authenticating with a single RADIUS database does not require you to set up a RADIUS provider group.

Before You Begin

Create one or more RADIUS providers.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ User Management ➤ RADIUS**.

Step 3 Right-click **RADIUS Provider Groups** and choose **Create RADIUS Provider Group**.

Step 4 In the **Create RADIUS Provider Group** dialog box, do the following:

a) In the **Name** field, enter a unique name for the group.
This name can be between 1 and 127 characters. You cannot use . (period), _ (underscore), or - (hyphen).

b) In the **RADIUS Providers** table, choose one or more providers to include in the group.

c) Click the >> button to add the providers to the **Included Providers** table.
You can use the << button to remove providers from the group.

d) After you have added all desired providers to the provider group, click **OK**.

What to Do Next

Configure an authentication domain or select a default authentication service.

Deleting a RADIUS Provider Group

You cannot delete a provider group if it is being used by an authentication configuration.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ User Management ➤ RADIUS**.

Step 3 Expand **RADIUS Provider Groups**.

Step 4 Right-click the RADIUS provider group you want to delete and choose **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Creating a TACACS+ Provider Group

Creating a TACACS+ provider group allows you to authenticate using multiple TACACS+ databases.

Note Authenticating with a single TACACS+ database does not require you to set up a TACACS+ provider group.

Before You Begin

Create one or more TACACS+ providers.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ User Management ➤ TACACS+**.

Step 3 Right-click **TACACS+ Provider Groups** and choose **Create TACACS+ Provider Group**.

Step 4 In the **Create TACACS+ Provider Group** dialog box, do the following:

a) In the **Name** field, enter a unique name for the group.
This name can be between 1 and 127 characters. You cannot use . (period), _ (underscore), or - (hyphen).

b) In the **TACACS+ Providers** table, choose one or more providers to include in the group.

c) Click the >> button to add the providers to the **Included Providers** table.
You can use the << button to remove providers from the group.

d) After you have added all desired providers to the provider group, click **OK**.

Deleting a TACACS+ Provider Group

You cannot delete a provider group if it is being used by an authentication configuration.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ User Management ➤ TACACS+**.

Step 3 Expand **TACACS+ Provider Groups**.

Step 4 Right-click the TACACS+ provider group you want to delete and choose **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Authentication Domains

Authentication domains are used by Cisco UCS Manager to leverage multiple authentication systems. Each authentication domain is specified and configured during login. If no authentication domain is specified, the default authentication service configuration is used.

You can create up to eight authentication domains. Each authentication domain is associated with a provider group and realm in Cisco UCS Manager. If no provider group is specified, all servers within the realm are used.

Creating an Authentication Domain

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ User Management ➤ Authentication**.

Step 3 Right-click **Authentication Domains** and choose **Create a Domain**.

Step 4 In the **Create a Domain** dialog box, complete the following fields:

Name	Description
Name field	The name of the domain. This name can be between 1 and 127 characters. You cannot use . (period), _ (underscore), or - (hyphen).
Realm field	The authentication protocol that will be applied to users in this domain. This can be: • **local**—The user account must be defined locally in this Cisco UCS instance. • **radius**—The user must be defined on the RADIUS server specified for this Cisco UCS instance. • **tacacs**—The user must be defined on the TACACS+ server specified for this Cisco UCS instance. • **ldap**—The user must be defined on the LDAP server specified for this Cisco UCS instance.
Provider Group drop-down list	If the **Realm** is set to anything other than **local**, this field allows you to select the associated provider group, if any.

Step 5 Click **OK**.

Selecting a Primary Authentication Service

Selecting the Console Authentication Service

Before You Begin

If the system uses a remote authentication service, create a provider for that authentication service. If the system uses only local authentication through Cisco UCS, you do not need to create a provider first.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ User Management ➤ Authentication**.

Step 3 Click **Native Authentication**.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Console Authentication** area, complete the following fields:

Name	Description
Realm field	The method by which a user logging into the console is authenticated. This can be: • **local**—The user account must be defined locally in this Cisco UCS instance. • **radius**—The user must be defined on the RADIUS server specified for this Cisco UCS instance. • **tacacs**—The user must be defined on the TACACS+ server specified for this Cisco UCS instance. • **ldap**—The user must be defined on the LDAP server specified for this Cisco UCS instance. • **none**—If the user account is local to this Cisco UCS instance, no password is required when the user logs into the console.
Provider Group drop-down list	The provider group to be used to authenticate a user logging into the console.

Step 6 Click **Save Changes**.

Selecting the Default Authentication Service

Before You Begin

If the system uses a remote authentication service, create a provider for that authentication service. If the system uses only local authentication through Cisco UCS, you do not need to create a provider first.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ User Management ➤ Authentication**.

Step 3 Click **Native Authentication**.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Default Authentication** area, complete the following fields:

Name	Description
Realm field	The default method by which a user is authenticated during remote login. This can be: • **local**—The user account must be defined locally in this Cisco UCS instance. • **radius**—The user must be defined on the RADIUS server specified for this Cisco UCS instance. • **tacacs**—The user must be defined on the TACACS+ server specified for this Cisco UCS instance. • **ldap**—The user must be defined on the LDAP server specified for this Cisco UCS instance. • **none**—If the user account is local to this Cisco UCS instance, no password is required when the user logs in remotely.
Provider Group drop-down list	The default provider group to be used to authenticate the user during remote login.

Step 6 Click **Save Changes**.

Role Policy for Remote Users

By default, if user roles are not configured in Cisco UCS Manager read-only access is granted to all users logging in to Cisco UCS Manager from a remote server using the LDAP, RADIUS, or TACACS protocols. For security reasons, it might be desirable to restrict access to those users matching an established user role in Cisco UCS Manager.

You can configure the role policy for remote users in the following ways:

assign-default-role Does not restrict user access to Cisco UCS Manager based on user roles. Read-only access is granted to all users unless other user roles have been defined in Cisco UCS Manager.

This is the default behavior.

no-login	Restricts user access to Cisco UCS Manager based on user roles. If user roles have not been assigned for the remote authentication system, access is denied.

Configuring the Role Policy for Remote Users

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ User Management ➤ Authentication**.

Step 3 Click **Native Authentication**.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Role Policy for Remote Users** field, click one of the following radio buttons to determine what happens when a user attempts to log in and the remote authentication provider does not supply a user role with the authentication information:

- **no-login**—The user is not allowed to log in to the system, even if the username and password are correct.
- **assign-default-role**—The user is allowed to log in with a read-only user role.

Step 6 Click **Save Changes**.

CHAPTER 8

Configuring Organizations

This chapter includes the following sections:

Organizations in a Multi-Tenancy Environment

Multi-tenancy allows you to divide up the large physical infrastructure of an instance into logical entities known as organizations. As a result, you can achieve a logical isolation between organizations without providing a dedicated physical infrastructure for each organization.

You can assign unique resources to each tenant through the related organization, in the multi-tenant environment. These resources can include different policies, pools, and quality of service definitions. You can also implement locales to assign or restrict user privileges and roles by organization, if you do not want all users to have access to all organizations.

If you set up a multi-tenant environment, all organizations are hierarchical. The top-level organization is always root. The policies and pools that you create in root are system-wide and are available to all organizations in the system. However, any policies and pools created in other organizations are only available to organizations that are above it in the same hierarchy. For example, if a system has organizations named Finance and HR that are not in the same hierarchy, Finance cannot use any policies in the HR organization, and HR cannot access any policies in the Finance organization. However, both Finance and HR can use policies and pools in the root organization.

If you create organizations in a multi-tenant environment, you can also set up one or more of the following for each organization or for a sub-organization in the same hierarchy:

- Resource pools
- Policies
- Service profiles

- Service profile templates

The root organization is always the top level organization.

Hierarchical Name Resolution in a Multi-Tenancy Environment

In a multi-tenant environment, Cisco UCS uses the hierarchy of an organization to resolve the names of policies and resource pools. When Cisco UCS Manager searches for details of a policy or a resource assigned to a pool, the following occurs:

1. Cisco UCS Manager checks for policies and pools with the specified name within the organization assigned to the service profile or policy.
2. If a policy is found or an available resource is inside a pool, Cisco UCS Manager uses that policy or resource. If the pool does not have any available resources at the local level, Cisco UCS Manager moves up in the hierarchy to the parent organization and searches for a pool with the same name. Cisco UCS Manager repeats this step until the search reaches the root organization.
3. If the search reaches the root organization and has not found an available resource or policy, Cisco UCS Manager returns to the local organization and begins to search for a default policy or available resource in the default pool.
4. If an applicable default policy or available resource in a default pool is found, Cisco UCS Manager uses that policy or resource. If the pool does not have any available resources, Cisco UCS Manager moves up in the hierarchy to the parent organization and searches for a default pool. Cisco UCS Manager repeats this step until the search reaches the root organization.
5. If Cisco UCS Manager cannot find an applicable policy or available resource in the hierarchy, it returns an allocation error.

Example: Server Pool Name Resolution in a Single-Level Hierarchy

In this example, all organizations are at the same level below the root organization. For example, a service provider creates separate organizations for each customer. In this configuration, organizations only have access to the policies and resource pools assigned to that organization and to the root organization.

In this example, a service profile in the XYZcustomer organization is configured to use servers from the XYZcustomer server pool. When resource pools and policies are assigned to the service profile, the following occurs:

1. Cisco UCS Manager checks for an available server in the XYZcustomer server pool.
2. If the XYZcustomer server pool has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the pool does not have an available server, Cisco UCS Manager checks the root organization for a server pool with the same name.
3. If the root organization includes an XYZcustomer server pool and that pool has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the pool does not have an available server, Cisco UCS Manager returns to the XYZcustomer organization to check the default server pool.
4. If the default pool in the XYZcustomer organization has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the default pool does not have an available server, Cisco UCS Manager checks the default server pool in the root organization.

5 If the default server pool in the root organization has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the default pool does not have an available server, Cisco UCS Manager returns an allocation error.

Example: Server Pool Name Resolution in a Multi-Level Hierarchy

In this example, each organization includes at least one suborganization. For example, a company could create organizations for each major division in the company and for subdivisions of those divisions. In this configuration, each organization has access to its local policies and resource pools and to the resource pools in the parent hierarchy.

In this example, the Finance organization includes two sub-organizations, AccountsPayable and AccountsReceivable. A service profile in the AccountsPayable organization is configured to use servers from the AP server pool. When resource pools and policies are assigned to the service profile, the following occurs:

1 Cisco UCS Manager checks for an available server in the AP server pool defined in the service profile.

2 If the AP server pool has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the pool does not have an available server, Cisco UCS Manager moves one level up the hierarchy and checks the Finance organization for a pool with the same name.

3 If the Finance organization includes a pool with the same name and that pool has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the pool does not have an available server, Cisco UCS Manager moves one level up in the hierarchy and checks the root organization for a pool with the same name.

4 If the root organization includes a pool with the same name and that pool has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the pool does not have an available server, Cisco UCS Manager returns to the AccountsPayable organization to check the default server pool.

5 If the default pool in the AccountsPayable organization has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the default pool does not have an available server, Cisco UCS Manager moves one level up in the hierarchy and checks the default server pool in the Finance organization.

6 If the default pool in the Finance organization has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the default pool does not have an available server, Cisco UCS Manager moves one level up in the hierarchy and checks the default server pool in the root organization.

7 If the default server pool in the root organization has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the default pool does not have an available server, Cisco UCS Manager returns an allocation error.

Creating an Organization under the Root Organization

Procedure

Step 1 On the toolbar, choose **New ➤ Create Organization**.

Step 2 In the **Name** field of the **Create Organization** dialog box, enter a unique name for the organization.

This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

Step 3 In the **Description** field, enter a description for the organization.

Step 4 Click **OK**.

Creating an Organization under a Sub-Organization

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 In the **Servers** tab, expand **Service Profiles ➤ root**.
You can also access the **Sub-Organizations** node under the **Policies** or **Pools** nodes.

Step 3 Expand the **Sub-Organizations** node and do one of the following:

- To create an organization directly under root, right-click **Sub-Organizations** and choose **Create Organization**.
- To create an organization under a lower-level sub-organization, expand the sub-organization nodes in the hierarchy and then right-click the sub-organization under which you want to create the new organization and choose **Create Organization**.

Step 4 In the **Name** field of the **Create Organization** dialog box, enter a unique name for the organization.
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

Step 5 In the **Description** field, enter a description for the organization.

Step 6 Click **OK**.

Deleting an Organization

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 Navigate to the organization that you want to delete.

Step 3 Right-click the organization and choose **Delete**.

Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

CHAPTER 9

Configuring Role-Based Access Control

This chapter includes the following sections:

Role-Based Access Control

Role-Based Access Control (RBAC) is a method of restricting or authorizing system access for users based on user roles and locales. A role defines the privileges of a user in the system and the locale defines the organizations (domains) that a user is allowed access. Because users are not directly assigned privileges, management of individual user privileges is simply a matter of assigning the appropriate roles and locales.

A user is granted write access to desired system resources only if the assigned role grants the access privileges and the assigned locale allows access. For example, a user with the Server Administrator role in the Engineering organization could update server configurations in the Engineering organization but could not update server configurations in the Finance organization unless the locales assigned to the user include the Finance organization.

User Accounts for Cisco UCS Manager

User accounts are used to access the system. Up to 48 user accounts can be configured in each Cisco UCS instance. Each user account must have a unique username and password.

A user account can be set with a SSH public key. The public key can be set in either of the two formats: OpenSSH and SECSH.

Default User Account

Each Cisco UCS instance has a default user account, admin, which cannot be modified or deleted. This account is the system administrator or superuser account and has full privileges. There is no default password assigned to the admin account; you must choose the password during the initial system setup.

The admin account is always active and does not expire. You cannot configure the admin account as inactive.

Expiration of User Accounts

User accounts can be configured to expire at a predefined time. When the expiration time is reached, the user account is disabled.

By default, user accounts do not expire.

Note After you configure a user account with an expiration date, you cannot reconfigure the account to not expire. You can, however, configure the account with the latest date available.

Guidelines for Cisco UCS Manager Usernames

The username is also used as the login ID for Cisco UCS Manager. When you assign usernames to Cisco UCS Manager user accounts, consider the following guidelines and restrictions:

- The login ID can contain between 1 and 32 characters, including the following:
  - Any alphabetic character
  - Any digit
  - _ (underscore)
  - - (dash)
  - . (dot)
- The unique username for each user account cannot be all-numeric. You cannot create a local user with an all-numeric username.
- The unique username must start with an alphabetic character. It cannot start with a number or a special character, such as an underscore.

After you create a user account, you cannot change the username. You must delete the user account and create a new one.

Guidelines for Cisco UCS Manager Passwords

A password is required for each locally authenticated user account. A user with admin or aaa privileges can configure Cisco UCS Manager to perform a password strength check on user passwords. If the password strength check is enabled, each user must have a strong password.

Cisco recommends that each user have a strong password. If you enable the password strength check for locally authenticated users, Cisco UCS Manager rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters and a maximum of 64 characters.

- Must contain at least three of the following:
  - Lower case letters
  - Upper case letters
  - Digits
  - Special characters
- Must not contain a character that is repeated more than 3 times consecutively, such as aaabbb.
- Must not be identical to the username or the reverse of the username.
- Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word.
- Must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign).
- Should not be blank for local user and admin accounts.

User Roles

User roles contain one or more privileges that define the operations allowed for the user who is assigned the role. A user can be assigned one or more roles. A user assigned multiple roles has the combined privileges of all assigned roles. For example, if Role1 has storage related privileges, and Role2 has server related privileges, users who are assigned to both Role1 and Role2 have storage and server related privileges.

A Cisco UCS instance can contain up to 48 user roles, including the default user roles.

All roles include read access to all configuration settings in the Cisco UCS instance. The difference between the read-only role and other roles is that a user who is only assigned the read-only role cannot modify the system state. A user assigned another role can modify the system state in that user's assigned area or areas.

Roles can be created, modified to add new or remove existing privileges, or deleted. When a role is modified, the new privileges are applied to all users assigned to that role. Privilege assignment is not restricted to the privileges defined for the default roles. That is, you can use a custom set of privileges to create a unique role. For example, the default Server Administrator and Storage Administrator roles have different set of privileges, but a new Server and Storage Administrator role can be created that combines the privileges of both roles.

If a role is deleted after it has been assigned to users, it is also deleted from those user accounts.

User profiles on AAA servers (RADIUS or TACACS+) should be modified to add the roles corresponding to the privileges granted to that user. The attribute is used to store the role information. The AAA servers return this attribute with the request and parse it to get the roles. LDAP servers return the roles in the user profile attributes.

Note If a local user account and a remote user account have the same username, any roles assigned to the remote user are overridden by those assigned to the local user.

Default User Roles

The system contains the following default user roles:

AAA Administrator	Read-and-write access to users, roles, and AAA configuration. Read access to the rest of the system.
Administrator	Complete read-and-write access to the entire system. The default admin account is assigned this role by default and it cannot be changed.
Facility Manager	Read-and-write access to power management operations through the power-mgmt privilege. Read access to the rest of the system.
Network Administrator	Read-and-write access to fabric interconnect infrastructure and network security operations. Read access to the rest of the system.
Operations	Read-and-write access to systems logs, including the syslog servers, and faults. Read access to the rest of the system.
Read-Only	Read-only access to system configuration with no privileges to modify the system state.
Server Equipment Administrator	Read-and-write access to physical server related operations. Read access to the rest of the system.
Server Profile Administrator	Read-and-write access to logical server related operations. Read access to the rest of the system.
Server Security Administrator	Read-and-write access to server security related operations. Read access to the rest of the system.
Storage Administrator	Read-and-write access to storage operations. Read access to the rest of the system.

Privileges

Privileges give users assigned to user roles access to specific system resources and permission to perform specific tasks. The following table lists each privilege and the user role given that privilege by default.

Table 6: User Privileges

Privilege	Description	Default Role Assignment
aaa	System security and AAA	AAA Administrator
admin	System administration	Administrator
ext-lan-config	External LAN configuration	Network Administrator
ext-lan-policy	External LAN policy	Network Administrator
ext-lan-qos	External LAN QoS	Network Administrator
ext-lan-security	External LAN security	Network Administrator

Privilege	Description	Default Role Assignment
ext-san-config	External SAN configuration	Storage Administrator
ext-san-policy	External SAN policy	Storage Administrator
ext-san-qos	External SAN QoS	Storage Administrator
ext-san-security	External SAN security	Storage Administrator
fault	Alarms and alarm policies	Operations
operations	Logs and Smart Call Home	Operations
pod-config	Pod configuration	Network Administrator
pod-policy	Pod policy	Network Administrator
pod-qos	Pod QoS	Network Administrator
pod-security	Pod security	Network Administrator
power-mgmt	Read-and-write access to power management operations	Facility Manager
read-only	Read-only access Read-only cannot be selected as a privilege; it is assigned to every user role.	Read-Only
server-equipment	Server hardware management	Server Equipment Administrator
server-maintenance	Server maintenance	Server Equipment Administrator
server-policy	Server policy	Server Equipment Administrator
server-security	Server security	Server Security Administrator
service-profile-config	Service profile configuration	Server Profile Administrator
service-profile-config-policy	Service profile configuration policy	Server Profile Administrator
service-profile-ext-access	Service profile end point access	Server Profile Administrator
service-profile-network	Service profile network	Network Administrator
service-profile-network-policy	Service profile network policy	Network Administrator
service-profile-qos	Service profile QoS	Network Administrator

Privilege	Description	Default Role Assignment
service-profile-qos-policy	Service profile QoS policy	Network Administrator
service-profile-security	Service profile security	Server Security Administrator
service-profile-security-policy	Service profile security policy	Server Security Administrator
service-profile-server	Service profile server management	Server Profile Administrator
service-profile-server-oper	Service profile consumer	Server Profile Administrator
service-profile-server-policy	Service profile pool policy	Server Security Administrator
service-profile-storage	Service profile storage	Storage Administrator
service-profile-storage-policy	Service profile storage policy	Storage Administrator

User Locales

A user can be assigned one or more locales. Each locale defines one or more organizations (domains) the user is allowed access, and access would be limited to the organizations specified in the locale. One exception to this rule is a locale without any organizations, which gives unrestricted access to system resources in all organizations.

A Cisco UCS instance can contain up to 48 user locales.

Users with AAA privileges (AAA Administrator role) can assign organizations to the locale of other users. The assignment of organizations is restricted to only those in the locale of the user assigning the organizations. For example, if a locale contains only the Engineering organization then a user assigned that locale can only assign the Engineering organization to other users.

Note You cannot assign a locale to users with one or more of the following privileges:

- aaa
- admin
- operations

You can hierarchically manage organizations. A user that is assigned at a top level organization has automatic access to all organizations under it. For example, an Engineering organization can contain a Software Engineering organization and a Hardware Engineering organization. A locale containing only the Software Engineering organization has access to system resources only within that organization; however, a locale that contains the Engineering organization has access to the resources for both the Software Engineering and Hardware Engineering organizations.

Configuring User Roles

Creating a User Role

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All ➤ User Management ➤ User Services**.

Step 3 Right-click **User Services** and choose **Create Role**.
You can also right-click **Roles** to access that option.

Step 4 In the **Create Role** dialog box, complete the following fields:

Name	Description
Name field	A user-defined name for this user role. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Privileges list box	A list of the privileges defined in the system. Click a privilege to view a description of that privilege. Check the check box to assign that privilege to the selected user.
Help Section	
Description field	A description of the most recent privilege you clicked in the **Privileges** list box.

Step 5 Click **OK**.

Adding Privileges to a User Role

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All ➤ User Management ➤ User Services**.

Step 3 Expand the **Roles** node.

Step 4 Choose the role to which you want to add privileges.

Step 5 In the **General** tab, check the boxes for the privileges you want to add to the role.

Step 6 Click **Save Changes**.

Removing Privileges from a User Role

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, expand **All ➤ User Management ➤ User Services**.
Step 3 Expand the **Roles** node.
Step 4 Choose the role from which you want to remove privileges.
Step 5 In the **General** tab, uncheck the boxes for the privileges you want to remove from the role.
Step 6 Click **Save Changes**.

Deleting a User Role

When you delete a user role, Cisco UCS Manager removes that role from all user accounts to which the role has been assigned.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, expand **All ➤ User Management ➤ User Services**.
Step 3 Expand the **Roles** node.
Step 4 Right-click the role you want to delete and choose **Delete**.
Step 5 In the **Delete** dialog box, click **Yes**.

Configuring Locales

Creating a Locale

Before You Begin

One or more organizations must exist before you create a locale.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All ➤ User Management ➤ User Services**.

Step 3 Right-click **Locales** and choose **Create a Locale**.

Step 4 In the **Create Locale** page, do the following:

a) In the **Name** field, enter a unique name for the locale.
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

b) Click **Next**.

Step 5 In the **Assign Organizations** dialog box, do the following:

a) Expand the **Organizations** area to view the organizations in the Cisco UCS instance.
b) Expand the **root** node to see the sub-organizations.
c) Click an organization that you want to assign to the locale.
d) Drag the organization from the **Organizations** area and drop it into the design area on the right.
e) Repeat Steps b and c until you have assigned all desired organizations to the locale.

Step 6 Click **Finish**.

What to Do Next

Add the locale to one or more user accounts. For more information, see Changing the Locales Assigned to a Locally Authenticated User Account, page 144.

Assigning an Organization to a Locale

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All ➤ User Management ➤ User Services**.

Step 3 Expand the **Locales** node and click the locale to which you want to add an organization.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Organizations** area, click + on the table icon bar.

Step 6 In the **Assign Organizations** dialog box, do the following:

a) Expand the **Organizations** area to view the organizations in the Cisco UCS instance.
b) Expand the **root** node to see the sub-organizations.
c) Click an organization that you want to assign to the locale.
d) Drag the organization from the **Organizations** area and drop it into the design area on the right.
e) Repeat Steps b and c until you have assigned all desired organizations to the locale.

Step 7 Click **OK**.

Deleting an Organization from a Locale

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, expand **All ➤ User Management ➤ User Services**.
Step 3 Expand the **Locales** node and click the locale from which you want to delete an organization.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Organizations** area, right-click the organization that you want to delete from the locale and choose **Delete**.
Step 6 Click **Save Changes**.

Deleting a Locale

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, expand **All ➤ User Management ➤ User Services**.
Step 3 Expand the **Locales** node.
Step 4 Right-click the locale you want to delete and choose **Delete**.
Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring User Accounts

Creating a User Account

At a minimum, we recommend that you create the following users:

- Server administrator account
- Network administrator account
- Storage administrator

Before You Begin

Perform the following tasks, if the system includes any of the following:

- Remote authentication services, ensure the users exist in the remote authentication server with the appropriate roles and privileges.

- Multi-tenancy with organizations, create one or more locales. If you do not have any locales, all users are created in root and are assigned roles and privileges in all organizations.
- SSH authentication, obtain the SSH key.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All ➤ User Management ➤ User Services**.

Step 3 Right-click **User Services** and choose **Create User** to open the **User Properties** dialog box.
You can also right-click **Locally Authenticated Users** to access that option.

Step 4 Complete the following fields with the required information about the user:

Name	Description
Login ID field	The account name that is used when logging into this account. This account must be unique and meet the guidelines and restrictions for Cisco UCS Manager user accounts. • The login ID can contain between 1 and 32 characters, including the following: ◦ Any alphabetic character ◦ Any digit ◦ _ (underscore) ◦ - (dash) ◦ . (dot) • The unique username for each user account cannot be all-numeric. You cannot create a local user with an all-numeric username. • The unique username must start with an alphabetic character. It cannot start with a number or a special character, such as an underscore. After you save the user, the login ID cannot be changed. You must delete the user account and create a new one.
First Name field	The first name of the user. This field can contain up to 32 characters.
Last Name field	The last name of the user. This field can contain up to 32 characters.
Email field	The email address for the user.
Phone field	The telephone number for the user.
Password field	The password associated with this account. If password strength check is enabled, a user's password must be strong and Cisco UCS Manager rejects any password that does not meet the following requirements:

Name	Description
	• Must contain a minimum of 8 characters and a maximum of 64 characters. • Must contain at least three of the following: ◦ Lower case letters ◦ Upper case letters ◦ Digits ◦ Special characters • Must not contain a character that is repeated more than 3 times consecutively, such as aaabbb. • Must not be identical to the username or the reverse of the username. • Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word. • Must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign). • Should not be blank for local user and admin accounts.
Confirm Password field	The password a second time for confirmation purposes.
Account Status field	If the status is set to **active**, a user can log into Cisco UCS Manager with this login ID and password.
Account Expires check box	If checked, this account expires and cannot be used after the date specified in the **Expiration Date** field. **Note** After you configure a user account with an expiration date, you cannot reconfigure the account to not expire. You can, however, configure the account with the latest date available.
Expiration Date field	The date on which the account expires. The date should be in the format yyyy-mm-dd. Click the down arrow at the end of this field to view a calendar that you can use to select the expiration date. **Note** Cisco UCS Manager GUI displays this field when you check the **Account Expires** check box.

Step 5 In the **Roles** area, check one or more boxes to assign roles and privileges to the user account.

Note Do not assign locales to users with an admin or aaa role.

Step 6 (Optional) If the system includes organizations, check one or more check boxes in the **Locales** area to assign the user to the appropriate locales.

Step 7 In the **SSH** area, complete the following fields:

a) In the **Type** field, do the following:

- **Password Required**—The user must enter a password when they log in.
- **Key**—SSH encryption is used when this user logs in.

b) If you chose **Key**, enter the SSH key in the **SSH data** field.

Step 8 Click **OK**.

Enabling the Password Strength Check for Locally Authenticated Users

You must be a user with admin or aaa privileges to enable the password strength check. If the password strength check is enabled, Cisco UCS Manager does not permit a user to choose a password that does not meet the guidelines for a strong password.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, expand **All ➤ User Management ➤ User Services**.
Step 3 Click the **Locally Authenticated Users** node.
Step 4 In the **Work** pane, check the **Password Strength Check** check box in the **Properties** area.
Step 5 Click **Save Changes**.

Setting the Web Session Limits for Cisco UCS Manager GUI Users

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.
Step 3 Click the **Communication Services** tab.
Step 4 In the **Web Session Limits** area, complete the following fields:

Name	Description
Maximum Sessions Per User field	The maximum number of concurrent HTTP and HTTPS sessions allowed for each user. Enter an integer between 1 and 256.
Maximum Sessions field	The maximum number of concurrent HTTP and HTTPS sessions allowed for all users within the system. Enter an integer between 1 and 256.

Step 5 Click **Save Changes**.

Changing the Locales Assigned to a Locally Authenticated User Account

Note Do not assign locales to users with an admin or aaa role.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All ➤ User Management ➤ User Services ➤ Locally Authenticated Users**.

Step 3 Click the user account that you want to modify.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Locales** area, do the following:

- To assign a new locale to the user account, check the appropriate check boxes.
- To remove a locale from the user account, uncheck the appropriate check boxes.

Step 6 Click **Save Changes**.

Changing the Roles Assigned to a Locally Authenticated User Account

Changes in user roles and privileges do not take effect until the next time the user logs in. If a user is logged in when you assign a new role to or remove an existing role from a user account, the active session continues with the previous roles and privileges.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All ➤ User Management ➤ User Services ➤ Locally Authenticated Users**.

Step 3 Click the user account that you want to modify.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Roles** area, do the following:

- To assign a new role to the user account, check the appropriate check boxes.
- To remove a role from the user account, uncheck the appropriate check boxes.

Step 6 Click **Save Changes**.

Deleting a Locally Authenticated User Account

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All ➤ User Management ➤ User Services**.

Step 3 Expand the **Locally Authenticated Users** node.

Step 4 Right-click the user account you want to delete and choose **Delete**.

Step 5 In the **Delete** dialog box, click **Yes**.

Monitoring User Sessions

You can monitor Cisco UCS Manager sessions for both locally authenticated users and remotely authenticated users, whether they logged in through the CLI or the GUI.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ User Management**.

Step 3 Click the **User Services** node.

Step 4 In the **Work** pane, click the **Sessions** tab.
The tab displays the following details of user sessions:

Name	Description
Name column	The name for the session.
User column	The username that is involved in the session.
Fabric ID column	The fabric interconnect that the user logged in to for the session.
Login Time column	The date and time the session started.
Terminal Type column	The kind of terminal the user is logged in through.
Host column	The IP address from which the user is logged in.
Current Session column	If this column displays **Y**, the associated user session is currently active.

CHAPTER 10

Managing Firmware

This chapter includes the following sections:

Overview of Firmware

Cisco UCS uses firmware obtained from and certified by Cisco to support the endpoints in a Cisco UCS instance. Each endpoint is a component in the instance that requires firmware to function. A Cisco UCS instance includes the following firmware endpoints that need to be upgraded when you upgrade the firmware:

- Endpoints physically located on servers, such as the BIOS, storage controller (RAID controller), and Cisco Integrated Management Controller (CIMC)
- Endpoints physically located on adapters, including NIC and HBA firmware, and Option ROM (where applicable)
- I/O modules
- Fabric interconnects

- Cisco UCS Manager

Note Beginning with Cisco UCS, Release 1.4(1), Cisco is releasing firmware upgrades in multiple bundles, rather than one large firmware package. For more information see Firmware Image Management, page 148.

Cisco maintains a set of best practices for managing firmware images and updates in this document and in the following technical note: Unified Computing System Firmware Management Best Practices.

This document uses the following definitions for managing firmware:

Upgrade	Changes the firmware running on an endpoint to another image, such as a release or patch. Upgrade includes both update and activation.
Update	Copies the firmware image to the backup partition on an endpoint.
Activate	Sets the firmware in the backup partition as the active firmware version on the endpoint. Activation can require or cause the reboot of an endpoint.

For Management Extensions and Capability Catalog upgrades, update and activate occur simultaneously. You only need to update or activate those upgrades. You do not need to perform both steps.

Firmware Image Management

Cisco delivers all firmware updates to Cisco UCS components in bundles of images. Cisco UCS firmware updates are available to be downloaded in the following bundles:

Cisco UCS Infrastructure Software Bundle	This bundle includes the following firmware images to update the following components: • Cisco UCS Manager software • Kernel and system firmware for the fabric interconnects • I/O module firmware
Cisco UCS B-Series Blade Server Software Bundle	This bundle includes the following firmware images required update the firmware for the blade servers in a Cisco UCS instance. In addition to the bundles created for a release, these bundles can also be released between infrastructure bundles to enable Cisco UCS Manager to support a blade server that is not included in the most recent infrastructure bundle. • CIMC firmware • BIOS firmware • Board controller firmware • Third-party firmware images required by the new server

Cisco UCS C-Series Rack-Mount Server Software Bundle This bundle includes firmware images to update the following components on rack-mount servers that have been integrated with and are managed by Cisco UCS Manager:

- CIMC
- BIOS
- Adapters
- Storage controllers

Note You cannot use this bundle for standalone C-series servers. The firmware management system in those servers cannot interpret the header required by Cisco UCS Manager.

Cisco UCS C-Series Standalone Server Software Bundle This bundle includes firmware images to update the following components on standalone rack-mount servers:

- CIMC
- BIOS
- Adapters
- Storage controllers

Cisco also provides release notes, which you can obtain on the same website from which you obtained the bundles.

Firmware Image Headers

Every firmware image has a header, which includes the following:

- Checksum
- Version information
- Compatibility information that the system can use to verify the compatibility of component images and any dependencies

Firmware Image Catalog

Cisco UCS Manager provides you with two views of the catalog of firmware images and their contents that have been downloaded to the fabric interconnect:

Packages This view provides you with a read-only representation of the firmware bundles that have been downloaded onto the fabric interconnect. This view is sorted by image, not by the contents of the image. For packages, you can use this view to see which component images are in each downloaded firmware bundle.

Images The images view lists the component images available on the system. You cannot use this view to see complete firmware bundles or to group the images by bundle. The information available about each component image includes the name of the component, the image size, the image version, and the vendor and model of the component.

You can use this view to identify the firmware updates available for each component. You can also use this view to delete obsolete and unneeded images. Cisco UCS Manager deletes a package after all images in the package have been deleted.

Tip Cisco UCS Manager stores the images in bootflash on the fabric interconnect. In a cluster system, space usage in bootflash on both fabric interconnects is the same, because all images are synchronized between them. If Cisco UCS Manager reports that the bootflash is out of space, delete obsolete images to free up space.

Firmware Versions

The firmware versions on an endpoint depend upon the type of endpoint. The endpoints physically located on a fabric interconnect have different versions than those physically located on a server or I/O module.

Firmware Versions in CIMC, I/O Modules, and Adapters

Each CIMC, I/O module, and adapter has two slots for firmware in flash. Each slot holds a version of firmware. One slot is active and the other is the backup slot. A component boots from whichever slot is designated as active.

The following firmware version terminology is used in Cisco UCS Manager:

Running Version The running version is the firmware that is active and in use by the endpoint.

Startup Version The startup version is the firmware that will be used when the endpoint next boots up. Cisco UCS Manager uses the activate operation to change the startup version.

Backup Version The backup version is the firmware in the other slot and is not in use by the endpoint. This version can be firmware that you have updated to the endpoint but have not yet activated, or it can be an older firmware version that was replaced by a recently activated version. Cisco UCS Manager uses the update operation to replace the image in the backup slot.

If the endpoint cannot boot from the startup version, it boots from the backup version.

Firmware Versions in the Fabric Interconnect and Cisco UCS Manager

You can only activate the fabric interconnect firmware and Cisco UCS Manager on the fabric interconnect. The fabric interconnect and Cisco UCS Manager firmware do not have backup versions, because all the images are stored on the fabric interconnect. As a result, the number of bootable fabric interconnect images is not limited to two, like the server CIMC and adapters. Instead, the number of bootable fabric interconnect images is limited by the available space in the memory of the fabric interconnect and the number of images stored there.

The fabric interconnect and Cisco UCS Manager firmware have running and startup versions of the kernel and system firmware. The kernel and system firmware must run the same versions of firmware.

Firmware Upgrades

Cisco UCS firmware is upgraded through a combination of the following methods:

- Direct upgrade at the endpoints. For a cluster configuration with two fabric interconnects, a direct upgrade can be minimally disruptive to data traffic. However, it requires that the Cisco UCS instance does not include firmware policies for those endpoints that you upgrade directly. You cannot avoid disruption to traffic in a Cisco UCS instance with only one fabric interconnection.
- Upgrades to server endpoints through service profiles that include a host firmware package, a management firmware package, or both. This method is disruptive to data traffic and should be performed during a maintenance window.

Note Direct upgrade is not available for all endpoints, including the server BIOS, storage controller, HBA firmware, and HBA option ROM. You must upgrade those endpoints through the host firmware package included in the service profile associated with the server.

Guidelines and Cautions for Firmware Upgrades

Before you upgrade the firmware for any endpoint in a Cisco UCS instance, consider the following guidelines and cautions:

Determine Appropriate Type of Firmware Upgrade for Each Endpoint

Some endpoints, such as adapters and the server CIMC, can be upgraded through either a direct firmware upgrade or a firmware package included in a service profile. The configuration of a Cisco UCS instance determines how you upgrade these endpoints. If the service profiles associated with the servers include a host firmware package, upgrade the adapters for those servers through the firmware package. In the same way, if the service profiles associated with the servers include a management firmware package, upgrade the CIMC for those servers through the firmware package.

Upgrades of a CIMC through a management firmware package or an adapter through a firmware package in the service profile associated with the server take precedence over direct firmware upgrades. You cannot directly upgrade an endpoint if the service profile associated with the server includes a firmware package. To perform a direct upgrade, you must remove the firmware package from the service profile.

No Server or Chassis Maintenance

Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process has completed. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure may corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Number of Fabric Interconnects

For a cluster configuration with two fabric interconnects, you can take advantage of the failover between the fabric interconnects and perform a direct firmware upgrade of the endpoints without disrupting data traffic. However, you cannot avoid disrupting data traffic for those endpoints which must be upgraded through a host or management firmware package.

For a standalone configuration with a single fabric interconnect, you can minimize the disruption to data traffic when you perform a direct firmware upgrade of the endpoints. However, you must reboot the fabric interconnect to complete the upgrade and, therefore, cannot avoid disrupting traffic.

Do Not Activate All Endpoints Simultaneously in Cisco UCS Manager GUI

If you use Cisco UCS Manager GUI to update the firmware, do not select **ALL** from the **Filter** drop-down list in the **Activate Firmware** dialog box to activate all endpoints simultaneously. Many firmware releases and patches have dependencies that require the endpoints to be activated in a specific order for the firmware update to succeed. This order can change depending upon the contents of the release or patch. Activating all endpoints does not guarantee that the updates occur in the required order and can disrupt communications between the endpoints and the fabric interconnects and Cisco UCS Manager. For information about the dependencies in a specific release or patch, see the release notes provided with that release or patch.

Impact of Activation for Adapters and I/O Modules

During a direct upgrade, you should configure **Set Startup Version Only** for an adapter. With this setting, the activated firmware moves into the pending-next-boot state, and the server is not immediately rebooted. The activated firmware does not become the running version of firmware on the adapter until the server is rebooted. You cannot configure **Set Startup Version Only** for an adapter in the host firmware package.

If a server is not associated with a service profile, the activated firmware moves into the pending-next-boot state. Cisco UCS Manager does not reboot the endpoints or activate the firmware until the server is associated with a service profile. If necessary, you can manually reboot an unassociated server to activate the firmware.

When you configure **Set Startup Version Only** for an I/O module, the I/O module is rebooted when the fabric interconnect in its data path is rebooted. If you do not configure **Set Startup Version Only** for an I/O module, the I/O module reboots and disrupts traffic. In addition, if Cisco UCS Manager detects a protocol and firmware version mismatch between it and the I/O module, Cisco UCS Manager automatically updates the I/O module with the firmware version that matches its own and then activates the firmware and reboots the I/O module again.

Avoid Replacing RAID-Configured Hard Disks Prior to Upgrade

Under the following circumstances, Cisco UCS Manager may scrub all data on a hard disk as part of the RAID synchronization process during an upgrade of the server firmware:

- The hard disks in the server are configured for RAID.
- One or more of the RAID-configured hard disks in the server are removed.
- The hard disk or disks are replaced with hard disks that are configured with a pre-existing RAID and the local disk configuration policy included in the service profile on the server is not used to configure those hard disks.
- The server firmware is upgraded, causing the server to reboot and Cisco UCS Manager to begin the RAID synchronization process.

If the original hard disks contained vital data that needs to preserved, avoid inserting new hard disks that are already configured for RAID.

Impact of Upgrade to Release 1.3(1i) or Higher

An upgrade from an earlier Cisco UCS firmware release to release 1.3(1i) or higher has the following impact on the Protect Configuration property of the local disk configuration policy the first time servers are associated with service profiles after the upgrade:

Unassociated Servers

After you upgrade the Cisco UCS instance, the initial server association proceeds without configuration errors whether or not the local disk configuration policy matches the server hardware. Even if you enable the Protect Configuration property, Cisco UCS does not protect the user data on the server if there are configuration mismatches between the local disk configuration policy on the previous service profile and the policy in the new service profile.

Note If you enable the Protect Configuration property and the local disk configuration policy encounters mismatches between the previous service profile and the new service profile, all subsequent service profile associations with the server are blocked.

Associated Servers

Any servers that are already associated with service profiles do not reboot after the upgrade. Cisco UCS Manager does not report any configuration errors if there is a mismatch between the local disk configuration policy and the server hardware.

When a service profile is disassociated from a server and a new service profile associated, the setting for the Protect Configuration property in the new service profile takes precedence and overwrites the setting in the previous service profile.

Cannot Upgrade Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter

The firmware on the Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter (N20-AI0002), Intel-based adapter card, is burned into the hardware at manufacture. You cannot upgrade the firmware on this adapter.

Required Order of Components for Firmware Activation

If you upgrade firmware by individual components in a Cisco UCS instance, activate the updates in the required order for quicker activation and to avoid potential issues with conflicting firmware versions.

Required Order when Updating from Cisco UCS, Release 1.3(1) and Later

1. Adapter (interface card)—If you plan to upgrade the adapters directly, perform this step first. However, if you prefer, you can omit this step and upgrade the adapters as part of the last step, in a host firmware package.
2. CIMC—If you upgrade the adapters in the host firmware package, perform this step first.
3. I/O module.
4. Cisco UCS Manager.
5. Fabric interconnect.

6 Host firmware package—Must be the last step in the upgrade process. We recommend that you upgrade the board controller firmware during this step to avoid an additional reboot of the server. You must upgrade the BIOS and storage controller firmware in a host firmware package.

Required Order when Updating from Cisco UCS, Release 1.0(2) and Later

1 Adapter (interface card)—If you plan to upgrade the adapters directly, perform this step first. However, if you prefer, you can omit this step and upgrade the adapters as part of the last step, in a host firmware package.

2 BMC—If you upgrade the adapters in the host firmware package, perform this step first.

3 I/O module.

4 Cisco UCS Manager.

5 Fabric interconnect.

6 Host firmware package—Must be the last step in the upgrade process. We recommend that you upgrade the board controller firmware during this step to avoid an additional reboot of the server. You must upgrade the BIOS and storage controller firmware in a host firmware package.

Required Order when Updating from Cisco UCS, Release 1.0(1)

1 Adapter (interface card)—If you plan to upgrade the adapters directly, perform this step first. However, if you prefer, you can omit this step and upgrade the adapters as part of the last step, in a host firmware package.

2 BMC—If you upgrade the adapters in the host firmware package, perform this step first.

3 I/O module.

4 Fabric interconnect.

5 Cisco UCS Manager.

6 Host firmware package—Must be the last step in the upgrade process. We recommend that you upgrade the board controller firmware during this step to avoid an additional reboot of the server. You must upgrade the BIOS and storage controller firmware in a host firmware package.

Required Order for Adding Support for Previously Unsupported Servers

From Cisco UCS, Release 1.4(1) and later, the method for adding support for previously unsupported type of servers, such as a new blade server or a rack-mount server, to an existing Cisco UCS instance requires the following additional steps after you upgrade your existing firmware to the new release.

Adding Support for a Previously Unsupported Cisco UCS Blade Server

After you upgrade the firmware for the existing components, you can add support for a previously unsupported server that was released between infrastructure bundle releases. When you add the first server of a previously unsupported type of blade server, you must perform the steps to enable Cisco UCS Manager to support that type of server in the following order:

1. Insert the blade server into the chassis as described in the server installation guide. Cisco UCS Manager cannot discover the server as it is unsupported, and the finite state machine (FSM) for the discovery fails with an unsupported server error.
2. Obtain the B-Series server bundle for the new blade server from Cisco.com and download it to the fabric interconnect.
3. Activate the Capability Catalog image from the server bundle.
4. Activate the Management Extension from the server bundle.
5. Wait for Cisco UCS Manager to retry discovery of the new server. If server discovery does not begin within a few minutes, acknowledge the server.

Note You only need to perform these steps for the first server of a previously unsupported type of blade server. Cisco UCS Manager discovers all subsequent servers of that type automatically.

Integrating a Cisco UCS Rack-Mount Server

After you upgrade the firmware for the existing components, you can integrate a Cisco UCS rack-mount server. When you integrate a rack-mount server, you must perform the steps in the following order:

1. If you have not already done so, configure the rack server discovery policy in Cisco UCS Manager.
2. Follow the instructions in the server installation guide for installing and integrating a rack-mount server in a system managed by Cisco UCS Manager.
3. Wait for Cisco UCS Manager to discover the new server. If server discovery does not begin within a few minutes, acknowledge the server.

Direct Firmware Upgrade at Endpoints

If you follow the correct procedure and apply the upgrades in the correct order, a direct firmware upgrade and the activation of the new firmware version on the endpoints is minimally disruptive to traffic in a Cisco UCS instance.

You can directly upgrade the firmware on the following endpoints:

- Adapters
- CIMCs
- I/O modules
- Board controllers
- Cisco UCS Manager
- Fabric interconnects

The adapter and board controller firmware can also be upgraded through the host firmware package in the service profile. If you use a host firmware package to upgrade this firmware, you can reduce the number of times a server needs to be rebooted during the firmware upgrade process.

Note Upgrades of a CIMC through a management firmware package or an adapter through a firmware package in the service profile associated with the server take precedence over direct firmware upgrades. You cannot directly upgrade an endpoint if the service profile associated with the server includes a firmware package. To perform a direct upgrade, you must remove the firmware package from the service profile.

Stages of a Direct Firmware Upgrade

Cisco UCS Manager separates the direct upgrade process into two stages to ensure that you can push the firmware to an endpoint while the system is running without affecting uptime on the server or other endpoints.

Update

During this stage, the system copies the selected firmware version from the primary fabric interconnect to the backup partition in the endpoint and verifies that the firmware image is not corrupt. The update process always overwrites the firmware in the backup slot.

The update stage applies only to the following endpoints:

- Adapters
- CIMCs
- I/O modules

You can set the update as Startup Version Only to avoid rebooting the endpoint immediately. This allows you to perform the update at any time and then activate and reboot during a maintenance period.

Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process has completed. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure may corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Activate

During this stage, the system sets the specified image version (normally the backup version) as the startup version and, if you do not specify **Set Startup Version Only**, immediately reboots the endpoint. When the endpoint is rebooted, the backup partition becomes the active partition, and the active partition becomes the backup partition. The firmware in the new active partition becomes the startup version and the running version.

The following endpoints only require activation because the specified firmware image already exists on the endpoint:

- Cisco UCS Manager
- Fabric interconnects
- Board controllers on those servers that support them

When the firmware is activated, the endpoint is rebooted and the new firmware becomes the active kernel version and system version. If the endpoint cannot boot from the startup firmware, it defaults to the backup version and raises a fault.

Caution When you configure **Set Startup Version Only** for an I/O module, the I/O module is rebooted when the fabric interconnect in its data path is rebooted. If you do not configure **Set Startup Version Only** for an I/O module, the I/O module reboots and disrupts traffic. In addition, if Cisco UCS Manager detects a protocol and firmware version mismatch between it and the I/O module, Cisco UCS Manager automatically updates the I/O module with the firmware version that matches its own and then activates the firmware and reboots the I/O module again.

Outage Impacts of Direct Firmware Upgrades

When you perform a direct firmware upgrade on an endpoint, you can disrupt traffic or cause an outage in one or more of the endpoints in the Cisco UCS instance.

Outage Impact of a Fabric Interconnect Firmware Upgrade

When you upgrade the firmware for a fabric interconnect, you cause the following outage impacts and disruptions:

- The fabric interconnect reboots.
- The corresponding I/O modules reboot.

Outage Impact of a Cisco UCS Manager Firmware Upgrade

A firmware upgrade to Cisco UCS Manager causes the following disruptions:

- Cisco UCS Manager GUI—All users logged in to Cisco UCS Manager GUI are logged out and their sessions ended.

  Any unsaved work in progress is lost.
- Cisco UCS Manager CLI—All users logged in through telnet are logged out and their sessions ended. Console sessions are not ended.

Outage Impact of an I/O Module Firmware Upgrade

When you upgrade the firmware for an I/O module, you cause the following outage impacts and disruptions:

- For a standalone configuration with a single fabric interconnect, data traffic is disrupted when the I/O module reboots. For a cluster configuration with two fabric interconnects, data traffic fails over to the other I/O module and the fabric interconnect in its data path.
- If you activate the new firmware as the startup version only, the I/O module reboots when the corresponding fabric interconnect is rebooted.
- If you activate the new firmware as the running and startup version, the I/O module reboots immediately.
- An I/O module can take up to ten minutes to become available after a firmware upgrade.

Outage Impact of a CIMC Firmware Upgrade

When you upgrade the firmware for a CIMC in a server, you impact only the CIMC and internal processes. You do not interrupt server traffic. This firmware upgrade causes the following outage impacts and disruptions to the CIMC:

- Any activities being performed on the server through the KVM console and vMedia are interrupted.
- Any monitoring or IPMI polling is interrupted.

Outage Impact of an Adapter Firmware Upgrade

If you activate the firmware for an adapter and do not configure the **Set Startup Version Only** option, you cause the following outage impacts and disruptions:

- The server reboots.
- Server traffic is disrupted.

Firmware Upgrades through Service Profiles

You can use service profiles to upgrade the server and adapter firmware, including the BIOS on the server, by defining the following policies and including them in the service profile associated with a server:

- Host Firmware Package policy
- Management Firmware Package policy

Note You cannot upgrade the firmware on an I/O module, fabric interconnect, or Cisco UCS Manager through service profiles. You must upgrade the firmware on those endpoints directly.

Host Firmware Package

This policy enables you to specify a set of firmware versions that make up the host firmware package (also known as the host firmware pack). The host firmware includes the following firmware for server and adapter endpoints:

- **Adapter**
- **BIOS**
- **Board Controller**
- **FC Adapters**
- **HBA Option ROM**
- **Storage Controller**

Tip You can include more than one type of firmware in the same host firmware package. For example, a host firmware package can include both BIOS firmware and storage controller firmware or adapter firmware for two different models of adapters. However, you can only have one firmware version with the same type, vendor, and model number. The system recognizes which firmware version is required for an endpoint and ignores all other firmware versions.

The firmware package is pushed to all servers associated with service profiles that include this policy.

This policy ensures that the host firmware is identical on all servers associated with service profiles which use the same policy. Therefore, if you move the service profile from one server to another, the firmware versions are maintained. Also, if you change the firmware version for an endpoint in the firmware package, new versions are applied to all the affected service profiles immediately, which could cause server reboots.

You must include this policy in a service profile, and that service profile must be associated with a server for it to take effect.

Prerequisites

This policy is not dependent upon any other policies. However, you must ensure that the appropriate firmware has been downloaded to the fabric interconnect. If the firmware image is not available when Cisco UCS Manager is associating a server with a service profile, Cisco UCS Manager ignores the firmware upgrade and completes the association.

Management Firmware Package

This policy enables you to specify a set of firmware versions that make up the management firmware package (also known as a management firmware pack). The management firmware package includes the Cisco Integrated Management Controller (CIMC) on the server. You do not need to use this package if you upgrade the CIMC directly.

The firmware package is pushed to all servers associated with service profiles that include this policy. This policy ensures that the CIMC firmware is identical on all servers associated with service profiles which use the same policy. Therefore, if you move the service profile from one server to another, the firmware versions are maintained.

You must include this policy in a service profile, and that service profile must be associated with a server for it to take effect.

This policy is not dependent upon any other policies. However, you must ensure that the appropriate firmware has been downloaded to the fabric interconnect.

Stages of a Firmware Upgrade through Service Profiles

You can use the host and management firmware package policies in service profiles to upgrade server and adapter firmware.

Caution If you modify a host firmware package by adding an endpoint or changing firmware versions for an existing endpoint, Cisco UCS Manager upgrades the endpoints and reboots all servers associated with that firmware package as soon as the changes are saved, disrupting data traffic to and from the servers.

New Service Profile

For a new service profile, this upgrade takes place over the following stages:

Firmware Package Policy Creation	During this stage, you create the host and/or management firmware packages and include them in the appropriate firmware policies.
Service Profile Association	During this stage, you include the firmware packages in a service profile, and then associate the service profile with a server. The system pushes the selected firmware versions to the endpoints. For a host firmware package, the server is

rebooted to ensure that the endpoints are running the versions specified in the firmware package.

Existing Service Profile

If the service profile is already associated with a server, Cisco UCS Manager upgrades the firmware as soon as you save the changes to the host firmware packages. For a host firmware package, Cisco UCS Manager reboots the server as soon as the change is saved.

Firmware Downgrades

You downgrade firmware in a Cisco UCS instance in the same way that you upgrade firmware. The package or version that you select when you update the firmware determines whether you are performing an upgrade or a downgrade.

Completing the Prerequisites for Upgrading the Firmware

Prerequisites for Upgrading and Downgrading Firmware

All endpoints in a Cisco UCS instance must be fully functional and all processes must be complete before you begin a firmware upgrade or downgrade on those endpoints. You cannot upgrade or downgrade an endpoint that is not in a functional state. For example, the firmware on a server that has not been discovered cannot be upgraded or downgraded. An incomplete process, such as an FSM that has failed after the maximum number of retries, can cause the upgrade or downgrade on an endpoint to fail. If an FSM is in progress, Cisco UCS Manager queues up the update and activation and runs them when the FSM has completed successfully.

Colored boxes around components on the **Equipment** tab may indicate that an endpoint on that component cannot be upgraded or downgraded. Verify the status of that component before you attempt to upgrade the endpoints.

Note The **Installed Firmware** tab in Cisco UCS Manager GUI does not provide sufficient information to complete these prerequisites.

Before you upgrade or downgrade firmware in a Cisco UCS instance, complete the following prerequisites:

- Back up the configuration into an All Configuration backup file.
- For a cluster configuration, verify that the high availability status of the fabric interconnects shows that both are up and running.
- For a standalone configuration, verify that the Overall Status of the fabric interconnect is Operable.
- Verify that all servers, I/O modules, and adapters are fully functional. An inoperable server cannot be upgraded.
- Verify that all servers have been discovered. They do not need to be powered on or associated with a service profile.

Creating an All Configuration Backup File

This procedure assumes that you do not have an existing backup operation for an All Configuration backup file.

Before You Begin

Obtain the backup server IP address and authentication credentials.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 Click the **All** node.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area, click **Backup Configuration**.

Step 5 In the **Backup Configuration** dialog box, click **Create Backup Operation**.

Step 6 In the **Create Backup Operation** dialog box, do the following:

a) Complete the following fields:

- **Admin State** field—Click the **enabled** radio button to run the backup operation as soon as you click OK.
- **Type** field—Click the **All Configuration** radio button to create an XML backup file that includes all system and logical configuration information.
- **Preserve Identities** check box—If the Cisco UCS instance includes any identities derived from pools that you need to preserve, check this check box.

  Identities such as MAC addresses, WWNNs, WWPNs, or UUIDS are assigned at runtime. If you do not want these identities to change after you import the backup file, you must check this check box. If you do not, these identities may be changed after the import and operations such as a PXE boot or a SAN boot may no longer function.
- **Protocol** field—Click the one of the following radio buttons to indicate the protocol you want to use to transfer the file to the backup server:
  - **FTP**
  - **TFTP**
  - **SCP**
  - **SFTP**
- **Hostname** field—Enter the IP address or hostname of the location where the backup file is to be stored. This can be a server, storage array, local drive, or any read/write media that the fabric interconnect can access through the network. If you use a hostname, you must configure Cisco UCS Manager to use a DNS server.
- **Remote File** field—Enter the full path to the backup configuration file. This field can contain the filename as well as the path. If you omit the filename, the backup procedure assigns a name to the file.

- **User** field—Enter the username that Cisco UCS Manager should use to log in to the backup location. You do not need to complete this field if you selected TFTP for the protocol.
- **Password** field—Enter the password associated with the username. You do not need to complete this field if you selected TFTP for the protocol.

b) Click **OK**.

Step 7 If Cisco UCS Manager displays a confirmation dialog box, click **OK**.
If you set the **Admin State** field to enabled, Cisco UCS Manager takes a snapshot of the configuration type that you selected and exports the file to the network location. The backup operation displays in the **Backup Operations** table in the **Backup Configuration** dialog box.

Step 8 (Optional) To view the progress of the backup operation, do the following:

a) If the operation does not display in the **Properties** area, click the operation in the **Backup Operations** table.

b) In the **Properties** area, click the down arrows on the **FSM Details** bar.

The **FSM Details** area expands and displays the operation status.

Step 9 Click **OK** to close the **Backup Configuration** dialog box.
The backup operation continues to run until it is completed. To view the progress, re-open the **Backup Configuration** dialog box.

Verifying the Overall Status of the Fabric Interconnects

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Fabric Interconnects**.

Step 3 Click the node for the fabric interconnect that you want to verify.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Status** area, verify that the **Overall Status** is **operable**.
If the status is not **operable**, run a **show tech-support** command and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about the **show tech-support** command, see *Cisco UCS Troubleshooting Guide*.

Verifying the High Availability Status and Roles of a Cluster Configuration

The high availability status is the same for both fabric interconnects in a cluster configuration.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Fabric Interconnects**.

Step 3 Click the node for one of the fabric interconnects in the cluster.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 If the fields in the **High Availability Details** area are not displayed, click the **Expand** icon to the right of the heading.

Step 6 Verify that the following fields display the following values:

Field Name	Required Value
Ready field	**Yes**
State field	**Up**

If the values are different, run a **show tech-support** command and contact Cisco Technical Support. Do not proceed with the firmware upgrade.

Step 7 Note the value in the **Leadership** field to determine whether the fabric interconnect is the primary or subordinate.
You need to know this information to upgrade the firmware on the fabric interconnects.

Verifying the Status of I/O Modules

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis**.

Step 3 Click on the chassis for which you want to verify the status of the I/O modules.

Step 4 In the **Work** pane, click the **IO Modules** tab.

Step 5 For each I/O module, verify that the following columns display the following values:

Field Name	Desired Value
Overall Status column	**ok**
Operability column	**operable**

If the values are different, run a **show tech-support** command and contact Cisco Technical Support. Do not proceed with the firmware upgrade.

Step 6 Repeat Steps 3 through 5 to verify the status of the I/O modules in each chassis.

Verifying the Status of Servers

If a server is inoperable, you can proceed with the upgrade for other servers in the Cisco UCS instance. However, you cannot upgrade the inoperable server.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, click **Equipment**.

Step 3 In the **Work** pane, click the **Servers** tab to display a list of all servers in all chassis.

Step 4 For each server, verify that the following columns display the following values:

Field Name	Desired Value
Overall Status column	**ok**, **unassociated**, or any value that does not indicate a failure. If the value indicates a failure, such as **discovery-failed**, the endpoints on that server cannot be upgraded.
Operability column	**operable**

Step 5 If you need to verify that a server has been discovered, do the following:

a) Right-click the server for which you want to verify the discovery status and choose **Show Navigator**.

b) In the **Status Details** area of the **General** tab, verify that the **Discovery State** field displays a value of **complete**.
If the fields in the **Status Details** area are not displayed, click the **Expand** icon to the right of the heading.

Verifying the Status of Adapters on Servers in a Chassis

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.

Step 3 Click the server for which you want to verify the status of the adapters.

Step 4 In the **Work** pane, click the **Inventory** tab.

Step 5 In the **Inventory** tab, click the **Interface Cards** subtab.

Step 6 For each adapter, verify that the following columns display the following values:

Field Name	Desired Value
Overall Status column	**ok**

Field Name	Desired Value
Operability column	**operable**

If the fields show a different value and the adapter is inoperable, you can proceed with the upgrade for other adapters on the servers in the Cisco UCS instance. However, you cannot upgrade the inoperable adapter.

Downloading and Managing Firmware Packages

Obtaining Software Bundles from Cisco

Before You Begin

Determine which of the following software bundles you need to update the Cisco UCS instance:

- Cisco UCS Infrastructure Software Bundle—Required for all Cisco UCS instances.
- Cisco UCS B-Series Blade Server Software Bundle—Required for all Cisco UCS instances that include blade servers.
- Cisco UCS C-Series Rack-Mount Server Software Bundle—Only required for Cisco UCS instances that include integrated rack-mount servers. This bundle contains firmware to enable Cisco UCS Manager to manage those servers and is not applicable to standalone C-Series rack-mount servers.

Procedure

Step 1 In a web browser, navigate to http://www.cisco.com.

Step 2 Under **Support**, click **Download Software**.

Step 3 Click **Unified Computing**.

Step 4 If prompted, enter your Cisco.com username and password to log in.

Step 5 Navigate to the software bundles you need, as follows:

- Cisco UCS Infrastructure Software Bundle—Click **Cisco UCS Infrastructure Software ➤ Unified Computing System (UCS) Infrastructure Software Bundle**.
- Cisco UCS B-Series Blade Server Software Bundle—Click **Cisco UCS Manager Server Software ➤ UCS B-Series Blade Server Software ➤ Unified Computing System (UCS) Server Software**.
- Cisco UCS C-Series Rack-Mount Server Software Bundle—Navigate to **Cisco UCS Manager Server Software ➤ UCS C-Series RackMount Server Software ➤ Unified Computing System (UCS) Server Software**.

Step 6 On any page where you download a software bundle, click the **Release Notes** link to download the latest version of the Release Notes.

Step 7 For each software bundle that you want to download, do the following:

a) Click the link for the release you want to download.

b) Click one of the following buttons and follow the instructions provided:

- **Download Now**—Allows you to download the software bundle immediately.
- **Add to Cart**—Adds the software bundle to your cart to be downloaded at a later time.

c) Follow the prompts to complete your download of the software bundle(s).

Step 8 Read the Release Notes before upgrading Cisco UCS.

What to Do Next

Download the software bundles to the fabric interconnect.

Downloading Firmware Images to the Fabric Interconnect from a Remote Location

Note In a cluster setup, the image file for the firmware bundle is downloaded to both fabric interconnects, regardless of which fabric interconnect is used to initiate the download. Cisco UCS Manager maintains all firmware packages and images in both fabric interconnects in sync. If one fabric interconnect is down, the download still finishes successfully. The images are synced to the other fabric interconnect when it comes back online.

Before You Begin

Obtain the required firmware bundles from Cisco.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 Click the **Installed Firmware** tab.

Step 5 Click **Download Firmware**.

Step 6 In the **Download Firmware** dialog box, click the **Remote File System** radio button in the **Location of the Image File** field.

Step 7 Complete the following fields:

Name	Description
Protocol field	The protocol to use when communicating with the remote server. This can be: • **FTP** • **TFTP** • **SCP** • **SFTP**

Name	Description
	Note TFTP has a file size limitation of 32 MB. Because firmware bundles can be much larger than that, we recommend that you do not select TFTP for firmware downloads.
Server field	If the file came from a remote server, this is the IP address or hostname of the remote server on which the files resides. If the file came from a local source, this field displays "local". **Note** If you use a hostname rather than an IP address, you must configure a DNS server in Cisco UCS Manager.
Filename field	The name of the firmware file.
Path field	The absolute path to the file on the remote server. If you use SCP, the absolute path is always required. If you use any other protocol, you may not need to specify a remote path if the file resides in the default download folder. For details about how your file server is configured, contact your system administrator.
User field	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP.
Password field	The password for the remote server username. This field does not apply if the protocol is TFTP.

Step 8 Click **OK**.
Cisco UCS Manager GUI begins downloading the firmware bundle to the fabric interconnect.

Step 9 (Optional) Monitor the status of the download on the **Download Tasks** tab.
Note If Cisco UCS Manager reports that the bootflash is out of space, delete obsolete bundles on the **Packages** tab to free up space. To view the available space in bootflash, navigate to the fabric interconnect on the **Equipment** tab and expand the **Local Storage Information** area on the **General** tab.

Step 10 Repeat this task until all the required firmware bundles have been downloaded to the fabric interconnect.

What to Do Next

After the image file for the firmware bundles have downloaded completely, update the firmware on the endpoints.

Downloading Firmware Images to the Fabric Interconnect from the Local File System

Note In a cluster setup, the image file for the firmware bundle is downloaded to both fabric interconnects, regardless of which fabric interconnect is used to initiate the download. Cisco UCS Manager maintains all firmware packages and images in both fabric interconnects in sync. If one fabric interconnect is down, the download still finishes successfully. The images are synced to the other fabric interconnect when it comes back online.

Before You Begin

Obtain the required firmware bundles from Cisco.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 Click the **Installed Firmware** tab.

Step 5 Click **Download Firmware**.

Step 6 In the **Download Firmware** dialog box, click the **Local File System** radio button in the **Location of the Image File** field.

Step 7 In the **Filename** field, type the full path and and name of the image file.
If you do not know the exact path to the folder where the firmware image file is located, click **Browse** and navigate to the file.

Step 8 Click **OK**.
Cisco UCS Manager GUI begins downloading the firmware bundle to the fabric interconnect.

Step 9 (Optional) Monitor the status of the firmware bundle download on the **Download Tasks** tab.

Note If Cisco UCS Manager reports that the bootflash is out of space, delete obsolete bundles on the **Packages** tab to free up space. To view the available space in bootflash, navigate to the fabric interconnect on the **Equipment** tab and expand the **Local Storage Information** area on the **General** tab.

Step 10 Repeat this task until all the required firmware bundles have been downloaded to the fabric interconnect.

What to Do Next

After the image file for the firmware bundles have downloaded completely, update the firmware on the endpoints.

Canceling an Image Download

You can cancel the download task for an image only while it is in progress. After the image has downloaded, deleting the download task does not delete the image that was downloaded. You cannot cancel the FSM related to the image download task.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 Expand the **Equipment** node.
Step 3 In the **Work** pane, click the **Firmware Management** tab.
Step 4 On the **Download Tasks** tab, right-click the task you want to cancel and select **Delete**.

Determining the Contents of a Firmware Package

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, click the **Equipment** node.
Step 3 In the **Work** pane, click the **Firmware Management** tab.
Step 4 On the **Packages** subtab, click the + icon next to a package to view its contents.
Step 5 To take a snapshot of the package contents, do the following:
a) Highlight the rows that include the image name and its contents.
b) Right-click and choose **Copy**.
c) Paste the contents of your clipboard into a text file or other document.

Checking the Available Space on a Fabric Interconnect

If an image download fails, check whether the bootflash on the fabric interconnect or fabric interconnects in the Cisco UCS has sufficient available space.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, expand **Equipment ➤ Fabric Interconnects**.
Step 3 Click the fabric interconnect on which you want to check the available space.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 Expand the **Local Storage Information** area.
When you download a firmware image bundle, a fabric interconnect needs at least twice as much available space as the size of the firmware image bundle. If the bootflash does not have sufficient space, delete the obsolete firmware, core files, and other unneeded objects from the fabric interconnect.

Deleting Firmware Packages from a Fabric Interconnect

Use this procedure if you want to an entire firmware package or bundle. If you prefer you can also delete one or more of the individual images in a package.

For releases prior to Cisco UCS, Release 1.3(1), you cannot delete firmware packages from the **Packages** tab. After you delete all images from the package, Cisco UCS Manager removes the packages.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, click the **Equipment** node.
Step 3 In the **Work** pane, click the **Firmware Management** tab.
Step 4 On the **Firmware Management** tab, click the **Packages** tab.
Step 5 In the table, click the package that you want to delete.
You can use the Shift key or Ctrl key to select multiple entries.
Step 6 Right-click the highlighted package or packages and choose **Delete**.
Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Cisco UCS Manager deletes the selected package or packages and all images contained within each package.

Deleting Firmware Images from a Fabric Interconnect

Use this procedure if you want to delete only a single image from a package.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, click the **Equipment** node.
Step 3 In the **Work** pane, click the **Firmware Management** tab.
Step 4 On the **Firmware Management** tab, click the **Images** tab.
Step 5 In the table, click the image that you want to delete.
You can use the Shift key or Ctrl key to select multiple entries.
Step 6 Right-click the highlighted image or images and choose **Delete**.
Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Directly Updating Firmware at Endpoints

Updating the Firmware on Multiple Endpoints

You can use this procedure to update the firmware on the following endpoints:

- Adapters
- CIMCs
- I/O modules

Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process has completed. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure may corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 On the **Installed Firmware** subtab, click **Update Firmware**.
Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS instance. This step may take a few minutes, depending upon the number of chassis and servers.

Step 5 In the **Update Firmware** dialog box, do the following:

a) From the **Filter** drop-down list on the menu bar, select **ALL**.
If you want to update all endpoints of a specific type, such as all adapters, select that type from the drop-down list.

b) From the **Set Version** drop-down list on the menu bar, select the firmware version to which you want to update the endpoints.

c) Click **OK**.
If the service profile for the server includes a host firmware package, Cisco UCS Manager cannot update the adapter firmware for that server. After you acknowledge the notification message, Cisco UCS Manager updates the firmware for all other endpoints on servers that do not have associated host firmware packages. If you want to update the adapter firmware for a server directly, you must remove all host firmware packages from the associated service profiles. Removing the adapter firmware from the host firmware package is not sufficient to enable you to update the adapters directly.

Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that the image is not corrupt. The image remains as the backup version until you explicitly activate it. Cisco UCS Manager begins all updates at the same time. However, some updates may complete at different times.

The update is complete when the **Update Firmware** dialog box displays **ready** in the **Update Status** column for all updated endpoints.

Step 6 (Optional) To monitor the progress of the update to a specific endpoint, right-click the endpoint and choose **Show Navigator**.
Cisco UCS Manager displays the progress in the **Update Status** area on the **General** tab. If the navigator has an **FSM** tab, you can also monitor the progress there. An entry in the **Retry #** field may not indicate that the update has failed. The retry count also includes retries that occur when Cisco UCS Manager retrieves the update status.

What to Do Next

Activate the firmware.

Updating the Firmware on an Adapter

Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process has completed. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure may corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.

Step 3 Expand the node for the server which includes the adapter you want to update.

Step 4 Expand **Interface Cards** and select the interface card for the adapter you want to upgrade.

Step 5 In the **General** tab, click **Update Firmware**.

Step 6 In the **Update Firmware** dialog box, do the following:

a) From the **Version** drop-down list, select the firmware version to which you want to update the endpoint.

b) (Optional) If you want to update the firmware regardless of any possible incompatibilities or currently executing tasks, check the **Ignore Compatibility Check** check box.

c) Click **OK**.
If the service profile for the server includes a host firmware package, Cisco UCS Manager cannot update the adapter firmware for that server. After you acknowledge the notification message, Cisco UCS Manager updates the firmware for all other endpoints on servers that do not have associated host firmware packages. If you want to update the adapter firmware for a server directly, you must remove all host firmware packages from the associated service profiles. Removing the adapter firmware from the host firmware package is not sufficient to enable you to update the adapters directly.

Cisco UCS Manager copies the selected firmware package to the backup memory slot, where it remains until you explicitly activate it.

Step 7 (Optional) Monitor the status of the update in the **Update Status** area.
The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Firmware** area of the **General** tab.

What to Do Next

Activate the firmware.

Activating the Firmware on an Adapter

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.

Step 3 Expand the node for the server that includes the adapter for which you want to activate the updated firmware.

Step 4 Expand **Interface Cards** and select the interface card for the adapter.

Step 5 In the **General** tab, click **Activate Firmware**.

Step 6 In the **Activate Firmware** dialog box, do the following:

a) Select the appropriate version from the **Version To Be Activated** drop-down list.
If one or more of the selected endpoints are not configured with the desired version as the backup version, Cisco UCS Manager GUI does not display that version in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

b) (Optional) If you want to activate the firmware regardless of any possible incompatibilities or currently executing tasks, check the **Ignore Compatibility Check** check box.

c) If you want to set the start up version and not change the version running on the endpoint, check the **Set Startup Version Only** check box.
During a direct upgrade, you should configure **Set Startup Version Only** for an adapter. With this setting, the activated firmware moves into the pending-next-boot state, and the server is not immediately rebooted. The activated firmware does not become the running version of firmware on the adapter until the server is rebooted. You cannot configure **Set Startup Version Only** for an adapter in the host firmware package.

d) Click **OK**.

Updating the CIMC Firmware on a Server

Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process has completed. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure may corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.

Step 3 Expand the node for the server for which you want to update the CIMC.

Step 4 In the **General** tab, click the **Inventory** tab.

Step 5 Click the **CIMC** tab.

Step 6 In the **Actions** area, click **Update Firmware**.

Step 7 In the **Update Firmware** dialog box, do the following:

a) From the **Version** drop-down list, select the firmware version to which you want to update the endpoint.

b) (Optional) If you want to update the firmware regardless of any possible incompatibilities or currently executing tasks, check the **Ignore Compatibility Check** check box.

c) Click **OK**.

Cisco UCS Manager copies the selected firmware package to the backup memory slot, where it remains until you explicitly activate it.

Step 8 (Optional) Monitor the status of the update in the **Update Status** area.
The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Firmware** area of the **General** tab.

What to Do Next

Activate the firmware.

Activating the CIMC Firmware on a Server

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.

Step 3 Expand the node for the server that includes the CIMC for which you want to activate the updated firmware.

Step 4 On the **General** tab, click the **Inventory** tab.

Step 5 Click the **CIMC** tab.

Step 6 In the **Actions** area, click **Activate Firmware**.

Step 7 In the **Activate Firmware** dialog box, do the following:

a) Select the appropriate version from the **Version To Be Activated** drop-down list.
If one or more of the selected endpoints are not configured with the desired version as the backup version, Cisco UCS Manager GUI does not display that version in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

b) (Optional) If you want to activate the firmware regardless of any possible incompatibilities or currently executing tasks, check the **Ignore Compatibility Check** check box.

c) If you want to set the start up version and not change the version running on the endpoint, check the **Set Startup Version Only** check box.
If you configure **Set Startup Version Only**, the activated firmware moves into the pending-next-reboot state and the endpoint is not immediately rebooted. The activated firmware does not become the running version of firmware until the endpoint is rebooted.

d) Click **OK**.

Updating the Firmware on an IOM

Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process has completed. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure may corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ IO Modules**.

Step 3 Click the I/O module that you want to update.

Step 4 In the **General** tab, click **Update Firmware**.

Step 5 In the **Update Firmware** dialog box, do the following:

a) From the **Version** drop-down list, select the firmware version to which you want to update the endpoint.

b) (Optional) If you want to update the firmware regardless of any possible incompatibilities or currently executing tasks, check the **Ignore Compatibility Check** check box.

c) Click **OK**.

Cisco UCS Manager copies the selected firmware package to the backup memory slot, where it remains until you explicitly activate it.

Step 6 (Optional) Monitor the status of the update in the **Update Status** area.
The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Firmware** area of the **General** tab.

What to Do Next

Activate the firmware.

Activating the Firmware on an IOM

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ IO Modules**.

Step 3 Select the **IO Module** node that includes the I/O module for which you want to activate the updated firmware.

Step 4 In the **General** tab, click **Activate Firmware**.

Step 5 In the **Activate Firmware** dialog box, do the following:

a) Select the appropriate version from the **Version To Be Activated** drop-down list.
If one or more of the selected endpoints are not configured with the desired version as the backup version, Cisco UCS Manager GUI does not display that version in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

b) (Optional) If you want to activate the firmware regardless of any possible incompatibilities or currently executing tasks, check the **Ignore Compatibility Check** check box.

c) If you want to set the start up version and not change the version running on the endpoint, check the **Set Startup Version Only** check box.
If you configure **Set Startup Version Only**, the activated firmware moves into the pending-next-reboot state and the endpoint is not immediately rebooted. The activated firmware does not become the running version of firmware until the endpoint is rebooted.

d) Click **OK**.

Activating the Board Controller Firmware on a Server

Only certain servers, such as the Cisco UCS B440 High Performance blade server and the Cisco UCS B230 blade server, have board controller firmware. The board controller firmware controls many of the server functions, including eUSBs, LEDs, and I/O connectors.

Note This activation procedure causes the server to reboot. Depending upon whether or not the service profile associated with the server includes a maintenance policy, the reboot can occur immediately. To reduce the number of times a server needs to be rebooted during the upgrade process, we recommend that you upgrade the board controller firmware through the host firmware package in the service profile.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 On the **Installed Firmware** subtab, click **Activate Firmware**.

Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS instance. This step may take a few minutes, depending upon the number of chassis and servers.

Step 5 From the **Filter** drop-down list on the menu bar of the **Activate Firmware** dialog box, select **Board Controller**. Cisco UCS Manager GUI displays all servers that have board controllers in the **Activate Firmware** dialog box.

Step 6 From the drop-down list in the **Startup Version** column, select the version to which you want to update the software.

Step 7 If you want to activate the firmware regardless of any possible incompatibilities or currently executing tasks, check the **Ignore Compatibility Check** check box.

Step 8 Click **OK**.

Activating the Cisco UCS Manager Software

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 On the **Installed Firmware** subtab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS instance. This step may take a few minutes, depending upon the number of chassis and servers.

Step 5 On the **UCS Manager** row of the **Activate Firmware** dialog box, do the following:

a) From the drop-down list in the **Startup Version** column, select the version to which you want to update the software.

b) (Optional) If you want to activate the firmware regardless of any possible incompatibilities or currently executing tasks, check the **Ignore Compatibility Check** check box.

c) Click **OK**.

Cisco UCS Manager makes the selected version the startup version and schedules the activation to occur when the fabric interconnects are upgraded.

Activating the Firmware on a Subordinate Fabric Interconnect

Before You Begin

Determine which fabric interconnect in the cluster is the subordinate fabric interconnect.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 On the **Installed Firmware** subtab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS instance. This step may take a few minutes, depending upon the number of chassis and servers.

Step 5 From the **Filter** drop-down list on the menu bar, choose **Fabric Interconnects**.

Step 6 On the menu bar, check the **Ignore Compatibility Check** check box.

Step 7 On the row of the **Activate Firmware** dialog box for the subordinate fabric interconnect, do the following:

a) In the **Kernel** row, choose the firmware version to which you want to upgrade from the drop-down list in the **Startup Version** column.

b) In the **System** row, choose the firmware version to which you want to upgrade from the drop-down list in the **Startup Version** column.

Step 8 Click **Apply**.
Cisco UCS Manager updates and activates the firmware and reboots the fabric interconnect and any I/O module in the data path to that fabric interconnect, disrupting data traffic to and from that fabric interconnect. However, assuming the Cisco UCS instance is configured to permit traffic and port failover, data traffic fails over to the primary fabric interconnect and is not disrupted.

Step 9 Verify the high availability status of the subordinate fabric interconnect.
If the **High Availability Details** area for the fabric interconnect does not show the following values, contact Cisco Technical Support immediately. Do not continue to update the primary fabric interconnect.

Field Name	Required Value
Ready field	**Yes**
State field	**Up**

What to Do Next

If the high availability status of the subordinate fabric interconnect contains the required values, update and activate the primary fabric interconnect.

Activating the Firmware on a Primary Fabric Interconnect

This procedure continues directly from Activating the Firmware on a Subordinate Fabric Interconnect, page 177 and assumes you are on the **Firmware Management** tab.

Before You Begin

Activate the subordinate fabric interconnect.

Procedure

Step 1 On the **Installed Firmware** subtab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS instance. This step may take a few minutes, depending upon the number of chassis and servers.

Step 2 From the **Filter** drop-down list on the menu bar, choose **Fabric Interconnects**.

Step 3 On the menu bar, check the **Ignore Compatibility Check** check box.

Step 4 On the row of the **Activate Firmware** dialog box for the subordinate fabric interconnect, do the following:

a) In the **Kernel** row, choose the firmware version to which you want to upgrade from the drop-down list in the **Startup Version** column.
b) In the **System** row, choose the firmware version to which you want to upgrade from the drop-down list in the **Startup Version** column.

Step 5 Click **Apply**.
Cisco UCS Manager updates and activates the firmware and reboots the fabric interconnect and any I/O module in the data path to that fabric interconnect, disrupting data traffic to and from that fabric interconnect. However, assuming the Cisco UCS instance is configured to permit traffic and port failover, data traffic fails over to the other fabric interconnect, which becomes the primary. When it comes back up, this fabric interconnect is the subordinate fabric interconnect.

Step 6 Verify the high availability status of the fabric interconnect.
If the **High Availability Details** area for the fabric interconnect does not show the following values, contact Cisco Technical Support immediately.

Field Name	Required Value
Ready field	**Yes**
State field	**Up**

Activating the Firmware on a Standalone Fabric Interconnect

For a standalone configuration with a single fabric interconnect, you can minimize the disruption to data traffic when you perform a direct firmware upgrade of the endpoints. However, you must reboot the fabric interconnect to complete the upgrade and, therefore, cannot avoid disrupting traffic.

Tip If you ever need to recover the password to the admin account that was created when you configured the fabric interconnects for the Cisco UCS instance, you must know the running kernel version and the running system version. If you do not plan to create additional accounts, we recommend that you save the path to these firmware versions in a text file so that you can access them if required.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, click the **Equipment** node.

Step 3 Expand the **Fabric Interconnects** node and click the standalone fabric interconnect.

Step 4 On the **General** tab, click **Activate Firmware**.

Step 5 In the **Activate Firmware** dialog box, complete the following fields:

Name	Description
Kernel Version drop-down list	Choose the version that you want to use for the kernel.
System Version drop-down list	Choose the version you want to use for the system.
Ignore Compatibility Check check box	By default, Cisco UCS makes sure that the firmware version is compatible with everything running on the server before it activates that version. Check this check box if you want Cisco UCS to activate the firmware without making sure that it is compatible first. **Note** We recommend that you use this option only when explicitly directed to do so by a technical support representative.

Step 6 Click **OK**.

Cisco UCS Manager activates the firmware and reboots the fabric interconnect and any I/O module in the data path to that fabric interconnect. For a standalone fabric interconnect, this disrupts all data traffic in the Cisco UCS instance.

Updating Firmware through Service Profiles

Host Firmware Package

This policy enables you to specify a set of firmware versions that make up the host firmware package (also known as the host firmware pack). The host firmware includes the following firmware for server and adapter endpoints:

- **Adapter**
- **BIOS**
- **Board Controller**
- **FC Adapters**
- **HBA Option ROM**
- **Storage Controller**

Tip You can include more than one type of firmware in the same host firmware package. For example, a host firmware package can include both BIOS firmware and storage controller firmware or adapter firmware for two different models of adapters. However, you can only have one firmware version with the same type, vendor, and model number. The system recognizes which firmware version is required for an endpoint and ignores all other firmware versions.

The firmware package is pushed to all servers associated with service profiles that include this policy.

This policy ensures that the host firmware is identical on all servers associated with service profiles which use the same policy. Therefore, if you move the service profile from one server to another, the firmware versions are maintained. Also, if you change the firmware version for an endpoint in the firmware package, new versions are applied to all the affected service profiles immediately, which could cause server reboots.

You must include this policy in a service profile, and that service profile must be associated with a server for it to take effect.

Prerequisites

This policy is not dependent upon any other policies. However, you must ensure that the appropriate firmware has been downloaded to the fabric interconnect. If the firmware image is not available when Cisco UCS Manager is associating a server with a service profile, Cisco UCS Manager ignores the firmware upgrade and completes the association.

Creating a Host Firmware Package

Tip You can include more than one type of firmware in the same host firmware package. For example, a host firmware package can include both BIOS firmware and storage controller firmware or adapter firmware for two different models of adapters. However, you can only have one firmware version with the same type, vendor, and model number. The system recognizes which firmware version is required for an endpoint and ignores all other firmware versions.

Before You Begin

Ensure that the appropriate firmware has been downloaded to the fabric interconnect.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **Host Firmware Packages** and choose **Create Package**.

Step 5 In the **Create Host Firmware Package** dialog box, enter a unique name and description for the package. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

Step 6 On each sub-tab, do the following for each type of firmware you want to include in the package:

a) In the **Select** column, ensure that the check box for the appropriate lines are checked.
b) In the **Vendor**, **Model**, and **PID** columns, verify that the information matches the servers you want to update with this package.
The model and model number (PID) must match the servers that are associated with this firmware package. If you select the wrong model or model number, Cisco UCS Manager cannot install the firmware update.
c) In the **Version** column, choose the firmware version to which you want to update the firmware.

Step 7 When you have added all the desired firmware to the package, click **OK**.

What to Do Next

Include the policy in a service profile and/or template.

Updating a Host Firmware Package

If the policy is included in one or more service profiles associated with a server and those service profiles do not include maintenance policies, Cisco UCS Manager updates and activates the firmware in the server and adapter with the new versions and reboots the server as soon as you save the host firmware package policy.

Before You Begin

Ensure that the appropriate firmware has been downloaded to the fabric interconnect.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.
Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.
Step 3 Expand the node for the organization that includes the policy you want to update.
If the system does not include multi-tenancy, expand the **root** node.
Step 4 Expand **Host Firmware Packages** and choose the policy you want to update.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 On each sub-tab, do the following for each type of firmware you want to include in the package:
a) In the **Select** column, ensure that the check box for the appropriate lines are checked.
b) In the **Vendor**, **Model**, and **PID** columns, verify that the information matches the servers you want to update with this package.
The model and model number (PID) must match the servers that are associated with this firmware package. If you select the wrong model or model number, Cisco UCS Manager cannot install the firmware update.
c) In the **Version** column, choose the firmware version to which you want to update the firmware.
Step 7 Click **Save Changes**.
Cisco UCS Manager verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS Manager updates the firmware according to the settings in the maintenance policies included in the service profiles.

Management Firmware Package

This policy enables you to specify a set of firmware versions that make up the management firmware package (also known as a management firmware pack). The management firmware package includes the Cisco Integrated Management Controller (CIMC) on the server. You do not need to use this package if you upgrade the CIMC directly.

The firmware package is pushed to all servers associated with service profiles that include this policy. This policy ensures that the CIMC firmware is identical on all servers associated with service profiles which use the same policy. Therefore, if you move the service profile from one server to another, the firmware versions are maintained.

You must include this policy in a service profile, and that service profile must be associated with a server for it to take effect.

This policy is not dependent upon any other policies. However, you must ensure that the appropriate firmware has been downloaded to the fabric interconnect.

Creating a Management Firmware Package

Before You Begin

Ensure that the appropriate firmware has been downloaded to the fabric interconnect.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **Management Firmware Packages** and select **Create Package**.

Step 5 In the **Create Management Firmware Package** dialog box, enter a unique name and description for the package.
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

Step 6 In the firmware table, do the following:

a) In the **Select** column, ensure that the check box for the appropriate lines are checked.

b) In the **Vendor**, **Model**, and **PID** columns, verify that the information matches the servers you want to update with this package.
The model and model number (PID) must match the servers that are associated with this firmware package. If you select the wrong model or model number, Cisco UCS Manager cannot install the firmware update.

c) In the **Version** column, choose the firmware version to which you want to update the firmware.

Step 7 When you have added the desired firmware to the package, click **OK**.

What to Do Next

Include the policy in a service profile and/or template.

Updating a Management Firmware Package

If the policy is included in one or more service profiles associated with a server and those service profiles do not include maintenance policies, Cisco UCS Manager updates and activates the management firmware in the server with the new versions and reboots the server as soon as you save the management firmware package policy

Before You Begin

Ensure that the appropriate firmware has been downloaded to the fabric interconnect.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.

Step 3 Expand the node for the organization that includes the policy you want to update.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Expand **Management Firmware Packages** and choose the policy you want to update.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the firmware table, do the following:

a) In the **Select** column, ensure that the check box for the appropriate lines are checked.

b) In the **Vendor**, **Model**, and **PID** columns, verify that the information matches the servers you want to update with this package.
The model and model number (PID) must match the servers that are associated with this firmware package. If you select the wrong model or model number, Cisco UCS Manager cannot install the firmware update.

c) In the **Version** column, choose the firmware version to which you want to update the firmware.

Step 7 Click **Save Changes**.
Cisco UCS Manager verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS Manager updates the firmware according to the settings in the maintenance policies included in the service profiles.

Adding Firmware Packages to an Existing Service Profile

If the service profile does not include a maintenance policy and is associated with a server, Cisco UCS Manager updates and activates the firmware in the server with the new versions and reboots the server as soon as you save the changes to the service profile.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization that includes the service profile that you want to update.

If the system does not include multi-tenancy, expand the **root** node.

Step 4 Click the service profile to which you want to add the firmware packages.

Step 5 In the **Work** pane, click the **Policies** tab.

Step 6 Click the down arrows to expand the **Firmware Policies** section.

Step 7 To add a host firmware package, select the desired policy from the **Host Firmware** drop-down list.

Step 8 To add a management firmware package, select the desired policy from the **Management Firmware** drop-down list.

Step 9 Click **Save Changes**.

Verifying Firmware Versions on Components

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 On the **Installed Firmware** tab, review the firmware versions listed for each component.

Managing the Capability Catalog

Capability Catalog

The capability catalog is a set of tunable parameters, strings, and rules. Cisco UCS Manager uses the catalog to update the display and configurability of components such as newly qualified DIMMs and disk drives for servers.

The catalog is divided by hardware components, such as the chassis, CPU, local disk, and I/O module. You can use the catalog to view the list of providers available for that component. There is one provider per hardware component. Each provider is identified by the vendor, model (PID), and revision. For each provider, you can also view details of the equipment manufacturer and the form factor.

Contents of the Capability Catalog

The contents of the capability catalog include the following:

Implementation-Specific Tunable Parameters	• Power and thermal constraints • Slot ranges and numbering • Adapter capacities

Hardware-Specific Rules	• Firmware compatibility for components such as the BIOS, CIMC, RAID controller, and adapters • Diagnostics • Hardware-specific reboot
User Display Strings	• Part numbers, such as the CPN, PID/VID • Component descriptions • Physical layout/dimensions • OEM information

Updates to the Capability Catalog

Capability catalog updates are included in each Cisco UCS Manager update. Unless otherwise instructed by Cisco Technical Support, you only need to activate the capability catalog update after you've downloaded, updated, and activated an Cisco UCS Infrastructure Software Bundle.

As soon as you activate a capability catalog update, Cisco UCS Manager immediately updates to the new baseline catalog. You do not have to perform any further tasks. Updates to the capability catalog do not require you to reboot any component in the Cisco UCS instance or to reinstall Cisco UCS Manager.

Each Cisco UCS Manager release contains a baseline catalog. In rare circumstances, Cisco releases an update to the capability catalog and makes it available on the same site where you download firmware images. The catalog update is compatible with Cisco UCS, Release 1.3(1) and later.

Activating a Capability Catalog Update

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All**.

Step 3 Click the **Capability Catalog** node.

Step 4 In the **Work** pane, click the **Catalog Update Tasks** tab.

Step 5 Click **Activate Catalog**.

Step 6 In the **Activate Catalog** dialog box, choose the capability catalog update that you want to activate from the **Version to be Activated** drop-down list.

Step 7 Click **OK**.

Verifying that the Capability Catalog Is Current

Before You Begin

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All**.

Step 3 Click the **Capability Catalog** node.

Step 4 In the **Work** pane, click the **Catalog Update Tasks** tab.
The current version of the capability catalog is located on the upper right of that tab.

Step 5 On Cisco.com, determine the most recent release of the capability catalog available.
For more information about the location of capability catalog updates, see Obtaining Capability Catalog Updates from Cisco, page 188.

Step 6 If a more recent version of the capability catalog is available on Cisco.com, update the capability catalog with that version.

Viewing a Capability Catalog Provider

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All** ➤ **Capability Catalog**.

Step 3 In the **Work** pane, click the tab for the provider you want to view.

Step 4 To view the details of a provider, do the following:

a) In the table, click the row with the vendor, model, and revision of the provider you want to view.

b) Click the **Expand** icon to the right of the heading to display the properties for the following areas:

- **Equipment Manufacturing** area
- **Form Factor** area

Downloading Individual Capability Catalog Updates

Obtaining Capability Catalog Updates from Cisco

Procedure

Step 1 In a web browser, navigate to http://www.cisco.com.

Step 2 Under **Support**, click **Download Software**.

Step 3 Click **Unified Computing**.

Step 4 If prompted, enter your Cisco.com username and password to log in.

Step 5 Click **Cisco UCS Manager Capability Catalog Software ➤ Unified Computing System (UCS) Manager Capability Catalog**.

Step 6 Click the link for the latest release of the capability catalog.

Step 7 Click one of the following buttons and follow the instructions provided:

- **Download Now**—Allows you to download the catalog update immediately
- **Add to Cart**—Adds the catalog update to your cart to be downloaded at a later time

Step 8 Follow the prompts to complete your download of the catalog update.

What to Do Next

Update the capability catalog.

Updating the Capability Catalog from a Remote Location

You cannot perform a partial update to the capability catalog. When you update the capability catalog, all components included in the catalog image are updated.

A B-series server bundle includes the capability catalog update for that server. You do not need to download a separate capability catalog update. You only need to activate the capability catalog update.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All**.

Step 3 Click the **Capability Catalog** node.

Step 4 In the **Work** pane, click the **Catalog Update Tasks** tab.

Step 5 Click **Update Catalog**.

Step 6 In the **Update Catalog** dialog box, click the **Remote File System** radio button in the **Location of the Image File** field.

Step 7 Complete the following fields:

Name	Description
Protocol field	The protocol to use when communicating with the remote server. This can be: • **FTP** • **TFTP** • **SCP** • **SFTP**
Server field	The IP address or hostname of the remote server on which the catalog image resides.
Filename field	The name of the catalog executable you want to download.
Path field	The absolute path to the catalog image file on the remote server, if required. If you use SCP, the absolute path is always required. If you use any other protocol, you may not need to specify a remote path if the file resides in the default download folder. For details about how your file server is configured, contact your system administrator.
User field	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP.
Password field	The password for the remote server username. This field does not apply if the protocol is TFTP.

Step 8 Click **OK**.

Cisco UCS Manager downloads the image and updates the capability catalog. You do not need to reboot any hardware components.

What to Do Next

Activate the capability catalog update.

Updating the Capability Catalog from the Local File System

You cannot perform a partial update to the capability catalog. When you update the capability catalog, all components included in the catalog image are updated.

A B-series server bundle includes the capability catalog update for that server. You do not need to download a separate capability catalog update. You only need to activate the capability catalog update.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All**.

Step 3 Click the **Capability Catalog** node.

Step 4 In the **Work** pane, click the **Catalog Update Tasks** tab.

Step 5 Click **Update Catalog**.

Step 6 In the **Download Firmware** dialog box, click the **Local File System** radio button in the **Location of the Image File** field.

Step 7 In the **Filename** field, type the full path and and name of the image file.
If you do not know the exact path to the folder where the firmware image file is located, click **Browse** and navigate to the file.

Step 8 Click **OK**.

Cisco UCS Manager downloads the image and updates the capability catalog. You do not need to reboot any hardware components.

What to Do Next

Activate the capability catalog update.

Updating Management Extensions

Management Extensions

Management extension updates are included in each Cisco UCS Manager update. Unless otherwise instructed by Cisco Technical Support, you only need to activate the management extension update after you've downloaded, updated, and activated an Cisco UCS Infrastructure Software Bundle.

Management extensions enable you to add support for previously unsupported servers and other hardware to Cisco UCS Manager. For example, you may need to activate a management extension if you want to add a new, previously unsupported server to an existing Cisco UCS instance.

The management extension image contains the images, information, and firmware required by Cisco UCS Manager to be able to manage the new hardware.

Cisco UCS Manager may need to access a management extension when you activate. Therefore, the management extension is locked during the activation and update process.

Activating a Management Extension

The management extension is included in the server bundle that you have already downloaded. You do not need to download the management extension separately.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All**.

Step 3 Click the **Management Extension** node.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Activate Management Extension**.

Step 6 In the **Activate Management Extension** dialog box, choose the management extension that you want to activate from the **Version to be Activated** drop-down list.

Step 7 Click **OK**.

CHAPTER 11

Configuring DNS Servers

This chapter includes the following sections:

DNS Servers in Cisco UCS

You need to specify an external DNS server for each Cisco UCS instance to use if the system requires name resolution of hostnames. For example, you cannot use a name such as www.cisco.com when you are configuring a setting on a fabric interconnect if you do not configure a DNS server. You would need to use the IP address of the server.

Adding a DNS Server

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.

Step 3 Click **DNS Management**.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **DNS Server** area, click +.

Step 6 In the **Specify DNS Server** dialog box, enter the IP address of the DNS server.

Step 7 Click **OK**.

Deleting a DNS Server

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.

Step 3 Click **DNS Management**.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **DNS Server** area, right-click the DNS server you want to delete and choose **Delete**.

Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 7 Click **Save Changes**.

CHAPTER 12

Configuring System-Related Policies

This chapter includes the following sections:

Configuring the Chassis Discovery Policy

Chassis Discovery Policy

The chassis discovery policy determines how the system reacts when you add a new chassis. Cisco UCS Manager uses the settings in the chassis discovery policy to determine the minimum threshold for the number of links between the chassis and the fabric interconnect. However, the configuration in the chassis discovery policy does not prevent you from connecting multiple chassis to the fabric interconnects in a Cisco UCS instance and wiring those chassis with a different number of links.

If you have a Cisco UCS instance that has some chassis wired with 1 link, some with 2 links, and some with 4 links, we recommend that you configure the chassis discovery policy for the minimum number links in the instance so that Cisco UCS Manager can discover all chassis. After the initial discovery, you must reacknowledge the chassis that are wired for a greater number of links and Cisco UCS Manager configures the chassis to use all available links.

Cisco UCS Manager cannot discover any chassis that is wired for fewer links than are configured in the chassis discovery policy. For example, if the chassis discovery policy is configured for 4 links, Cisco UCS Manager cannot discover any chassis that is wired for 1 link or 2 links. Reacknowledgement of the chassis does not resolve this issue.

The following table provides an overview of how the chassis discovery policy works in a multi-chassis Cisco UCS instance:

Table 7: Chassis Discovery Policy and Chassis Links

Number of Links Wired for the Chassis	1-Link Chassis Discovery Policy	2-Link Chassis Discovery Policy	4-Link Chassis Discovery Policy
1 link between IOM and fabric interconnects	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS instance as a chassis wired with 1 link.	Chassis cannot be discovered by Cisco UCS Manager and is not added to the Cisco UCS instance.	Chassis cannot be discovered by Cisco UCS Manager and is not added to the Cisco UCS instance.
2 links between IOM and fabric interconnects	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS instance as a chassis wired with 1 link. After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS instance as a chassis wired with 2 link.	Chassis cannot be discovered by Cisco UCS Manager and is not added to the Cisco UCS instance.
4 links between IOM and fabric interconnects	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS instance as a chassis wired with 1 link. After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS instance as a chassis wired with 2 links. After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS instance as a chassis wired with 4 link.

Configuring the Chassis Discovery Policy

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, click the **Equipment** node.

Step 3 In the **Work** pane, click the **Policies** tab.

Step 4 Click the **Global Policies** subtab.

Step 5 In the **Chassis Discovery Policy** area, choose the number of links to be used by the chassis from the **Action** drop-down list.

Step 6 Click **Save Changes**.

Configuring the Rack Server Discovery Policy

Rack Server Discovery Policy

The rack server discovery policy determines how the system reacts when you add a new rack-mount server. Cisco UCS Manager uses the settings in the rack server discovery policy to determine whether any data on the hard disks are scrubbed and whether server discovery occurs immediately or needs to wait for explicit user acknowledgement.

Cisco UCS Manager cannot discover any rack-mount server that has not been correctly cabled and connected to the fabric interconnects. For information about how to integrate a supported Cisco UCS rack-mount server with Cisco UCS Manager, see the hardware installation guide for that server.

Configuring the Rack Server Discovery Policy

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, click the **Equipment** node.

Step 3 In the **Work** pane, click the **Policies** tab.

Step 4 Click the **Global Policies** subtab.

Step 5 In the **Rack Server Discovery Policy** area, complete the following fields:

Name	Description
Action field	The way the system reacts when you add a new rack-mount server. This can be: • **immediate**—The system attempts to discover new servers automatically • **user-acknowledged**—The system waits until the user tells it to search for new servers
Scrub Policy drop-down list	The scrub policy to run on a newly discovered server if that server meets the criteria in the selected server pool policy qualification.

Step 6 Click **Save Changes**.

Configuring the Aging Time for the MAC Address Table

Aging Time for the MAC Address Table

To efficiently switch packets between ports, the fabric interconnect maintains a MAC address table. It dynamically builds the MAC address table by using the MAC source address from the packets received and the associated port on which the packets were learned. The fabric interconnect uses an aging mechanism, defined by a configurable aging timer, to determine how long an entry remains in the MAC address table. If an address remains inactive for a specified number of seconds, it is removed from the MAC address table.

You can configure the amount of time (age) that a MAC address entry (MAC address and associated port) remains in the MAC address table.

Configuring the Aging Time for the MAC Address Table

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, click the **Equipment** node.

Step 3 In the **Work** pane, click the **Policies** tab.

Step 4 Click the **Global Policies** subtab.

Step 5 In the **MAC Address Table Aging** area, complete the following fields:

Name	Description
Aging Time field	The length of time an idle MAC address remains in the MAC address table before it is removed by Cisco UCS. This can be: • **never**—MAC addresses are never removed from the table regardless of how long they have been idle. • **mode-default**—The system uses the default value. If the fabric interconnect is set to end-host mode, the default is 14,500 seconds. If it is set to switching mode, the default is 300 seconds. • **other**—Cisco UCS Manager GUI displays the **dd:hh:mm:ss** field which allows you to enter a custom value.
dd:hh:mm:ss field	The length of time a MAC address must remain idle before Cisco UCS removes it from the MAC address table. This field is only visible if you choose **other** for the aging time. Enter a time in the format days:hours:minutes:seconds.

Step 6 Click **Save Changes**.

CHAPTER 13

Managing Licenses

This chapter includes the following sections:

Licenses

Port licenses for each Cisco UCS fabric interconnect are factory installed and shipped with the hardware. At a minimum, each fabric interconnect ships with the following counted licenses pre-installed:

- Cisco UCS 6120XP fabric interconnect—pre-installed licenses for the first eight Ethernet ports enabled in Cisco UCS Manager and any Fibre Channel ports on expansion modules
- Cisco UCS 6140XP fabric interconnect—pre-installed licenses for the first sixteen Ethernet ports enabled in Cisco UCS Manager and any Fibre Channel ports on expansion modules

Port licenses are not bound to physical ports. When you disable a licensed port, that license is then retained for use with the next enabled port.

If you want to use additional fixed ports, you must purchase and install licenses for those ports.

Grace Period

If you attempt to use a port that does not have an installed license, Cisco UCS initiates a 120 day grace period. The grace period is measured from the first use of the port without a license and is paused when a valid license file is installed. The amount of time used in the grace period is retained by the system.

Note Each physical port has its own grace period. Initiating the grace period on a single port does not initiate the grace period for all ports.

If a licensed port is unconfigured, that license is transferred to a port functioning within a grace period. If multiple ports are acting within grace periods, the license is moved to the port whose grace period is closest to expiring.

High Availability Configurations

To avoid inconsistencies during failover, we recommend that both fabric interconnects in the cluster have the same number of ports licensed. If symmetry is not maintained and failover occurs, Cisco UCS enables the missing licenses and initiates the grace period for each port being used on the failover node.

Obtaining the Host ID for a Fabric Interconnect

The host ID is also known as the serial number.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Fabric Interconnects**.

Step 3 Click the node for the fabric interconnect for which you want to obtain the host ID.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Properties** area, the host ID is listed in the **Serial Number (SN)** field.

What to Do Next

Obtain the required licenses from Cisco.

Determining the Grace Period Available for a Port or Feature

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All ➤ License Management**.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 Click a feature in the table to view the following details, including the used grace period, of that feature in the **General** tab below:

Name	Description
Name field	The name of the feature to which the license applies.
Scope field	The fabric associated with the license.
Absolute Quantity field	The total number of licenses available. This value is the sum of the number of default licenses plus the number of purchased licenses.
Used Quantity field	The number of licenses currently being used by the system. If this value exceeds the total number of licenses available, then some ports will stop functioning after their associated grace period expires.
Default Quantity field	The default number of licenses provided for this Cisco UCS instance.
Operational State field	The operational state of the license.
Grace Period Used field	The number of grace period days that this license has used. After the grace period ends, Cisco UCS disables the feature until a new license is purchased. To view the total number of grace period days available, see the **Grace Period** column in the License table.
Peer Status field	If this field displays **matching**, than the license is installed on both fabrics.

Obtaining a License

Note This process may change after the release of this document. If one or more of these steps no longer applies, contact your Cisco representative for information on how to obtain a license file.

Before You Begin

Obtain the following:

- Host ID or serial number for the fabric interconnect
- Claim certificate or other proof of purchase document for the fabric interconnect or expansion module

Procedure

Step 1 Obtain the product authorization key (PAK) from the claim certificate or other proof of purchase document.

Step 2 Locate the website URL in the claim certificate or proof of purchase document.

Step 3 Access the website URL for the fabric interconnect and enter the serial number and the PAK.
Cisco sends you the license file by email. The license file is digitally signed to authorize use on only the requested fabric interconnect. The requested features are also enabled once Cisco UCS Manager accesses the license file.

What to Do Next

Install the license on the fabric interconnect.

Downloading Licenses to the Fabric Interconnect from the Local File System

Note In a cluster setup, we recommend that you download and install licenses to both fabric interconnects in matching pairs. An individual license is only downloaded to the fabric interconnect that is used to initiate the download.

Before You Begin

Obtain the required licenses from Cisco.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All ➤ License Management**.

Step 3 Click the node for the fabric interconnect to which you want to download the license.

Step 4 In the **Work** pane, click the **Download Tasks** tab.

Step 5 Click **Download License**.

Step 6 In the **Download License** dialog box, click the **Local File System** radio button in the **Location of the Image File** field.

Step 7 In the **Filename** field, type the full path and and name of the license file.
If you do not know the exact path to the folder where the license file is located, click **Browse** and navigate to the file.

Step 8 Click **OK**.
Cisco UCS Manager GUI begins downloading the license to the fabric interconnect.

Step 9 (Optional) Monitor the status of the download on the **Download Tasks** tab.

Note If Cisco UCS Manager reports that the bootflash is out of space, delete obsolete bundles on the **Packages** tab to free up space. To view the available space in bootflash, navigate to the fabric interconnect on the **Equipment** tab and expand the **Local Storage Information** area on the **General** tab.

Step 10 Repeat this task until all the required licenses have been downloaded to the fabric interconnect.

What to Do Next

After all of the download tasks have completed, install the licenses.

Downloading Licenses to the Fabric Interconnect from a Remote Location

Note In a cluster setup, we recommend that you download and install licenses to both fabric interconnects in matching pairs. An individual license is only downloaded to the fabric interconnect that is used to initiate the download.

Before You Begin

Obtain the required licenses from Cisco.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All ➤ License Management**.

Step 3 Click the node for the fabric interconnect to which you want to download the license.

Step 4 In the **Work** pane, click the **Download Tasks** tab.

Step 5 Click **Download License**.

Step 6 In the **Download License** dialog box, click the **Remote File System** radio button in the **Location of the Image File** field.

Step 7 Complete the following fields:

Name	Description
Protocol field	The protocol to use when communicating with the remote server. This can be: • **FTP** • **TFTP** • **SCP** • **SFTP**
Server field	The IP address or hostname of the remote server on which the files resides. **Note** If you use a hostname rather than an IP address, you must configure a DNS server in Cisco UCS Manager.
Filename field	The name of the license file you want to download.

Name	Description
Path field	The absolute path to the license file on the remote server, if required. If you use SCP, the absolute path is always required. If you use any other protocol, you may not need to specify a remote path if the file resides in the default download folder. For details about how your file server is configured, contact your system administrator.
User field	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP.
Password field	The password for the remote server username. This field does not apply if the protocol is TFTP.

Step 8 Click **OK**.
Cisco UCS Manager GUI begins downloading the license to the fabric interconnect.

Step 9 (Optional) Monitor the status of the download on the **Download Tasks** tab.

Note If Cisco UCS Manager reports that the bootflash is out of space, delete obsolete bundles on the **Packages** tab to free up space. To view the available space in bootflash, navigate to the fabric interconnect on the **Equipment** tab and expand the **Local Storage Information** area on the **General** tab.

Step 10 Repeat this task until all the required licenses have been downloaded to the fabric interconnect.

What to Do Next

After all of the download tasks have completed, install the licenses.

Installing a License

Before You Begin

Obtain the required licenses from Cisco.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All ➤ License Management**.

Step 3 In the **Work** pane, click the **Downloaded License Files** tab.

Step 4 Choose the license you want to install from the table.

Step 5 Click the **Install License** button.

Step 6 In the **Install License** dialog box, click **Yes**.
Cisco UCS Manager GUI installs the license and activates the unlicensed port or feature.

Viewing the Licenses Installed on a Fabric Interconnect

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All ➤ License Management**.

Step 3 In the **Work** pane, click the **Installed Licenses** tab to view the following details of all licenses installed on the fabric interconnect:

Name	Description
License File ID column	The unique identifier for the license.
Operational State column	The operational state of the license.
Operational State Description column	Details about the operational state.
Scope column	The fabric on which this license is installed.
Version column	The version of the license.
Administrative State column	The administrative state of the license.

Step 4 Click a license in the table to view the following details of that license in the **Contents** tab below:
You may need to expand the license file to view the details of individual licenses in the file.

Name	Description
Name column	A navigation tree that lets you view a particular component along with its subcomponents. You can right-click a component to view any actions available for that component.
Total Qty column	The total number of licenses available in the license package file.
Type column	The license type.
Expiry column	The date that the licenses expire.
Quantity column	The quantity of licenses of the given type in the license package file.
PAK column	
Signature column	The signature key associated with the licenses of the given type.
Vendor column	The company that issued the license package file.
Version column	The version of the license package file.

Determining the Expiry Date of a License

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, expand **All ➤ License Management**.
Step 3 In the **Work** pane, click the **Installed Licenses** tab.
Step 4 Click a license in the table to view the details of that license in the **Contents** tab below.
Step 5 In the **Contents** tab, expand the license file to view all licenses in the file.
Step 6 In the **Expiry** column, view the expiry date of the license.

Uninstalling a License

Note Permanent licenses cannot be uninstalled if they are in use. You can only uninstall a permanent license that is not in use. If you try to delete a permanent license that is being used, Cisco UCS Manager rejects the request with an error message.

Before You Begin

- Back up the Cisco UCS Manager configuration.
- Disable the feature or port associated with the license you want to uninstall.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, expand **All ➤ License Management**.
Step 3 In the **Work** pane, click the **Downloaded License Files** tab.
Step 4 Choose the license you want to install from the table.
Step 5 Click the **Install License** button.
Step 6 In the **Install License** dialog box, click **Yes**.
Cisco UCS Manager GUI clears the license from the fabric interconnect.

Cisco UCS Manager deactivates the license, removes the license from the list of licenses, and deletes the license from the fabric interconnect. In a cluster setup, you must uninstall the license from the other fabric interconnect.

PART III

Network Configuration

CHAPTER 14

Using the LAN Uplinks Manager

This chapter includes the following sections:

LAN Uplinks Manager

The LAN Uplinks Manager provides a single interface where you can configure the connections between Cisco UCS and the LAN. You can use the LAN Uplinks Manager to create and configure the following:

- Ethernet switching mode
- Uplink Ethernet ports
- Port channels
- LAN pin groups
- Named VLANs
- Server ports
- QoS system classes

Some of the configuration that you can do in the LAN Uplinks Manager can also be done in nodes on other tabs, such as the **Equipment** tab or the **LAN** tab.

Launching the LAN Uplinks Manager

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, click the **LAN** node.

Step 3 In the **Work** pane, click the **LAN Uplinks Manager** link on the **LAN Uplinks** tab.
The LAN Uplinks Manager opens in a separate window.

Changing the Ethernet Switching Mode with the LAN Uplinks Manager

Important When you change the Ethernet switching mode, Cisco UCS Manager logs you out and restarts the fabric interconnect. For a cluster configuration, Cisco UCS Manager restarts both fabric interconnects sequentially. The second fabric interconnect can take several minutes to complete the change in Ethernet switching mode and become system ready.

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.

Step 2 In the **Uplink Mode** area, click one of the following buttons:

- **Set Ethernet Switching Mode**
- **Set Ethernet End-Host Mode**

The button for the current switching mode is dimmed.

Step 3 In the dialog box, click **Yes**.
Cisco UCS Manager restarts the fabric interconnect, logs you out, and disconnects Cisco UCS Manager GUI.

Configuring a Port with the LAN Uplinks Manager

You can only configure server ports on the fixed port module. Expansion modules do not include server ports.

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.

Step 2 In the **Ports** area, click the down arrows to expand the **Unconfigured Ports** section.

Step 3 Expand **Fabric Interconnects** ➤ ***Fabric_Interconnect_Name*** .

Step 4 Expand one of the following:

- **Fixed Module**—To configure a port in the fixed module as a server port or an uplink Ethernet port.
- **Expansion Module** ***Number***—To enable a port in an expansion module as an uplink Ethernet port. You cannot configure ports in expansion modules as server ports.

If no ports are listed below the node that you expanded, all ports in that module have already been configured.

Step 5 Right-click the port that you want to configure and choose one of the following:

- **Configure as Server Port**
- **Configure as Uplink Port**

Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring Server Ports

Enabling a Server Port with the LAN Uplinks Manager

This procedure assumes that the port has been configured as a server port, but is disabled.

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.

Step 2 In the **Ports** area, click the down arrows to expand the **Server Ports** section.

Step 3 Expand **Fabric Interconnects** ➤ ***Fabric_Interconnect_Name***.

Step 4 Right-click the port that you want to enable and choose **Enable**.

Disabling a Server Port with the LAN Uplinks Manager

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.
Step 2 In the **Ports** area, click the down arrows to expand the **Server Ports** section.
Step 3 Expand **Fabric Interconnects** ➤ ***Fabric_Interconnect_Name***.
Step 4 Right-click the port that you want to disable and choose **Disable**.
Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Unconfiguring a Server Port with the LAN Uplinks Manager

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.
Step 2 In the **Ports** area, click the down arrows to expand the **Server Ports** section.
Step 3 Expand **Fabric Interconnects** ➤ ***Fabric_Interconnect_Name***.
Step 4 Right-click the port that you want to unconfigure and choose **Unconfigure**.
Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring Uplink Ethernet Ports

Enabling an Uplink Ethernet Port with the LAN Uplinks Manager

This procedure assumes that the port has been configured as an uplink Ethernet port, but is disabled.

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.
Step 2 In the **Ports and Port Channels** area, expand **Interfaces** ➤ **Fabric Interconnects** ➤ ***Fabric_Interconnect_Name***.
Step 3 Right-click the port that you want to enable and choose **Enable Interface**.
Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Disabling an Uplink Ethernet Port with the LAN Uplinks Manager

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.

Step 2 In the **Ports and Port Channels** area, expand **Interfaces ➤ Fabric Interconnects ➤ *Fabric_Interconnect_Name***.

Step 3 Right-click the port that you want to disable and choose **Disable Interfaces**.
You can select multiple ports if you want to disable more than one uplink Ethernet port.

Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

The disabled port is removed from the list of enabled interfaces and returned to the **Unconfigured Ports** list.

Unconfiguring an Uplink Ethernet Port with the LAN Uplinks Manager

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.

Step 2 In the **Ports and Port Channels** area, expand **Interfaces ➤ Fabric Interconnects ➤ *Fabric_Interconnect_Name***.

Step 3 Click the port that you want to unconfigure.
You can select multiple ports if you want to unconfigure more than one uplink Ethernet port.

Step 4 Click **Disable Interface**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

The disabled port is removed from the list of enabled interfaces and returned to the **Unconfigured Ports** list.

Configuring Uplink Ethernet Port Channels

Creating a Port Channel with the LAN Uplinks Manager

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.

Step 2 In the **Ports and Port Channels** area, click **Create Port Channel**.

Step 3 From the pop-up menu, select one of the following fabric interconnects where you want to create the port channel:

- **Fabric Interconnect A**

- **Fabric Interconnect B**

Step 4 In the **Set Port Channel Name** page of the **Create Port Channel** wizard, do the following:

a) Complete the following fields:

Name	Description
ID field	The identifier for the port channel. Enter an integer between 1 and 256. This ID cannot be changed after the port channel has been saved.
Name field	A user-defined name for the port channel. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

b) Click **Next**.

Step 5 In the **Add Ports** page of the **Create Port Channel** wizard, do the following:

a) In the **Ports** table, choose one or more ports to include in the port channel.

b) Click the **>>** button to add the ports to the **Ports in the port channel** table.
You can use the **<<** button to remove ports from the port channel.

Note Cisco UCS Manager warns you if you select a port that has been configured as a server port. You can click **Yes** in the dialog box to reconfigure that port as an uplink Ethernet port and include it in the port channel.

Step 6 Click **Finish**.

Enabling a Port Channel with the LAN Uplinks Manager

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.

Step 2 In the **Ports and Port Channels** area, expand **Port Channels ➤ Fabric Interconnects ➤ *Fabric_Interconnect_Name***.

Step 3 Right-click the port channel that you want to enable and choose **Enable Port Channel**.

Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Disabling a Port Channel with the LAN Uplinks Manager

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.

Step 2 In the **Ports and Port Channels** area, expand **Port Channels ➤ Fabric Interconnects ➤** ***Fabric_Interconnect_Name***.

Step 3 Right-click the port channel that you want to disable and choose **Disable Port Channel**.

Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Adding Ports to a Port Channel with the LAN Uplinks Manager

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.

Step 2 In the **Ports and Port Channels** area, expand **Port Channels ➤ Fabric Interconnects ➤** ***Fabric_Interconnect_Name***.

Step 3 Right-click the port channel to which you want to add ports and choose **Add Ports**.

Step 4 In the **Add Ports** dialog box, do the following:

a) In the **Ports** table, choose one or more ports to include in the port channel.

b) Click the >> button to add the ports to the **Ports in the port channel** table.
You can use the << button to remove ports from the port channel.

Note Cisco UCS Manager warns you if you select a port that has been configured as a server port. You can click **Yes** in the dialog box to reconfigure that port as an uplink Ethernet port and include it in the port channel.

Step 5 Click **OK**.

Removing Ports from a Port Channel with the LAN Uplinks Manager

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.

Step 2 In the **Ports and Port Channels** area, expand **Port Channels ➤ Fabric Interconnects ➤** ***Fabric_Interconnect_Name***.

Step 3 Expand the port channel from which you want to remove ports.

Step 4 Right-click the port you want to remove from the port channel and choose **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Deleting a Port Channel with the LAN Uplinks Manager

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.

Step 2 In the **Ports and Port Channels** area, expand **Port Channels ➤ Fabric Interconnects ➤ *Fabric_Interconnect_Name***.

Step 3 Right-click the port channel you want to delete and choose **Delete**.

Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring LAN Pin Groups

Creating a Pin Group with the LAN Uplinks Manager

In a system with two fabric interconnects, you can associate the pin group with only one fabric interconnect or with both fabric interconnects.

Before You Begin

Configure the ports and port channels with which you want to configure the pin group. You can only include ports and port channels configured as uplink ports in a LAN pin group.

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.

Step 2 In the **Ports and Port Channels** area, click **Create Pin Group**.

Step 3 In the **Create LAN Pin Group** dialog box, enter a unique name and description for the pin group.

Step 4 To pin traffic for fabric interconnect A, do the following in the **Targets** area:

a) Check the **Fabric Interconnect A** check box.

b) Click the drop-down arrow on the **Interface** field and navigate through the tree-style browser to select the port or port channel you want to associate with the pin group.

Step 5 To pin traffic for fabric interconnect B, do the following in the **Targets** area:

a) Check the **Fabric Interconnect B** check box.

b) Click the drop-down arrow on the **Interface** field and navigate through the tree-style browser to select the port or port channel you want to associate with the pin group.

Step 6 Click **OK**.

What to Do Next

Include the pin group in a vNIC template.

Deleting a Pin Group with the LAN Uplinks Manager

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.

Step 2 In the **Pin Groups** area, right-click the pin group you want to delete and choose **Delete**.

Step 3 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring Named VLANs

Creating a Named VLAN with the LAN Uplinks Manager

In a Cisco UCS instance with two switches, you can create a named VLAN that is accessible to both switches or to only one switch.

Important You cannot create VLANs with IDs from 3968 to 4047. This range of VLAN IDs is reserved.

The VLAN name is case sensitive.

Procedure

Step 1 In the LAN Uplinks Manager, click the **VLANs** tab.

Step 2 On the icon bar to the right of the table, click +.
If the + icon is disabled, click an entry in the table to enable it.

Step 3 In the **Create VLAN** dialog box, complete the following fields:

Name	Description
VLAN Name/Prefix field	For a single VLAN, this is the VLAN name. For a range of VLANs, this is the prefix that the system uses for each VLAN name. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Configuration options	You can select: • **Common/Global**—The VLANs apply to both fabrics and use the same configuration parameters in both cases • **Fabric A**—The VLANs only apply to fabric A.

Name	Description
	• **Fabric B**—The VLAN only apply to fabric B. • **Both Fabrics Configured Differently**—The VLANs apply to both fabrics but you can specify different VLAN IDs for each fabric.
VLAN IDs field	To create one VLAN, enter a single numeric ID. To create multiple VLANs, enter individual IDs or ranges of IDs separated by commas. A VLAN ID can: • Be between 1 and 3967 • Be between 4049 and 4093 • Overlap with other VLAN IDs already defined on the system For example, to create six VLANs with the IDs 4, 22, 40, 41, 42, and 43, you would enter 4, 22, 40-43. **Important** The VLAN IDs from 3968 to 4048 are reserved. You cannot specify an ID within this range.
Sharing Type field	Whether this VLAN is subdivided into private or secondary VLANs. This can be: • **none**—This VLAN does not have any secondary or private VLANs. • **primary**—This VLAN can have one or more secondary VLANs, as shown in the **Secondary VLANs** area. • **isolated**—This is a private VLAN. The primary VLAN with which it is associated is shown in the **Primary VLAN** drop-down list.
Primary VLAN drop-down list	If the **Sharing Type** field is set to **isolated**, this is the primary VLAN associated with this private VLAN.
Check Overlap button	Click this button to determine whether the VLAN ID overlaps with any other IDs on the system.

Step 4 Click **OK**.
Cisco UCS Manager adds the VLAN to one of the following **VLANs** nodes:

- The **LAN Cloud ➤ VLANs** node for a VLAN accessible to both fabric interconnects.
- The ***Fabric_Interconnect_Name*** **➤ VLANs** node for a VLAN accessible to only one fabric interconnect.

Deleting a Named VLAN with the LAN Uplinks Manager

If Cisco UCS Manager includes a named VLAN with the same VLAN ID as the one you delete, the VLAN is not removed from the fabric interconnect configuration until all named VLANs with that ID are deleted.

Procedure

Step 1 In the LAN Uplinks Manager, click the **VLANs** tab.

Step 2 Click one of the following subtabs, depending upon what type of VLAN you want to delete:

Subtab	Description
All	Displays all VLANs in the Cisco UCS instance.
Dual Mode	Displays the VLANs that are accessible to both fabric interconnects.
Fabric A	Displays the VLANs that are accessible to only fabric interconnect A.
Fabric B	Displays the VLANs that are accessible to only fabric interconnect B.

Step 3 In the table, click the VLAN you want to delete.
You can use the Shift key or Ctrl key to select multiple entries.

Step 4 Right-click the highlighted VLAN or VLANs and select **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring QoS System Classes with the LAN Uplinks Manager

The type of adapter in a server may limit the maximum MTU supported. For example, network MTU above the maximums may cause the packet to be dropped for the following adapters:

- The Cisco UCS CNA M71KR adapter, which supports a maximum MTU of 9216.
- The Cisco UCS 82598KR-CI adapter, which supports a maximum MTU of 14000.

Procedure

Step 1 In the LAN Uplinks Manager, click the **QoS** tab.

Step 2 Update the following properties for the system class you want to configure to meet the traffic management needs of the system:

Note Some properties may not be configurable for all system classes.

Name	Description
Enabled check box	If checked, the associated QoS class is configured on the fabric interconnect and can be assigned to a QoS policy.

Name	Description
	If unchecked, the class is not configured on the fabric interconnect and any QoS policies associated with this class default to **Best Effort** or, if a system class is configured with a Cos of 0, to the Cos 0 system class. **Note** This field is always checked for **Best Effort** and **Fibre Channel**.
Cos field	The class of service. You can enter an integer value between 0 and 6, with 0 being the lowest priority and 6 being the highest priority. We recommend that you do not set the value to 0, unless you want that system class to be the default system class for traffic if the QoS policy is deleted or the assigned system class is disabled. **Note** This field is set to 7 for internal traffic and to **any** for **Best Effort**. Both of these values are reserved and cannot be assigned to any other priority.
Packet Drop check box	If checked, packet drop is allowed for this class. If unchecked, packets cannot be dropped during transmission. This field is always unchecked for the **Fibre Channel** class, which never allows dropped packets, and always checked for **Best Effort**, which always allows dropped packets.
Weight drop-down list	This can be: • An integer between 1 and 10. If you enter an integer, Cisco UCS determines the percentage of network bandwidth assigned to the priority level as described in the **Weight (%)** field. • **best-effort**. • **none**.
Weight (%) field	To determine the bandwidth allocated to a channel, Cisco UCS: **1** Adds the weights for all the channels **2** Divides the channel weight by the sum of all weights to get a percentage **3** Allocates that percentage of the bandwidth to the channel
MTU drop-down list	The maximum transmission unit for the channel. This can be: • An integer between 1500 and 9216. This value corresponds to the maximum packet size. • **fc**—A predefined packet size of 2240. • **normal**—A predefined packet size of 1500. **Note** This field is always set to **fc** for **Fibre Channel**.

Name	Description
Multicast Optimized check box	If checked, the class is optimized to send packets to multiple destinations simultaneously. **Note** This option is not applicable to the **Fibre Channel**.

Step 3 Do one of the following:

- Click **OK** to save your changes and exit from the LAN Uplinks Manager.
- Click **Apply** to save your changes without exiting from the LAN Uplinks Manager.

CHAPTER 15

Configuring Named VLANs

This chapter includes the following sections:

Named VLANs

A named VLAN creates a connection to a specific external LAN. The VLAN isolates traffic to that external LAN, including broadcast traffic.

The name that you assign to a VLAN ID adds a layer of abstraction that allows you to globally update all servers associated with service profiles that use the named VLAN. You do not need to reconfigure the servers individually to maintain communication with the external LAN.

You can create more than one named VLAN with the same VLAN ID. For example, if servers that host business services for HR and Finance need to access the same external LAN, you can create VLANs named HR and Finance with the same VLAN ID. Then, if the network is reconfigured and Finance is assigned to a different LAN, you only have to change the VLAN ID for the named VLAN for Finance.

In a cluster configuration, you can configure a named VLAN to be accessible only to one fabric interconnect or to both fabric interconnects.

Creating a Named VLAN

In a Cisco UCS instance with two switches, you can create a named VLAN that is accessible to both switches or to only one switch.

Important You cannot create VLANs with IDs from 3968 to 4047. This range of VLAN IDs is reserved.

The VLAN name is case sensitive.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, click the **LAN** node.

Step 3 In the **Work** pane, click the **VLANs** tab.

Step 4 On the icon bar to the right of the table, click +.
If the + icon is disabled, click an entry in the table to enable it.

Step 5 In the **Create VLAN** dialog box, complete the following fields:

Name	Description
VLAN Name/Prefix field	For a single VLAN, this is the VLAN name. For a range of VLANs, this is the prefix that the system uses for each VLAN name. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Configuration options	You can select: • **Common/Global**—The VLANs apply to both fabrics and use the same configuration parameters in both cases • **Fabric A**—The VLANs only apply to fabric A. • **Fabric B**—The VLAN only apply to fabric B. • **Both Fabrics Configured Differently**—The VLANs apply to both fabrics but you can specify different VLAN IDs for each fabric.
VLAN IDs field	To create one VLAN, enter a single numeric ID. To create multiple VLANs, enter individual IDs or ranges of IDs separated by commas. A VLAN ID can: • Be between 1 and 3967 • Be between 4049 and 4093 • Overlap with other VLAN IDs already defined on the system For example, to create six VLANs with the IDs 4, 22, 40, 41, 42, and 43, you would enter 4, 22, 40-43. **Important** The VLAN IDs from 3968 to 4048 are reserved. You cannot specify an ID within this range.

Name	Description
Sharing Type field	Whether this VLAN is subdivided into private or secondary VLANs. This can be: • **none**—This VLAN does not have any secondary or private VLANs. • **primary**—This VLAN can have one or more secondary VLANs, as shown in the **Secondary VLANs** area. • **isolated**—This is a private VLAN. The primary VLAN with which it is associated is shown in the **Primary VLAN** drop-down list.
Primary VLAN drop-down list	If the **Sharing Type** field is set to **isolated**, this is the primary VLAN associated with this private VLAN.
Check Overlap button	Click this button to determine whether the VLAN ID overlaps with any other IDs on the system.

Step 6 Click **OK**.
Cisco UCS Manager adds the VLAN to one of the following **VLANs** nodes:

- The **LAN Cloud ➤ VLANs** node for a VLAN accessible to both fabric interconnects.
- The ***Fabric_Interconnect_Name*** **➤ VLANs** node for a VLAN accessible to only one fabric interconnect.

Deleting a Named VLAN

If Cisco UCS Manager includes a named VLAN with the same VLAN ID as the one you delete, the VLAN is not removed from the fabric interconnect configuration until all named VLANs with that ID are deleted.

If you are deleting a private primary VLAN, make sure to reassign the secondary VLANs to another working primary VLAN.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.
Step 2 On the **LAN** tab, click the **LAN** node.
Step 3 In the **Work** pane, click the **VLANs** tab.
Step 4 Click one of the following subtabs, depending upon what type of VLAN you want to delete:

Subtab	Description
All	Displays all VLANs in the Cisco UCS instance.
Dual Mode	Displays the VLANs that are accessible to both fabric interconnects.

Subtab	Description
Fabric A	Displays the VLANs that are accessible to only fabric interconnect A.
Fabric B	Displays the VLANs that are accessible to only fabric interconnect B.

Step 5 In the table, click the VLAN you want to delete.
You can use the Shift key or Ctrl key to select multiple entries.

Step 6 Right-click the highlighted VLAN or VLANs and select **Delete**.

Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Private VLANs

A private VLAN (PVLAN) partitions the Ethernet broadcast domain of a VLAN into subdomains and allows you to isolate some ports. Each subdomain in a PVLAN includes a primary VLAN and one or more secondary VLANs. All secondary VLANs in a PVLAN must share the same primary VLAN. The secondary VLAN ID differentiates one subdomain from another.

Isolated VLANs

All secondary VLANs in a Cisco UCS instance must be isolated VLANs. Cisco UCS does not support community VLANs.

Ports on Isolated VLANs

Communications on an isolated VLAN can only use the associated port in the primary VLAN. These ports are isolated ports and are not configurable in Cisco UCS Manager. If the primary VLAN includes multiple secondary VLANs, those isolated VLANs cannot communicate directly with each other.

An isolated port is a host port that belongs to an isolated secondary VLAN. This port has complete isolation from other ports within the same private VLAN domain. PVLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports. You can have more than one isolated port in a specified isolated VLAN. Each port is completely isolated from all other ports in the isolated VLAN.

Guidelines for Uplink Ports

When you create PVLANs, be aware of the following guidelines:

- The uplink Ethernet port channel cannot be in promiscuous mode.
- Each primary VLAN can have only one isolated VLAN.
- VIFs on VNTAG adapters can have only one isolated VLAN.

Creating a Primary VLAN for a Private VLAN

In a Cisco UCS instance with two switches, you can create a named VLAN that is accessible to both switches or to only one switch.

Important You cannot create VLANs with IDs from 3968 to 4047. This range of VLAN IDs is reserved.

The VLAN name is case sensitive.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, click the **LAN** node.

Step 3 In the **Work** pane, click the **VLANs** tab.

Step 4 On the icon bar to the right of the table, click +.
If the + icon is disabled, click an entry in the table to enable it.

Step 5 In the **Create VLAN** dialog box, complete the following fields:

Name	Description
VLAN Name/Prefix field	For a single VLAN, this is the VLAN name. For a range of VLANs, this is the prefix that the system uses for each VLAN name. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Configuration options	You can select: • **Common/Global**—The VLANs apply to both fabrics and use the same configuration parameters in both cases • **Fabric A**—The VLANs only apply to fabric A. • **Fabric B**—The VLAN only apply to fabric B. • **Both Fabrics Configured Differently**—The VLANs apply to both fabrics but you can specify different VLAN IDs for each fabric.
VLAN IDs field	To create one VLAN, enter a single numeric ID. To create multiple VLANs, enter individual IDs or ranges of IDs separated by commas. A VLAN ID can: • Be between 1 and 3967 • Be between 4049 and 4093 • Overlap with other VLAN IDs already defined on the system

Name	Description
	For example, to create six VLANs with the IDs 4, 22, 40, 41, 42, and 43, you would enter 4, 22, 40-43. **Important** The VLAN IDs from 3968 to 4048 are reserved. You cannot specify an ID within this range.
Sharing Type field	Click the **primary** radio button.
Check Overlap button	Click this button to determine whether the VLAN ID overlaps with any other IDs on the system.

Step 6 Click **OK**.
Cisco UCS Manager adds the primary VLAN to one of the following **VLANs** nodes:

- The **LAN Cloud ➤ VLANs** node for a primary VLAN accessible to both fabric interconnects.
- The ***Fabric_Interconnect_Name*** **➤ VLANs** node for a primary VLAN accessible to only one fabric interconnect.

Creating a Secondary VLAN for a Private VLAN

In a Cisco UCS instance with two switches, you can create a named VLAN that is accessible to both switches or to only one switch.

Important You cannot create VLANs with IDs from 3968 to 4047. This range of VLAN IDs is reserved.

The VLAN name is case sensitive.

Before You Begin

Create the primary VLAN.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.
Step 2 On the **LAN** tab, click the **LAN** node.
Step 3 In the **Work** pane, click the **VLANs** tab.
Step 4 On the icon bar to the right of the table, click +.
If the + icon is disabled, click an entry in the table to enable it.
Step 5 In the **Create VLAN** dialog box, complete the following fields:

Name	Description
VLAN Name/Prefix field	For a single VLAN, this is the VLAN name. For a range of VLANs, this is the prefix that the system uses for each VLAN name. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Configuration options	You can select: • **Common/Global**—The VLANs apply to both fabrics and use the same configuration parameters in both cases • **Fabric A**—The VLANs only apply to fabric A. • **Fabric B**—The VLAN only apply to fabric B. • **Both Fabrics Configured Differently**—The VLANs apply to both fabrics but you can specify different VLAN IDs for each fabric.
VLAN IDs field	To create one VLAN, enter a single numeric ID. To create multiple VLANs, enter individual IDs or ranges of IDs separated by commas. A VLAN ID can: • Be between 1 and 3967 • Be between 4049 and 4093 • Overlap with other VLAN IDs already defined on the system For example, to create six VLANs with the IDs 4, 22, 40, 41, 42, and 43, you would enter 4, 22, 40-43. **Important** The VLAN IDs from 3968 to 4048 are reserved. You cannot specify an ID within this range.
Sharing Type field	Click the **isolated** radio button.
Primary VLAN drop-down list	Choose the primary VLAN to be associated with this secondary VLAN from the drop-down list.
Check Overlap button	Click this button to determine whether the VLAN ID overlaps with any other IDs on the system.

Step 6 Click **OK**.
Cisco UCS Manager adds the primary VLAN to one of the following **VLANs** nodes:

- The **LAN Cloud ➤ VLANs** node for a primary VLAN accessible to both fabric interconnects.
- The ***Fabric_Interconnect_Name*** **➤ VLANs** node for a primary VLAN accessible to only one fabric interconnect.

CHAPTER 16

Configuring LAN Pin Groups

This chapter includes the following sections:

LAN Pin Groups

Cisco UCS uses LAN pin groups to pin Ethernet traffic from a vNIC on a server to an uplink Ethernet port or port channel on the fabric interconnect. You can use this pinning to manage the distribution of traffic from the servers.

To configure pinning for a server, you must include the LAN pin group in a vNIC policy. The vNIC policy is then included in the service profile assigned to that server. All traffic from the vNIC travels through the I/O module to the specified uplink Ethernet port.

Note If you do not assign a pin group to a server interface through a vNIC policy, Cisco UCS Manager chooses an uplink Ethernet port or port channel for traffic from that server interface dynamically. This choice is not permanent. A different uplink Ethernet port or port channel may be used for traffic from that server interface after an interface flap or a server reboot.

Creating a LAN Pin Group

In a system with two fabric interconnects, you can associate the pin group with only one fabric interconnect or with both fabric interconnects.

Before You Begin

Configure the ports and port channels with which you want to configure the pin group. You can only include ports and port channels configured as uplink ports in a LAN pin group.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN ➤ LAN Cloud**.

Step 3 Right-click **LAN Pin Groups** and select **Create LAN Pin Group**.

Step 4 In the **Create LAN Pin Group** dialog box, enter a unique name and description for the pin group.

Step 5 To pin traffic for fabric interconnect A, do the following in the **Targets** area:

a) Check the **Fabric Interconnect A** check box.

b) Click the drop-down arrow on the **Interface** field and navigate through the tree-style browser to select the port or port channel you want to associate with the pin group.

Step 6 To pin traffic for fabric interconnect B, do the following in the **Targets** area:

a) Check the **Fabric Interconnect B** check box.

b) Click the drop-down arrow on the **Interface** field and navigate through the tree-style browser to select the port or port channel you want to associate with the pin group.

Step 7 Click **OK**.

What to Do Next

Include the pin group in a vNIC template.

Deleting a LAN Pin Group

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 In the **LAN** tab, expand **LAN ➤ LAN Cloud ➤ LAN Pin Groups** .

Step 3 Right-click the LAN pin group you want to delete and select **Delete**.

Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

CHAPTER 17

Configuring MAC Pools

This chapter includes the following sections:

MAC Pools

A MAC pool is a collection of network identities, or MAC addresses, that are unique in their layer 2 environment and are available to be assigned to vNICs on a server. If you use MAC pools in service profiles, you do not have to manually configure the MAC addresses to be used by the server associated with the service profile.

In a system that implements multi-tenancy, you can use the organizational hierarchy to ensure that MAC pools can only be used by specific applications or business services. Cisco UCS Manager uses the name resolution policy to assign MAC addresses from the pool.

To assign a MAC address to a server, you must include the MAC pool in a vNIC policy. The vNIC policy is then included in the service profile assigned to that server.

You can specify your own MAC addresses or use a group of MAC addresses provided by Cisco.

Creating a MAC Pool

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 In the **LAN** tab, expand **LAN ➤ Pools** .

Step 3 Expand the node for the organization where you want to create the pool.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **MAC Pools** and select **Create MAC Pool**.

Step 5 In the first page of the **Create MAC Pool** wizard:

a) Enter a unique name and description for the MAC Pool.
b) Click **Next**.

Step 6 In the second page of the **Create MAC Pool** wizard:

a) Click **Add**.
b) In the **Create a Block of MAC Addresses** page, enter the first MAC address in the pool and the number of MAC addresses to include in the pool.
c) Click **OK**.
d) Click **Finish**.

What to Do Next

Include the MAC pool in a vNIC template.

Deleting a MAC Pool

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 In the **LAN** tab, expand **LAN ➤ Pools ➤** ***Organization_Name*** .

Step 3 Expand the **MAC Pools** node.

Step 4 Right-click the MAC pool you want to delete and select **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

CHAPTER 18

Configuring Quality of Service

This chapter includes the following sections:

Quality of Service

Cisco UCS provides the following methods to implement quality of service:

- System classes that specify the global configuration for certain types of traffic across the entire system
- QoS policies that assign system classes for individual vNICs
- Flow control policies that determine how uplink Ethernet ports handle pause frames

Configuring System Classes

System Classes

Cisco UCS uses Data Center Ethernet (DCE) to handle all traffic inside a Cisco UCS instance. This industry standard enhancement to Ethernet divides the bandwidth of the Ethernet pipe into eight virtual lanes. Two virtual lanes are reserved for internal system and management traffic. You can configure quality of service for the other six virtual lanes. System classes determine how the DCE bandwidth in these six virtual lanes is allocated across the entire Cisco UCS instance.

Each system class reserves a specific segment of the bandwidth for a specific type of traffic. This provides a level of traffic management, even in an oversubscribed system. For example, you can configure the Fibre Channel Priority system class to determine the percentage of DCE bandwidth allocated to FCoE traffic.

The following table describes the system classes that you can configure:

Table 8: System Classes

System Class	Description
Platinum Gold Silver Bronze	A configurable set of system classes that you can include in the QoS policy for a service profile. Each system class manages one lane of traffic. All properties of these system classes are available for you to assign custom settings and policies.
Best Effort	A system class that sets the quality of service for the lane reserved for Basic Ethernet traffic. Some properties of this system class are preset and cannot be modified. For example, this class has a drop policy that allows it to drop data packets if required. You cannot disable this system class.
Fibre Channel	A system class that sets the quality of service for the lane reserved for Fibre Channel over Ethernet traffic. Some properties of this system class are preset and cannot be modified. For example, this class has a no-drop policy that ensures it never drops data packets. You cannot disable this system class.

Configuring QoS System Classes

The type of adapter in a server may limit the maximum MTU supported. For example, network MTU above the maximums may cause the packet to be dropped for the following adapters:

- The Cisco UCS CNA M71KR adapter, which supports a maximum MTU of 9216.
- The Cisco UCS 82598KR-CI adapter, which supports a maximum MTU of 14000.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 In the **LAN** tab, expand **LAN ➤ LAN Cloud** .

Step 3 Select the **QoS System Class** node.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 Update the following properties for the system class you want to configure to meet the traffic management needs of the system:

Note Some properties may not be configurable for all system classes.

Name	Description
Enabled check box	If checked, the associated QoS class is configured on the fabric interconnect and can be assigned to a QoS policy.

Name	Description
	If unchecked, the class is not configured on the fabric interconnect and any QoS policies associated with this class default to **Best Effort** or, if a system class is configured with a Cos of 0, to the Cos 0 system class. **Note** This field is always checked for **Best Effort** and **Fibre Channel**.
Cos field	The class of service. You can enter an integer value between 0 and 6, with 0 being the lowest priority and 6 being the highest priority. We recommend that you do not set the value to 0, unless you want that system class to be the default system class for traffic if the QoS policy is deleted or the assigned system class is disabled. **Note** This field is set to 7 for internal traffic and to **any** for **Best Effort**. Both of these values are reserved and cannot be assigned to any other priority.
Packet Drop check box	If checked, packet drop is allowed for this class. If unchecked, packets cannot be dropped during transmission. This field is always unchecked for the **Fibre Channel** class, which never allows dropped packets, and always checked for **Best Effort**, which always allows dropped packets.
Weight drop-down list	This can be: • An integer between 1 and 10. If you enter an integer, Cisco UCS determines the percentage of network bandwidth assigned to the priority level as described in the **Weight (%)** field. • **best-effort**. • **none**.
Weight (%) field	To determine the bandwidth allocated to a channel, Cisco UCS: **1** Adds the weights for all the channels **2** Divides the channel weight by the sum of all weights to get a percentage **3** Allocates that percentage of the bandwidth to the channel
MTU drop-down list	The maximum transmission unit for the channel. This can be: • An integer between 1500 and 9216. This value corresponds to the maximum packet size. • **fc**—A predefined packet size of 2240. • **normal**—A predefined packet size of 1500. **Note** This field is always set to **fc** for **Fibre Channel**.

Name	Description
Multicast Optimized check box	If checked, the class is optimized to send packets to multiple destinations simultaneously. **Note** This option is not applicable to the **Fibre Channel**.

Step 6 Click **Save Changes**.

Enabling a QoS System Class

The Best Effort or Fibre Channel system classes are enabled by default.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.
Step 2 In the **LAN** tab, expand **LAN ➤ LAN Cloud** .
Step 3 Select the **QoS System Class** node.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 Check the **Enabled** check box for the QoS system that you want to enable.
Step 6 Click **Save Changes**.

Disabling a QoS System Class

You cannot disable the Best Effort or Fibre Channel system classes.

All QoS policies that are associated with a disabled system class default to Best Effort or, if the disabled system class is configured with a Cos of 0, to the Cos 0 system class.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.
Step 2 In the **LAN** tab, expand **LAN ➤ LAN Cloud** .
Step 3 Select the **QoS System Class** node.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 Uncheck the **Enabled** check box for the QoS system that you want to disable.
Step 6 Click **Save Changes**.

Configuring Quality of Service Policies

Quality of Service Policy

A quality of service (QoS) policy assigns a system class to the outgoing traffic for a vNIC or vHBA. This system class determines the quality of service for that traffic. For certain adapters you can also specify additional controls on the outgoing traffic, such as burst and rate.

You must include a QoS policy in a vNIC policy or vHBA policy and then include that policy in a service profile to configure the vNIC or vHBA.

Creating a QoS Policy

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 In the **LAN** tab, expand **LAN ➤ Policies** .

Step 3 Expand the node for the organization where you want to create the pool.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **QoS Policy** and select **Create QoS Policy**.

Step 5 In the **Create QoS Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Priority drop-down list	The priority assigned to this QoS definition. This can be: • **fc**—Use this priority for QoS policies that control vHBA traffic only. • **platinum**—Use this priority for QoS policies that control vNIC traffic only. • **gold**—Use this priority for QoS policies that control vNIC traffic only. • **silver**—Use this priority for QoS policies that control vNIC traffic only. • **bronze**—Use this priority for QoS policies that control vNIC traffic only. • **best-effort**—Do not use this priority. It is reserved for the Basic Ethernet traffic lane. If you assign this priority to a QoS policy and configure another system class as CoS 0, Cisco UCS Manager

Name	Description
	does not default to this system class. It defaults to the priority with CoS 0 for that traffic.
Burst field	The normal burst size for servers which use this policy. This field determines how large traffic bursts can be before some traffic is considered to exceed the rate limit. The default is 10240. The minimum value is 0, and the maximum value is 65535. This setting is not applicable to all adapters.
Rate field	The expected average rate of traffic. Traffic that falls under this rate will always conform. The default is line-rate, which equals a value of 0 and specifies no rate limiting. The minimum value is 0, and the maximum value is 10,000,000. The granularity for rate limiting on a Cisco M81KR VIC adapter is 1Mbps. These adapters treat the requested rate as a "not-to-exceed" rate. Therefore, a value of 4.5Mbps is interpreted as 4Mbps. Any requested rate of more than 0 and less than 1Mbps is interpreted as 1Mbps, which is the lowest supported hardware rate limit. This setting is not applicable to all adapters.
Host Control field	Whether Cisco UCS controls the class of service (CoS). This can be: • **None**—Cisco UCS uses the CoS value associated with the priority selected in the **Priority** drop-down list regardless of the CoS value assigned by the host. • **Full**—If the packet has a valid CoS value assigned by the host, Cisco UCS uses that value. Otherwise, Cisco UCS uses the CoS value associated with the priority selected in the **Priority** drop-down list. This setting is not applicable to all adapters.

Step 6 Click **OK**.

What to Do Next

Include the QoS policy in a vNIC or vHBA template.

Deleting a QoS Policy

If you delete a QoS policy that is in use or you disable a system class that is used in a QoS policy, any vNIC or vHBA that uses that QoS policy is assigned to the Best Effort system class or to the system class with a CoS of 0. In a system that implements multi-tenancy, Cisco UCS Manager first attempts to find a matching QoS policy in the organization hierarchy.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies ➤ *Organization_Name***.

Step 3 Expand the **QoS Policies** node.

Step 4 Right-click the QoS policy you want to delete and select **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring Flow Control Policies

Flow Control Policy

Flow control policies determine whether the uplink Ethernet ports in a Cisco UCS instance send and receive IEEE 802.3x pause frames when the receive buffer for a port fills. These pause frames request that the transmitting port stop sending data for a few milliseconds until the buffer clears.

For flow control to work between a LAN port and an uplink Ethernet port, you must enable the corresponding receive and send flow control parameters for both ports. For Cisco UCS, the flow control policies configure these parameters.

When you enable the send function, the uplink Ethernet port sends a pause request to the network port if the incoming packet rate becomes too high. The pause remains in effect for a few milliseconds before traffic is reset to normal levels. If you enable the receive function, the uplink Ethernet port honors all pause requests from the network port. All traffic is halted on that uplink port until the network port cancels the pause request.

Because you assign the flow control policy to the port, changes to the policy have an immediate effect on how the port reacts to a pause frame or a full receive buffer.

Creating a Flow Control Policy

Before You Begin

Configure the network port with the corresponding setting for the flow control that you need. For example, if you enable the send setting for flow-control pause frames in the policy, make sure that the receive parameter in the network port is set to on or desired. If you want the Cisco UCS port to receive flow-control frames, make sure that the network port has a send parameter set to on or desired. If you do not want to use flow control, you can set the send and receive parameters on the network port to off.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN ➤ Policies**.

Step 3 Expand the **root** node.
You can only create a flow control policy in the root organization. You cannot create a flow control policy in a sub-organization.

Step 4 Right-click the **Flow Control Policies** node and select **Create Flow Control Policy**.

Step 5 In the **Create Flow Control Policy** wizard, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Priority field	This can be: • **auto**—Cisco UCS and the network negotiate whether PPP is used on this fabric interconnect • **on**—PPP is enabled on this fabric interconnect
Receive field	This can be: • **off**—Pause requests from the network are ignored and traffic flow continues as normal • **on**—Pause requests are honored and all traffic is halted on that uplink port until the network cancels the pause request
Send field	This can be: • **off**—Traffic on the port flows normally regardless of the packet load. • **on**—Cisco UCS sends a pause request to the network if the incoming packet rate becomes too high. The pause remains in effect for a few milliseconds before traffic is reset to normal levels.

Step 6 Click **OK**.

What to Do Next

Associate the flow control policy with an uplink Ethernet port or port channel.

Deleting a Flow Control Policy

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN ➤ Policies ➤** ***Organization_Name***.

Step 3 Expand the **Flow Control Policies** node.

Step 4 Right-click the policy you want to delete and select **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

CHAPTER 19

Configuring Network-Related Policies

This chapter includes the following sections:

Configuring vNIC Templates

vNIC Template

This policy defines how a vNIC on a server connects to the LAN. This policy is also referred to as a vNIC LAN connectivity policy.

You need to include this policy in a service profile for it to take effect.

Creating a vNIC Template

Before You Begin

This policy requires that one or more of the following resources already exist in the system:

- Named VLAN
- MAC pool
- QoS policy
- LAN pin group
- Statistics threshold policy

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the **vNIC Templates** node and choose **Create vNIC Template**.

Step 5 In the **Create vNIC Template** dialog box:

a) In the **General** area, complete the following fields:

Name	Description
Name field	The name of the vNIC template. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A user-defined description of the template. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Fabric ID field	The fabric interconnect associated with the component. If you want vNICs created from this template to be able to access the second fabric interconnect if the default one is unavailable, check the **Enable Failover** check box. **Note** Do not select **Enable Failover** if you plan to associate vNICs created from this template with servers that have adapters which do not support fabric failover, such as a Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter. If you do so, Cisco UCS Manager generates a configuration fault when you associate the service profile with the server.
Target list box	A list of the possible targets for vNICs created from this template. This can be: • **Adapter**—The vNICs apply to all adapters. • **VM**—The vNICs apply to all virtual machines.
Template Type field	This can be: • **Initial Template**—vNICs created from this template are not updated if the template changes. • **Updating Template**—vNICs created from this template are updated if the template changes.

b) In the **VLANs** area, use the table to select the VLAN to assign to vNICs created from this template. The table contains the following columns:

Name	Description
Select column	Check the check box in this column for each VLAN you want to use.
Name column	The name of the VLAN.
Native VLAN column	To designate one of the VLANs as the native VLAN, click the radio button in this column.
Create VLAN link	Click this link if you want to create a VLAN.

c) In the **Policies** area, complete the following fields:

Name	Description
MTU field	The maximum transmission unit, or packet size, that vNICs created from this vNIC template should use. Enter an integer between 1500 and 9216.
MAC Pool drop-down list	The MAC address pool that vNICs created from this vNIC template should use.
QoS Policy drop-down list	The quality of service policy that vNICs created from this vNIC template should use.
Network Control Policy drop-down list	The network control policy that vNICs created from this vNIC template should use.
Pin Group drop-down list	The LAN pin group that vNICs created from this vNIC template should use.
Stats Threshold Policy drop-down list	The statistics collection policy that vNICs created from this vNIC template should use.

Step 6 Click **OK**.

What to Do Next

Include the vNIC template in a service profile.

Deleting a vNIC Template

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN ➤ Policies ➤** ***Organization_Name***.

Step 3 Expand the **vNIC Templates** node.

Step 4 Right-click the policy you want to delete and choose **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Binding a vNIC to a vNIC Template

You can bind a vNIC associated with a service profile to a vNIC template. When you bind the vNIC to a vNIC template, Cisco UCS Manager configures the vNIC with the values defined in the vNIC template. If the existing vNIC configuration does not match the vNIC template, Cisco UCS Manager reconfigures the vNIC. You can only change the configuration of a bound vNIC through the associated vNIC template. You cannot bind a vNIC to a vNIC template if the service profile that includes the vNIC is already bound to a service profile template.

Important If the vNIC is reconfigured when you bind it to a template, Cisco UCS Manager reboots the server associated with the service profile.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization that includes the service profile with the vNIC you want to bind. If the system does not include multi-tenancy, expand the **root** node.

Step 4 Expand ***Service_Profile_Name*** **➤ vNICs**.

Step 5 Click the vNIC you want to bind to a template.

Step 6 In the **Work** pane, click the **General** tab.

Step 7 In the **Actions** area, click **Bind to a Template**.

Step 8 In the **Bind to a vNIC Template** dialog box, do the following:

a) From the **vNIC Template** drop-down list, choose the template to which you want to bind the vNIC.

b) Click **OK**.

Step 9 In the warning dialog box, click **Yes** to acknowledge that Cisco UCS Manager may need to reboot the server if the binding causes the vNIC to be reconfigured.

Unbinding a vNIC from a vNIC Template

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization that includes the service profile with the vNIC you want to unbind. If the system does not include multi-tenancy, expand the **root** node.

Step 4 Expand ***Service_Profile_Name*** **➤ vNICs**.

Step 5 Click the vNIC you want to unbind from a template.

Step 6 In the **Work** pane, click the **General** tab.

Step 7 In the **Actions** area, click **Unbind from a Template**.

Step 8 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring Ethernet Adapter Policies

Ethernet and Fibre Channel Adapter Policies

These policies govern the host-side behavior of the adapter, including how the adapter handles traffic. For example, you can use these policies to change default settings for the following:

- Queues
- Interrupt handling
- Performance enhancement
- RSS hash
- Failover in an cluster configuration with two fabric interconnects

Note For Fibre Channel adapter policies, the values displayed by Cisco UCS Manager may not match those displayed by applications such as QLogic SANsurfer. For example, the following values may result in an apparent mismatch between SANsurfer and Cisco UCS Manager:

- Max LUNs Per Target—SANsurfer has a maximum of 256 LUNs and does not display more than that number. Cisco UCS Manager supports a higher maximum number of LUNs.
- Link Down Timeout—In SANsurfer, you configure the timeout threshold for link down in seconds. In Cisco UCS Manager, you configure this value in milliseconds. Therefore, a value of 5500 ms in Cisco UCS Manager displays as 5s in SANsurfer.
- Max Data Field Size—SANsurfer has allowed values of 512, 1024, and 2048. Cisco UCS Manager allows you to set values of any size. Therefore, a value of 900 in Cisco UCS Manager displays as 512 in SANsurfer.

Operating System Specific Adapter Policies

By default, Cisco UCS provides a set of Ethernet adapter policies and Fibre Channel adapter policies. These policies include the recommended settings for each supported server operating system. Operating systems are sensitive to the settings in these policies. Storage vendors typically require non-default adapter settings. You can find the details of these required settings on the support list provided by those vendors.

Important We recommend that you use the values in these policies for the applicable operating system. Do not modify any of the values in the default policies unless directed to do so by Cisco Technical Support.

However, if you are creating an Ethernet adapter policy for a Windows OS (instead of using the default Windows adapter policy), you must use the following formulas to calculate values that work with Windows:

Completion Queues = Transmit Queues + Receive Queues
Interrupt Count = (Completion Queues + 2) rounded up to nearest power of 2

For example, if Transmit Queues = 1 and Receive Queues = 8 then:

Completion Queues = 1 + 8 = 9
Interrupt Count = (9 + 2) rounded up to the nearest power of 2 = 16

Creating an Ethernet Adapter Policy

Tip If the fields in an area are not displayed, click the **Expand** icon to the right of the heading.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **Adapter Policies** and choose **Create Ethernet Adapter Policy**.

Step 5 Enter a name and description for the policy in the following fields:

Name	Description
Name field	The name of the policy.
Description field	A description of the policy. We recommend including information about where and when the policy should be used. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).

Step 6 (Optional) In the **Resources** area, adjust the following values:

Name	Description
Transmit Queues field	The number of transmit queue resources to allocate. Enter an integer between 1 and 256.
Ring Size field	The number of descriptors in each transmit queue. Enter an integer between 64 and 4096.
Receive Queues field	The number of receive queue resources to allocate. Enter an integer between 1 and 256.
Ring Size field	The number of descriptors in each receive queue. Enter an integer between 64 and 4096.
Completion Queues field	The number of completion queue resources to allocate. In general, the number of completion queue resources you should allocate is equal to the number of transmit queue resources plus the number of receive queue resources. Enter an integer between 1 and 512.
Interrupts field	The number of interrupt resources to allocate. In general, this value should be equal to the number of completion queue resources. Enter an integer between 1 and 514.

Step 7 (Optional) In the **Options** area, adjust the following values:

Name	Description
Transmit Checksum Offload field	This can be: • **disabled**—The CPU calculates all packet checksums. • **enabled**—The CPU sends all packets to the hardware so that the checksum can be calculated. This option may reduce CPU overhead.
Receive Checksum Offload field	This can be: • **disabled**—The CPU validates all packet checksums. • **enabled**—The CPU sends all packet checksums to the hardware for validation. This option may reduce CPU overhead.
TCP Segmentation Offload field	This can be: • **disabled**—The CPU segments large TCP packets. • **enabled**—The CPU sends large TCP packets to the hardware to be segmented. This option may reduce CPU overhead and increase throughput rate. **Note** This option is also known as Large Send Offload (LSO).
TCP Large Receive Offload field	This can be: • **disabled**—The CPU processes all large packets. • **enabled**—The hardware reassembles all segmented packets before sending them to the CPU. This option may reduce CPU utilization and increase inbound throughput.
Receive Side Scaling field	RSS distributes network receive processing across multiple CPUs in multiprocessor systems. This can be: • **disabled**—Network receive processing is always handled by a single processor even if additional processors are available. • **enabled**—Network receive processing is shared across processors whenever possible.
Failback Timeout field	After a vNIC has started using its secondary interface, this setting controls how long the primary interface must be available before the system resumes using the primary interface for the vNIC. Enter a number of seconds between 0 and 600.
Interrupt Mode field	The preferred driver interrupt mode. This can be:

Name	Description
	• **MSI-X**—Message Signaled Interrupts(MSI) with the optional extension. This is the recommended option. • **MSI**—MSI only. • **INTx**—PCI INTx interrupts.
Interrupt Coalescing Type field	This can be: • **min**—The system waits for the time specified in the **Interrupt Timer** field before sending another interrupt event. • **idle**—The system does not send an interrupt until there is a period of no activity lasting as least as long as the time specified in the **Interrupt Timer** field.
Interrupt Timer field	The time to wait between interrupts or the idle period that must be encountered before an interrupt is sent. Enter a value between 1 and 65535. To turn off interrupt coalescing, enter 0 (zero) in this field.

Step 8 Click **OK**.

Step 9 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Deleting an Ethernet Adapter Policy

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN ➤ Policies ➤** ***Organization_Name***.

Step 3 Expand the **Adapter Policies** node.

Step 4 Right-click the Ethernet adapter policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring Network Control Policies

Network Control Policy

This policy configures the network control settings for the Cisco UCS instance, including the following:

- Whether the Cisco Discovery Protocol (CDP) is enabled or disabled
- How the VIF behaves if no uplink port is available in end-host mode
- Whether the server can use different MAC addresses when sending packets to the fabric interconnect

The network control policy also determines the action that Cisco UCS Manager takes on the remote Ethernet port or the vEthernet interface when the associated border port fails. By default, the **Action on Uplink Fail** property in the network control policy is configured with a value of link-down. This default behavior directs Cisco UCS Manager to bring the remote Ethernet or vEthernet port down if the border port fails.

Note The default behaviour of the **Action on Uplink Fail** property is optimal for most Cisco UCS that support link failover at the adapter level or only carry Ethernet traffic. However, for those converged network adapters that support both Ethernet and Fibre Channel traffic, such as the Cisco UCS CNA M72KR-Q and the Cisco UCS CNA M72KR-E, the default behavior can affect and interrupt Fibre Channel traffic as well. Therefore, if the server includes one of those converged network adapters and the the adapter is expected to handle both Ethernet and Fibre Channel traffic, we recommend that you configure the **Action on Uplink Fail** property with a value of warning. Please note that this configuration may result in an Ethernet teaming driver not being able to detect a link failure when the border port goes down.

Creating a Network Control Policy

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the **Network Control Policies** node and select **Create Network Control Policy**.

Step 5 In the **Create Network Control Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
CDP field	This option determines whether Cisco Discovery Protocol (CDP) is enabled on servers associated with a service profile that includes this policy. This can be: • **disabled** • **enabled**

Name	Description
Action on Uplink Fail field	This option determines how the VIF behaves if no uplink port is available when the fabric interconnect is in end-host mode. This can be: • **link-down**— Changes the operational state of a vNIC to down when uplink connectivity is lost on the fabric interconnect, and enables fabric failover for vNICs. • **warning**— Maintains server-to-server connectivity even when no uplink port is available, and disables fabric failover when uplink connectivity is lost on the fabric interconnect. The default is **link-down**. **Note** The default behaviour of the **Action on Uplink Fail** property is optimal for most Cisco UCS that support link failover at the adapter level or only carry Ethernet traffic. However, for those converged network adapters that support both Ethernet and Fibre Channel traffic, such as the Cisco UCS CNA M72KR-Q and the Cisco UCS CNA M72KR-E, the default behavior can affect and interrupt Fibre Channel traffic as well. Therefore, if the server includes one of those converged network adapters and the the adapter is expected to handle both Ethernet and Fibre Channel traffic, we recommend that you configure the **Action on Uplink Fail** property with a value of warning. Please note that this configuration may result in an Ethernet teaming driver not being able to detect a link failure when the border port goes down.

Step 6 In the **MAC Security** area, do the following to determine whether the server can use different MAC addresses when sending packets to the fabric interconnect:

a) Click the **Expand** icon to expand the area and display the radio buttons.

b) Click one of the following radio buttons to determine whether forged MAC addresses are allowed or denied when packets are sent from the server to the fabric interconnect:

- **allow**— All server packets are accepted by the fabric interconnect, regardless of the MAC address associated with the packets.
- **deny**— After the first packet has been sent to the fabric interconnect, all other packets must use the same MAC address or they will be silently rejected by the fabric interconnect. In effect, this option enables port security for the associated vNIC.

If you plan to install VMware ESX on the associated server, you must configure the **MAC Security** to **allow** for the network control policy applied to the default vNIC. If you do not configure **MAC Security** for **allow**, the ESX installation may fail because the MAC security permits only one MAC address while the installation process requires more than one MAC address.

Step 7 Click **OK**.

Deleting a Network Control Policy

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN ➤ Policies ➤** ***Organization_Name***.

Step 3 Expand the **Network Control Policies** node.

Step 4 Right-click the policy you want to delete and select **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

PART IV

Storage Configuration

CHAPTER 20

Configuring Named VSANs

This chapter includes the following sections:

Named VSANs

A named VSAN creates a connection to a specific external SAN. The VSAN isolates traffic to that external SAN, including broadcast traffic. The traffic on one named VSAN knows that the traffic on another named VSAN exists, but cannot read or access that traffic.

Like a named VLAN, the name that you assign to a VSAN ID adds a layer of abstraction that allows you to globally update all servers associated with service profiles that use the named VSAN. You do not need to reconfigure the servers individually to maintain communication with the external SAN. You can create more than one named VSAN with the same VSAN ID.

Named VSANs in Cluster Configurations

In a cluster configuration, a named VSAN can be configured to be accessible only to the Fibre Channel uplink ports on one fabric interconnect or to the Fibre Channel uplink ports on both fabric interconnects.

Named VSANs and the FCoE VLAN ID

You must configure each named VSAN with an FCoE VLAN ID. This property determines which VLAN is used for transporting the VSAN and its Fibre Channel packets.

For FIP capable, converged network adapters, such as the Cisco UCS CNA M72KR-Q and the Cisco UCS CNA M72KR-E, the named VSAN must be configured with a named VLAN that is not the native VLAN for the FCoE VLAN ID. This configuration ensures that FCoE traffic can pass through these adapters.

In the following sample configuration, a service profile with a vNIC and vHBA mapped to fabric A is associated with a server that has FIP capable, converged network adapters:

- The vNIC is configured to use VLAN 10.
- VLAN 10 is also designated as the native VLAN for the vNIC.
- The vHBA is configured to use VSAN 2.
- Therefore, VSAN 2 cannot be configured with VLAN 10 as the FCoE VLAN ID. VSAN 2 can be mapped to any other VLAN configured on fabric A.

Fibre Channel Uplink Trunking for Named VSANs

You can configure Fibre Channel uplink trunking for the named VSANs on each fabric interconnect. If you enable trunking on a fabric interconnect, all named VSANs in a Cisco UCS instance are allowed on all FC uplink ports on that fabric interconnect.

Guidelines and Recommendations for VSANs

The following guidelines and recommendations apply to all named VSANs, including storage VSANs.

VSAN 4079 is a Reserved VSAN ID

Do not configure a VSAN as 4079. This VSAN is reserved and cannot be used in either FC switch mode or FC end-host mode.

If you create a named VSAN with ID 4079, Cisco UCS Manager marks that VSAN with an error and raises a fault.

Range Restrictions for Named VSAN IDs in FC End-Host Mode

If you plan to use FC end-host mode in a Cisco UCS instance, do not configure VSANs with an ID in the range from 3840 to 4079.

VSANs in that range are not operational if the following conditions exist in a Cisco UCS instance:

- The fabric interconnects are configured to operate in FC end-host mode.
- The Cisco UCS instance is configured with Fibre Channel trunking or SAN port channels.

If these configurations exist, Cisco UCS Manager does the following:

1. Renders all VSANs with an ID in the range from 3840 to 4079 non-operational.
2. Raises a fault against the non-operational VSANs.
3. Transfers all non-operational VSANs to the default VSAN.
4. Transfers all vHBAs associated with the non-operational VSANs to the default VSAN.

If you disable Fibre Channel trunking and delete any existing SAN port channels, Cisco UCS Manager returns all VSANs in the range from 3840 to 4078 to an operational state and restores any associated vHBAs back to those VSANs.

Range Restrictions for Named VSAN IDs in FC Switch Mode

If you plan to use FC switch mode in a Cisco UCS instance, do not configure VSANs in the range from 3040 to 4078.

When a fabric interconnect operating in FC switch mode is connected to MDS as the upstream switch, VSANs configured in Cisco UCS Manager in the range from 3040 to 4078 and assigned as port VSANs cannot be created in MDS. This configuration results in a possible port VSAN mismatch.

Creating a Named VSAN

You can create a named VSAN with IDs from 1 to 4093.

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 On the **SAN** tab, expand **SAN ➤ SAN Cloud**.

Step 3 In the **Work** pane, click the **VSANs** tab.

Step 4 On the icon bar to the right of the table, click +.
If the + icon is disabled, click an entry in the table to enable it.

Step 5 In the **Create VSAN** dialog box, complete the following fields:

Name	Description
Name field	The name assigned to the network. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Default Zoning field	Whether default zoning is enabled for this VSAN. You cannot change the zoning after the object has been saved.
Type radio button	Click the radio button to determine how the VSAN should be configured. You can choose: • **Common/Global**—The VSAN maps to the same VSAN ID in all available fabrics. • **Fabric A**—The VSAN maps to the a VSAN ID that exists only in fabric A. • **Fabric B**—The VSAN maps to the a VSAN ID that exists only in fabric B. • **Both Fabrics Configured Differently**—The VSAN maps to a different VSAN ID in each available fabric. If you choose this

Name	Description
	option, Cisco UCS Manager GUI displays a **VSAN ID** field and a **FCoE VLAN** field for each fabric.
VSAN ID field	The unique identifier assigned to the network. The ID can be between 1 and 4093.
FCoE VLAN field	The unique identifier assigned to the VLAN used for Fibre Channel connections. For FIP capable, converged network adapters, such as the Cisco UCS CNA M72KR-Q and the Cisco UCS CNA M72KR-E, the named VSAN must be configured with a named VLAN that is not the native VLAN for the FCoE VLAN ID. This configuration ensures that FCoE traffic can pass through these adapters.

Step 6 Click **OK**.
Cisco UCS Manager GUI adds the VSAN to one of the following **VSANs** nodes:

- The **SAN Cloud ➤ VSANs** node for a storage VSAN accessible to both fabric interconnects.
- The **SAN Cloud ➤ *Fabric_Name* ➤ VSANs** node for a VSAN accessible to only one fabric interconnect.

Creating a Storage VSAN

You can create a named VSAN with IDs from 1 to 4093.

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.
Step 2 On the **SAN** tab, expand **SAN ➤ Storage Cloud**.
Step 3 In the **Work** pane, click the **VSANs** tab.
Step 4 On the icon bar to the right of the table, click +.
If the + icon is disabled, click an entry in the table to enable it.
Step 5 In the **Create VSAN** dialog box, complete the following fields:

Name	Description
Name field	The name assigned to the network. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

Name	Description
Default Zoning field	Whether default zoning is enabled for this VSAN. You cannot change the zoning after the object has been saved.
Type radio button	Click the radio button to determine how the VSAN should be configured. You can choose: • **Common/Global**—The VSAN maps to the same VSAN ID in all available fabrics. • **Fabric A**—The VSAN maps to the a VSAN ID that exists only in fabric A. • **Fabric B**—The VSAN maps to the a VSAN ID that exists only in fabric B. • **Both Fabrics Configured Differently**—The VSAN maps to a different VSAN ID in each available fabric. If you choose this option, Cisco UCS Manager GUI displays a **VSAN ID** field and a **FCoE VLAN** field for each fabric.
VSAN ID field	The unique identifier assigned to the network. The ID can be between 1 and 4093.
FCoE VLAN field	The unique identifier assigned to the VLAN used for Fibre Channel connections. For FIP capable, converged network adapters, such as the Cisco UCS CNA M72KR-Q and the Cisco UCS CNA M72KR-E, the named VSAN must be configured with a named VLAN that is not the native VLAN for the FCoE VLAN ID. This configuration ensures that FCoE traffic can pass through these adapters.

Step 6 Click **OK**.
Cisco UCS Manager GUI adds the VSAN to one of the following **VSANs** nodes:

- The **Storage Cloud ➤ VSANs** node for a storage VSAN accessible to both fabric interconnects.
- The **Storage Cloud ➤** ***Fabric_Name*** **➤ VSANs** node for a VSAN accessible to only one fabric interconnect.

Deleting a VSAN

If Cisco UCS Manager includes a named VSAN with the same VSAN ID as the one you delete, the VSAN is not removed from the fabric interconnect configuration until all named VSANs with that ID are deleted.

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 In the **SAN** tab, click the **SAN** node.

Step 3 In the **Work** pane, click the **VSANs** tab.

Step 4 Click one of the following subtabs, depending upon what type of VSAN you want to delete:

Subtab	Description
All	Displays all VSANs in the Cisco UCS instance.
Dual Mode	Displays the VSANs that are accessible to both fabric interconnects.
Switch A	Displays the VSANs that are accessible to only fabric interconnect A.
Switch B	Displays the VSANs that are accessible to only fabric interconnect B.

Step 5 In the table, click the VSAN you want to delete.
You can use the Shift key or Ctrl key to select multiple entries.

Step 6 Right-click the highlighted VSAN or VSANs and choose **Delete**.

Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Changing the VLAN ID for the FCoE Native VLAN

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 On the **SAN** tab, expand **SAN ➤ Storage Cloud**.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **FCoE Native VLAN** area, enter the desired VLAN ID in the **VLAN ID** field.

Step 5 Click **Save Changes**.

Enabling Fibre Channel Uplink Trunking

Note If the fabric interconnects are configured for FC end-host mode, enabling Fibre Channel uplink trunking renders all VSANs with an ID in the range from 3840 to 4079 non-operational.

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.
Step 2 On the **SAN** tab, expand **SAN ➤ SAN Cloud**.
Step 3 Click the node for the fabric where you want to enable FC uplink trunking.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Actions** area, click **Enable FC Uplink Trunking**.
Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Disabling Fibre Channel Uplink Trunking

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.
Step 2 On the **SAN** tab, expand **SAN ➤ SAN Cloud**.
Step 3 Click the node for the fabric where you want to disable Fibre Channel uplink trunking.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Actions** area, click **Disable FC Uplink Trunking**.
Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

CHAPTER 21

Configuring SAN Pin Groups

This chapter includes the following sections:

SAN Pin Groups

Cisco UCS uses SAN pin groups to pin Fibre Channel traffic from a vHBA on a server to an uplink Fibre Channel port on the fabric interconnect. You can use this pinning to manage the distribution of traffic from the servers.

Note In Fibre Channel switch mode, SAN pin groups are irrelevant. Any existing SAN pin groups will be ignored.

To configure pinning for a server, you must include the SAN pin group in a vHBA policy. The vHBA policy is then included in the service profile assigned to that server. All traffic from the vHBA will travel through the I/O module to the specified uplink Fibre Channel port.

You can assign the same pin group to multiple vHBA policies. As a result, you do not need to manually pin the traffic for each vHBA.

Important Changing the target interface for an existing SAN pin group disrupts traffic for all vHBAs which use that pin group. The fabric interconnect performs a log in and log out for the Fibre Channel protocols to re-pin the traffic.

Creating a SAN Pin Group

In a system with two fabric interconnects, you can associate the pin group with only one fabric interconnect or with both fabric interconnects.

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 In the **SAN** tab, expand **SAN ➤ SAN Cloud** .

Step 3 Right-click **SAN Pin Groups** and select **Create SAN Pin Group**.

Step 4 Enter a unique name and description for the pin group.

Step 5 To pin traffic for fabric interconnect A, do the following in the **Targets** area:

a) Check the **Fabric A** check box.

b) Click the drop-down arrow on the **Interface** field and navigate through the tree-style browser to select the uplink Fibre Channel port you want to associate with the pin group.

Step 6 To pin traffic for fabric interconnect B, do the following in the **Targets** area:

a) Check the **Fabric B** check box.

b) Click the drop-down arrow on the **Interface** field and navigate through the tree-style browser to select the uplink Fibre Channel port you want to associate with the pin group.

Step 7 Click **OK**.

What to Do Next

Include the pin group in a vHBA template.

Deleting a SAN Pin Group

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 In the **SAN** tab, expand **SAN ➤ SAN Cloud ➤ SAN Pin Groups** .

Step 3 Right-click the SAN pin group you want to delete and select **Delete**.

Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

CHAPTER 22

Configuring WWN Pools

This chapter includes the following sections:

WWN Pools

A WWN pool is a collection of WWNs for use by the Fibre Channel vHBAs in a Cisco UCS instance. You create separate pools for the following:

- WW node names assigned to the server
- WW port names assigned to the vHBA

Important A WWN pool can include only WWNNs or WWPNs in the ranges from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF. All other WWN ranges are reserved. To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, we recommend that you use the following WWN prefix for all blocks in a pool: 20:00:00:25:B5:XX:XX:XX

If you use WWN pools in service profiles, you do not have to manually configure the WWNs that will be used by the server associated with the service profile. In a system that implements multi-tenancy, you can use a WWN pool to control the WWNs used by each organization.

You assign WWNs to pools in blocks. For each block or individual WWN, you can assign a boot target.

WWNN Pools

A WWNN pool is a WWN pool that contains only WW node names. If you include a pool of WWNNs in a service profile, the associated server is assigned a WWNN from that pool.

WWPN Pools

A WWPN pool is a WWN pool that contains only WW port names. If you include a pool of WWPNs in a service profile, the port on each vHBA of the associated server is assigned a WWPN from that pool.

Configuring WWNN Pools

Creating a WWNN Pool

Important A WWN pool can include only WWNNs or WWPNs in the ranges from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF. All other WWN ranges are reserved. To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, we recommend that you use the following WWN prefix for all blocks in a pool: 20:00:00:25:B5:XX:XX:XX

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 In the **SAN** tab, expand **SAN ➤ Pools** .

Step 3 Expand the node for the organization where you want to create the pool.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **WWNN Pools** and select **Create WWNN Pool**.

Step 5 In the **Define Name and Description** page of the **Create WWNN Pool** wizard:

a) Enter a unique name and description for the WWNN Pool.
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

b) Click **Next**.

Step 6 In the **Add WWN Blocks** page of the **Create WWNN Pool** wizard, click **Add**.

Step 7 In the **Create WWN Block** page, complete the following fields:

a) In the **From** field, enter the first WWNN in the pool.
b) In the **Size** field, enter the number of WWNNs to include in the pool.
c) Click **OK**.

Step 8 Do one of the following:

- Repeat Steps 6 through 7 to add another block to the pool.
- Click **Next** to move to the next page.

Step 9 Click **Finish**.

Adding a WWN Block to a WWNN Pool

Important A WWN pool can include only WWNNs or WWPNs in the ranges from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF. All other WWN ranges are reserved. To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, we recommend that you use the following WWN prefix for all blocks in a pool: 20:00:00:25:B5:XX:XX:XX

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 In the **SAN** tab, expand **SAN** ➤ **Pools** ➤ *Organization_Name* .

Step 3 Expand the **WWNN Pools** node.

Step 4 Right-click the WWNN pool to which you want to add a WWN block and select **Create WWN Block**.

Step 5 In the **Create WWN Block** page, complete the following fields:

a) In the **From** field, enter the first WWNN in the pool.

b) In the **Size** field, enter the number of WWNNs to include in the pool.

c) Click **OK**.

Deleting a WWN Block from a WWNN Pool

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 In the **SAN** tab, expand **SAN** ➤ **Pools** ➤ *Organization_Name* ➤ **WWNN Pools** ➤ *WWNN_Pool_Name*.

Step 3 Right-click the WWN block that you want to delete and select **Delete**.

Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Adding a WWNN Initiator to a WWNN Pool

Important A WWN pool can include only WWNNs or WWPNs in the ranges from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF. All other WWN ranges are reserved. To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, we recommend that you use the following WWN prefix for all blocks in a pool: 20:00:00:25:B5:XX:XX:XX

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 In the **SAN** tab, expand **SAN ➤ Pools ➤** ***Organization_Name*** .

Step 3 Expand the **WWNN Pools** node.

Step 4 Right-click the WWNN pool to which you want to add a WWNN initiator and select **Create WWNN Initiiator**.

Step 5 In the **Create WWNN Initiator** dialog box, complete the following fields:

Name	Description
World Wide Name field	The WWN.
Name field	The name of the WWNN initiator. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A user-defined description of the WWNN initiator. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).

Step 6 Click **OK**.

Deleting a WWNN Initiator from a WWNN Pool

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 In the **SAN** tab, expand **SAN ➤ Pools ➤** ***Organization_Name*** .

Step 3 Expand the **WWPN Pools** node.

Step 4 Choose the WWNN pool from which you want to delete a WWNN initiator.

Step 5 In the **Work** pane, click the **Initiators** tab.

Step 6 Right-click the initiator that you want to delete and choose **Delete**.

Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Deleting a WWNN Pool

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 In the **SAN** tab, expand **SAN ➤ Pools ➤** ***Organization_Name*** .

Step 3 Expand the **WWNN Pools** node.

Step 4 Right-click the WWNN pool you want to delete and select **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring WWPN Pools

Creating a WWPN Pool

Important A WWN pool can include only WWNNs or WWPNs in the ranges from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF. All other WWN ranges are reserved. To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, we recommend that you use the following WWN prefix for all blocks in a pool: 20:00:00:25:B5:XX:XX:XX

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 In the **SAN** tab, expand **SAN ➤ Pools** .

Step 3 Expand the node for the organization where you want to create the pool.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **WWPN Pools** and select **Create WWPN Pool**.

Step 5 In the **Define Name and Description** page of the **Create WWN Pool** wizard:

a) Enter a unique name and description for the WWPN Pool.
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

b) Click **Next**.

Step 6 In the **Add WWN Blocks** page of the **Create WWPN Pool** wizard, click **Add**.

Step 7 In the **Create WWN Block** page, complete the following fields:

a) In the **From** field, enter the first WWPN in the pool.

b) In the **Size** field, enter the number of WWPNs to include in the pool.

c) Click **OK**.

Step 8 Click **Finish**.

What to Do Next

Include the WWPN pool in a vHBA template.

Adding a WWN Block to a WWPN Pool

Important A WWN pool can include only WWNNs or WWPNs in the ranges from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF. All other WWN ranges are reserved. To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, we recommend that you use the following WWN prefix for all blocks in a pool: 20:00:00:25:B5:XX:XX:XX

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 In the **SAN** tab, expand **SAN ➤ Pools ➤** ***Organization_Name*** .

Step 3 Expand the **WWPN Pools** node.

Step 4 Right-click the WWPN pool to which you want to add a WWN block and select **Create WWN Block**.

Step 5 In the **Create WWN Block** page, complete the following fields:

a) In the **From** field, enter the first WWPN in the pool.

b) In the **Size** field, enter the number of WWPNs to include in the pool.

c) Click **OK**.

Deleting a WWN Block from a WWPN Pool

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 In the **SAN** tab, expand **SAN ➤ Pools ➤** ***Organization_Name*** **➤ WWPN Pools ➤** ***WWPN_Pool_Name***.

Step 3 Right-click the WWN block that you want to delete and select **Delete**.

Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Adding a WWPN Initiator to a WWPN Pool

Important A WWN pool can include only WWNNs or WWPNs in the ranges from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF. All other WWN ranges are reserved. To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, we recommend that you use the following WWN prefix for all blocks in a pool: 20:00:00:25:B5:XX:XX:XX

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 In the **SAN** tab, expand **SAN** ➤ **Pools** ➤ ***Organization_Name*** .

Step 3 Expand the **WWPN Pools** node.

Step 4 Right-click the WWPN pool to which you want to add a WWPN initiator and select **Create WWPN Initiator**.

Step 5 In the **Create WWPN Initiator** dialog box, complete the following fields:

Name	Description
World Wide Name field	The WWN.
Name field	The name of the WWPN initiator. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A user-defined description of the WWPN initiator.

Step 6 If you want to add a SAN boot target, expand the **Boot Target** area and complete the following fields:

Name	Description
Boot Target WWPN field	The WWPN that corresponds to the location of the boot image.
Boot Target LUN field	The LUN that corresponds to the location of the boot image.

Step 7 Click **OK**.

Deleting a WWPN Initiator from a WWPN Pool

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.
Step 2 In the **SAN** tab, expand **SAN ➤ Pools ➤** ***Organization_Name*** .
Step 3 Expand the **WWPN Pools** node.
Step 4 Choose the WWPN pool from which you want to delete a WWPN initiator.
Step 5 In the **Work** pane, click the **Initiators** tab.
Step 6 Right-click the initiator that you want to delete and choose **Delete**.
Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Deleting a WWPN Pool

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.
Step 2 In the **SAN** tab, expand **SAN ➤ Pools ➤** ***Organization_Name*** .
Step 3 Expand the **WWPN Pools** node.
Step 4 Right-click the WWPN pool you want to delete and select **Delete**.
Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

CHAPTER 23

Configuring Storage-Related Policies

This chapter includes the following sections:

Configuring vHBA Templates

vHBA Template

This template is a policy that defines how a vHBA on a server connects to the SAN. It is also referred to as a vHBA SAN connectivity template.

You need to include this policy in a service profile for it to take effect.

Creating a vHBA Template

Before You Begin

This policy requires that one or more of the following resources already exist in the system:

- Named VSAN
- WWNN pool or WWPN pool
- SAN pin group
- Statistics threshold policy

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 On the **SAN** tab, expand **SAN ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the **vHBA Templates** node and choose **Create vHBA Template**.

Step 5 In the **Create vHBA Template** dialog box, complete the following fields:

Name	Description
Name field	The name of the virtual HBA template. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A user-defined description of the template. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Fabric ID field	The name of the fabric interconnect that vHBAs created with this template are associated with.
Select VSAN drop-down list	The VSAN to associate with vHBAs created from this template.
Create VSAN link	Click this link if you want to create a VSAN.
Template Type field	This can be: • **Initial Template**—vHBAs created from this template are not updated if the template changes. • **Updating Template**—vHBAs created from this template are updated if the template changes.
Max Data Field Size field	The maximum size of the Fibre Channel frame payload bytes that the vHBA supports. Enter an integer between 256 and 2112. The default is 2048.
WWN Pool drop-down list	The WWN pool that a vHBA created from this template uses to derive its WWN address.
QoS Policy drop-down list	The QoS policy that is associated with vHBAs created from this template.
Pin Group drop-down list	The LAN pin group that is associated with vHBAs created from this template.
Stats Threshold Policy drop-down list	The statistics collection policy that is associated with vHBAs created from this template.

Step 6 Click **OK**.

What to Do Next

Include the vHBA template in a service profile.

Deleting a vHBA Template

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 On the **SAN** tab, expand **SAN** ➤ **Policies** ➤ ***Organization_Name***.

Step 3 Expand the **vHBA Templates** node.

Step 4 Right-click the vHBA template that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Binding a vHBA to a vHBA Template

You can bind a vHBA associated with a service profile to a vHBA template. When you bind the vHBA to a vHBA template, Cisco UCS Manager configures the vHBA with the values defined in the vHBA template. If the existing vHBA configuration does not match the vHBA template, Cisco UCS Manager reconfigures the vHBA. You can only change the configuration of a bound vHBA through the associated vHBA template. You cannot bind a vHBA to a vHBA template if the service profile that includes the vHBA is already bound to a service profile template.

Important If the vHBA is reconfigured when you bind it to a template, Cisco UCS Manager reboots the server associated with the service profile.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers** ➤ **Service Profiles**.

Step 3 Expand the node for the organization that includes the service profile with the vHBA you want to bind. If the system does not include multi-tenancy, expand the **root** node.

Step 4 Expand ***Service_Profile_Name*** ➤ **vHBAs**.

Step 5 Click the vHBA you want to bind to a template.

Step 6 In the **Work** pane, click the **General** tab.

Step 7 In the **Actions** area, click **Bind to a Template**.

Step 8 In the **Bind to a vHBA Template** dialog box, do the following:

a) From the **vHBA Template** drop-down list, choose the template to which you want to bind the vHBA.
b) Click **OK**.

Step 9 In the warning dialog box, click **Yes** to acknowledge that Cisco UCS Manager may need to reboot the server if the binding causes the vHBA to be reconfigured.

Unbinding a vHBA from a vHBA Template

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization that includes the service profile with the vHBA you want to unbind. If the system does not include multi-tenancy, expand the **root** node.

Step 4 Expand ***Service_Profile_Name*** **➤ vHBAs**.

Step 5 Click the vHBA you want to unbind from a template.

Step 6 In the **Work** pane, click the **General** tab.

Step 7 In the **Actions** area, click **Unbind from a Template**.

Step 8 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring Fibre Channel Adapter Policies

Ethernet and Fibre Channel Adapter Policies

These policies govern the host-side behavior of the adapter, including how the adapter handles traffic. For example, you can use these policies to change default settings for the following:

- Queues
- Interrupt handling
- Performance enhancement
- RSS hash
- Failover in an cluster configuration with two fabric interconnects

Note For Fibre Channel adapter policies, the values displayed by Cisco UCS Manager may not match those displayed by applications such as QLogic SANsurfer. For example, the following values may result in an apparent mismatch between SANsurfer and Cisco UCS Manager:

- Max LUNs Per Target—SANsurfer has a maximum of 256 LUNs and does not display more than that number. Cisco UCS Manager supports a higher maximum number of LUNs.
- Link Down Timeout—In SANsurfer, you configure the timeout threshold for link down in seconds. In Cisco UCS Manager, you configure this value in milliseconds. Therefore, a value of 5500 ms in Cisco UCS Manager displays as 5s in SANsurfer.
- Max Data Field Size—SANsurfer has allowed values of 512, 1024, and 2048. Cisco UCS Manager allows you to set values of any size. Therefore, a value of 900 in Cisco UCS Manager displays as 512 in SANsurfer.

Operating System Specific Adapter Policies

By default, Cisco UCS provides a set of Ethernet adapter policies and Fibre Channel adapter policies. These policies include the recommended settings for each supported server operating system. Operating systems are sensitive to the settings in these policies. Storage vendors typically require non-default adapter settings. You can find the details of these required settings on the support list provided by those vendors.

Important We recommend that you use the values in these policies for the applicable operating system. Do not modify any of the values in the default policies unless directed to do so by Cisco Technical Support.

However, if you are creating an Ethernet adapter policy for a Windows OS (instead of using the default Windows adapter policy), you must use the following formulas to calculate values that work with Windows:

Completion Queues = Transmit Queues + Receive Queues
Interrupt Count = (Completion Queues + 2) rounded up to nearest power of 2

For example, if Transmit Queues = 1 and Receive Queues = 8 then:

Completion Queues = 1 + 8 = 9
Interrupt Count = (9 + 2) rounded up to the nearest power of 2 = 16

Creating a Fibre Channel Adapter Policy

Tip If the fields in an area are not displayed, click the **Expand** icon to the right of the heading.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **Fibre Channel Policies** and choose **Create Fibre Channel Adapter Policy**.

Step 5 Enter a name and description for the policy in the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).

Step 6 (Optional) In the **Resources** area, adjust the following values:

Name	Description
Transmit Queues field	The number of transmit queue resources to allocate. This value cannot be changed.
Ring Size field	The number of descriptors in each transmit queue. Enter an integer between 64 and 128.
Receive Queues field	The number of receive queue resources to allocate. This value cannot be changed.
Ring Size field	The number of descriptors in each receive queue. Enter an integer between 64 and 128.
SCSI I/O Queues field	The number of SCSI IO queue resources the system should allocate. Enter an integer between 1 and 8. **Note** At this time, the Cisco M81KR VIC adapter only supports one SCSI I/O queue.
Ring Size field	The number of descriptors in each SCSI I/O queue. Enter an integer between 64 and 512.

Step 7 (Optional) In the **Options** area, adjust the following values:

Name	Description
FCP Error Recovery field	Whether the system uses FCP Sequence Level Error Recovery protocol (FC-TAPE). This can be: • **disabled** • **enabled** **Note** This option only applies to a server with a VIC adapter, such as the Cisco M81KR VIC, running Windows or Linux.
Flogi Retries field	The number of times that the system tries to log in to the fabric after the first failure. Enter any integer. To specify that the system continue to try indefinitely, enter infinite or -1 in this field. **Note** This option only applies to a server with a VIC adapter, such as the Cisco M81KR VIC, running Windows.
Flogi Timeout field	The number of milliseconds that the system waits before it tries to log in again. Enter an integer between 1000 and 255000. **Note** This option only applies to a server with a VIC adapter, such as the Cisco M81KR VIC, running Windows.
Plogi Retries field	The number of times that the system tries to log into a port after the first failure. Enter an integer between 0 and 255. **Note** This option only applies to a server with a VIC adapter, such as the Cisco M81KR VIC, running Windows or Linux.
Plogi Timeout field	The number of milliseconds that the system waits before it tries to log in again. Enter an integer between 1000 and 255000. **Note** This option only applies to a server with a VIC adapter, such as the Cisco M81KR VIC, running Windows.
Error Detect Timeout field	The number of milliseconds to wait before the system assumes that an error has occurred. This value cannot be changed.
Port Down Timeout field	The number of milliseconds a remote Fibre Channel port should be offline before informing the SCSI upper layer that the port is unavailable. Enter an integer between 0 and 240000. **Tip** For a server with a VIC adapter, such as the Cisco M81KR VIC, running the ESX host, the recommended value is 10000.

Name	Description
Port Down IO Retry field	The number of times an IO request to a port is returned because the port is busy before the system decides the port is unavailable. Enter an integer between 0 and 255. **Note** This option only applies to a server with a VIC adapter, such as the Cisco M81KR VIC, running Windows.
Link Down Timeout field	The number of milliseconds the uplink port should be offline before it informs the system that the uplink port is down and fabric connectivity has been lost. Enter an integer between 0 and 240000. **Note** This option only applies to a server with a VIC adapter, such as the Cisco M81KR VIC, running Windows.
Resource Allocation Timeout field	The number of milliseconds to wait before the system assumes that a resource cannot be properly allocated. This value cannot be changed.
IO Throttle Count field	The number of I/O operations that can be pending in the vHBA at one time. Enter an integer between 1 and 1024. **Note** This option only applies to a server with a VIC adapter, such as the Cisco M81KR VIC, running Windows.
Max LUNs Per Target field	The maximum number of LUNs that the driver will export. This is usually an operating system platform limitation. Enter an integer between 1 and 1024. The recommended value is 1024. **Note** This option only applies to a server with a VIC adapter, such as the Cisco M81KR VIC, running Linux or ESX host.
Interrupt Mode field	The preferred driver interrupt mode. This can be: • **MSI-X**—Message Signaled Interrupts(MSI) with the optional extension. This is the recommended option. • **MSI**—MSI only. • **INTx**—PCI INTx interrupts. **Note** This option is not used by a VIC adapter, such as the Cisco M81KR VIC.

Step 8 Click **OK**.

Step 9 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Deleting a Fibre Channel Adapter Policy

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 On the **SAN** tab, expand **SAN** ➤ **Policies** ➤ ***Organization_Name***.

Step 3 Expand the **Fibre Channel Policies** node.

Step 4 Right-click the policy you want to delete and choose **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

PART V

Server Configuration

CHAPTER 24

Configuring Server-Related Pools

This chapter includes the following sections:

Configuring Server Pools

Server Pools

A server pool contains a set of servers. These servers typically share the same characteristics. Those characteristics can be their location in the chassis, or an attribute such as server type, amount of memory, local storage, type of CPU, or local drive configuration. You can manually assign a server to a server pool, or use server pool policies and server pool policy qualifications to automate the assignment.

If your system implements multi-tenancy through organizations, you can designate one or more server pools to be used by a specific organization. For example, a pool that includes all servers with two CPUs could be assigned to the Marketing organization, while all servers with 64 GB memory could be assigned to the Finance organization.

A server pool can include servers from any chassis in the system. A given server can belong to multiple server pools.

Creating a Server Pool

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers** ➤ **Pools**.

Step 3 Expand the node for the organization where you want to create the pool.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the **Server Pools** node and select **Create Server Pool**.

Step 5 On the **Set Name and Description** page of the **Create Server Pool** wizard, complete the following fields:

Name	Description
Name field	The name of the server pool. This name can be between 1 and 32 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A user-defined description of the server pool. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).

Step 6 Click **Next**.

Step 7 On the **Add Servers** page of the **Create Server Pool** wizard:

a) Select one or more servers from the **Available Servers** table.

b) Click the >> button to add the servers to the server pool.

c) When you have added all desired servers to the pool, click **Finish**.

Deleting a Server Pool

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Pools ➤** ***Organization_Name***.

Step 3 Expand the **Server Pools** node.

Step 4 Right-click the pool you want to delete and select **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Adding Servers to a Server Pool

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Pools ➤** ***Organization_Name***.

Step 3 Right-click the pool to which you want to add one or more servers and select **Add Servers to Server Pool**.

Step 4 In the **Add Servers to Server Pool** dialog box, do the following:

a) In the **Servers** table, select the servers that you want to add to the server pool.
You can use the Shift key or Ctrl key to select multiple entries.

b) Click the **>>** button to move those servers to the **Pooled Servers** table and add them to the server pool.

c) Click **OK**.

Removing Servers from a Server Pool

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Pools ➤ *Organization_Name***.

Step 3 Right-click the pool from which you want to remove one or more servers and select **Add Servers to Server Pool**.

Step 4 In the **Add Servers to Server Pool** dialog box, do the following:

a) In the **Pooled Servers** table, select the servers that you want to remove from the server pool.
You can use the Shift key or Ctrl key to select multiple entries.

b) Click the **<<** button to move those servers to the **Servers** table and remove them from the server pool.

c) Click **OK**.

Configuring UUID Suffix Pools

UUID Suffix Pools

A 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 ensures that these variable values are unique for each server associated with a service profile which uses that particular pool to avoid conflicts.

If you use UUID suffix pools in service profiles, you do not have to manually configure the UUID of the server associated with the service profile.

Creating a UUID Suffix Pool

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Pools**.

Step 3 Expand the node for the organization where you want to create the pool.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **UUID Suffix Pools** and select **Create UUID Suffix Pool**.

Step 5 In the **Define Name and Description** page of the **Create UUID Suffix Pool** wizard, fill in the following fields:

Name	Description
Name field	The name of the UUID pool. This name can be between 1 and 32 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	The user-defined description of the pool. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Prefix field	This can be: • **derived**—The system creates the suffix. • **other**—You specify the desired suffix. If you select this option, Cisco UCS Manager GUI displays a text field where you can enter the desired suffix, in the format *XXXXXXXX-XXXX-XXXX*.

Step 6 In the **Add UUID Blocks** page of the **Create UUID Suffix Pool** wizard:

a) Click **Add**.
b) In the **Create a Block of UUID Suffixes** page, enter the first UUID suffix in the pool and the number of UUID suffixes to include in the pool.
c) Click **OK**.
d) If you want to add another block to the pool, repeat steps a through c.

Step 7 Click **Finish** to complete the wizard.

What to Do Next

Include the UUID suffix pool in a service profile and/or template.

Deleting a UUID Suffix Pool

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Pools ➤ *Organization_Name***.

Step 3 Expand the **UUID Suffix Pools** node.

Step 4 Right-click the pool you want to delete and select **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

CHAPTER 25

Setting the Management IP Address

This chapter includes the following sections:

Management IP Address

Each server in a Cisco UCS instance must have a management IP address assigned to its Cisco Integrated Management Controller (CIMC) or to the service profile associated with the server. Cisco UCS Manager uses this IP address for external access that terminates in the CIMC. This external access can be through one of the following:

- KVM console
- Serial over LAN
- An IPMI tool

The management IP address used to access the CIMC on a server can be one of the following:

- A static IPv4 address assigned directly to the server.
- A static IPv4 address assigned to a service profile. You cannot configure a service profile template with a static IP address.
- An IP address drawn from the management IP address pool and assigned to a service profile or service profile template.

You can assign a management IP address to each CIMC on the server and to the service profile associated with the server. If you do so, you must use different IP addresses for each of them.

Note You cannot assign a static IP address to a server or service profile if that IP address has already been assigned to a server or service profile in the Cisco UCS instance. If you attempt to do so, Cisco UCS Manager warns you that the IP address is already in use and rejects the configuration.

A management IP address that is assigned to a service profile moves with the service profile. If a KVM or SoL session is active when you migrate the service profile to another server, Cisco UCS Manager terminates that session and does not restart it after the migration is completed. You configure this IP address when you create or modify a service profile.

Configuring the Management IP Address on a Blade Server

Configuring a Blade Server to Use a Static IP Address

If this action is greyed out, the server has already been assigned a static IP address.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.

Step 3 Click the server for which you want to configure an IP address.

Step 4 In the **Work** pane, click the **Inventory** tab.

Step 5 Click the **CIMC** subtab.

Step 6 In the **Actions** area, click **Create/Modify Static Management IP**.

Step 7 In the **Create/Modify Static Management IP** dialog box, complete the following fields:

Field	Description
IP Address	The static IPv4 address to be assigned to the server.
Subnet Mask	The subnet mask for the IP address.
Default Gateway	The default gateway that the IP address should use.

Step 8 Click **OK**.

Configuring a Blade Server to Use the Management IP Pool

If this action is greyed out, the server is already configured to use the management IP pool.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.
Step 3 Click the server that you want to configure to use the management IP pool.
Step 4 In the **Work** pane, click the **Inventory** tab.
Step 5 Click the **CIMC** subtab.
Step 6 In the **Actions** area, click **Use Pooled Management IP**.
Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
Step 8 Click **OK**.

Configuring the Management IP Address on a Rack Server

Configuring a Rack Server to Use a Static IP Address

If this action is greyed out, the server has already been assigned a static IP address.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, expand **Equipment ➤ Rack Mounts ➤ Servers**.
Step 3 Click the server for which you want to configure an IP address.
Step 4 In the **Work** pane, click the **Inventory** tab.
Step 5 Click the **CIMC** subtab.
Step 6 In the **Actions** area, click **Create/Modify Static Management IP**.
Step 7 In the **Create/Modify Static Management IP** dialog box, complete the following fields:

Field	Description
IP Address	The static IPv4 address to be assigned to the server.
Subnet Mask	The subnet mask for the IP address.
Default Gateway	The default gateway that the IP address should use.

Step 8 Click **OK**.

Configuring a Rack Server to Use the Management IP Pool

If this action is greyed out, the server is already configured to use the management IP pool.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, expand **Equipment ➤ Rack Mounts ➤ Servers**.
Step 3 Click the server that you want to configure to use the management IP pool.
Step 4 In the **Work** pane, click the **Inventory** tab.
Step 5 Click the **CIMC** subtab.
Step 6 In the **Actions** area, click **Use Pooled Management IP**.
Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
Step 8 Click **OK**.

Setting the Management IP Address on a Service Profile

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.
Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.
Step 3 Expand the node for the organization that contains the service profile for which you want to set the management IP address.
If the system does not include multi-tenancy, expand the **root** node.
Step 4 Click the service profile for which you want to set the management IP address.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 Expand the **Management IP Address** area.
Step 7 In the **Management IP Address Policy** field, click one of the following radio buttons:

- **none**—No management IP address is assigned to the service profile. The management IP address is set based on the CIMC management IP address settings on the server.
- **static**—A static management IP address is assigned to the service profile, based on the information entered in this area.
- **pooled**—A management IP address is assigned to the service profile from the management IP address pool.

Step 8 If you selected **static**, complete the following fields:

Field	Description
IP Address	The static IPv4 address to be assigned to the service profile
Subnet Mask	The subnet mask for the IP address.

Field	Description
Default Gateway	The default gateway that the IP address should use.

Step 9 Click **Save Changes**.

Setting the Management IP Address on a Service Profile Template

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profile Templates**.

Step 3 Expand the node for the organization that contains the service profile template for which you want to set the management IP address.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Click the service profile template for which you want to set the management IP address.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 Expand the **Management IP Address** area.

Step 7 In the **Management IP Address Policy** field, click one of the following radio buttons:

- **none**—No management IP address is assigned to the service profile. The management IP address is set based on the CIMC management IP address settings on the server.
- **pooled**—A management IP address is assigned to the service profile from the management IP address pool.

Step 8 Click **Save Changes**.

Configuring the Management IP Pool

Management IP Pool

The management IP pool is a collection of external IP addresses. Cisco UCS Manager reserves each block of IP addresses in the management IP pool for external access that terminates in the CIMC on a server.

You can configure service profiles and service profile templates to use IP addresses from the management IP pool. You cannot configure servers to use the management IP pool.

Note The management IP pool must not contain any IP addresses that have been assigned as static IP addresses for a server or service profile.

Creating an IP Address Block in the Management IP Pool

The management IP pool must not contain any IP addresses that have been assigned as static IP addresses for a server or service profile.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services** .

Step 3 Right-click **Management IP Pool (ext-mgmt)** and select **Create Block of IP Addresses**.

Step 4 In the **Create a Block of IP Addresses** dialog box, complete the following fields:

Name	Description
From field	The first IP address in the block.
Size field	The number of IP addresses in the pool.
Subnet Mask field	The subnet mask associated with the IP addresses in the block.
Default Gateway field	The default gateway associated with the IP addresses in the block.

Step 5 Click **OK**.

What to Do Next

Configure one or more service profiles or service profile templates to obtain the CIMC IP address from the management IP pool.

Deleting an IP Address Block from the Management IP Pool

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services ➤ Management IP Pool (ext-mgmt)**.

Step 3 Right-click the IP address block that you want to delete and select **Delete**.

Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

CHAPTER 26

Configuring Server-Related Policies

This chapter includes the following sections:

Configuring BIOS Settings

Server BIOS Settings

Cisco UCS provides two methods for making global modifications to the BIOS settings on servers in an instance. You can create one or more BIOS policies that include a specific grouping of BIOS settings that match the needs of a server or set of servers, or you can use the default BIOS settings for a specific server platform.

Both the BIOS policy and the default BIOS settings for a server platform enable you to fine tune the BIOS settings for a server managed by Cisco UCS Manager.

Depending upon the needs of the data center, you can configure BIOS policies for some service profiles and use the BIOS defaults in other service profiles in the same Cisco UCS instance, or you can use only one of

them. You can also use Cisco UCS Manager to view the actual BIOS settings on a server and determine whether they are meeting current needs.

Note Cisco UCS Manager pushes BIOS configuration changes through a BIOS policy or default BIOS settings to the CIMC buffer. These changes remain in the buffer and do not take effect until the server is rebooted.

We recommend that you verify the support for BIOS settings in the server that you want to configure. Some settings, such as Mirroring Mode and Sparing Mode for RAS Memory, are not supported by all Cisco UCS servers

Main BIOS Settings

The following table lists the main server BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description
Reboot on BIOS Settings Change	When the server is rebooted after you change one or more BIOS settings. If you enable this setting, the server is rebooted according to the maintenance policy in the server's service profile. For example, if the maintenance policy requires user acknowledgment, the server is not rebooted and the BIOS changes are not applied until a user acknowledges the pending activity. If you do not enable this setting, the BIOS changes are not applied until the next time the server is rebooted, whether as a result of another server configuration change or a manual reboot.
Quiet Boot	What the BIOS displays during Power On Self-Test (POST). This can be one of the following: • **disabled**—The BIOS displays all messages and Option ROM information during boot. • **enabled**—The BIOS displays the logo screen, but does not display any messages or Option ROM information during boot. • **platform-default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Post Error Pause	What happens when the server encounters a critical error during POST. This can be one of the following: • **disabled**—The BIOS continues to attempt to boot the server.

Name	Description
	• **enabled**—The BIOS pauses the attempt to boot the server and opens the Error Manager when a critical error occurs during POST. • **platform-default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Resume Ac On Power Loss	How the server behaves when power is restored after an unexpected power loss. This can be one of the following: • **stay-off**—The server remains off until manually powered on. • **last-state**—The server is powered on and the system attempts to restore its last state. • **reset**—The server is powered on and automatically reset. • **platform-default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Front Panel Lockout	Whether the power and reset buttons on the front panel are ignored by the server. This can be one of the following: • **disabled**—The power and reset buttons on the front panel are active and can be used to affect the server. • **enabled**—The power and reset buttons are locked out. The server can only be reset or powered on or off from the CIMC GUI. • **platform-default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
ACPI10 Support	Whether the BIOS publishes the ACPI 1.0 version of FADT in the Root System Description table. This version may be required for compatibility with OS versions that only support ACPI 1.0. This can be one of the following: • **disabled**—ACPI 1.0 version is not published. • **enabled**—ACPI 1.0 version is published. • **platform-default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Processor BIOS Settings

The following table lists the processor BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description
Turbo Boost	Whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running below power, temperature, or voltage specifications. This can be one of the following: • **disabled**—The processor does not increase its frequency automatically. • **enabled**—The processor utilizes Turbo Boost Technology if required. • **platform-default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Enhanced Intel Speedstep	Whether the processor uses Enhanced Intel SpeedStep Technology, which allows the system to dynamically adjust processor voltage and core frequency. This technology can result in decreased average power consumption and decreased average heat production. This can be one of the following: • **disabled**—The processor never dynamically adjusts its voltage or frequency. • **enabled**—The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. • **platform-default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Hyper Threading	Whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following: • **disabled**—The processor does not permit hyperthreading. • **enabled**—The processor allows for the parallel execution of multiple threads. • **platform-default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
	We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Core Multi Processing	Sets the state of logical processor cores in a package. If you disable this setting, Hyper Threading is also disabled. This can be one of the following: • **all**—Enables multi processing on all logical processor cores. • **1** through **8**—Specifies the number of logical processor cores that can run on the server. To disable multi processing and have only one logical processor core running on the server, select 1. • **platform-default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Execute Disabled Bit	Classifies memory areas on the server to specify where where application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks. This can be one of the following: • **disabled**—The processor does not classify memory areas. • **enabled**—The processor classifies memory areas. • **platform-default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Virtualization Technology (VT)	Whether the processor uses Intel Virtualization Technology, which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following: • **disabled**—The processor does not permit virtualization. • **enabled**—The processor allows multiple operating systems in independent partitions. • **platform-default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
	Note If you change this option, you must power cycle the server before the setting takes effect.
Direct Cache Access	Allows processors to increase I/O performance by placing data from I/O devices directly into the processor cache. This setting helps to reduce cache misses. This can be one of the following: • **disabled**—Data from I/O devices is not placed directly into the processor cache. • **enabled**—Data from I/O devices is placed directly into the processor cache. • **platform-default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Processor C3 Report	Whether the processor sends the C3 report to the operating system. This can be one of the following: • **disabled**—The processor does not send the C3 report. • **acpi-c2**—The processor sends the C3 report using the ACPI C2 format. • **acpi-c3**—The processor sends the C3 report using the ACPI C3 format. • **platform-default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. On the B400 server, the BIOS Setup menu uses enabled and disabled for these options. If you specify acpi-c2 or acpi-c2, the server sets the BIOS value for that option to enabled.
Processor C6 Report	Whether the processor sends the C6 report to the operating system. This can be one of the following: • **disabled**—The processor does not send the C6 report. • **enabled**—The processor sends the C6 report. • **platform-default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
CPU Performance	Sets the CPU performance profile for the server. This can be one of the following: • **enterprise**—All prefetchers and data reuse are disabled. • **high-throughput**—All prefetchers are enabled, and data reuse is disabled.

Name	Description
	• **hpc**—All prefetchers and data reuse are enabled. This setting is also known as high performance computing. • **platform-default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Intel Directed I/O BIOS Settings

The following table lists the Intel Directed I/O BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description
VT for Directed IO	Whether the processor uses Intel Virtualization Technology for Directed I/O. This can be one of the following: • **disabled**—The processor does not use virtualization technology. • **enabled**—The processor uses virtualization technology. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Interrupt Remap	Whether the processor supports Intel VT-d Interrupt Remapping. This can be one of the following: • **disabled**—The processor does not support remapping. • **enabled**—The processor uses VT-d Interrupt Remapping as required. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Coherency Support	Whether the processor supports Intel VT-d Coherency. This can be one of the following: • **disabled**—The processor does not support coherency. • **enabled**—The processor uses VT-d Coherency as required. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
ATS Support	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following:

Name	Description
	• **disabled**—The processor does not support ATS. • **enabled**—The processor uses VT-d ATS as required. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Pass Through DMA Support	Whether the processor supports Intel VT-d Pass-through DMA. This can be one of the following: • **disabled**—The processor does not support pass-through DMA. • **enabled**—The processor uses VT-d Pass-through DMA as required. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

RAS Memory BIOS Settings

The following table lists the RAS memory BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description
Memory RAS Config	How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following: • **maximum performance**—System performance is optimized. • **mirroring**—System reliability is optimized by using half the system memory as backup. • **lockstep**—If the DIMM pairs in the server have an identical type, size, and organization and are populated across the SMI channels, you can enable lockstep mode to minimize memory access latency and provide better performance. Lockstep is enabled by default for B400 servers. • **sparing**—System reliability is enhanced with a degree of memory redundancy while making more memory available to the operating system than mirroring. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
NUMA	Whether the BIOS supports NUMA. This can be one of the following: • **disabled**—The BIOS does not support NUMA • **enabled**—The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
LV DDR Mode	Whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following: • **power-saving-mode**—The system prioritizes low voltage memory operations over high frequency memory operations. This mode may lower memory frequency in order to keep the voltage low. • **performance-mode**—The system prioritizes high frequency operations over low voltage operations. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Mirroring Mode	Memory mirroring enhances system reliability by keeping two identical data images in memory. This option is only available if you choose the **mirroring** option for Memory RAS Config. It can be one of the following: • **inter-socket**—Memory is mirrored between two Integrated Memory Controllers (IMCs) across CPU sockets. • **intra-socket**—One IMC is mirrored with another IMC in the same socket. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Sparing Mode	Sparing optimizes reliability by holding memory in reserve so that it can be used in case other DIMMs fail. This option provides some memory redundancy, but does not provide as much redundancy as mirroring. The available sparing modes depend on the current memory population.

Name	Description
	This option is only available if you choose **sparing** option for Memory RAS Config. It can be one of the following: • **dimm-sparing**—One DIMM is held in reserve. If a DIMM fails, the contents of a failing DIMM are transferred to the spare DIMM. • **rank-sparing**—A spare rank of DIMMs is held in reserve. If a rank of DIMMs fails, the contents of the failing rank are transferred to the spare rank. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Serial Port BIOS Settings

The following table lists the serial port BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description
Serial Port A	Whether serial port A is enabled or disabled. This can be one of the following: • **disabled**—The serial port is disabled. • **enabled**—The serial port is enabled. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

USB BIOS Settings

The following table lists the USB BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description
Make Device Non Bootable	Whether the server can boot from a USB device. This can be one of the following: • **disabled**—The server cannot boot from a USB device. • **enabled**—The server can boot from a USB device. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

PCI Configuration BIOS Settings

The following table lists the PCI configuration BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description
Max Memory Below 4G	Whether the BIOS maximizes memory usage below 4GB for an operating without PAE support, depending on the system configuration. This can be one of the following: • **disabled**—Does not maximize memory usage. Choose this option for all operating systems with PAE support. • **enabled**—Maximizes memory usage below 4GB for an operating system without PAE support. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Memory Mapped IO Above 4Gb Config	Whether to enable or disable memory mapped I/O of 64-bit PCI devices to 4GB or greater address space. Legacy option ROMs are not able to access addresses above 4GB. PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled. This can be one of the following: • **disabled**—Does not map I/O of 64-bit PCI devices to 4GB or greater address space. • **enabled**—Maps I/O of 64-bit PCI devices to 4GB or greater address space. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Boot Options BIOS Settings

The following table lists the boot options BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description
Boot Option Retry	Whether the BIOS retries NON-EFI based boot options without waiting for user input. This can be one of the following: • **disabled**—Waits for user input before retrying NON-EFI based boot options. • **enabled**—Continually retries NON-EFI based boot options without waiting for user input.

Name	Description
	• **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Intel Entry SAS RAID	Whether the Intel SAS Entry RAID Module is enabled. This can be one of the following: • **disabled**—The Intel SAS Entry RAID Module is disabled. • **enabled**—The Intel SAS Entry RAID Module is enabled. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Intel Entry SAS RAID Module	How the Intel SAS Entry RAID Module is configured. This can be one of the following: • **it-ir-raid**—Configures the RAID module to use Intel IT/IR RAID. • **intel-esrtii**—Configures the RAID module to use Intel Embedded Server RAID Technology II. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Server Management BIOS Settings

The following tables list the server management BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

General Settings

Name	Description
Assert Nmi on Serr	Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a system error (SERR) occurs. This can be one of the following: • **disabled**—The BIOS does not generate an NMI or log an error when a SERR occurs. • **enabled**—The BIOS generates an NMI and logs an error when a SERR occurs. You must enable this setting if you want to enable **Assert Nmi on Perr**. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
Assert Nmi on Perr	Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a processor bus parity error (PERR) occurs. This can be one of the following: • **disabled**—The BIOS does not generate an NMI or log an error when a PERR occurs. • **enabled**—The BIOS generates an NMI and logs an error when a PERR occurs. You must enable **Assert Nmi on Serr** to use this setting. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
OS Boot Watchdog Timer	Whether the BIOS programs the watchdog timer with a predefined timeout value. If the operating system does not complete booting before the timer expires, the CIMC resets the system and an error is logged. This can be one of the following: • **disabled**—The watchdog timer is not used to track how long the server takes to boot. • **enabled**—The watchdog timer tracks how long the server takes to boot. If the server does not boot within the predefined length of time, the CIMC resets the system and logs an error. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. This feature requires either operating system support or Intel Management software.
OS Boot Watchdog Timer Timeout Policy	What action the system takes if the watchdog timer expires. This can be one of the following: • **power-off**—The server is powered off if the watchdog timer expires during OS boot. • **reset**—The server is reset if the watchdog timer expires during OS boot. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. This option is only available if you enable the OS Boot Watchdog Timer.

Name	Description
OS Boot Watchdog Timer Timeout	What timeout value the BIOS uses to configure the watchdog timer. This can be one of the following: • **5-minutes**—The watchdog timer expires 5 minutes after the OS begins to boot. • **10-minutes**—The watchdog timer expires 10 minutes after the OS begins to boot. • **15-minutes**—The watchdog timer expires 15 minutes after the OS begins to boot. • **20-minutes**—The watchdog timer expires 20 minutes after the OS begins to boot. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. This option is only available if you enable the OS Boot Watchdog Timer.

Console Redirection Settings

Name	Description
Console Redirection	Allows a serial port to be used for console redirection during POST and BIOS booting. After the BIOS has booted and the operating system is responsible for the server, console redirection is irrelevant and has no effect. This can be one of the following: • **disabled**—No console redirection occurs during POST. • **serial-port-a**—Enables serial port A for console redirection during POST. This option is valid for blade servers and rack-mount servers. • **serial-port-b**—Enables serial port B for console redirection and allows it to perform server management tasks. This option is only valid for rack-mount servers. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** If you enable this option, you also disable the display of the Quiet Boot logo screen during POST.
Flow Control	Whether a handshake protocol is used for flow control. Request to Send / Clear to Send (RTS/CTS) helps to reduce frame collisions that can be introduced by a hidden terminal problem. This can be one of the following: • **none**—No flow control is used.

Name	Description
	• **rts-cts**—RTS/CTS is used for flow control. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** This setting must match the setting on the remote terminal application.
BAUD Rate	What BAUD rate is used for the serial port transmission speed. If you disable Console Redirection, this option is not available. This can be one of the following: • **9600**—A 9600 BAUD rate is used. • **19200**—A 19200 BAUD rate is used. • **38400**—A 38400 BAUD rate is used. • **57600**—A 57600 BAUD rate is used. • **115200**—A 115200 BAUD rate is used. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** This setting must match the setting on the remote terminal application.
Terminal Type	What type of character formatting is used for console redirection. This can be one of the following: • **pc-ansi**—The PC-ANSI terminal font is used. • **vt100**—A supported vt100 video terminal and its character set are used. • **vt100-plus**—A supported vt100-plus video terminal and its character set are used. • **vt-utf8**—A video terminal with the UTF-8 character set is used. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** This setting must match the setting on the remote terminal application.
Legacy OS Redirect	Whether redirection from a legacy operating system, such as DOS, is enabled on the serial port. This can be one of the following:

Name	Description
	• **disabled**—The serial port enabled for console redirection is hidden from the legacy operating system. • **enabled**— The serial port enabled for console redirection is visible to the legacy operating system. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

BIOS Policy

The BIOS policy is a policy that automates the configuration of BIOS settings for a server or group of servers. You can create global BIOS policies available to all servers in the root organization, or you can create BIOS policies in sub-organizations that are only available to that hierarchy.

To use a BIOS policy, do the following:

1 Create the BIOS policy in Cisco UCS Manager.

2 Assign the BIOS policy to one or more service profiles.

3 Associate the service profile with a server.

During service profile association, Cisco UCS Manager modifies the BIOS settings on the server to match the configuration in the BIOS policy. If you do not create and assign a BIOS policy to a service profile, the server uses the default BIOS settings for that server platform.

Default BIOS Settings

Cisco UCS Manager includes a set of default BIOS settings for each type of server supported by Cisco UCS. The default BIOS settings are available only in the root organization and are global. Only one set of default BIOS settings can exist for each server platform supported by Cisco UCS. You can modify the default BIOS settings, but you cannot create an additional set of default BIOS settings.

Each set of default BIOS settings are designed for a particular type of supported server and are applied to all servers of that specific type which do not have a BIOS policy included in their service profiles.

Unless a Cisco UCS implementation has specific needs that are not met by the server-specific settings, we recommend that you use the default BIOS settings that are designed for each type of server in the instance.

Cisco UCS Manager applies these server platform-specific BIOS settings as follows:

- The service profile associated with a server does not include a BIOS policy.
- The BIOS policy is configured with the platform-default option for a specific setting.

You can modify the default BIOS settings provided by Cisco UCS Manager. However, any changes to the default BIOS settings apply to all servers of that particular type or platform. If you want to modify the BIOS settings for only certain servers, we recommend that you use a BIOS policy.

Creating a BIOS Policy

Note Cisco UCS Manager pushes BIOS configuration changes through a BIOS policy or default BIOS settings to the CIMC buffer. These changes remain in the buffer and do not take effect until the server is rebooted.

We recommend that you verify the support for BIOS settings in the server that you want to configure. Some settings, such as Mirroring Mode and Sparing Mode for RAS Memory, are not supported by all Cisco UCS servers

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **BIOS Policies** and select **Create BIOS Policy**.

Step 5 On the **Main** page of the **Create BIOS Policy** wizard, enter a name for the BIOS policy in the **Name** field. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

Step 6 In the **Create BIOS Policy** wizard, do the following to configure the BIOS settings:

a) If you want to change a BIOS setting, click the desired radio button or make the appropriate choice from the drop-down list.
For descriptions and information about the options for each BIOS setting, see the following topics:

- **Main** page: Main BIOS Settings, page 302
- **Processor** page: Processor BIOS Settings, page 304
- **Intel Directed IO** page: Intel Directed I/O BIOS Settings, page 307
- **RAS Memory** page: RAS Memory BIOS Settings, page 308
- **Serial Port** page: Serial Port BIOS Settings, page 310
- **USB** page: USB BIOS Settings, page 310
- **PCI Configuration** page: PCI Configuration BIOS Settings, page 311
- **Boot Options** page: Boot Options BIOS Settings, page 311
- **Server Management** page: Server Management BIOS Settings, page 312

b) Click **Next** after each page to move to the

Step 7 After you have configured all of the BIOS settings for the policy, click **Finish**.

Modifying the BIOS Defaults

We recommend that you verify the support for BIOS settings in the server that you want to configure. Some settings, such as Mirroring Mode and Sparing Mode for RAS Memory, are not supported by all Cisco UCS servers

Unless a Cisco UCS implementation has specific needs that are not met by the server-specific settings, we recommend that you use the default BIOS settings that are designed for each type of server in the instance.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Expand **BIOS Defaults** and select the server model number for which you want to modify the default BIOS settings.

Step 5 In the **Work** pane, click the appropriate tab and then click the desired radio button or make a choice from the drop-down list to modify the defult BIOS settings:
For descriptions and information about the options for each BIOS setting, see the following topics. Not all BIOS settings are available for each type of server.

- **Main** tab: Main BIOS Settings, page 302
- **Advanced** tab:
  - **Processor** subtab: Processor BIOS Settings, page 304
  - **Intel Directed IO** subtab: Intel Directed I/O BIOS Settings, page 307
  - **RAS Memory** subtab: RAS Memory BIOS Settings, page 308
  - **Serial Port** subtab: Serial Port BIOS Settings, page 310
  - **USB** subtab: USB BIOS Settings, page 310
  - **PCI Configuration** subtab: PCI Configuration BIOS Settings, page 311
- **Boot Options** tab: Boot Options BIOS Settings, page 311
- **Server Management** tab: Server Management BIOS Settings, page 312

Step 6 Click **Save Changes**.

Viewing the Actual BIOS Settings for a Server

Follow this procedure to see the actual BIOS settings on a server.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.

Step 3 Choose the server for which you want to view the actual BIOS settings.

Step 4 On the **Work** pane, click the **Inventory** tab.

Step 5 Click the **Motherboard** subtab.

Step 6 In the **BIOS Settings** area, click the **Expand** icon to the right of the heading to open that area.
Each tab in the **BIOS Settings** area displays the settings for that server platform. Some of the tabs contain subtabs with additional information.

Configuring Boot Policies

Boot Policy

The boot policy determines the following:

- Configuration of the boot device
- Location from which the server boots
- Order in which boot devices are invoked

For example, you can choose to have associated servers boot from a local device, such as a local disk or CD-ROM (VMedia), or you can select a SAN boot or a LAN (PXE) boot.

You must include this policy in a service profile, and that service profile must be associated with a server for it to take effect. If you do not include a boot policy in a service profile, the server uses the default settings in the BIOS to determine the boot order.

Important Changes to a boot policy may be propagated to all servers created with an updating service profile template that includes that boot policy. Reassociation of the service profile with the server to rewrite the boot order information in the BIOS is auto-triggered.

Guidelines

When you create a boot policy, you can add one or more of the following to the boot policy and specify their boot order:

Boot type	Description
SAN boot	Boots from an operating system image on the SAN. You can specify a primary and a secondary SAN boot. If the primary boot fails, the server attempts to boot from the secondary.

Boot type	Description
	We recommend that you use a SAN boot, because it offers the most service profile mobility within the system. If you boot from the SAN when you move a service profile from one server to another, the new server boots from the exact same operating system image. Therefore, the new server appears to be the exact same server to the network.
LAN boot	Boots from a centralized provisioning server. It is frequently used to install operating systems on a server from that server.
Local disk boot	If the server has a local drive, boots from that drive. **Note** Cisco UCS Manager does not differentiate between the types of local drives. If an operating system has been installed on more than one local drive or on an internal USB drive (eUSB), you cannot specify which of these local drives the server should use as the boot drive.
Virtual media boot	Mimics the insertion of a physical CD-ROM disk (read-only) or floppy disk (read-write) into a server. It is typically used to manually install operating systems on a server.

Note The default boot order is as follows:

1. Local disk boot
2. LAN boot
3. Virtual media read-only boot
4. Virtual media read-write boot

Creating a Boot Policy

You can also create a local boot policy that is restricted to a service profile or service profile template. However, we recommend that you create a global boot policy that can be included in multiple service profiles or service profile templates.

Tip We recommend that the boot order in a boot policy include either a local disk or a SAN LUN, but not both, to avoid the possibility of the server booting from the wrong storage type. If you configure a local disk and a SAN LUN for the boot order storage type and the operating system or logical volume manager (LVM) is configured incorrectly, the server may boot from the local disk rather than the SAN LUN.

For example, on a server with Red Hat Linux installed, where the LVM is configured with default LV names and the boot order is configured with a SAN LUN and a local disk, Linux reports that there are two LVs with the same name and boots from the LV with the lowest SCSI ID, which could be the local disk.

Before You Begin

If you are creating a boot policy that boots the server from a SAN LUN and you require reliable SAN boot operations, you must first remove all local disks from servers associated with a service profile that includes the boot policy.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **Boot Policies** and select **Create Boot Policy**.
The **Create Boot Policy** wizard displays.

Step 5 Enter a unique name and description for the policy.
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

Step 6 (Optional) To reboot all servers that use this boot policy after you make changes to the boot order, check the **Reboot on Boot Order Change** check box.
In Cisco UCS Manager GUI, if the **Reboot on Boot Order Change** check box is checked for a boot policy, and if CD-ROM or Floppy is the last device in the boot order, deleting or adding the device does not directly affect the boot order and the server does not reboot.

Step 7 (Optional) To ensure that Cisco UCS Manager uses any vNICs or vHBAs in the order shown in the **Boot Order** table, check the **Enforce vNIC/vHBA Name** check box.
If you do not check this check box, Cisco UCS Manager uses the priority specified in the vNIC or vHBA.

Step 8 To add a local disk, virtual CD-ROM, or virtual floppy to the boot order, do the following:

a) Click the down arrows to expand the **Local Devices** area.
b) Click one of the following links to add the device to the **Boot Order** table:

- **Add Local Disk**
- **Add CD-ROM**
- **Add Floppy**

c) Add another boot device to the **Boot Order** table, or click **OK** to finish.

Step 9 To add a LAN boot to the boot order, do the following:

a) Click the down arrows to expand the **vNICs** area.
b) Click the **Add LAN Boot** link.
c) In the **Add LAN Boot** dialog box, enter the name of the vNIC that you want to use for the LAN boot in the **vNIC** field, then click **OK**.
d) Add another device to the **Boot Order** table, or click **OK** to finish.

Step 10 To add a SAN boot to the boot order, do the following:

a) Click the down arrows to expand the **vHBAs** area.
b) Click the **Add SAN Boot** link.

c) In the **Add SAN Boot** dialog box, complete the following fields, then click **OK**:

Name	Description
vHBA field	Enter the name of the vHBA you want to use for the SAN boot.
Type field	This can be: • **primary**—If the server boots using a SAN WWN address, this is the first address it tries. Each boot policy can have only one primary SAN boot location. • **secondary**—If the server cannot boot from the primary SAN location, it attempts to boot from this location. Each boot policy can have only one secondary SAN boot location. The use of the terms primary or secondary boot devices does not imply a boot order. The effective order of boot devices within the same device class is determined by PCIe bus scan order.

d) If this vHBA points to a bootable SAN image, click the **Add SAN Boot Target** link and, in the **Add SAN Boot Target** dialog box, complete the following fields, then click **OK**:

Name	Description
Boot Target LUN field	The LUN that corresponds to the location of the boot image.
Boot Target WWPN field	The WWPN that corresponds to the location of the boot image.
Type field	This can be: • **primary**—If the server boots using a SAN WWN address, this is the first address it tries. Each boot policy can have only one primary SAN boot location. • **secondary**—If the server cannot boot from the primary SAN location, it attempts to boot from this location. Each boot policy can have only one secondary SAN boot location. The use of the terms primary or secondary boot devices does not imply a boot order. The effective order of boot devices within the same device class is determined by PCIe bus scan order.

e) Add another boot device to the **Boot Order** table, or click **OK** to finish.

What to Do Next

Include the boot policy in a service profile and/or template.

After a server is associated with a service profile that includes this boot policy, you can verify the actual boot order in the **Boot Order Details** area on the **General** tab for the server.

Deleting a Boot Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies ➤** ***Organization_Name***.

Step 3 Expand the **Boot Policies** node.

Step 4 Right-click the policy you want to delete and select **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring IPMI Access Profiles

IPMI Access Profile

This policy allows you to determine whether IPMI commands can be sent directly to the server, using the IP address. For example, you can send commands to retrieve sensor data from the CIMC. This policy defines the IPMI access, including a username and password that can be authenticated locally on the server, and whether the access is read-only or read-write.

You must include this policy in a service profile and that service profile must be associated with a server for it to take effect.

Creating an IPMI Access Profile

Before You Begin

An IPMI profile requires that one or more of the following resources already exist in the system:

- Username with appropriate permissions that can be authenticated by the operating system of the server
- Password for the username
- Permissions associated with the username

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **IPMI Profiles** and select **Create IPMI Profiles**.

Step 5 In the **Create IPMI Profile** dialog box:

a) Enter a unique name and description for the profile.

b) Click **OK**.

Step 6 In the **IPMI Profile Users** area of the navigator, click +.

Step 7 In the **User Properties** dialog box:

a) Complete the following fields:

Name	Description
Name field	The username to associate with this IPMI profile.
Password field	The password associated with this username.
Confirm Password field	The password a second time for confirmation purposes.
Role field	The user role. This can be: • **admin** • **Read Only**

b) Click **OK**.

Step 8 Repeat Steps 6 and 7 to add another user.

Step 9 Click **OK** to return to the IPMI profiles in the **Work** pane.

What to Do Next

Include the IPMI profile in a service profile and/or template.

Deleting an IPMI Access Profile

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 In the **Servers** tab, expand **Servers ➤ Policies ➤** *Organization_Name*

Step 3 Expand the **IPMI Profiles** node.

Step 4 Right-click the profile you want to delete and select **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring Local Disk Configuration Policies

Local Disk Configuration Policy

This policy configures any optional SAS local drives that have been installed on a server through the onboard RAID controller of the local drive. This policy enables you to set a local disk mode for all servers that are associated with a service profile that includes the local disk configuration policy.

The local disk modes include the following:

- **No Local Storage**—For a diskless server or a SAN only configuration. If you select this option, you cannot associate any service profile which uses this policy with a server that has a local disk.
- **RAID 0 Stripes**—Data is striped across all disks in the array, providing fast throughput. There is no data redundancy, and all data is lost if any disk fails.
- **RAID 1 Mirrored**—Data is written to two disks, providing complete data redundancy if one disk fails. The maximum array size is equal to the available space on the smaller of the two drives.
- **Any Configuration**—For a server configuration that carries forward the local disk configuration without any changes.
- **No RAID**—For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered.
- **RAID 6 Stripes Dual Parity**—Data is striped across all disks in the array and two parity disks are used to provide protection against the failure of up to two physical disks. In each row of data blocks, two sets of parity data are stored.
- **RAID 5 Striped Parity**—Data is striped across all disks in the array. Part of the capacity of each disk stores parity information that can be used to reconstruct data if a disk fails. RAID 5 provides good data throughput for applications with high read request rates.
- **RAID10 Mirrored and Striped**— RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates.

You must include this policy in a service profile, and that service profile must be associated with a server for the policy to take effect.

Guidelines and Considerations for a Local Disk Configuration Policy

Before you create a local disk configuration policy, consider the following guidelines:

No Mixed HDDs and SSDs

Do not include HDDs and SSDs in a single RAID configuration or in a single blade server.

Impact of Upgrade to Release 1.3(1i) or Higher

An upgrade from an earlier Cisco UCS firmware release to release 1.3(1i) or higher has the following impact on the Protect Configuration property of the local disk configuration policy the first time servers are associated with service profiles after the upgrade:

Unassociated Servers

After you upgrade the Cisco UCS instance, the initial server association proceeds without configuration errors whether or not the local disk configuration policy matches the server hardware. Even if you enable the Protect Configuration property, Cisco UCS does not protect the user data on the server if there are configuration mismatches between the local disk configuration policy on the previous service profile and the policy in the new service profile.

Note If you enable the Protect Configuration property and the local disk configuration policy encounters mismatches between the previous service profile and the new service profile, all subsequent service profile associations with the server are blocked.

Associated Servers

Any servers that are already associated with service profiles do not reboot after the upgrade. Cisco UCS Manager does not report any configuration errors if there is a mismatch between the local disk configuration policy and the server hardware.

When a service profile is disassociated from a server and a new service profile associated, the setting for the Protect Configuration property in the new service profile takes precedence and overwrites the setting in the previous service profile.

Maximum of One RAID Volume and One RAID Controller in Integrated Rack-Mount Servers

A rack-mount server that has been integrated with Cisco UCS Manager can have a maximum of one RAID volume irrespective of how many hard drives are present on the server.

All the local hard drives in an integrated rack-mount server must be connected to only one RAID Controller. Integration with Cisco UCS Manager does not support the connection of local hard drives to multiple RAID Controllers in a single rack-mount server. We therefore recommend that you request a single RAID Controller configuration when you order rack-mount servers to be integrated with Cisco UCS Manager.

In addition, do not use third party tools to create multiple RAID LUNs on rack-mount servers. Cisco UCS Manager does not support that configuration.

Do Not Use Any Configuration Mode with MegaRAID Storage Controllers

If a blade server or rack-mount server in a Cisco UCS instance includes a MegaRAID storage controller, do not configure the local disk configuration policy in the service profile for that server with the **Any**

Configuration mode. If you use this mode for servers with a MegaRAID storage controller, the installer for the operating system cannot detect any local storage on the server.

If you want to install an operating system on local storage on a server with a MegaRAID storage controller, you must configure the local disk configuration policy with a mode that creates a RAID LUN (RAID volume) on the server.

Creating a Local Disk Configuration Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **Local Disk Config Policies** and choose **Create Local Disk Configuration Policy**.

Step 5 In the **Create Local Disk Configuration Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Mode drop-down list	This can be one of the following local disk policy modes: • **No Local Storage**—For a diskless server or a SAN only configuration. If you select this option, you cannot associate any service profile which uses this policy with a server that has a local disk. • **RAID 0 Stripes**—Data is striped across all disks in the array, providing fast throughput. There is no data redundancy, and all data is lost if any disk fails. • **RAID 1 Mirrored**—Data is written to two disks, providing complete data redundancy if one disk fails. The maximum array size is equal to the available space on the smaller of the two drives. • **Any Configuration**—For a server configuration that carries forward the local disk configuration without any changes. • **No RAID**—For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered.

Name	Description
	• **RAID 6 Stripes Dual Parity**—Data is striped across all disks in the array and two parity disks are used to provide protection against the failure of up to two physical disks. In each row of data blocks, two sets of parity data are stored. • **RAID 5 Striped Parity**—Data is striped across all disks in the array. Part of the capacity of each disk stores parity information that can be used to reconstruct data if a disk fails. RAID 5 provides good data throughput for applications with high read request rates. • **RAID10 Mirrored and Striped**— RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates. **Note** If you choose **No RAID** and you apply this policy to a server that already has an operating system with RAID storage configured, the system does not remove the disk contents. Therefore, there may be no visible differences after you apply the **No RAID** mode. To make sure that any previous RAID configuration information is removed from a disk, apply a scrub policy that removes all disk information after you apply the **No RAID** configuration mode.
Protect Configuration check box	If checked, the server retains the configuration in the local disk configuration policy even if the server is disassociated from the service profile. This property is checked by default. When a service profile is disassociated from a server and a new service profile associated, the setting for the Protect Configuration property in the new service profile takes precedence and overwrites the setting in the previous service profile. **Note** If you disassociate the server from a service profile with this option enabled and then associate it with a new service profile that includes a local disk configuration policy with different properties, the server returns a configuration mismatch error and the association fails.

Step 6 Click **OK**.

Changing a Local Disk Configuration Policy

This procedure describes how to change a local disk configuration policy from an associated service profile. You can also change a local disk configuration policy from the **Policies** node of the **Servers** tab.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the organization that includes the service service profile with the local disk configuration policy you want to change.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Click the service profile that contains the local disk configuration policy you want to change.

Step 5 In the **Work** pane, click the **Policies** tab.

Step 6 In the **Actions** area, click **Change Local Disk Configuration Policy**.

Step 7 In the **Change Local Disk Configuration Policy** dialog box, choose one of the following options from the **Select the Local Disk Configuration Policy** drop-down list.

Option	Description
Use a Disk Policy	Select an existing local disk configuration policy from the list below this option. Cisco UCS Manager assigns this policy to the service profile.
Create a Local Disk Policy	Enables you to create a local disk configuration policy that can only be accessed by the selected service profile.
No Disk Policy	Does not use a local disk configuration policy for the selected service profile.

Step 8 Click **OK**.

Step 9 (Optional) Expand the **Local Disk Configuration Policy** area to confirm that the change has been made.

Deleting a Local Disk Configuration Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies ➤** ***Organization_Name***.

Step 3 Expand the **Local Disk Config Policies** node.

Step 4 Right-click the policy you want to delete and select **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring Scrub Policies

Scrub Policy

This policy determines what happens to local data and to the BIOS settings on a server during the discovery process and when the server is disassociated from a service profile. Depending upon how you configure a scrub policy, the following can occur at those times:

Disk Scrub — One of the following occurs to the data on any local drives on disassociation:

- If enabled, destroys all data on any local drives
- If disabled, preserves all data on any local drives, including local storage configuration

BIOS Settings Scrub — One of the following occurs to the BIOS settings when a service profile containing the scrub policy is disassociated from a server:

- If enabled, erases all BIOS settings for the server and and resets them to the BIOS defaults for that server type and vendor
- If disabled, preserves the existing BIOS settings on the server

Creating a Scrub Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **Scrub Policies** and select **Create Scrub Policy**.

Step 5 In the **Create Scrub Policy** wizard, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).

Name	Description
Disk Scrub field	If this field is set to **yes**, when a service profile containing this scrub policy is disassociated from a server, all data on the server local drives is completely erased. If this field is set to **no**, the data on the local drives is preserved, including all local storage configuration.
BIOS Settings Scrub field	If the field is set to **yes**, when a service profile containing this scrub policy is disassociated from a server, the BIOS settings for that server are erased and reset to the defaults for that server type and vendor. If this field is set to **no**, the BIOS settings are preserved.

Step 6 Click **OK**.

Deleting a Scrub Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.
Step 2 On the **Servers** tab, expand **Servers ➤ Policies ➤ *Organization_Name***.
Step 3 Expand the **Scrub Policies** node.
Step 4 Right-click the policy you want to delete and select **Delete**.
Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring Serial over LAN Policies

Serial over LAN Policy

This policy sets the configuration for the serial over LAN connection for all servers associated with service profiles that use the policy. By default, the serial over LAN connection is disabled.

If you implement a serial over LAN policy, we recommend that you also create an IPMI profile.

You must include this policy in a service profile and that service profile must be associated with a server for it to take effect.

Creating a Serial over LAN Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **Serial over LAN Policies** and select **Create Serial over LAN Policy**.

Step 5 In the **Create Serial over LAN Policy** wizard, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Serial over LAN State field	This can be: • **disable**—Serial over LAN access is blocked. • **enable**—Serial over LAN access is permitted.
Speed drop-down list	This can be: • **9600** • **19200** • **38400** • **57600** • **115200**

Step 6 Click **OK**.

Deleting a Serial over LAN Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.
Step 2 On the **Servers** tab, expand **Servers ➤ Policies ➤ *Organization_Name***.
Step 3 Expand the **Serial over LAN Policies** node.
Step 4 Right-click the policy you want to delete and select **Delete**.
Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring Server Autoconfiguration Policies

Server Autoconfiguration Policy

Cisco UCS Manager uses this policy to determine how to configure a new server. If you create a server autoconfiguration policy, the following occurs when a new server starts:

1 The qualification in the server autoconfiguration policy is executed against the server.
2 If the server meets the required qualifications, the server is associated with a service profile created from the service profile template configured in the server autoconfiguration policy. The name of that service profile is based on the name given to the server by Cisco UCS Manager.
3 The service profile is assigned to the organization configured in the server autoconfiguration policy.

Creating an Autoconfiguration Policy

Before You Begin

This policy requires that one or more of the following resources already exist in the system:

- Server pool policy qualifications
- Service profile template
- Organizations, if a system implements multi-tenancy

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, click the **Equipment** node.
Step 3 In the **Work** pane, click the **Policies** tab.
Step 4 Click the **Autoconfig Policies** subtab.
Step 5 On the icon bar to the right of the table, click +.

If the + icon is disabled, click an entry in the table to enable it.

Step 6 In the **Create Autoconfiguration Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Qualification drop-down list	The server pool policy qualification associated with this auto-configuration policy. If a new server is discovered that matches the criteria specified in the server pool policy qualification, Cisco UCS automatically creates a service profile based on the service profile template selected in the **Service Profile Template Name** drop-down list and associates the newly created service profile with the server.
Org drop-down list	The organization associated with this autoconfiguration policy. If Cisco UCS automatically creates a service profile to associate with a server, it places the service profile under the organization selected in this field.
Service Profile Template Name drop-down list	The service profile template associated with this policy.

Step 7 Click **OK**.

Deleting an Autoconfiguration Policy

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, click the **Equipment** node.
Step 3 In the **Work** pane, click the **Policies** tab.
Step 4 Click the **Autoconfig Policies** subtab.
Step 5 Right-click the autoconfiguration policy that you want to delete and choose **Delete**.
Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring Server Discovery Policies

Server Discovery Policy

This discovery policy determines how the system reacts when you add a new server. If you create a server discovery policy, you can control whether the system conducts a deep discovery when a server is added to a chassis, or whether a user must first acknowledge the new server. By default, the system conducts a full discovery.

If you create a server discovery policy, the following occurs when a new server starts:

1. The qualification in the server discovery policy is executed against the server.
2. If the server meets the required qualifications, Cisco UCS Manager applies the following to the server:
   - Depending upon the option selected for the action, either discovers the new server immediately or waits for a user to acknowledge the new server
   - Applies the scrub policy to the server

Creating a Server Discovery Policy

Before You Begin

If you plan to associate this policy with a server pool, create server pool policy qualifications.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, click the **Equipment** node.
Step 3 In the **Work** pane, click the **Policies** tab.
Step 4 Click the **Server Discovery Policies** subtab.
Step 5 Click the + icon on the table icon bar to open the **Create Server Discovery Policy** dialog box.
Step 6 In the **Description** field, enter a description for the discovery policy.
Step 7 In the **Action** field, select one of the following options:
- **immediate**—The system attempts to discover new servers automatically
- **user-acknowledged**—The system waits until the user tells it to search for new servers

Step 8 (Optional) To associate this policy with a server pool, select server pool policy qualifications from the **Qualification** drop-down list.
Step 9 (Optional) To include a scrub policy, select a policy from the **Scrub Policy** drop-down list.
Step 10 Click **OK**.

What to Do Next

Include the server discovery policy in a service profile and/or template.

Deleting a Server Discovery Policy

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, click the **Equipment** node.
Step 3 In the **Work** pane, click the **Policies** tab.
Step 4 Click the **Server Discovery Policies** subtab.
Step 5 Right-click the server discover policy that you want to delete and choose **Delete**.
Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring Server Inheritance Policies

Server Inheritance Policy

This policy is invoked during the server discovery process to create a service profile for the server. All service profiles created from this policy use the values burned into the blade at manufacture. The policy performs the following:

- Analyzes the inventory of the server
- If configured, assigns the server to the selected organization
- Creates a service profile for the server with the identity burned into the server at manufacture

You cannot migrate a service profile created with this policy to another server.

Creating a Server Inheritance Policy

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, click the **Equipment** node.
Step 3 In the **Work** pane, click the **Policies** tab.
Step 4 Click the **Server Inheritance Policies** subtab.
Step 5 On the icon bar to the right of the table, click +.
If the + icon is disabled, click an entry in the table to enable it.
Step 6 In the **Create Server Inheritance Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Qualification drop-down list	If you want to associate this policy with one or more specific server pools, choose the server pool qualification policy that identifies these pools from the drop-down list.
Org drop-down list	If you want to associate an organization with this policy, or if you want to change the current association, choose the desired organization from the drop-down list.

Step 7 Click **OK**.

Deleting a Server Inheritance Policy

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, click the **Equipment** node.
Step 3 In the **Work** pane, click the **Policies** tab.
Step 4 Click the **Server Inheritance Policies** subtab.
Step 5 Right-click the server inheritance policy that you want to delete and choose **Delete**.
Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring Server Pool Policies

Server Pool Policy

This policy is invoked during the server discovery process. It determines what happens if server pool policy qualifications match a server to the target pool specified in the policy.

If a server qualifies for more than one pool and those pools have server pool policies, the server is added to all those pools.

Creating a Server Pool Policy

Before You Begin

This policy requires that one or more of the following resources already exist in the system:

- A minimum of one server pool
- Server pool policy qualifications, if you choose to have servers automatically added to pools

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **Server Pool Policies** and select **Create Server Pool Policy**.

Step 5 In the **Create Server Pool Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Target Pool drop-down list	If you want to associate this policy with a server pool, select that pool from the drop-down list.
Qualification drop-down list	If you want to associate this policy with one or more specific server pools, choose the server pool qualification policy that identifies these pools from the drop-down list.

Step 6 Click **OK**.

Deleting a Server Pool Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies ➤ *Organization_Name***.

Step 3 Expand the **Server Pool Policies** node.

Step 4 Right-click the policy you want to delete and select **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring Server Pool Policy Qualifications

Server Pool Policy Qualifications

This policy qualifies servers based on the inventory of a server conducted during the discovery process. The qualifications are individual rules that you configure in the policy to determine whether a server meets the selection criteria. For example, you can create a rule that specifies the minimum memory capacity for servers in a data center pool.

Qualifications are used in other policies to place servers, not just by the server pool policies. For example, if a server meets the criteria in a qualification policy, it can be added to one or more server pools or have a service profile automatically associated with it.

You can use the server pool policy qualifications to qualify servers according to the following criteria:

- Adapter type
- Chassis location
- Memory type and configuration
- Power group
- CPU cores, type, and configuration
- Storage configuration and capacity
- Server model

Depending upon the implementation, you may configure several policies with server pool policy qualifications including the following:

- Autoconfiguration policy
- Chassis discovery policy
- Server discovery policy
- Server inheritance policy
- Server pool policy

Creating Server Pool Policy Qualifications

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the **Server Pool Policy Qualifications** node and select **Create Server Pool Policy Qualification**.

Step 5 In the **Create Server Pool Policy Qualification** dialog box, enter a unique name and description for the policy.

Step 6 (Optional) To use this policy to qualify servers according to their adapter configuration, do the following:

a) Click **Create Adapter Qualifications**.

b) In the **Create Adapter Qualifications** dialog box, complete the following fields:

Name	Description
Type drop-down list	The adapter type. This can be: • **fcoe**—Fibre Channel over Ethernet • **non-virtualized-eth-if** • **non-virtualized-fc-if** • **path-encap-consolidated** • **path-encap-virtual** • **protected-eth-if** • **protected-fc-if** • **protected-fcoe** • **virtualized-eth-if** • **virtualized-fc-if** • **virtualized-scsi-if** Once you save the adapter qualification, this type cannot be changed.
Model field	A regular expression that the adapter model name must match.
Maximum Capacity field	The maximum capacity for the selected type. To specify a capacity, choose **select** and enter the desired maximum capacity.

c) Click **OK**.

Step 7 (Optional) To use this policy to qualify servers according to the chassis in which they physically reside, do the following:

a) Click **Create Chassis/Server Qualifications**.

b) In the **Chassis Qualifications** area of the **Create Chassis and Server Qualifications** dialog box, complete the following fields to specify the range of chassis you want to use:

- **First Chassis ID** field—The first chassis ID from which server pools associated with this policy can draw.
- **Number of Chassis** field—The total number of chassis to include in the pool, starting with the chassis identified in the **First Chassis ID** field.

Example:
For example, if you want to use chassis 5, 6, 7, and 8, enter 5 in the **First Chassis ID** field and 4 in the **Number of Chassis** field. If you want to use only chassis 3, enter 3 in the **First Chassis ID** field and 1 in the **Number of Chassis** field.

Tip If you want to use chassis 5, 6, and 9, create a chassis/server qualification for the range 5-6 and another qualification for chassis 9. You can add as many chassis/server qualifications as needed.

c) Click **Finish**.

Step 8 (Optional) To use this policy to qualify servers according to both the chassis and slot in which they physically reside, do the following:

a) Click **Create Chassis/Server Qualifications**.

b) In the **Chassis Qualifications** area of the **Create Chassis and Server Qualifications** dialog box, complete the following fields to specify the range of chassis you want to use:

- **First Chassis ID** field—The first chassis ID from which server pools associated with this policy can draw.
- **Number of Chassis** field—The total number of chassis to include in the pool, starting with the chassis identified in the **First Chassis ID** field.

c) In the **Server Qualifications** table, click **Add**.

d) In the **Create Server Qualifications** dialog box, complete the following fields to specify the range of server locations you want to use:

- **First Slot ID** field—The first slot ID from which server pools associated with this policy can draw.
- **Number of Slots** field—The total number of slots from which server pools associated with this policy can draw.

e) Click **Finish Stage**.

f) To add another range of slots, click **Add** and repeat steps d and e.

g) When you have finished specifying the slot ranges, click **Finish**.

Step 9 (Optional) To use this policy to qualify servers according to their memory configuration, do the following:

a) Click **Create Memory Qualifications**.

b) In the **Create Memory Qualifications** dialog box, complete the following fields:

Name	Description
Clock field	The minimum clock speed required, in megahertz.
Latency field	The maximum latency allowed, in nanoseconds.
Min Cap field	The minimum CPU capacity required, in megabytes.
Max Cap field	The maximum CPU capacity allowed, in megabytes.
Width field	The minimum width of the data bus.
Units field	The unit of measure to associate with the value in the **Width** field.

c) Click **OK**.

Step 10 (Optional) To use this policy to qualify servers according to their CPU/Cores configuration, do the following:

a) Click **Create CPU/Cores Qualifications**.

b) In the **Create CPU/Cores Qualifications** dialog box, complete the following fields:

Name	Description
Processor Architecture drop-down list	The CPU architecture to which this policy applies.
Model field	A regular expression that the processor model name must match.
Min Number of Cores field	The minimum number of CPU cores required. To specify a capacity, choose **select** and enter the minimum number of cores.
Max Number of Cores field	The maximum number of CPU cores allowed. To specify a capacity, choose **select** and enter the maximum number of cores.
Min Number of Threads field	The minimum number of CPU threads required. To specify a capacity, choose **select** and enter the minimum number of threads.
Max Number of Threads field	The maximum number of CPU threads allowed. To specify a capacity, choose **select** and enter the maximum number of threads.
CPU Speed field	The minimum CPU speed required. To specify a capacity, choose **select** and enter the minimum CPU speed.
CPU Stepping field	The minimum CPU version required.

Name	Description
	To specify a capacity, choose **select** and enter the maximum CPU speed.

c) Click **OK**.

Step 11 (Optional) To use this policy to qualify servers according to their storage configuration and capacity, do the following:

a) Click **Create Storage Qualifications**.

b) In the **Create Storage Qualifications** dialog box, complete the following fields:

Name	Description
Diskless field	Whether the available storage must be diskless. This can be: • **unspecified**—Either storage type is acceptable. • **yes**—The storage must be diskless. • **no**—The storage cannot be diskless.
Number of Blocks field	The minimum number of blocks required. To specify a capacity, choose **select** and enter the number of blocks.
Block Size field	The minimum block size required, in bytes. To specify a capacity, choose **select** and enter the block size.
Min Cap field	The minimum storage capacity across all disks in the server, in megabytes. To specify a capacity, choose **select** and enter the minimum storage capacity.
Max Cap field	The maximum storage capacity allowed, in megabytes. To specify a capacity, choose **select** and enter the maximum storage capacity.
Per Disk Cap field	The minimum storage capacity per disk required, in gigabytes. To specify a capacity, choose **select** and enter the minimum capacity on each disk.
Units field	The number of units. To specify a capacity, choose **select** and enter the desired units.

c) Click **OK**.

Step 12 (Optional) To use this policy to qualify servers according to the model of the server, do the following:

a) Click **Create Server Model Qualifications**.

b) In the **Create Server Model Qualifications** dialog box, enter a regular expression that the server model must match in the **Model** field.
c) Click **OK**.

Step 13 (Optional) To use this policy to qualify servers according to power group, do the following:
a) Click **Create Power Group Qualifications**.
b) In the **Create Power Group Qualifications** dialog box, choose a power gruup from the **Power Group** drop-down list.
c) Click **OK**.

Step 14 (Optional) To use this policy to qualify the rack-mount servers that can be added to the associated server pool, do the following:
a) Click **Create Rack Qualifications**.
b) In the **Create Rack Qualifications** dialog box, complete the following fields:

Name	Description
First Slot ID field	The first rack-mount server slot ID from which server pools associated with this policy can draw.
Number of Slots field	The total number of rack-mount server slots from which server pools associated with this policy can draw.

Step 15 Verify the qualifications in the table and correct if necessary.
Step 16 Click **OK**.

Deleting Server Pool Policy Qualifications

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.
Step 2 On the **Servers** tab, expand **Servers ➤ Policies ➤ *Organization_Name***.
Step 3 Expand the **Server Pool Policy Qualifications** node.
Step 4 Right-click the policy qualifications you want to delete and select **Delete**.
Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Deleting Qualifications from Server Pool Policy Qualifications

Use this procedure to modify Server Pool Policy Qualifications by deleting one or more sets of qualifications.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies ➤ *Organization_Name***.

Step 3 Expand the **Server Pool Policy Qualifications** node.

Step 4 Choose the policy you want to modify.

Step 5 In the **Work** pane, choose the **Qualifications** tab.

Step 6 To delete a set of qualifications:

a) In the table, choose the row that represents the set of qualifications.

b) Right-click the row and select **Delete**.

Step 7 Click **Save Changes**.

Configuring vNIC/vHBA Placement Policies

vNIC/vHBA Placement Policies

vNIC/vHBA placement policies are used to assign vNICs or vHBAs to the physical adapters on a server. Each vNIC/vHBA placement policy contains two virtual network interface connections (vCons) that are virtual representations of the physical adapters. When a vNIC/vHBA placement policy is assigned to a service profile, and the service profile is associated to a server, the vCons in the vNIC/vHBA placement policy are assigned to the physical adapters. For servers with only one adapter, both vCons are assigned to the adapter; for servers with two adapters, one vCon is assigned to each adapter.

You can assign vNICs or vHBAs to either of the two vCons, and they are then assigned to the physical adapters based on the vCon assignment during server association. Additionally, vCons use the following selection preference criteria to assign vHBAs and vNICs:

All	The vCon is used for vNICs or vHBAs assigned to it, vNICs or vHBAs not assigned to either vCon, and dynamic vNICs or vHBAs.
Assigned-Only	The vCon is reserved for only vNICs or vHBAs assigned to it.
Exclude-Dynamic	The vCon is not used for dynamic vNICs or vHBAs.
Exclude-Unassigned	The vCon is not used for vNICs or vHBAs not assigned to the vCon. The vCon is used for dynamic vNICs and vHBAs.

For servers with two adapters, if you do not include a vNIC/vHBA placement policy in a service profile, or you do not configure vCons for a service profile, Cisco UCS equally distributes the vNICs and vHBAs between the two adapters.

Creating a vNIC/vHBA Placement Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **vNIC/vHBA Placement Policies** and choose **Create Placement Policy**.

Step 5 In the **Create Placement Policy** dialog box, do the following:

a) In the **Name** field, enter a unique name for the placement policy.
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

b) In the **Selection Preference** column for each **Virtual Slot**, choose one of the following from the drop-down list:

- **all**
- **assigned-only**
- **exclude-dynamic**
- **exclude-unassigned**

c) Click **OK**.

Deleting a vNIC/vHBA Placement Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies ➤** ***Organization_Name***.

Step 3 Expand the **vNIC/vHBA Placement Policies** node.

Step 4 Right-click the policy you want to delete and choose **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

CHAPTER 27

Deferring Deployment of Service Profile Updates

This chapter includes the following sections:

Deferred Deployment of Service Profiles

Some modifications to a service profile or to an updating service profile template can be disruptive and require a reboot of the server. You can, however, configure deferred deployment to control when those disruptive configuration changes are implemented. For example, you can choose to deploy the service profile changes immediately or have them deployed during a specified maintenance window. You can also choose whether or not a service profile deployment requires explicit user acknowledgement.

Deferred deployment is available for all configuration changes that occur through the association of a service profile with a server. These configuration changes can be prompted by a change to a service profile, to a policy that is included in a service profile, or to an updating service profile template. For example, you can defer the upgrade and activation of firmware through host firmware packages and management firmware packages, such as server BIOS, RAID controller, host HBA, and network adapters. However, you cannot defer the direct deployment of firmware images for components that do not use either of the firmware packages, such as Cisco UCS Manager, fabric interconnects, and I/O modules.

Deferred deployment is not available for the following actions which require the reboot of a server:

- Initial association of a service profile with a server
- Final disassociation of a service profile from a server, without associating the service profile with a different server
- Decommissioning a server
- Reacknowledging a server
- Resetting a server

If you want to defer the deployment of service profile changes, you must configure one or more maintenance policies and configure each service profile with a maintenance policy. If you want to define the time period when the deployment should occur, you also need to create at least one schedule with one or more recurring occurrences or one time occurrences, and include that schedule in a maintenance policy.

Deferred Deployment Schedules

A schedule contains a set of occurrences. These occurrences can be one time only or can recur at a specified time and day each week. The options defined in the occurrence, such as the duration of the occurrence or the maximum number of tasks to be run, determine whether a service profile change is deployed. For example, if a change cannot be deployed during a given maintenance window because the maximum duration or number of tasks has been reached, that deployment is carried over to the next maintenance window.

Each schedule checks periodically to see whether the Cisco UCS instance has entered one or more maintenance windows. If it has, the schedule executes the deployments that are eligible according to the constraints specified in the maintenance policy

A schedule contains one or more occurrences, which determine the maintenance windows associated with that schedule. An occurrence can be one of the following:

One Time Occurrence	One time occurrences define a single maintenance window. These windows continue until the maximum duration of the window or the maximum number of tasks that can be run in the window has been reached.
Recurring Occurrence	Recurring occurrences define a series of maintenance windows. These windows continue until the maximum number of tasks or the end of the day specified in the occurrence has been reached.

Maintenance Policy

A maintenance policy determines how Cisco UCS Manager reacts when a change that requires a server reboot is made to a service profile associated with a server or to an updating service profile bound to one or more service profiles.

The maintenance policy specifies how Cisco UCS Manager deploys the service profile changes. The deployment can occur in one of the following ways:

- Immediately
- When acknowledged by a user with admin privileges
- Automatically at the time specified in the schedule

If the maintenance policy is configured to deploy the change during a scheduled maintenance window, the policy must include a valid schedule. The schedule deploys the changes in the first available maintenance window.

Pending Activities

If you configure deferred deployment in a Cisco UCS instance, Cisco UCS Manager enables you to view all pending activities. You can see activities that are waiting for user acknowledgement and those that have been scheduled.

If a Cisco UCS instance has pending activities, Cisco UCS Manager GUI notifies users with admin privileges when they log in.

Cisco UCS Manager displays information about all pending activities, including the following:

- Name of the service profile to be deployed and associated with a server
- Server affected by the deployment
- Disruption caused by the deployment
- Change performed by the deployment

Note You cannot specify the maintenance window in which a specific pending activity is applied to the server. The maintenance window depends upon how many activities are pending and which maintenance policy is assigned to the service profile. However, any user with admin privileges can manually initiate a pending activity and reboot the server immediately, whether it is waiting for user acknowledgement or for a maintenance window.

Guidelines and Limitations for Deferred Deployment

Cannot Undo All Changes to Service Profiles or Service Profile Templates

If you cancel a pending change, Cisco UCS Manager attempts to roll back the change without rebooting the server. However, for complex changes, Cisco UCS Manager may have to reboot the server a second time to roll back the change. For example, if you delete a vNIC, Cisco UCS Manager reboots the server according to the maintenance policy included in the service profile. You cannot cancel this reboot and change, even if you restore the original vNIC in the service profile. Instead, Cisco UCS Manager schedules a second deployment and reboot of the server.

Association of Service Profile Can Exceed Boundaries of Maintenance Window

After Cisco UCS Manager begins the association of the service profile, the scheduler and maintenance policy do not have any control over the procedure. If the service profile association does not complete within the allotted maintenance window, the process continues until it is completed. For example, this can occur if the association does not complete in time because of retried stages or other issues.

Cannot Specify Order of Pending Activities

Scheduled deployments run in parallel and independently. You cannot specify the order in which the deployments occur. You also cannot make the deployment of one service profile change dependent upon the completion of another.

Cannot Perform Partial Deployment of Pending Activity

Cisco UCS Manager applies all changes made to a service profile in the scheduled maintenance window. You cannot make several changes to a service profile at the same time and then have those changes be spread across several maintenance windows. When Cisco UCS Manager deploys the service profile changes, it updates the service profile to match the most recent configuration in the database.

Configuring Schedules

Creating a Schedule

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, right-click **Schedules** and choose **Create Schedule**.

Step 3 In the **Identify Schedule** page of the **Create Schedule** wizard, complete the following fields:

Name	Description
Name field	The name of the schedule. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the schedule. We recommend including information about where and when the schedule should be used. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).

Step 4 Click **Next**.

Step 5 On the **One Time Occurrences** page, click one of the following:

Option	Description
Next	Moves to the next page. Choose this option if you do not want to create a one time occurrence for this schedule. If you choose this option, continue with Step 8.
Add	Opens the **Create a One Time Occurrence** dialog box, where you can specify a single time when this schedule should be run. If you choose this option, continue with Step 6.

Step 6 (Optional) In the **Create a One Time Occurrence** dialog box, do the following:

a) Complete the following fields:

Name	Description
Name field	The name of the one time occurrence of this schedule. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

Name	Description
Start Time field	The date and time that the occurrence should run. Click the down arrow at the end of the field to select the date from a calendar.

b) Click the down arrows to expand the **Options** area.
c) In the **Options** area, complete the following fields:

Name	Description
Max Duration field	The maximum length of time that this scheduled occurrence can run. This can be: • **none**—The occurrence runs until all tasks are completed. • **other**—Cisco UCS Manager GUI displays the **dd:hh:mm:ss** field allowing you to specify the maximum amount of time that the occurrence can run. Cisco UCS completes as many scheduled tasks as possible within the specified time. By default, the maximum duration is set to **none**. If you do not change this setting and you do not set a maximum number of tasks, the maintenance window continues until all pending activities are completed.
Max Number of Tasks field	The maximum number of scheduled tasks that can be run during this occurrence. This can be: • **Unlimited**—Cisco UCS runs all scheduled tasks unless those tasks exceed the maximum time specified in the **Max Duration** field. If **Max Duration** is set to **none** and you select this option, the maintenance window continues until all pending activities are completed. • **other**—Cisco UCS Manager GUI displays a text field allowing you to specify the maximum number of tasks that can be run during this occurrence. Enter an integer between 1 and 65535.
Max Number of Concurrent Tasks field	The maximum number of tasks that can run concurrently during this occurrence. This can be: • **Unlimited**—Cisco UCS runs as many concurrent tasks as the system can handle. • **other**—Cisco UCS Manager GUI displays a text field allowing you to specify the maximum number of concurrent tasks that can be run during this occurrence. Enter an integer between 1 and 65535.
Minimum Interval Between Tasks field	The minimum length of time that the system should wait before starting a new task. This setting is meaningful only if the maximum

Name	Description
	number of concurrent tasks is set to a value other than none. This can be: • **none**—Cisco UCS runs the next task as soon as possible. • **other**—Cisco UCS Manager GUI displays the **dd:hh:mm:ss** field allowing you to specify the minimum amount of time that Cisco UCS will wait between tasks.

d) Click **OK**.

Step 7 To add another one time occurrence, click **Add** and repeat step 6. Otherwise, click **Next**.

Step 8 (Optional) If you want to define a recurring occurrence for this schedule, on the **Recurring Occurrences** page, click **Add**.

a) In the **Create a Recurring Occurrence** dialog box, complete the following fields:

Name	Description
Name field	The name of the recurring occurrence of this schedule. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Day field	The day on which Cisco UCS runs an occurrence of this schedule. This can be: • **every day** • **Monday** • **Tuesday** • **Wednesday** • **Thursday** • **Friday** • **Saturday** • **Sunday** • **odd days** • **even days**
Hour field	The hour of the specified day at which this occurrence of the schedule starts. This can be an integer between 0 and 24, where 0 and 24 are both equivalent to midnight.
Minute field	The minute of the hour at which the schedule occurrence starts. This can be an integer between 0 and 60.

b) Click the down arrows to expand the **Options** area.
c) In the **Options** area, complete the following fields:

Name	Description
Max Duration field	The maximum length of time that each occurrence of this schedule can run. This can be: • **none**—The occurrence runs until all tasks are completed. • **other**—Cisco UCS Manager GUI displays the **dd:hh:mm:ss** field allowing you to specify the maximum amount of time that the occurrence can run. Cisco UCS completes as many scheduled tasks as possible within the specified time.
Max Number of Tasks field	The maximum number of scheduled tasks that can be run during each occurrence. This can be: • **Unlimited**—Cisco UCS runs all scheduled tasks unless those tasks exceed the maximum time specified in the **Max Duration** field. If **Max Duration** is set to **none** and you select this option, the maintenance window continues until all pending activities are completed. • **other**—Cisco UCS Manager GUI displays a text field allowing you to specify the maximum number of tasks that can be run during this occurrence. Enter an integer between 1 and 65535.
Max Number of Concurrent Tasks field	The maximum number of tasks that can run concurrently during each occurrence. This can be: • **Unlimited**—Cisco UCS runs as many concurrent tasks as the system can handle. • **other**—Cisco UCS Manager GUI displays a text field allowing you to specify the maximum number of concurrent tasks that can be run during this occurrence. Enter an integer between 1 and 65535.
Minimum Interval Between Tasks field	The minimum length of time that the system should wait before starting a new task. This setting is meaningful only if the maximum number of concurrent tasks is set to a value other than none. This can be: • **none**—Cisco UCS runs the next task as soon as possible. • **other**—Cisco UCS Manager GUI displays the **dd:hh:mm:ss** field allowing you to specify the minimum amount of time that Cisco UCS will wait between tasks.

d) Click **OK**.

e) To add another recurring occurrence, click **Add** and repeat this step.

Step 9 Click **Finish**.

Creating a One Time Occurrence for a Schedule

Note By default, the maximum duration and the maximum number of tasks are set to **none**. If you do not change either of these defaults, Cisco UCS Manager does not impose any limit to the length of time that the maintenance window lasts. All pending activities are applied as soon as the scheduled maintenance window begins, and Cisco UCS Manager continues to reboot the servers impacted by the pending activities until all of those tasks are complete.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Schedules**.

Step 3 Right-click the schedule to which you want to add an occurrence and choose **Create a One Time Occurrence**.

Step 4 In the **Create a One Time Occurrence** dialog box, complete the following fields:

Name	Description
Name field	The name of the one time occurrence of this schedule. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Start Time field	The date and time that the occurrence should run. Click the down arrow at the end of the field to select the date from a calendar.

Step 5 Click the down arrows to expand the **Options** area.

Step 6 In the **Options** area, complete the following fields:

Name	Description
Max Duration field	The maximum length of time that this scheduled occurrence can run. This can be: • **none**—The occurrence runs until all tasks are completed. • **other**—Cisco UCS Manager GUI displays the **dd:hh:mm:ss** field allowing you to specify the maximum amount of time that the occurrence can run. Cisco UCS completes as many scheduled tasks as possible within the specified time.

Name	Description
	By default, the maximum duration is set to **none**. If you do not change this setting and you do not set a maximum number of tasks, the maintenance window continues until all pending activities are completed.
Max Number of Tasks field	The maximum number of scheduled tasks that can be run during this occurrence. This can be: • **Unlimited**—Cisco UCS runs all scheduled tasks unless those tasks exceed the maximum time specified in the **Max Duration** field. If **Max Duration** is set to **none** and you select this option, the maintenance window continues until all pending activities are completed. • **other**—Cisco UCS Manager GUI displays a text field allowing you to specify the maximum number of tasks that can be run during this occurrence. Enter an integer between 1 and 65535.
Max Number of Concurrent Tasks field	The maximum number of tasks that can run concurrently during this occurrence. This can be: • **Unlimited**—Cisco UCS runs as many concurrent tasks as the system can handle. • **other**—Cisco UCS Manager GUI displays a text field allowing you to specify the maximum number of concurrent tasks that can be run during this occurrence. Enter an integer between 1 and 65535.
Minimum Interval Between Tasks field	The minimum length of time that the system should wait before starting a new task. This setting is meaningful only if the maximum number of concurrent tasks is set to a value other than none. This can be: • **none**—Cisco UCS runs the next task as soon as possible. • **other**—Cisco UCS Manager GUI displays the **dd:hh:mm:ss** field allowing you to specify the minimum amount of time that Cisco UCS will wait between tasks.

Step 7 Click **OK**.

Creating a Recurring Occurrence for a Schedule

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Schedules**.

Step 3 Right-click the schedule to which you want to add an occurrence and choose **Create a Recurring Occurrence**.

Step 4 In the **Create a Recurring Occurrence** dialog box, complete the following fields:

Name	Description
Name field	The name of the recurring occurrence of this schedule. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Day field	The day on which Cisco UCS runs an occurrence of this schedule. This can be: • **every day** • **Monday** • **Tuesday** • **Wednesday** • **Thursday** • **Friday** • **Saturday** • **Sunday** • **odd days** • **even days**
Hour field	The hour of the specified day at which this occurrence of the schedule starts. This can be an integer between 0 and 24, where 0 and 24 are both equivalent to midnight.
Minute field	The minute of the hour at which the schedule occurrence starts. This can be an integer between 0 and 60.

Step 5 Click the down arrows to expand the **Options** area.

Step 6 In the **Options** area, complete the following fields:

Name	Description
Max Duration field	The maximum length of time that each occurrence of this schedule can run. This can be: • **none**—The occurrence runs until all tasks are completed. • **other**—Cisco UCS Manager GUI displays the **dd:hh:mm:ss** field allowing you to specify the maximum amount of time that the occurrence can run. Cisco UCS completes as many scheduled tasks as possible within the specified time.
Max Number of Tasks field	The maximum number of scheduled tasks that can be run during each occurrence. This can be: • **Unlimited**—Cisco UCS runs all scheduled tasks unless those tasks exceed the maximum time specified in the **Max Duration** field. If **Max Duration** is set to **none** and you select this option, the maintenance window continues until all pending activities are completed. • **other**—Cisco UCS Manager GUI displays a text field allowing you to specify the maximum number of tasks that can be run during this occurrence. Enter an integer between 1 and 65535.
Max Number of Concurrent Tasks field	The maximum number of tasks that can run concurrently during each occurrence. This can be: • **Unlimited**—Cisco UCS runs as many concurrent tasks as the system can handle. • **other**—Cisco UCS Manager GUI displays a text field allowing you to specify the maximum number of concurrent tasks that can be run during this occurrence. Enter an integer between 1 and 65535.
Minimum Interval Between Tasks field	The minimum length of time that the system should wait before starting a new task. This setting is meaningful only if the maximum number of concurrent tasks is set to a value other than none. This can be: • **none**—Cisco UCS runs the next task as soon as possible. • **other**—Cisco UCS Manager GUI displays the **dd:hh:mm:ss** field allowing you to specify the minimum amount of time that Cisco UCS will wait between tasks.

Step 7 Click **OK**.

Deleting a One Time Occurrence from a Schedule

If this is the only occurrence in a schedule, that schedule is reconfigured with no occurrences. If the schedule is included in a maintenance policy and that policy is assigned to a service profile, any pending activities related to the server associated with the service profile cannot be deployed. You must add a one time ocurrence or a recurring occurrence to the schedule to deploy the pending activity.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Schedules** ➤ ***Schedule_Name***.

Step 3 Expand **One Time Occurrences**.

Step 4 Right-click the occurrence you want to delete and choose **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Deleting a Recurring Occurrence from a Schedule

If this is the only occurrence in a schedule, that schedule is reconfigured with no occurrences. If the schedule is included in a maintenance policy and that policy is assigned to a service profile, any pending activities related to the server associated with the service profile cannot be deployed. You must add a one time ocurrence or a recurring occurrence to the schedule to deploy the pending activity.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Schedules** ➤ ***Schedule_Name***.

Step 3 Expand **Recurring Occurrences**.

Step 4 Right-click the occurrence you want to delete and choose **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Deleting a Schedule

If this schedule is included in a maintenance policy, the policy is reconfigured with no schedule. If that policy is assigned to a service profile, any pending activities related to the server associated with the service profile cannot be deployed. You must add a schedule to the maintenance policy to deploy the pending activity.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.
Step 2 On the **Servers** tab, expand **Schedules**.
Step 3 Right-click the schedule you want to delete and choose **Delete**.
Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring Maintenance Policies

Creating a Maintenance Policy

Before You Begin

If you plan to configure this maintenance policy for automatic deferred deployment, create a schedule.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.
Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.
Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.
Step 4 Right-click **Maintenance Policies** and choose **Create Maintenance Policy**.
Step 5 In the **Create Maintenance Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Reboot Policy field	When a service profile is associated with a server, or when changes are made to a service profile that is already associated with a server, the server needs to be rebooted to complete the process. The **Reboot Policy** field determines when the reboot occurs for servers associated with any service profiles that include this maintenance policy. This can be:

Name	Description
	• **immediate**—The server is rebooted automatically as soon as the service profile association is complete or service profile changes are saved by the user. • **user-ack**—The user must reboot the server manually after the service profile association is complete or changes are made. • **timer-automatic**—Cisco UCS defers all service profile associations and changes until the maintenance window defined by the schedule shown in the **Schedule** field.
Schedule drop-down list	If the **Reboot Policy** is set to **timer-automatic**, the schedule specifies when maintenance operations can be applied to the server. Cisco UCS reboots the server and completes the service profile changes at the scheduled time.

Step 6 Click **OK**.

What to Do Next

Include the policy in a service profile or service profile template.

Deleting a Maintenance Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.
Step 2 On the **Servers** tab, expand **Servers ➤ Policies ➤ *Organization_Name***.
Step 3 Expand **Maintenance Policies**.
Step 4 Right-click the maintenance policy you want to delete and choose **Delete**.
Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Managing Pending Activities

Viewing Pending Activities

Procedure

Step 1 On the toolbar, click **Pending Activities**.
Step 2 Click one of the following tabs:

- **User Acknowledged Activities**—Displays the tasks that require user acknowledgement before they can complete.
- **Scheduled Activities**—Displays the tasks that will be performed based on the associated maintenance schedule.

Step 3 Click a row in the table to view the details of that pending activity.
If you click the link in the **Server** column, Cisco UCS Manager displays the properties of that server.

Deploying a Service Profile Change Waiting for User Acknowledgement

Important You cannot stop Cisco UCS Manager from rebooting the affected server after you acknowledge a pending activity.

Procedure

Step 1 On the toolbar, click **Pending Activities**.
Step 2 In the **Pending Activities** dialog box, click the **User Acknowledged Activities** tab.
Step 3 In the **Reboot Now** column of the table, check the **Acknowledge All** check box for the pending activity you want to deploy immediately.
Step 4 Click **OK**.
Cisco UCS Manager immediately reboots the server affected by the pending activity.

Deploying All Service Profile Changes Waiting for User Acknowledgement

Important You cannot stop Cisco UCS Manager from rebooting the affected server after you acknowledge a pending activity.

Procedure

Step 1 On the toolbar, click **Pending Activities**.
Step 2 In the **Pending Activities** dialog box, click the **User Acknowledged Activities** tab.
Step 3 In the toolbar, check the **Acknowledge All** check box.
Cisco UCS Manager GUI checks the **Reboot Now** check boxes for all pending activities listed in the table.
Step 4 Click **OK**.
Cisco UCS Manager immediately reboots all servers affected by the pending activities listed in the table.

Deploying a Scheduled Service Profile Change Immediately

Important You cannot stop Cisco UCS Manager from rebooting the affected server after you acknowledge a pending activity.

Procedure

Step 1 On the toolbar, click **Pending Activities**.

Step 2 In the **Pending Activities** dialog box, click the **Scheduled Activities** tab.

Step 3 In the **Reboot Now** column of the table, check the **Acknowledge All** check box for the pending activity you want to deploy immediately.

Step 4 Click **OK**.
Cisco UCS Manager immediately reboots the server affected by the pending activity.

Deploying All Scheduled Service Profile Changes Immediately

Important You cannot stop Cisco UCS Manager from rebooting the affected server after you acknowledge a pending activity.

Procedure

Step 1 On the toolbar, click **Pending Activities**.

Step 2 In the **Pending Activities** dialog box, click the **Scheduled Activities** tab.

Step 3 In the toolbar, check the **Acknowledge All** check box.
Cisco UCS Manager GUI checks the **Reboot Now** check boxes for all pending activities listed in the table.

Step 4 Click **OK**.
Cisco UCS Manager immediately reboots all servers affected by the pending activities listed in the table.

CHAPTER 28

Configuring Service Profiles

This chapter includes the following sections:

Service Profiles that Override Server Identity

This type of service profile provides the maximum amount of flexibility and control. This profile allows you to override the identity values that are on the server at the time of association and use the resource pools and policies set up in Cisco UCS Manager to automate some administration tasks.

You can disassociate this service profile from one server and then associate it with another server. This re-association can be done either manually or through an automated server pool policy. The burned-in settings, such as UUID and MAC address, on the new server are overwritten with the configuration in the service profile. As a result, the change in server is transparent to your network. You do not need to reconfigure any component or application on your network to begin using the new server.

This profile allows you to take advantage of and manage system resources through resource pools and policies, such as the following:

- Virtualized identity information, including pools of MAC addresses, WWN addresses, and UUIDs
- Ethernet and Fibre Channel adapter profile policies
- Firmware package policies
- Operating system boot order policies

Unless the service profile contains power management policies, a server pool qualification policy, or another policy that requires a specific hardware configuration, the profile can be used for any type of server in the Cisco UCS instance.

You can associate these service profiles with either a rack-mount server or a blade server. The ability to migrate the service profile depends upon whether you choose to restrict migration of the service profile.

Service Profiles that Inherit Server Identity

This hardware-based service profile is the simplest to use and create. This profile uses the default values in the server and mimics the management of a rack-mounted server. It is tied to a specific server and cannot be moved or migrated to another server.

You do not need to create pools or configuration policies to use this service profile.

This service profile inherits and applies the identity and configuration information that is present at the time of association, such as the following:

- MAC addresses for the two NICs
- For a converged network adapter or a virtual interface card, the WWN addresses for the two HBAs
- BIOS versions
- Server UUID

Important The server identity and configuration information inherited through this service profile may not be the values burned into the server hardware at manufacture if those values were changed before this profile is associated with the server.

Service Profile Templates

With a service profile template, you can quickly create several service profiles with the same basic parameters, such as the number of vNICs and vHBAs, and with identity information drawn from the same pools.

Tip If you need only one service profile with similar values to an existing service profile, you can clone a service profile in the Cisco UCS Manager GUI.

For example, if you need several service profiles with similar values to configure servers to host database software, you can create a service profile template, either manually or from an existing service profile. You then use the template to create the service profiles.

Cisco UCS supports the following types of service profile templates:

Initial template	Service profiles created from an initial template inherit all the properties of the template. However, after you create the profile, it is no longer connected to the template. If you need to make changes to one or more profiles created from this template, you must change each profile individually.

Updating template	Service profiles created from an updating template inherit all the properties of the template and remain connected to the template. Any changes to the template automatically update the service profiles created from the template.

Guidelines and Recommendations for Service Profiles

In addition to any guidelines or recommendations that are specific to policies and pools included in service profiles and service profile templates, such as the local disk configuration policy, you need to be aware of the following guidelines and recommendations that impact the ability to associate a service profile with a server:

Limit to the Number of vNICs that Can Be Configured on a Rack-Mount Server

You can configure up to 56 vNICs per supported adapter, such as the Cisco UCS P81E Virtual Interface Card (N2XX-ACPCI01), on any rack-mount server that is integrated with Cisco UCS Manager.

No Power Capping Support for Rack-Mount Servers

Power capping is not supported for rack servers. If you include a power control policy in a service profile that is associated with a rack-mount server, the policy is not implemented.

Creating Service Profiles

Creating a Service Profile with the Expert Wizard

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization where you want to create the service profile.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the organization and select **Create Service Profile (expert)**.

Step 5 In the **Create Service Profile (expert)** wizard, complete the following:

- Page 1: Identifying the Service Profile , page 366
- Page 2: Configuring the Storage Options, page 367
- Page 3: Configuring the Networking Options, page 372
- Page 4: Setting the vNIC/vHBA Placement, page 376
- Page 5: Setting the Server Boot Order, page 378
- Page 6: Adding the Maintenance Policy, page 381
- Page 7: Specifying the Server Assignment, page 382
- Page 8: Adding Operational Policies, page 384

Page 1: Identifying the Service Profile

This procedure directly follows the steps in Creating a Service Profile with the Expert Wizard, page 365. It describes how to set the identity of a service proflie on the **Identify Service Profile** page of the **Create Service Profile (expert)** wizard.

Procedure

Step 1 In the **Name** field, enter a unique name that you can use to identify the service profile.
This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

This name must be unique within the organization or sub-organization in which you are creating the service profile.

Step 2 From the **UUID Assignment** drop-down list, do one of the following:

Option	Description
Select (pool default used by default)	Assigns a UUID from the default UUID Suffix pool. Continue with Step 5.
Hardware Default	Uses the UUID assigned to the server by the manufacturer. If you choose this option, the UUID remains unassigned until the service profile is associated with a server. At that point, the UUID is set to the UUID value assigned to the server by the manufacturer. If the service profile is later moved to a different server, the UUID is changed to match the new server. Continue with Step 5.
XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX	Uses the UUID that you manually assign. Continue with Step 3.

Option	Description
Pools *Pool_Name*	Assigns a UUID from the UUID Suffix pool that you select from the list at the bottom of the drop-down list. Each pool name is followed by two numbers in parentheses that show the number of UUIDs still available in the pool and the total number of UUIDs in the pool. If you do not want use any of the existing pools, but instead want to create a pool that all serivce profiles can access, continue with Step 4. Otherwise, continue with Step 5.

Step 3 (Optional) If you selected the **XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX** option, do the following:

a) In the **UUID** field, enter the valid UUID that you want to assign to the server which uses this service profile.

b) To verify that the selected UUID is available, click the **here** link.

Step 4 (Optional) If you want to create a new UUID Suffix pool to use to use in this service profile, click **Create UUID Suffix Pool** and complete the fields in the **Create UUID Suffix Pool** wizard.
For more information, see Creating a UUID Suffix Pool, page 291.

Step 5 (Optional) In the text box, enter a description of this service profile.
The user-defined description for this service profile.

Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).

Step 6 Click **Next**.

What to Do Next

Complete the steps in Page 2: Configuring the Storage Options, page 367.

Page 2: Configuring the Storage Options

This procedure directly follows Page 1: Identifying the Service Profile , page 366. It describes how to configure the storage options for a service profile on the **Storage** page of the **Create Service Profile (expert)** wizard.

Procedure

Step 1 From the **Local Storage** drop-down list, choose one of the following:

Option	Description
Select Local Storage Policy to use	Assigns the default local disk storage policy to this service profile. Continue with Step 4.

Option	Description
Create a Specific Storage Policy	Enables you to create a local disk policy that can only be accessed by this service profile. Continue with Step 2.
Storage Policies *Policy_Name*	Select an existing local disk policy from the list at the bottom of the drop-down list. Cisco UCS Manager assigns this policy to the service profile. If you do not want use any of the existing policies, but instead want to create a policy that all service profiles can access, continue with Step 3. Otherwise, continue with Step 4.

Step 2 (Optional) If you chose **Create a Specific Storage Policy** and want to create a new policy that can only be used by this service profile, do the following:

a) From the **Mode** drop-down list, choose one of the following:

- **No Local Storage**—For a diskless server or a SAN only configuration. If you select this option, you cannot associate any service profile which uses this policy with a server that has a local disk.
- **RAID 0 Stripes**—Data is striped across all disks in the array, providing fast throughput. There is no data redundancy, and all data is lost if any disk fails.
- **RAID 1 Mirrored**—Data is written to two disks, providing complete data redundancy if one disk fails. The maximum array size is equal to the available space on the smaller of the two drives.
- **Any Configuration**—For a server configuration that carries forward the local disk configuration without any changes.
- **No RAID**—For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered.
- **RAID 6 Stripes Dual Parity**—Data is striped across all disks in the array and two parity disks are used to provide protection against the failure of up to two physical disks. In each row of data blocks, two sets of parity data are stored.
- **RAID 5 Striped Parity**—Data is striped across all disks in the array. Part of the capacity of each disk stores parity information that can be used to reconstruct data if a disk fails. RAID 5 provides good data throughput for applications with high read request rates.
- **RAID10 Mirrored and Striped**— RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates.

Note If you choose **No RAID** and you apply this policy to a server that already has an operating system with RAID storage configured, the system does not remove the disk contents. Therefore, there may be no visible differences after you apply the **No RAID** mode.

To make sure that any previous RAID configuration information is removed from a disk, apply a scrub policy that removes all disk information after you apply the **No RAID** configuration mode.

b) If you want to ensure that the server retains the configuration in the local disk configuration policy even if the server is disassociated from the service profile, check the **Protect Configuration** check box.

When a service profile is disassociated from a server and a new service profile associated, the setting for the Protect Configuration property in the new service profile takes precedence and overwrites the setting in the previous service profile.

Note If you disassociate the server from a service profile with this option enabled and then associate it with a new service profile that includes a local disk configuration policy with different properties, the server returns a configuration mismatch error and the association fails.

c) Continue with Step 4.

Step 3 (Optional) To create a local disk configuration policy that will be available to all service profiles, do the following:

a) Click the **Create Local Disk Configuration Policy** link.

b) In the **Create Local Disk Configuration** dialog box, complete the fields.
For more information, see Creating a Local Disk Configuration Policy, page 327.

c) Click **OK**.

d) From the **Local Storage** drop-down list, choose the policy you created.

Step 4 In the **How would you like to configure SAN storage?** field, click one of the following options:

Option	Description
Simple	Allows you to create a maximum of two vHBAs for this service profile. Continue with Step 7.
Expert	Allows you to create an unlimited number of vHBAs for this service profile. Continue with Step 8.
No vHBAs	Does not include any vHBAs for connections to a Fibre Channel SAN in the service profile. Continue with Step 9.
Hardware Inherited	Uses the vHBAs assigned to the Fibre Channel adapter profile associated with the server. Continue with Step 9.

Step 5 (Optional) If you chose the simple SAN storage option, do the following:

a) From the **WWNN Assignment** drop-down list, choose one of the following:

- Choose **Select (pool default used by default)** to use the default WWN pool.
- Choose one of the options listed under **Manual Using OUI** and then enter the WWN in the **World Wide Node Name** field.

  You can specify a WWNN in the range from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF. You can click the **here** link to verify that the WWNN you specified is available.
- Choose a WWN pool name from the list to have a WWN assigned from the specified pool. Each pool name is followed by two numbers in parentheses that show the number of WWNs still available in the pool and the total number of WWNs in the pool.

b) In the **vHBA 0 (Fabric A)** area, complete the following fields:

- In the **Name** field, enter a unique name for the vHBA.
- From the **Select VSAN** drop-down list, choose the name of the VSAN with which this vHBA should be associated.

If the VSAN you need is not in the drop-down list, click the **Create VSAN** link. For more information, see Creating a Named VSAN, page 261.

c) Repeat Step 7b in the **vHBA 1 (Fabric B)** area to create a VSAN for that vHBA.

d) Continue with Step 9.

Step 6 (Optional) If you chose the expert SAN storage option, do the following:

a) From the **WWNN Assignment** drop-down list, choose one of the following:

- Choose **Select (pool default used by default)** to use the default WWN pool.
- Choose one of the options listed under **Manual Using OUI** and then enter the WWN in the **World Wide Node Name** field.

  You can specify a WWNN in the range from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF. You can click the **here** link to verify that the WWNN you specified is available.
- Choose a WWN pool name from the list to have a WWN assigned from the specified pool. Each pool name is followed by two numbers in parentheses that show the number of WWNs still available in the pool and the total number of WWNs in the pool.

b) Click **Add** on the icon bar of the table to open the **Create vHBA** dialog box.

c) Complete the following fields to specify the identity information for the vHBA:

Name	Description
Name field	The name of this vHBA. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Use SAN Connectivity Template check box	Check this check box if you want to use a template to create the vHBA. Cisco UCS Manager GUI displays the **vHBA Template** drop-down list from which you can select the appropriate template, and the **Adapter Performance Profile** area from which you can select an adapter profile. **Note** You can only select this option if one or more SAN connectivity templates exist in the system.
Create vHBA Template link	Click this link if you want to create a vHBA template.
WWPN Assignment drop-down list	If you want to: • Use the default WWPN pool, leave this field set to **Select (pool default used by default)**.

Name	Description
	• Use the WWPN assigned to the server by the manufacturer, select **Hardware Default**. • A specific WWPN, select **20:00:00:25:B5:00:00:00**, **20:XX:XX:XX:XX:XX:XX:XX**, or **5X:XX:XX:XX:XX:XX:XX:XX** and enter the WWPN in the **WWPN** field. To verify that this WWPN is available, click the corresponding link. • A WWPN from a pool, select the pool name from the list. Each pool name is followed by a pair of numbers in parentheses. The first number is the number of available WWN addresses in the pool and the second is the total number of WWPN addresses in the pool. To create a new WWPN pool, click **WWPN Pool**.

d) In the **VSAN** area, complete the following fields:

Name	Description
Fabric ID field	The fabric interconnect associated with the component.
Select VSAN drop-down list box	The VSAN with which this vHBA is associated.
Create VSAN link	Click this link if you want to create a VSAN.
Pin Group drop-down list box	The pin group with which this vHBA is associated.
Create SAN Pin Group link	Click this link if you want to create a pin group.
Persistent Binding field	This can be: • **disabled** • **enabled**
Max Data Field Size field	The maximum size of the Fibre Channel frame payload bytes that the vHBA supports. Enter an integer between 256 and 2112. The default is 2048.
Operational Parameters Section	
Stats Threshold Policy drop-down list box	The threshold policy with which this vHBA is associated.

e) In the **Adapter Performance Profile** area, complete the following fields:

Name	Description
Adapter Policy drop-down list box	The Fibre Channel adapter policy with which this vHBA is associated.
Create Fibre Channel Adapter Policy link	Click this link if you want to create a Fibre Channel adapter policy.
QoS drop-down list box	The quality of service policy with which this vHBA is associated.
Create QoS Policy link	Click this link if you want to create a QoS policy.

f) Click **OK**.

Step 7 Click **Next**.

What to Do Next

Complete Page 3: Configuring the Networking Options, page 372.

Page 3: Configuring the Networking Options

This procedure directly follows Page 2: Configuring the Storage Options, page 367. It describes how to configure the networking options, including LAN connectivity, on the **Networking** page of the **Create Service Profile (expert)** wizard.

Procedure

Step 1 (Optional) If you plan to assign this service profile to a server with an adapter that supports dynamic vNICs, choose one of the following options from the **Dynamic vNIC Connection** drop-down list:

Option	Description
Select a Policy to use	Enables you to create a service profile without a dynamic vNIC connection policy for a server with an adapter that does not support dynamic vNICs. This option does not include a dynamic vNIC connection policy in the service profile. Continue with Step 4.
Create a Specific Dynamic vNIC Connection Policy	Enables you to create a dynamic vNIC connection policy that can only be accessed by this service profile. Continue with Step 2.

Option	Description
Dynamic vNIC Connection Policies *Policy_Name*	Select an existing dynamic vNIC connection policy from the list at the bottom of the drop-down list. Cisco UCS Manager assigns this policy to the service profile. If you do not want use any of the existing policies, but instead want to create a policy that all service profiles can access, continue with Step 3. Otherwise, continue with Step 4.

Step 2 (Optional) If you clicked **Create a Specific Dynamic vNIC Connection Policy**, do the following to create a new dynamic vNIC connection policy that can only be used by this service profile:

a) Complete the following fields:

Name	Description
Number of Dynamic vNICs field	The number of dynamic vNICs that this policy affects.
Adapter Policy drop-down list	The adapter profile associated with this policy. The profile must already exist to be included in the drop-down list.

b) Continue with Step 4.

Step 3 (Optional) To create a dynamic vNIC connection policy that will be available to all service profiles, do the following:

a) Click **Create Dynamic vNIC Connection Policy**.
b) In the **Create Dynamic vNIC Connect Policy** dialog box, complete the fields.
For more information, see Creating a Dynamic vNIC Connection Policy, page 485.
c) Click **OK**.
d) From the **Dynamic vNIC Connection** drop-down list, choose the policy you created.
e) Continue with Step 4.

Step 4 In the **How would you like to configure LAN connectivity?** field, click one of the following options:

Option	Description
Simple	Allows you to create a maximum of two vNICs, in dual fabric mode, for this service profile. Continue with Step 5.
Expert	Allows you to create an unlimited number of vNICs for this service profile. Continue with Step 6.
No vNICs	Does not include any vNICs for connections to a LAN in the service profile. Any server associated with this service profile cannot be able to communicate with a LAN unless you modify the service profile to add vNICs. Continue with Step 7.

Option	Description
Hardware Inherited	Uses the vNICs assigned to the Ethernet adapter profile associated with the server. Continue with Step 7.

Step 5 (Optional) If you chose the simple LAN connectivity option, do the following:

a) In the **vNIC 0 (Fabric A)** area, complete the following fields:

- In the **Name** field, enter a unique name for the vNIC.
- From the **Select Native VLAN** drop-down list, choose the name of the VLAN with which this vNIC should communicate.

If the VLAN you need is not in the drop-down list, click the **Create VLAN** link. For more information, see Creating a Named VLAN, page 223.

b) Repeat Step 2a in the **vNIC 1 (Fabric B)** area to create a VLAN for that vNIC.

c) Continue with Step 4.

Step 6 If you chose the expert LAN connectivity option, do the following:

a) Click **Add** on the icon bar of the table to open the **Create vNICs** dialog box.

b) Complete the following fields to specify the identity information for the vNIC:

Name	Description
Name field	Enter a name for this vNIC. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Use LAN Connectivity Template check box	Check this check box if you want to use a template to create the vNIC. Cisco UCS Manager GUI displays the **vNIC Template** drop-down list from which you can select the appropriate template, and the **Adapter Performance Profile** area from which you can select an adapter profile. **Note** You can only select this option if one or more LAN connectivity templates exist in the system.
Create vNIC Template link	Click this link if you want to create a vNIC template.
MAC Address Assignment drop-down list	If you want to: • Use the default MAC address pool, leave this field set to **Select (pool default used by default)**. • Use the MAC address assigned to the server by the manufacturer, select **Hardware Default**. • A specific MAC address, select **02:25:B5:XX:XX:XX** and enter the address in the **MAC Address** field. To verify that this address is available, click the corresponding link.

Name	Description
	• A MAC address from a pool, select the pool name from the list. Each pool name is followed by a pair of numbers in parentheses. The first number is the number of available MAC addresses in the pool and the second is the total number of MAC addresses in the pool.

c) In the **Fabric Interconnect** area, complete the following fields:

Name	Description
Fabric ID field	The fabric interconnect associated with the component. If you want this vNIC to be able to access the second fabric interconnect if the default one is unavailable, check the **Enable Failover** check box. **Note** Do not select **Enable Failover** if you plan to associate this vNIC configuration with a server that has an adapter which does not support fabric failover, such as the Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter. If you do so, Cisco UCS Manager generates a configuration fault when you associate the service profile with the server.
VLANs table	This table lists the VLANs that can be associated with this vNIC. The columns are: • **Select**—Check the check box in this column for each VLAN you want to use. • **Name**—The name of the VLAN. • **Native VLAN**—To designate one of the VLANs as the native VLAN, click the radio button in this column.
Create VLAN link	Click this link if you want to create a VLAN.
MTU field	The maximum transmission unit, or packet size, that this vNIC accepts. Enter an integer between 1500 and 9216.
Pin Group drop-down list	Choose the LAN pin group you want associated with this vNIC.
Create LAN Pin Group link	Click this link if you want to create a LAN pin group.
Operational Parameters Section	
Stats Threshold Policy drop-down list	The statistics collection policy with which this vNIC is associated.

d) In the **Adapter Performance Profile** area, complete the following fields:

Name	Description
Adapter Policy drop-down list	The Ethernet adapter policy with which this vNIC is associated.
Create Ethernet Adapter Policy link	Click this link if you want to create an Ethernet adapter policy.
QoS drop-down list	The quality of service policy with which this vNIC is associated.
Create QoS Policy link	Click this link if you want to create a quality of service policy.
Network Control Policy drop-down list	The network control policy with which this vNIC is associated.
Create Network Control Policy Policy link	Click this link if you want to create a network control policy.

e) Click **OK**.

Step 7 Click **Next**.

What to Do Next

Complete Page 4: Setting the vNIC/vHBA Placement, page 376.

Page 4: Setting the vNIC/vHBA Placement

This procedure directly follows Page 3: Configuring the Networking Options, page 372. It describes how to set the vNIC and vHBA placement options on the **vNIC/vHBA Placement** page of the **Create Service Profile (expert)** wizard.

Procedure

Step 1 From the **Select Placement** drop-down list, choose one of the following:

Option	Description
Let System Perform Placement	Specifies that Cisco UCS Manager determines the vNIC/vHBA placement for the server associated with the service profile. The placement is determined by the order set in the PCI Order table. Continue with Step 2.
Specify Manually	Enables you to specify the virtual network connection to which each vNIC and vHBA is assigned for the server associated with the service profile. Continue with Step 3.

Option	Description
vNIC/vHBA Placement Profiles *Placement Profile Name*	Assigns an existing vNIC/vHBA placement policy to the service profile. If you choose this option, Cisco UCS Manager displays the details of the policy. If you do not want use any of the existing policies, but instead want to create a policy that all service profiles can access, click **Create Placement Policy** and continue with Step 4. Otherwise, continue with Step 5.

Step 2 (Optional) If you chose **Let System Perform Placement**, do the following:

a) Use one or more of the following buttons to adjust the order of the vNICs and vHBAs:

Name	Description
Move Up button	Moves the selected virtual interface to a higher priority in the list.
Move Down button	Moves the selected virtual interface to a lower priority in the list.
Delete button	Deletes the selected virtual interface.
Reorder button	Returns the virtual interfaces to their original order.
Modify button	Enables you to modify the currently-selected virtual interface. **Note** You can change any options for the virtual interface except its name.

b) Continue with Step 5.

Step 3 (Optional) If you chose **Specify Manually**, do the following:

a) On the appropriate tab in the **vNIC/vHBA** table, click a vNIC or vHBA.

b) In the **Virtual Host Interface** table, click a vCON row and if necessary, choose one of the following values from the **Selection Preference** column:

- **all**
- **assigned-only**
- **exclude-dynamic**
- **exclude-unassigned**

c) Click **Assign**.
If you need to undo an assignment, click **Remove**.

d) Repeat Steps a through c until you have assigned all vNICs and vHBAs.

e) When you have specified all vNIC and vHBA placements, continue with Step 5.

Step 4 If you clicked **Create Placement Policy**, do the following in the **Create Placement Policy** dialog box:

a) In the **Name** field, enter a unique name for the placement policy.

This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

b) In the **Selection Preference** column for each **Virtual Slot**, choose one of the following from the drop-down list:

- **all**
- **assigned-only**
- **exclude-dynamic**
- **exclude-unassigned**

c) Click **OK**.

d) After the dialog box closes, choose the policy you created from the **Select Placement** drop-down list.

Step 5 Click **Next**.

What to Do Next

Complete Page 5: Setting the Server Boot Order, page 378.

Page 5: Setting the Server Boot Order

This procedure directly follows Page 4: Setting the vNIC/vHBA Placement, page 376. It describes how to set the server boot order options on the **Server Boot Order** page of the **Create Service Profile (expert)** wizard.

Tip We recommend that the boot order in a boot policy include either a local disk or a SAN LUN, but not both, to avoid the possibility of the server booting from the wrong storage type. If you configure a local disk and a SAN LUN for the boot order storage type and the operating system or logical volume manager (LVM) is configured incorrectly, the server may boot from the local disk rather than the SAN LUN.

For example, on a server with Red Hat Linux installed, where the LVM is configured with default LV names and the boot order is configured with a SAN LUN and a local disk, Linux reports that there are two LVs with the same name and boots from the LV with the lowest SCSI ID, which could be the local disk.

Procedure

Step 1 From the **Boot Policy** drop-down list, choose one of the following:

Option	Description
Select Boot Policy to use	Assigns the default boot policy to this service profile. Continue with Step 9.
Create a Specific Boot Policy	Enables you to create a local boot policy that can only be accessed by this service profile. Continue with Step 3.

Option	Description
Boot Policies *Policy_Name*	Assigns an existing boot policy to the service profile. If you choose this option, Cisco UCS Manager displays the details of the policy. If you do not want use any of the existing policies but instead want to create a policy that all service profiles can access, click **Create Boot Policy** and continue with Step 2. Otherwise, choose a policy from the list and continue with Step 9.

Step 2 If you clicked **Create Boot Policy** to create a boot policy that all service profiles and templates can use, do the following:

a) In the **Create Boot Policy** dialog box, enter a unique name and description for the policy.
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

b) Continue with Step 3.

Step 3 (Optional) To reboot all servers that use this boot policy after you make changes to the boot order, check the **Reboot on Boot Order Change** check box.
In Cisco UCS Manager GUI, if the **Reboot on Boot Order Change** check box is checked for a boot policy, and if CD-ROM or Floppy is the last device in the boot order, deleting or adding the device does not directly affect the boot order and the server does not reboot.

Step 4 (Optional) To ensure that Cisco UCS Manager uses any vNICs or vHBAs in the order shown in the **Boot Order** table, check the **Enforce vNIC/vHBA Name** check box.
If you do not check this check box, Cisco UCS Manager uses the priority specified in the vNIC or vHBA.

Step 5 To add a local disk, virtual CD-ROM, or virtual floppy to the boot order, do the following:

a) Click the down arrows to expand the **Local Devices** area.

b) Click one of the following links to add the device to the **Boot Order** table:

- **Add Local Disk**
- **Add CD-ROM**
- **Add Floppy**

c) Add another boot device to the **Boot Order** table, or click **OK** to finish.

Step 6 To add a LAN boot to the boot order, do the following:

a) Click the down arrows to expand the **vNICs** area.

b) Click the **Add LAN Boot** link.

c) In the **Add LAN Boot** dialog box, enter the name of the vNIC that you want to use for the LAN boot in the **vNIC** field, then click **OK**.

d) Add another device to the **Boot Order** table, or click **OK** to finish.

Step 7 To add a SAN boot to the boot order, do the following:

a) Click the down arrows to expand the **vHBAs** area.

b) Click the **Add SAN Boot** link.

c) In the **Add SAN Boot** dialog box, complete the following fields, then click **OK**:

Name	Description
vHBA field	Enter the name of the vHBA you want to use for the SAN boot.
Type field	This can be: • **primary**—If the server boots using a SAN WWN address, this is the first address it tries. Each boot policy can have only one primary SAN boot location. • **secondary**—If the server cannot boot from the primary SAN location, it attempts to boot from this location. Each boot policy can have only one secondary SAN boot location. The use of the terms primary or secondary boot devices does not imply a boot order. The effective order of boot devices within the same device class is determined by PCIe bus scan order.

d) If this vHBA points to a bootable SAN image, click the **Add SAN Boot Target** link and, in the **Add SAN Boot Target** dialog box, complete the following fields, then click **OK**:

Name	Description
Boot Target LUN field	The LUN that corresponds to the location of the boot image.
Boot Target WWPN field	The WWPN that corresponds to the location of the boot image.
Type field	This can be: • **primary**—If the server boots using a SAN WWN address, this is the first address it tries. Each boot policy can have only one primary SAN boot location. • **secondary**—If the server cannot boot from the primary SAN location, it attempts to boot from this location. Each boot policy can have only one secondary SAN boot location. The use of the terms primary or secondary boot devices does not imply a boot order. The effective order of boot devices within the same device class is determined by PCIe bus scan order.

e) Add another boot device to the **Boot Order** table, or click **OK** to finish.

Step 8 If you created a new boot policy accessible to all service profiles and template, select that policy from the **Boot Policy** drop-down list.

Step 9 Click **Next**.

What to Do Next

Complete Page 6: Adding the Maintenance Policy, page 381.

Page 6: Adding the Maintenance Policy

This procedure directly follows Page 5: Setting the Server Boot Order, page 378. It describes how to add a maintenance policy to the service profile on the **Maintenance Policy** page of the **Create Service Profile (expert)** wizard.

Procedure

Step 1 From the **Maintenance Policy** drop-down list, choose one of the following:

Option	Description
Select a Maintenance Policy to Use (default policy shown)	Assigns the default maintenance policy to this service profile. Continue with Step 4.
Maintenance Policies *Policy_Name*	Assigns an existing maintenance policy to the service profile. If you choose this option, Cisco UCS Manager displays the details of the policy. If you do not want use any of the existing policies but instead want to create a policy that all service profiles can access, click **Create Maintenance Policy** and continue with Step 2. Otherwise, choose a policy from the list and continue with Step 4.

Step 2 If you clicked **Create Maintenance Policy** to create a maintenance policy that all service profiles and templates can use, do the following:

a) In the **Create Maintenance Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Reboot Policy field	When a service profile is associated with a server, or when changes are made to a service profile that is already associated with a server, the server needs to be rebooted to complete the process. The **Reboot Policy** field determines when the reboot occurs for servers associated with any service profiles that include this maintenance policy. This can be:

Name	Description
	• **immediate**—The server is rebooted automatically as soon as the service profile association is complete or service profile changes are saved by the user. • **user-ack**—The user must reboot the server manually after the service profile association is complete or changes are made. • **timer-automatic**—Cisco UCS defers all service profile associations and changes until the maintenance window defined by the schedule shown in the **Schedule** field.
Schedule drop-down list	If the **Reboot Policy** is set to **timer-automatic**, the schedule specifies when maintenance operations can be applied to the server. Cisco UCS reboots the server and completes the service profile changes at the scheduled time.

b) Click **OK** and continue with Step 3.

Step 3 If you created a new boot policy accessible to all service profiles and template, select that policy from the **Maintenance Policy** drop-down list.

Step 4 Click **Next**.

What to Do Next

Complete Page 7: Specifying the Server Assignment, page 382.

Page 7: Specifying the Server Assignment

This procedure directly follows Page 6: Adding the Maintenance Policy, page 381. It describes how to specify the way a server is assigned and which firmware packages are associated with the service profile on the **Server Assignment** page of the **Create Service Profile (expert)** wizard.

Procedure

Step 1 From the **Server Assignment** drop-down list, choose one of the following:

Option	Description
Assign Later	Allows you to assign a server after you have created and configured the service profile. Continue with Step 6.
Pre-provision a slot	Specifies the chassis and slot that contains the server which will be assigned to the service profile. If the server is not in the slot or is otherwise unavailable, the service profile will be associated with the server when it becomes available. Continue with Step 2.

Option	Description
Select existing Server	Displays a table of available, unassociated servers that you can use to select the server which will be assigned to the service profile. Continue with Step 3.
Select from a Pool ***Pool_Name***	Select a server pool from the list at the bottom of the drop-down list. Cisco UCS Manager assigns a server from this pool to the service profile. Continue with Step 4.

Step 2 If you chose **Pre-provision a slot**, do the following:

a) In the **Chassis Id** field, enter the number of the chassis where the selected server is located.
b) In the **Slot Id** field, enter the number of the slot where the selected server is located.
c) Continue with Step 4.

Step 3 If you chose **Select existing Server**, do the following:

a) In the **Select** column of the table of available servers, click the radio button for the server that meets the needs of this service profile.
b) Continue with Step 4.

Step 4 In the **Power State** field, click one of the following radio buttons to set the power state that will be applied to the server when it is associated with this service profile:

- **Down** if you want the server to be powered down before the profile is associated with the server.
- **Up** if you want the server to be powered up before the profile is associated with the server

By default, the server is powered up.

Step 5 (Optional) In the **Firmware Management** area, do the following to use policies to update the firmware on the server associated with the service profile:

a) Click the down arrows on the **Firmware Management** bar to expand the area.
b) Complete the following fields:

Name	Description
Host Firmware drop-down list	To associate a host firmware package with this service profile, choose its name from the drop-down list.
Create Host Firmware Package link	Click this link if you want to create a host firmware package.
Management Firmware drop-down list	To associate a management firmware package with this service profile, choose its name from the drop-down list.
Create Management Firmware Package link	Click this link if you want to create a management firmware package.

Step 6 Click **Next**.

What to Do Next

Complete Page 8: Adding Operational Policies, page 384.

Page 8: Adding Operational Policies

This procedure directly follows Page 7: Specifying the Server Assignment, page 382. It describes how to add operational policies to the service profile on the **Operational Policies** page of the **Create Service Profile (expert)** wizard. These policies are optional.

Procedure

Step 1 To override the default BIOS settings and configure them through the service profile, click the down arrows to expand the **BIOS Configuration** bar and do one of the following:

- To add an existing policy, select the desired BIOS policy from the **BIOS Policy** drop-down list .
- To create a BIOS policy that is available to all service profiles, click **Create BIOS Policy**, complete the fields in the dialog box, and then select that policy from the **BIOS Policy** drop-down list .

For more information about how to create a BIOS policy, see Creating a BIOS Policy, page 317.

Step 2 To provide external access to the CIMC on the server, click the down arrows to expand the **External IPMI Management Configuration** bar and add an IPMI profile and a serial over LAN policy.
If you do not want to provide external access, continue with Step 4.

Step 3 To add an IPMI profile to the service profile, do one of the following:

- To add an existing policy, select the desired IPMI profile from the **IPMI Access Profile** drop-down list.
- If the **IPMI Access Profile** drop-down list does not include an IPMI profile with the desired user access, click the **Create Access IPMI Profile** link to create an IPMI profile that is available to all service profiles and then select that profile from the **IPMI Access Profile** drop-down list.

For more information about how to create an IPMI profile, see Creating an IPMI Access Profile, page 323.

Step 4 To add a Serial over LAN policy to the service profile, do one of the following:

- To add an existing policy, select the desired Serial over LAN policy from the **SoL Configuration Profile** drop-down list.
- To create a Serial over LAN policy that is only available to service profile created from this template, select **Create a Specific SoL Policy** from the **SoL Configuration Profile** drop-down list and complete the **Admin State** field and the **Speed** drop-down list.
- To create a Serial over LAN policy that is available to all service profile templates, click the **Create Serial over LAN Policy** link, complete the fields in the dialog box, and then select that policy from the **SoL Configuration Profile** drop-down list.

For more information about how to create a serial over LAN policy, see Creating a Serial over LAN Policy, page 332.

Step 5 To configure the management IP required for external access to the CIMC on the server, click the down arrows to expand the **Management IP Address** bar and do the following:

a) Click one of the following radio buttons:

- **none**—No management IP address is assigned to the service profile. The management IP address is set based on the CIMC management IP address settings on the server.
- **static**—A static management IP address is assigned to the service profile, based on the information entered in this area.
- **pooled**—A management IP address is assigned to the service profile from the management IP address pool.

b) If you selected **static**, complete the following fields:

Field	Description
IP Address	The static IPv4 address to be assigned to the service profile
Subnet Mask	The subnet mask for the IP address.
Default Gateway	The default gateway that the IP address should use.

Step 6 To monitor thresholds and collect statistics for the associated server, click the down arrows to expand the **Monitoring Configuration (Thresholds)** bar and do one of the following:

- To add an existing policy, select the desired threshold policy from the **Threshold Policy** drop-down list.
- To create a threshold policy that is available to all service profiles, click the **Create Threshold Policy** link, complete the fields in the dialog box, and then select that policy from the **Threshold Policy** drop-down list.

For more information about how to create a threshold policy, see Creating a Server and Server Component Threshold Policy , page 576.

Step 7 To associate a power control policy with the service profile, click the down arrows to expand the **Power Control Policy Configuration** bar and do one of the following:

- To add an existing policy, select the desired power control policy from the **Power Control Policy** drop-down list.
- To create a power control policy that is available to all service profiles, click the **Create Power Control Policy** link , complete the fields in the dialog box, and then select that policy from the **Power Control Policy** drop-down list.

For more information about how to create a power control policy, see Creating a Power Control Policy, page 437.

Step 8 To associate a scrub policy with the service profile, click the down arrows to expand the **Scrub Policy** bar and do one of the following:

- To add an existing policy, select the desired scrub policy from the **Scrub Policy** drop-down list .

- To create a scrub policy that is available to all service profiles, click the **Create Scrub Policy** link , complete the fields in the dialog box, and then select that policy from the **Scrub Policy** drop-down list .

For more information about how to create a scrub policy, see Creating a Scrub Policy, page 330.

Step 9 Click **Finish**.

Creating a Service Profile that Inherits Server Identity

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization where you want to create the service profile.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the organization and select **Create Service Profile**.

Step 5 In the **Naming** area of the **Create Service Profile** dialog box, complete the following fields:

a) In the **Name** field, enter a unique name that you can use to identify the service profile.
This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

b) In the **Description** field, enter a description of this service profile.

Step 6 In the **vNICs** area of the **Create Service Profile** dialog box, complete the following fields:

Name	Description
Primary vNIC Section	
Primary vNIC check box	Check this check box if you want to create a vNIC for this service profile. If you check this box, Cisco UCS Manager GUI displays the rest of the fields in this section.
Name field	The name of the vNIC.
Fabric field	The fabric interconnect that this vNIC is associated with.
Network drop-down list	The LAN that this vNIC is associated with.
Secondary vNIC Section	
Secondary vNIC check box	Check this check box if you want to create a second vNIC for this service profile. If you check this box, Cisco UCS Manager GUI displays the rest of the fields in this section.
Name field	The name of the vNIC.

Name	Description
Fabric field	The fabric interconnect that this vNIC is associated with.
Network drop-down list	The LAN that this vNIC is associated with.

Step 7 In the **vHBAs** area of the **Create Service Profile** dialog box, complete the following fields:

Name	Description
Primary vHBA Section	
Primary vHBA check box	Check this check box if you want to create a vHBA for this service profile. If you check this box, Cisco UCS Manager GUI displays the rest of the fields in this section.
Name field	The name of the vHBA.
Fabric field	The fabric interconnect that this vHBA is associated with. Do not associate the primary vHBA with the same fabric as the secondary vHBA.
Secondary vHBA Section	
Secondary vHBA check box	Check this check box if you want to create a second vHBA for this service profile. If you check this box, Cisco UCS Manager GUI displays the rest of the fields in this section.
Name field	The name of the vHBA.
Fabric field	The fabric interconnect that this vHBA is associated with. Do not associate the secondary vHBA with the same fabric as the primary vHBA.

Step 8 In the **Boot Order** area of the **Create Service Profile** dialog box, complete the following fields:

Name	Description
Primary Boot Device Section	
Primary Boot Device check box	Check this check box if you want to set a boot device for this service profile. If you check this box, Cisco UCS Manager GUI displays the rest of the fields in this section.
Type field	This can be: • **local-disk**—The server boots from its local disk. **Note** If you select this option, you cannot select **local-disk** or **san** as your secondary boot type.

Name	Description
	• **san**—The server boots from an image stored in a SAN. If you select this option, Cisco UCS Manager GUI displays the **SAN** area. • **lan**—The server boots from the LAN. If you select this option, Cisco UCS Manager GUI displays the **Network** area that lets you specify which vNIC the server should use for the PXE boot. • **CD-ROM**—The server boots from a virtual CD-ROM. • **Floppy**—The server boots from a virtual floppy.
SAN area	If **Type** is set to **san**, this area contains the following field: • **vHBA**—The vHBA used to access the SAN boot image • **LUN**—The LUN that corresponds to the location of the boot image • **WWN**—The WWN that corresponds to the location of the boot image
Network (PXE) area	If **Type** is set to **lan**, this area contains the **vNIC** drop-down list from which you can choose the vNIC from which the server should boot.
Secondary Boot Device Section	
Secondary Boot Device check box	Check this check box if you want to set a second boot device for this service profile. If you check this box, Cisco UCS Manager GUI displays the rest of the fields in this section.
Type field	This can be: • **local-disk**—The server boots from its local disk. • **san**—The server boots from an image stored in a SAN. If you select this option, Cisco UCS Manager GUI displays the **SAN** area. • **lan**—The server boots from the LAN. If you select this option, Cisco UCS Manager GUI displays the **Network** area that lets you specify which vNIC the server should use for the PXE boot. • **CD-ROM**—The server boots from a virtual CD-ROM. • **Floppy**—The server boots from a virtual floppy.
SAN area	If **Type** is set to **san**, this area contains the following field: • **vHBA**—The vHBA used to access the SAN boot image • **LUN**—The LUN that corresponds to the location of the boot image

Name	Description
	• **WWN**—The WWN that corresponds to the location of the boot image
Network (PXE) area	If **Type** is set to **lan**, this area contains the **vNIC** drop-down list from which you can choose the vNIC from which the server should boot.

Step 9 (Optional) In the **Select** column of the **Server Association (optional)** area, click the radio button for a server to associate this service profile with that server.

Step 10 Click **OK**.

Creating a Hardware Based Service Profile for a Blade Server

You cannot move a hardware based service profile to another server.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.

Step 3 Choose the server for which you want to create a hardware based service profile.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Create Service Profile**.

Step 6 In the **Create Service Profile for Server** dialog box, do the following:

a) Click the **Hardware Based Service Profile** radio button.

b) In the **Name** field, enter a unique name for the service profile.
This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

c) If you want Cisco UCS Manager to create vNICs for the service profile, check the **Create Default vNICs** check box.

d) If you want Cisco UCS Manager to create vHBAs for the service profile, check the **Create Default vHBAs** check box.

e) Click **OK**.

Cisco UCS Manager inherits and automatically applies the identity and configuration information in the server, creates the service profile, and associates it with the server.

Creating a Hardware Based Service Profile for a Rack-Mount Server

You cannot move a hardware based service profile to another server.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Rack Mounts ➤ Servers**.

Step 3 Choose the server for which you want to create a hardware based service profile.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Create Service Profile**.

Step 6 In the **Create Service Profile for Server** dialog box, do the following:

a) Click the **Hardware Based Service Profile** radio button.

b) In the **Name** field, enter a unique name for the service profile.
This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

c) If you want Cisco UCS Manager to create vNICs for the service profile, check the **Create Default vNICs** check box.

d) If you want Cisco UCS Manager to create vHBAs for the service profile, check the **Create Default vHBAs** check box.

e) Click **OK**.

Cisco UCS Manager inherits and automatically applies the identity and configuration information in the server, creates the service profile, and associates it with the server.

Working with Service Profile Templates

Creating a Service Profile Template

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profile Templates**.

Step 3 Expand the node for the organization where you want to create the service profile template.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the organization and select **Create Service Profile Template**.

Step 5 In the **Create Service Profile Template** wizard, complete the following:

- Page 1: Identifying the Service Profile Template, page 391
- Page 2: Specifying the Storage Options, page 392
- Page 3: Specifying the Networking Options, page 396
- Page 4: Setting the vNIC/vHBA Placement, page 400
- Page 5: Setting the Server Boot Order, page 402

• Page 6: Adding the Maintenance Policy, page 405
• Page 7: Specifying the Server Assignment Options, page 406
• Page 8: Adding Operational Policies, page 408

Page 1: Identifying the Service Profile Template

This procedure directly follows the steps in Creating a Service Profile Template, page 390. It describes how to set the identity of a service profile template on the **Identify Service Profile Template** page of the **Create Service Profile Template** wizard.

Procedure

Step 1 In the **Name** field, enter a unique name that you can use to identify this service profile template.
This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

This name must be unique within the organization or sub-organization in which you are creating the service profile.

Step 2 In the **Type** field, click one of the following radio buttons:

- **Initial Template**—Any service profiles created from this template are not updated if the template changes
- **Updating Template**—Any service profiles created from this template are updated if the template changes

Step 3 From the **UUID Assignment** drop-down list, choose one of the following:

Option	Description
Select (pool default used by default)	Assigns a UUID from the default UUID Suffix pool.
Hardware Default	Uses the UUID assigned to the server by the manufacturer. If you choose this option, the UUID remains unassigned until the service profile is associated with a server. At that point, the UUID is set to the UUID value assigned to the server by the manufacturer. If the service profile is later moved to a different server, the UUID is changed to match the new server.
Pools ***Pool_Name***	Assigns a UUID from the UUID Suffix pool that you select from the list at the bottom of the drop-down list. Each pool name is followed by two numbers in parentheses that show the number of UUIDs still available in the pool and the total number of UUIDs in the pool.

Step 4 (Optional) In the text box, enter a description of this service profile template.
A user-defined description of the service profile template.

Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).

Step 5 Click **Next**.

What to Do Next

Complete the steps in Page 2: Specifying the Storage Options, page 392.

Page 2: Specifying the Storage Options

This procedure directly follows Page 1: Identifying the Service Profile Template, page 391. It describes how to configure the storage options for a service profile template on the **Storage** page of the **Create Service Profile Template** wizard.

Procedure

Step 1 From the **Local Storage** drop-down list, choose one of the following:

Option	Description
Select Local Storage Policy to use	Assigns the default local disk storage policy to every service profile created from this template. Continue with Step 4.
Create a Specific Storage Policy	Enables you to create a local disk policy that can only be accessed by a service profile created from this template. Continue with Step 2.
Storage Policies ***Policy_Name***	Select an existing local disk policy from the list at the bottom of the drop-down list. Cisco UCS Manager assigns this policy to every service profile created from this template. If you do not want use any of the existing policies but instead want to create a new policy that all service profiles and templates can access, continue with Step 3. Otherwise, continue with Step 4.

Step 2 (Optional) If you chose **Create a Specific Storage Policy** and want to create a new policy that can only be used by service profiles created from this service profile template, do the following:

a) From the **Mode** drop-down list, choose one of the following:

- **No Local Storage**—For a diskless server or a SAN only configuration. If you select this option, you cannot associate any service profile which uses this policy with a server that has a local disk.
- **RAID 0 Stripes**—Data is striped across all disks in the array, providing fast throughput. There is no data redundancy, and all data is lost if any disk fails.
- **RAID 1 Mirrored**—Data is written to two disks, providing complete data redundancy if one disk fails. The maximum array size is equal to the available space on the smaller of the two drives.

- **Any Configuration**—For a server configuration that carries forward the local disk configuration without any changes.
- **No RAID**—For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered.
- **RAID 6 Stripes Dual Parity**—Data is striped across all disks in the array and two parity disks are used to provide protection against the failure of up to two physical disks. In each row of data blocks, two sets of parity data are stored.
- **RAID 5 Striped Parity**—Data is striped across all disks in the array. Part of the capacity of each disk stores parity information that can be used to reconstruct data if a disk fails. RAID 5 provides good data throughput for applications with high read request rates.
- **RAID10 Mirrored and Striped**— RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates.

Note If you choose **No RAID** and you apply this policy to a server that already has an operating system with RAID storage configured, the system does not remove the disk contents. Therefore, there may be no visible differences after you apply the **No RAID** mode.

To make sure that any previous RAID configuration information is removed from a disk, apply a scrub policy that removes all disk information after you apply the **No RAID** configuration mode.

b) If you want to ensure that the server retains the configuration in the local disk configuration policy even if the server is disassociated from the service profile, check the **Protect Configuration** check box. When a service profile is disassociated from a server and a new service profile associated, the setting for the Protect Configuration property in the new service profile takes precedence and overwrites the setting in the previous service profile.

Note If you disassociate the server from a service profile with this option enabled and then associate it with a new service profile that includes a local disk configuration policy with different properties, the server returns a configuration mismatch error and the association fails.

c) Continue with Step 4.

Step 3 (Optional) To create a local disk configuration policy that will be available to all service profiles and templates, do the following:

a) Click the **Create Local Disk Configuration Policy** link.
b) In the **Create Local Disk Configuration** dialog box, complete the fields.
For more information, see Creating a Local Disk Configuration Policy, page 327.
c) Click **OK**.
d) From the **Local Storage** drop-down list, choose the policy you created.

Step 4 In the **How would you like to configure SAN storage?** field, click one of the following options:

Option	Description
Simple	Allows you to create a maximum of two vHBAs for every service profile created from this template. Continue with Step 5.
Expert	Allows you to create an unlimited number of vHBAs for every service profile created from this template. Continue with Step 6.

Option	Description
No vHBAs	Does not include any vHBAs for connections to a Fibre Channel SAN in a service profile created from this template. Continue with Step 7.

Step 5 (Optional) If you chose the simple SAN storage option, do the following:

a) From the **WWNN Assignment** drop-down list, choose one of the following:

- Choose **Select (pool default used by default)** to use the default WWN pool.
- Choose one of the options listed under **Manual Using OUI** and then enter the WWN in the **World Wide Node Name** field.

  You can specify a WWNN in the range from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF. You can click the **here** link to verify that the WWNN you specified is available.
- Choose a WWN pool name from the list to have a WWN assigned from the specified pool. Each pool name is followed by two numbers in parentheses that show the number of WWNs still available in the pool and the total number of WWNs in the pool.

b) In the **vHBA 0 (Fabric A)** area, complete the following fields:

- In the **Name** field, enter a unique name for the vHBA.
- From the **Select VSAN** drop-down list, choose the name of the VSAN with which this vHBA should be associated.

If the VSAN you need is not in the drop-down list, click the **Create VSAN** link. For more information, see Creating a Named VSAN, page 261.

c) Repeat Step 7b in the **vHBA 1 (Fabric B)** area to create a VSAN for that vHBA.

d) Continue with Step 9.

Step 6 (Optional) If you chose the expert SAN storage option, do the following:

a) From the **WWNN Assignment** drop-down list, choose one of the following:

- Choose **Select (pool default used by default)** to use the default WWN pool.
- Choose one of the options listed under **Manual Using OUI** and then enter the WWN in the **World Wide Node Name** field.

  You can specify a WWNN in the range from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF. You can click the **here** link to verify that the WWNN you specified is available.
- Choose a WWN pool name from the list to have a WWN assigned from the specified pool. Each pool name is followed by two numbers in parentheses that show the number of WWNs still available in the pool and the total number of WWNs in the pool.

b) Click **Add** on the icon bar of the table to open the **Create vHBA** dialog box.

c) Complete the following fields to specify the identity information for the vHBA:

Name	Description
Name field	The name of this vHBA. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Use SAN Connectivity Template check box	Check this check box if you want to use a template to create the vHBA. Cisco UCS Manager GUI displays the **vHBA Template** drop-down list from which you can select the appropriate template, and the **Adapter Performance Profile** area from which you can select an adapter profile. **Note** You can only select this option if one or more SAN connectivity templates exist in the system.
Create vHBA Template link	Click this link if you want to create a vHBA template.
WWPN Assignment drop-down list	If you want to: • Use the default WWPN pool, leave this field set to **Select (pool default used by default)**. • Use the WWPN assigned to the server by the manufacturer, select **Hardware Default**. • A specific WWPN, select **20:00:00:25:B5:00:00:00**, **20:XX:XX:XX:XX:XX:XX:XX**, or **5X:XX:XX:XX:XX:XX:XX:XX** and enter the WWPN in the **WWPN** field. To verify that this WWPN is available, click the corresponding link. • A WWPN from a pool, select the pool name from the list. Each pool name is followed by a pair of numbers in parentheses. The first number is the number of available WWN addresses in the pool and the second is the total number of WWPN addresses in the pool. To create a new WWPN pool, click **WWPN Pool**.

d) In the **VSAN** area, complete the following fields:

Name	Description
Fabric ID field	The fabric interconnect associated with the component.
Select VSAN drop-down list box	The VSAN with which this vHBA is associated.
Create VSAN link	Click this link if you want to create a VSAN.
Pin Group drop-down list box	The pin group with which this vHBA is associated.
Create SAN Pin Group link	Click this link if you want to create a pin group.

Name	Description
Persistent Binding field	This can be: • **disabled** • **enabled**
Max Data Field Size field	The maximum size of the Fibre Channel frame payload bytes that the vHBA supports. Enter an integer between 256 and 2112. The default is 2048.
Operational Parameters Section	
Stats Threshold Policy drop-down list box	The threshold policy with which this vHBA is associated.

e) In the **Adapter Performance Profile** area, complete the following fields:

Name	Description
Adapter Policy drop-down list box	The Fibre Channel adapter policy with which this vHBA is associated.
Create Fibre Channel Adapter Policy link	Click this link if you want to create a Fibre Channel adapter policy.
QoS drop-down list box	The quality of service policy with which this vHBA is associated.
Create QoS Policy link	Click this link if you want to create a QoS policy.

f) Click **OK**.

Step 7 Click **Next**.

What to Do Next

Complete Page 3: Specifying the Networking Options, page 396.

Page 3: Specifying the Networking Options

This procedure directly follows Page 2: Specifying the Storage Options, page 392. It describes how to configure the networking options, including LAN connectivity, on the **Networking** page of the **Create Service Profile Template** wizard.

Procedure

Step 1 (Optional) If you plan to assign service profiles created from this template to a server with an adapter that supports dynamic vNICs, choose one of the following options from the **Dynamic vNIC Connection** drop-down list:

Option	Description
Select a Policy to use	Enables you to create a service profile template without a dynamic vNIC connection policy for a server with an adapter that does not support dynamic vNICs. This option does not include a dynamic vNIC connection policy in the template. Continue with Step 4.
Create a Specific Dynamic vNIC Connection Policy	Enables you to create a dynamic vNIC connection policy that can only be accessed by this service profile template. Continue with Step 2.
Dynamic vNIC Connection Policies *Policy_Name*	Select an existing dynamic vNIC connection policy from the list at the bottom of the drop-down list. Cisco UCS Manager assigns this policy to the service profile template. If you do not want use any of the existing policies, but instead want to create a policy that all service profiles and templates can access, continue with Step 3. Otherwise, continue with Step 4.

Step 2 (Optional) If you clicked **Create a Specific Dynamic vNIC Connection Policy**, do the following to create a new dynamic vNIC connection policy that can only be used by service profiles created from this template:

a) Complete the following fields:

Name	Description
Number of Dynamic vNICs field	The number of dynamic vNICs that this policy affects.
Adapter Policy drop-down list	The adapter profile associated with this policy. The profile must already exist to be included in the drop-down list.

b) Continue with Step 4.

Step 3 (Optional) To create a dynamic vNIC connection policy that will be available to all service profiles and templates, do the following:

a) Click **Create Dynamic vNIC Connection Policy**.
b) In the **Create Dynamic vNIC Connect Policy** dialog box, complete the fields.
For more information, see Creating a Dynamic vNIC Connection Policy, page 485.
c) Click **OK**.
d) From the **Dynamic vNIC Connection** drop-down list, choose the policy you created.
e) Continue with Step 4.

Step 4 In the **How would you like to configure LAN connectivity?** field, click one of the following options:

Option	Description
Simple	Allows you to create a maximum of two vNICs, in dual fabric mode, for every service profile created from this template. Continue with Step 5.
Expert	Allows you to create an unlimited number of vNICs for every service profile created from this template. Continue with Step 6.
No vNICs	Does not include any vNICs for connections to a LAN in a service profile created from this template. Any server associated with these service profiles cannot communicate with a LAN unless you modify the individual service profile later. Continue with Step 7.

Step 5 (Optional) If you chose the simple LAN connectivity option, do the following:

a) In the **vNIC 0 (Fabric A)** area:

- In the **Name** field, enter a unique name for the vNIC.
- From the **Select Native VLAN** drop-down list, choose the name of the VLAN with which this vNIC should communicate.

If the VLAN you need is not in the drop-down list, click the **Create VLAN** link. For more information, see Creating a Named VLAN, page 223.

b) Repeat Step 2a in the **vNIC 1 (Fabric B)** area to create a VLAN for that vNIC.

c) Continue with Step 4.

Step 6 If you chose the expert LAN connectivity option, do the following:

a) Click **Add** on the icon bar of the table to open the **Create vNICs** dialog box.

b) Complete the following fields to specify the identity information for the vNIC:

Name	Description
Name field	Enter a name for this vNIC. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Use LAN Connectivity Template check box	Check this check box if you want to use a template to create the vNIC. Cisco UCS Manager GUI displays the **vNIC Template** drop-down list from which you can select the appropriate template, and the **Adapter Performance Profile** area from which you can select an adapter profile. **Note** You can only select this option if one or more LAN connectivity templates exist in the system.
Create vNIC Template link	Click this link if you want to create a vNIC template.

Name	Description
MAC Address Assignment drop-down list	If you want to: • Use the default MAC address pool, leave this field set to **Select (pool default used by default)**. • Use the MAC address assigned to the server by the manufacturer, select **Hardware Default**. • A specific MAC address, select **02:25:B5:XX:XX:XX** and enter the address in the **MAC Address** field. To verify that this address is available, click the corresponding link. • A MAC address from a pool, select the pool name from the list. Each pool name is followed by a pair of numbers in parentheses. The first number is the number of available MAC addresses in the pool and the second is the total number of MAC addresses in the pool.

c) In the **Fabric Interconnect** area, complete the following fields:

Name	Description
Fabric ID field	The fabric interconnect associated with the component. If you want this vNIC to be able to access the second fabric interconnect if the default one is unavailable, check the **Enable Failover** check box. **Note** Do not select **Enable Failover** if you plan to associate this vNIC configuration with a server that has an adapter which does not support fabric failover, such as the Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter. If you do so, Cisco UCS Manager generates a configuration fault when you associate the service profile with the server.
VLANs table	This table lists the VLANs that can be associated with this vNIC. The columns are: • **Select**—Check the check box in this column for each VLAN you want to use. • **Name**—The name of the VLAN. • **Native VLAN**—To designate one of the VLANs as the native VLAN, click the radio button in this column.
Create VLAN link	Click this link if you want to create a VLAN.
MTU field	The maximum transmission unit, or packet size, that this vNIC accepts. Enter an integer between 1500 and 9216.

Name	Description
Pin Group drop-down list	Choose the LAN pin group you want associated with this vNIC.
Create LAN Pin Group link	Click this link if you want to create a LAN pin group.
Operational Parameters Section	
Stats Threshold Policy drop-down list	The statistics collection policy with which this vNIC is associated.

d) In the **Adapter Performance Profile** area, complete the following fields:

Name	Description
Adapter Policy drop-down list	The Ethernet adapter policy with which this vNIC is associated.
Create Ethernet Adapter Policy link	Click this link if you want to create an Ethernet adapter policy.
QoS drop-down list	The quality of service policy with which this vNIC is associated.
Create QoS Policy link	Click this link if you want to create a quality of service policy.
Network Control Policy drop-down list	The network control policy with which this vNIC is associated.
Create Network Control Policy Policy link	Click this link if you want to create a network control policy.

e) Click **OK**.

Step 7 Click **Next**.

What to Do Next

Complete Page 4: Setting the vNIC/vHBA Placement, page 400.

Page 4: Setting the vNIC/vHBA Placement

This procedure directly follows Page 3: Specifying the Networking Options, page 396. It describes how to set the vNIC and vHBA placement options on the **vNIC/vHBA Placement** page of the **Create Service Profile Template** wizard.

Procedure

Step 1 From the **Select Placement** drop-down list, choose one of the following:

Option	Description
Let System Perform Placement	Specifies that Cisco UCS Manager determines the vNIC/vHBA placement for all servers associated with a service profile created from this template. The placement is determined by the order set in the PCI Order table. Continue with Step 2.
Specify Manually	Enables you to specify the virtual network connection to which each vNIC and vHBA is assigned for any server associated with a service profile created from this template. Continue with Step 3.
vNIC/vHBA Placement Profiles ***Placement Profile Name***	Assigns an existing vNIC/vHBA placement policy to a service profile created from this template. If you choose this option, Cisco UCS Manager displays the details of the policy. If you do not want use any of the existing policies, but instead want to create a policy that all service profiles and templates can access, click **Create Placement Policy** and continue with Step 4. Otherwise, continue with Step 5.

Step 2 (Optional) If you chose **Let System Perform Placement**, do the following:

a) Use one or more of the following buttons to adjust the order of the vNICs and vHBAs:

Name	Description
Move Up button	Moves the selected virtual interface to a higher priority in the list.
Move Down button	Moves the selected virtual interface to a lower priority in the list.
Delete button	Deletes the selected virtual interface.
Reorder button	Returns the virtual interfaces to their original order.
Modify button	Enables you to modify the currently-selected virtual interface. **Note** You can change any options for the virtual interface except its name.

b) Continue with Step 5.

Step 3 (Optional) If you chose **Specify Manually**, do the following:

a) On the appropriate tab in the **vNIC/vHBA** table, click a vNIC or vHBA.

b) In the **Virtual Host Interface** table, click a vCON row and if necessary, choose one of the following values from the **Selection Preference** column:

- **all**
- **assigned-only**

- **exclude-dynamic**
- **exclude-unassigned**

c) Click **Assign**.
If you need to undo an assignment, click **Remove**.

d) Repeat Steps a through c until you have assigned all vNICs and vHBAs.

e) When you have specified all vNIC and vHBA placements, continue with Step 5.

Step 4 If you clicked **Create Placement Policy**, do the following in the **Create Placement Policy** dialog box:

a) In the **Name** field, enter a unique name for the placement policy.
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

b) In the **Selection Preference** column for each **Virtual Slot**, choose one of the following from the drop-down list:

- **all**
- **assigned-only**
- **exclude-dynamic**
- **exclude-unassigned**

c) Click **OK**.

d) After the dialog box closes, choose the policy you created from the **Select Placement** drop-down list.

Step 5 Click **Next**.

What to Do Next

Complete Page 5: Setting the Server Boot Order, page 402

Page 5: Setting the Server Boot Order

This procedure directly follows Page 4: Setting the vNIC/vHBA Placement, page 400. It describes how to set the server boot order options on the **Server Boot Order** page of the **Create Service Profile Template** wizard.

Tip We recommend that the boot order in a boot policy include either a local disk or a SAN LUN, but not both, to avoid the possibility of the server booting from the wrong storage type. If you configure a local disk and a SAN LUN for the boot order storage type and the operating system or logical volume manager (LVM) is configured incorrectly, the server may boot from the local disk rather than the SAN LUN.

For example, on a server with Red Hat Linux installed, where the LVM is configured with default LV names and the boot order is configured with a SAN LUN and a local disk, Linux reports that there are two LVs with the same name and boots from the LV with the lowest SCSI ID, which could be the local disk.

Procedure

Step 1 From the **Boot Policy** drop-down list, choose one of the following:

Option	Description
Select Boot Policy to use	Assigns the default boot policy to every service profile created from this template. Continue with Step 9.
Create a Specific Boot Policy	Enables you to create a local boot policy that can only be accessed by a service profile created from this template. Continue with Step 3.
Boot Policies *Policy_Name*	Assigns an existing boot policy to every service profile created from this template. If you choose this option, Cisco UCS Manager displays the details of the policy. If you do not want use any of the existing policies, but instead want to create a policy that all service profiles and templates can access, continue with Step 2. Otherwise, choose a policy from the list and continue with Step 9.

Step 2 If you clicked **Create Boot Policy** to create a boot policy that all service profiles and templates can use, do the following:

a) In the **Create Boot Policy** dialog box, enter a unique name and description for the policy.
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

b) Continue with Step 3.

Step 3 (Optional) To reboot all servers that use this boot policy after you make changes to the boot order, check the **Reboot on Boot Order Change** check box.
In Cisco UCS Manager GUI, if the **Reboot on Boot Order Change** check box is checked for a boot policy, and if CD-ROM or Floppy is the last device in the boot order, deleting or adding the device does not directly affect the boot order and the server does not reboot.

Step 4 (Optional) To ensure that Cisco UCS Manager uses any vNICs or vHBAs in the order shown in the **Boot Order** table, check the **Enforce vNIC/vHBA Name** check box.
If you do not check this check box, Cisco UCS Manager uses the priority specified in the vNIC or vHBA.

Step 5 To add a local disk, virtual CD-ROM, or virtual floppy to the boot order, do the following:

a) Click the down arrows to expand the **Local Devices** area.

b) Click one of the following links to add the device to the **Boot Order** table:

- **Add Local Disk**
- **Add CD-ROM**
- **Add Floppy**

c) Add another boot device to the **Boot Order** table, or click **OK** to finish.

Step 6 To add a LAN boot to the boot order, do the following:

a) Click the down arrows to expand the **vNICs** area.
b) Click the **Add LAN Boot** link.
c) In the **Add LAN Boot** dialog box, enter the name of the vNIC that you want to use for the LAN boot in the **vNIC** field, then click **OK**.
d) Add another device to the **Boot Order** table, or click **OK** to finish.

Step 7 To add a SAN boot to the boot order, do the following:

a) Click the down arrows to expand the **vHBAs** area.
b) Click the **Add SAN Boot** link.
c) In the **Add SAN Boot** dialog box, complete the following fields, then click **OK**:

Name	Description
vHBA field	Enter the name of the vHBA you want to use for the SAN boot.
Type field	This can be: • **primary**—If the server boots using a SAN WWN address, this is the first address it tries. Each boot policy can have only one primary SAN boot location. • **secondary**—If the server cannot boot from the primary SAN location, it attempts to boot from this location. Each boot policy can have only one secondary SAN boot location. The use of the terms primary or secondary boot devices does not imply a boot order. The effective order of boot devices within the same device class is determined by PCIe bus scan order.

d) If this vHBA points to a bootable SAN image, click the **Add SAN Boot Target** link and, in the **Add SAN Boot Target** dialog box, complete the following fields, then click **OK**:

Name	Description
Boot Target LUN field	The LUN that corresponds to the location of the boot image.
Boot Target WWPN field	The WWPN that corresponds to the location of the boot image.
Type field	This can be: • **primary**—If the server boots using a SAN WWN address, this is the first address it tries. Each boot policy can have only one primary SAN boot location. • **secondary**—If the server cannot boot from the primary SAN location, it attempts to boot from this location. Each boot policy can have only one secondary SAN boot location.

Name	Description
	The use of the terms primary or secondary boot devices does not imply a boot order. The effective order of boot devices within the same device class is determined by PCIe bus scan order.

e) Add another boot device to the **Boot Order** table, or click **OK** to finish.

Step 8 If you created a new boot policy accessible to all service profiles and template, select that policy from the **Boot Policy** drop-down list.

Step 9 Click **Next**.

What to Do Next

Complete Page 6: Adding the Maintenance Policy, page 405.

Page 6: Adding the Maintenance Policy

This procedure directly follows Page 5: Setting the Server Boot Order, page 402. It describes how to add a maintenance policy to the service profile on the **Maintenance Policy** page of the **Create Service Profile (expert)** wizard.

Procedure

Step 1 From the **Maintenance Policy** drop-down list, choose one of the following:

Option	Description
Select a Maintenance Policy to Use (default policy shown)	Assigns the default maintenance policy to this service profile. Continue with Step 4.
Maintenance Policies *Policy_Name*	Assigns an existing maintenance policy to the service profile. If you choose this option, Cisco UCS Manager displays the details of the policy. If you do not want use any of the existing policies but instead want to create a policy that all service profiles can access, click **Create Maintenance Policy** and continue with Step 2. Otherwise, choose a policy from the list and continue with Step 4.

Step 2 If you clicked **Create Maintenance Policy** to create a maintenance policy that all service profiles and templates can use, do the following:

a) In the **Create Maintenance Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the policy.

Name	Description
	This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Reboot Policy field	When a service profile is associated with a server, or when changes are made to a service profile that is already associated with a server, the server needs to be rebooted to complete the process. The **Reboot Policy** field determines when the reboot occurs for servers associated with any service profiles that include this maintenance policy. This can be: • **immediate**—The server is rebooted automatically as soon as the service profile association is complete or service profile changes are saved by the user. • **user-ack**—The user must reboot the server manually after the service profile association is complete or changes are made. • **timer-automatic**—Cisco UCS defers all service profile associations and changes until the maintenance window defined by the schedule shown in the **Schedule** field.
Schedule drop-down list	If the **Reboot Policy** is set to **timer-automatic**, the schedule specifies when maintenance operations can be applied to the server. Cisco UCS reboots the server and completes the service profile changes at the scheduled time.

b) Click **OK** and continue with Step 3.

Step 3 If you created a new boot policy accessible to all service profiles and template, select that policy from the **Maintenance Policy** drop-down list.

Step 4 Click **Next**.

What to Do Next

Complete Page 7: Specifying the Server Assignment, page 382.

Page 7: Specifying the Server Assignment Options

This procedure directly follows Page 6: Adding the Maintenance Policy, page 405. It describes how to specify the way a server is assigned to a service profile created from this template on the **Server Assignment** page of the **Create Service Profile Template** wizard.

Procedure

Step 1 From the **Server Assignment** drop-down list, choose one of the following:

Option	Description
Assign Later	Allows you to assign a server after you have created and configured the service profile template. Continue with Step 2.
Select from a Pool ***Pool_Name***	Select a server pool from the list at the bottom of the drop-down list. Cisco UCS Manager assigns a server from this pool to a service profile created from this template. Continue with Step 2.

Step 2 In the **Power State** field, click one of the following radio buttons to set the power state that will be applied to the server when it is associated with a service profile created from this template:

- **Down** if you want the server to be powered down before the profile is associated with the server
- **Up** if you want the server to be powered up before the profile is associated with the server

By default, the server is powered up.

Step 3 (Optional) In the **Firmware Management** area, do the following to use policies to update the firmware on the server associated with a service profile created from this template:

a) Click the down arrows on the **Firmware Management** bar.

b) Complete the following fields:

Name	Description
Host Firmware drop-down list	To associate a host firmware package with this service profile, choose its name from the drop-down list.
Create Host Firmware Package link	Click this link if you want to create a host firmware package.
Management Firmware drop-down list	To associate a management firmware package with this service profile, choose its name from the drop-down list.
Create Management Firmware Package link	Click this link if you want to create a management firmware package.

Step 4 Click **Next**.

What to Do Next

Complete Page 8: Adding Operational Policies, page 408.

Page 8: Adding Operational Policies

This procedure directly follows Page 7: Specifying the Server Assignment Options, page 406. It describes how to add operational policies to the service profile template on the **Operational Policies** page of the **Create Service Profile Template** wizard. These policies are optional.

Procedure

Step 1 To override the default BIOS settings and configure them through the service profile, click the down arrows to expand the **BIOS Configuration** bar and do one of the following:

- To add an existing policy, select the desired BIOS policy from the **BIOS Policy** drop-down list .
- To create a BIOS policy that is available to all service profiles, click **Create BIOS Policy**, complete the fields in the dialog box, and then select the desired BIOS policy from the **BIOS Policy** drop-down list .

For more information about how to create a BIOS policy, see Creating a BIOS Policy, page 317.

Step 2 To provide external access to the CIMC on the server, click the down arrows to expand the **External IPMI Management Configuration** bar and add an IPMI profile and a serial over LAN policy.
If you do not want to provide external access, continue with Step 4.

Step 3 To add an IPMI profile to service profiles created from this template, do one of the following:

- To add an existing policy, select the desired IPMI profile from the **IPMI Access Profile** drop-down list.
- If the **IPMI Access Profile** drop-down list does not include an IPMI profile with the desired user access, click the **Create Access IPMI Profile** link to create an IPMI profile that is available to all service profiles and then select that profile from the **IPMI Access Profile** drop-down list.

For more information about how to create an IPMI profile, see Creating an IPMI Access Profile, page 323.

Step 4 To add a Serial over LAN policy to service profiles created from this template, do one of the following:

- To add an existing policy, select the desired Serial over LAN policy from the **SoL Configuration Profile** drop-down list.
- To create a Serial over LAN policy that is only available to service profile created from this template, select **Create a Specific SoL Policy** from the **SoL Configuration Profile** drop-down list and complete the **Admin State** field and the **Speed** drop-down list.
- To create a Serial over LAN policy that is available to all service profile templates, click the **Create Serial over LAN Policy** link and complete the fields in the dialog box and then select that policy from the **SoL Configuration Profile** drop-down list.

For more information about how to create a serial over LAN policy, see Creating a Serial over LAN Policy, page 332.

Step 5 To configure the management IP required for external access to the CIMC on the server, click the down arrows to expand the **Management IP Address** bar and click one of the following radio buttons:

- **none**—No management IP address is assigned to the service profile. The management IP address is set based on the CIMC management IP address settings on the server.

- **pooled**—A management IP address is assigned to the service profile from the management IP address pool.

Step 6 To monitor thresholds and collect statistics for the associated server, click the down arrows to expand the **Monitoring Configuration** bar and do one of the following:

- To add an existing policy, select the desired threshold policy from the **Threshold Policy** drop-down list.
- To create a threshold policy that is available to all service profiles, click the **Create Threshold Policy** link, complete the fields in the dialog box, and then select that policy from the **Threshold Policy** drop-down list.

For more information about how to create a threshold policy, see Creating a Server and Server Component Threshold Policy , page 576.

Step 7 To associate a power control policy with the service profile template, click the down arrows to expand the **Power Control Policy Configuration** bar and do one of the following:

- To add an existing policy, select the desired power control policy from the **Power Control Policy** drop-down list.
- To create a power control policy that is available to all service profiles and templatesw, click the **Create Power Control Policy** link , complete the fields in the dialog box, and then select that policy from the **Power Control Policy** drop-down list.

For more information about how to create a power control policy, see Creating a Power Control Policy, page 437.

Step 8 To associate a scrub policy with the service profile template, click the down arrows to expand the **Scrub Policy** bar and do one of the following:

- To add an existing policy, select the desired scrub policy from the **Scrub Policy** drop-down list .
- To create a scrub policy that is available to all service profiles and templates, click the **Create Scrub Policy** link , complete the fields in the dialog box, and then select hat policy from the **Scrub Policy** drop-down list .

For more information about how to create a scrub policy, see Creating a Scrub Policy, page 330.

Step 9 Click **Finish**.

Creating One or More Service Profiles from a Service Profile Template

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profile Templates**.

Step 3 Expand the node for the organization that contains the service profile template that you want to use as the basis for your service profiles.

If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the service profile template from which you want to create the profiles and select **Create Service Profiles From Template**.

Step 5 In the **Create Service Profiles From Template** dialog box, complete the following fields:

Name	Description
Naming Prefix field	The prefix to use for the template name. When the system creates the service profile, it appends a unique numeric identifier to this prefix. For example, if you specify the prefix MyProfile and request two profiles, the first service profile would be called MyProfile1 and the second would be MyProfile2. If you return at a later date and create three more profiles with the same prefix, they would be named MyProfile3, MyProfile4, and MyProfile5.
Number field	The number of service profiles to create.

Step 6 Click **OK**.

Creating a Template Based Service Profile for a Blade Server

Before You Begin

A qualified service profile template with the desired values must exist in Cisco UCS Manager.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.

Step 3 Choose the server for which you want to create a template based service profile.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Create Service Profile**.

Step 6 In the **Create Service Profile for Server** dialog box, do the following:

a) Click the **Template Based Service Profile** radio button.

b) In the **Name** field, enter a unique name for the service profile.
This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

c) From the **Service Profile Template** drop-down list, select the template from which you want to create the service profile associated with this server.

d) Click **OK**.

Creating a Template Based Service Profile for a Rack-Mount Server

Before You Begin

A qualified service profile template with the desired values must exist in Cisco UCS Manager.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Rack Mounts ➤ Servers**.

Step 3 Choose the server for which you want to create a template based service profile.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Create Service Profile**.

Step 6 In the **Create Service Profile for Server** dialog box, do the following:

a) Click the **Template Based Service Profile** radio button.

b) In the **Name** field, enter a unique name for the service profile.
This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

c) From the **Service Profile Template** drop-down list, select the template from which you want to create the service profile associated with this server.

d) Click **OK**.

Creating a Service Profile Template from a Service Profile

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization that contains the service profile that you want to use as the basis for your template.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the service profile from which you want to create the template and select **Create a Service Profile Template**.

Step 5 In the **Create Template From Service Profile** dialog box, complete the following fields:

Name	Description
Service Profile Template Name field	The name of the service profile template. This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

Name	Description
Org drop-down list	Select the organization that you want this template to be associated with.
Type field	This can be: • **Initial Template**—Any service profiles created from this template are not updated if the template changes • **Updating Template**—Any service profiles created from this template are updated if the template changes

Step 6 Click **OK**.

Managing Service Profiles

Cloning a Service Profile

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization where you want to create the service profile.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the service profile you want to clone and select **Create a Clone**.

Step 5 In the **Create Clone From Service Profile** dialog box:

a) Enter the name you want to use for the new profile in the **Clone Name** field.
This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

This name must be unique within the organization or sub-organization in which you are creating the service profile.

b) Click **OK**.

Step 6 Navigate to the service profile you just created and make sure that all options are correct.

Associating a Service Profile with a Server or Server Pool

Follow this procedure if you did not associate the service profile with a blade server or server pool when you created it, or to change the blade server or server pool with which a service profile is associated.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization that contains the service profile that you want to associate with a new server or server pool.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the service profile you want to associate with a server and select **Change Service Profile Association**.

Step 5 In the **Associate Service Profile** dialog box, select one of the following options:

Option	Description
Server Pool	Select a server pool from the drop-down list. Cisco UCS Manager assigns a server from this pool to the service profile. Continue with Step 7.
Server	Navigate to the desired available server in the navigation tree and select the server which will be assigned to the service profile. Continue with Step 7.
Custom Server	Specifies the chassis and slot that contains the server that will be assigned to the service profile. If the server is not in the slot or is otherwise unavailable, the service profile will be associated with the server when it becomes available. Continue with Step 6.

Step 6 If you chose **Custom Server**, do the following:

a) In the **Chassis Id** field, enter the number of the chassis where the selected server is located.

b) In the **Server Id** field, enter the number of the slot where the selected server is located.

Step 7 Click **OK**.

Disassociating a Service Profile from a Server or Server Pool

When you disassociate a service profile, Cisco UCS Manager attempts to shutdown the operating system on the server. If the operating system does not shutdown within a reasonable length of time, Cisco UCS Manager forces the server to shutdown.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization that contains the service profile that you want to disassociate from a server or server pool.

If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the service profile you want to disassociate from a server and select **Disassociate Service Profile**.

Step 5 In the **Disassociate Service Profile** dialog box, click **Yes** to confirm that you want to disassociate the service profile.

Step 6 (Optional) Monitor the status and FSM for the server to confirm that the disassociation completed.

Associating a Service Profile Template with a Server Pool

Follow this procedure if you did not associate the service profile template with a server pool when you created it, or to change the server pool with which a service profile created from this template is associated.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profile Templates**.

Step 3 Expand the node for the organization that contains the service profile that you want to associate with a server pool.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the service profile template you want to associate with a server pool and select **Associate with Server Pool**.
The **Associate with Server Pool** dialog box opens.

Step 5 From the **Server Pool** section of the **Pool Assignment** drop-down list, select a server pool.
If you select **Assign Later**, the service profile template is not associated with a server pool.

Step 6 Select one of the following radio buttons to determine the power state applied to a server which is associated with a service profile created from this template:

- **Down**
- **Up**

Step 7 From the **Select Qualification** drop-down list, select the server pool policy qualifications you want to apply to a server that is associated with a service profile created from this template.

Step 8 Click **OK**.

Disassociating a Service Profile Template from its Server Pool

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profile Templates**.

Step 3 Expand the node for the organization that contains the service profile that you want to disassociate from its server pool.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the service profile template you want to disassociate from its server pool and select **Disassociate Template**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Changing the UUID in a Service Profile

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization that contains the service profile for which you want to change the UUID.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Choose the service profile that requires the UUID for the associated server to be changed.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Actions** area, click **Change UUID**.

Step 7 From the **UUID Assignment** drop-down list, do one of the following:

Option	Description
Select (pool default used by default)	Assigns a UUID from the default UUID Suffix pool. Continue with Step 9.

Option	Description
Hardware Default	Uses the UUID assigned to the server by the manufacturer. If you choose this option, the UUID remains unassigned until the service profile is associated with a server. At that point, the UUID is set to the UUID value assigned to the server by the manufacturer. If the service profile is later moved to a different server, the UUID is changed to match the new server. Continue with Step 9.
XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX	Uses the UUID that you manually assign. Continue with Step 8.
Pools ***Pool_Name***	Assigns a UUID from the UUID Suffix pool that you select from the list at the bottom of the drop-down list. Each pool name is followed by two numbers in parentheses that show the number of UUIDs still available in the pool and the total number of UUIDs in the pool. Continue with Step 9.

Step 8 (Optional) If you selected the **XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX** option, do the following:

a) In the **UUID** field, enter the valid UUID that you want to assign to the server which uses this service profile.

b) To verify that the selected UUID is available, click the **here** link.

Step 9 Click **OK**.

Changing the UUID in a Service Profile Template

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profile Templates**.

Step 3 Expand the node for the organization that contains the service profile template for which you want to change the UUID.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Choose the service profile template whose UUID assignment you want to change.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Actions** area, click **Change UUID**.

Step 7 From the **UUID Assignment** drop-down list, choose one of the following:

Option	Description
Select (pool default used by default)	Assigns a UUID from the default UUID Suffix pool.
Hardware Default	Uses the UUID assigned to the server by the manufacturer. If you choose this option, the UUID remains unassigned until the service profile is associated with a server. At that point, the UUID is set to the UUID value assigned to the server by the manufacturer. If the service profile is later moved to a different server, the UUID is changed to match the new server.
Pools ***Pool_Name***	Assigns a UUID from the UUID Suffix pool that you select from the list at the bottom of the drop-down list. Each pool name is followed by two numbers in parentheses that show the number of UUIDs still available in the pool and the total number of UUIDs in the pool.

Step 8 Click **OK**.

Resetting the UUID Assigned to a Service Profile from a Pool in a Service Profile Template

If you change the UUID suffix pool assigned to an updating service profile template, Cisco UCS Manager does not change the UUID assigned to a service profile created with that template. If you want Cisco UCS Manager to assign a UUID from the newly assigned pool to the service profile, and therefore to the associated server, you must reset the UUID. You can only reset the UUID assigned to a service profile and its associated server under the following circumstances:

- The service profile was created from an updating service profile template and includes a UUID assigned from a UUID suffix pool.
- The UUID suffix pool name is specified in the service profile. For example, the pool name is not empty.
- The UUID value is not 0, and is therefore not derived from the server hardware.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization that contains the service profile for which you want to reset the UUID. If the system does not include multi-tenancy, expand the **root** node.

Step 4 Choose the service profile that requires the UUID for the associated server to be reset to a different UUID suffix pool.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Actions** area, click **Reset UUID**.
If this action is not visible, then the UUID configuration in the service profile does not meet the requirements for resetting a UUID.

Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 8 Click **OK**

Modifying the Boot Order in a Service Profile

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization that includes the service profile for which you want to change the boot order.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Click the service profile for which you want to change the boot order.

Step 5 In the **Work** pane, click the **Boot Order** tab.

Step 6 Click **Modify Boot Policy** to change the existing boot policy.

Step 7 In the **Modify Boot Policy** dialog box, choose one of the following from the **Boot Policy** drop-down list:

Option	Description
Select Boot Policy to use	Assigns the default boot policy to this service profile. Continue with Step 14.
Create a Specific Boot Policy	Enables you to create a local boot policy that can only be accessed by this service profile. Continue with Step 8.
Boot Policies *Policy_Name*	Assigns an existing boot policy to the service profile. If you choose this option, Cisco UCS Manager displays the details of the policy. If you do not want use any of the existing policies, but instead want to create a policy that all service profiles can access, click **Create Boot Policy** and continue with Step 2. Otherwise, continue with Step 14.

Step 8 If you chose to create a boot policy, in the **Create Boot Policy** dialog box, enter a unique name and description for the policy.
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

Step 9 (Optional) To reboot all servers that use this boot policy after you make changes to the boot order, check the **Reboot on Boot Order Change** check box.
In Cisco UCS Manager GUI, if the **Reboot on Boot Order Change** check box is checked for a boot policy, and if CD-ROM or Floppy is the last device in the boot order, deleting or adding the device does not directly affect the boot order and the server does not reboot.

Step 10 (Optional) To ensure that Cisco UCS Manager uses any vNICs or vHBAs in the order shown in the **Boot Order** table, check the **Enforce vNIC/vHBA Name** check box.
If you do not check this check box, Cisco UCS Manager uses the priority specified in the vNIC or vHBA.

Step 11 To add a local disk, virtual CD-ROM, or virtual floppy to the boot order, do the following:

a) Click the down arrows to expand the **Local Devices** area.
b) Click one of the following links to add the device to the **Boot Order** table:

- **Add Local Disk**
- **Add CD-ROM**
- **Add Floppy**

c) Add another boot device to the **Boot Order** table, or click **OK** to finish.

Step 12 To add a LAN boot to the boot order, do the following:

a) Click the down arrows to expand the **vNICs** area.
b) Click the **Add LAN Boot** link.
c) In the **Add LAN Boot** dialog box, enter the name of the vNIC that you want to use for the LAN boot in the **vNIC** field, then click **OK**.
d) Add another device to the **Boot Order** table, or click **OK** to finish.

Step 13 To add a SAN boot to the boot order, do the following:

a) Click the down arrows to expand the **vHBAs** area.
b) Click the **Add SAN Boot** link.
c) In the **Add SAN Boot** dialog box, complete the following fields, then click **OK**:

Name	Description
vHBA field	Enter the name of the vHBA you want to use for the SAN boot.
Type field	This can be: • **primary**—If the server boots using a SAN WWN address, this is the first address it tries. Each boot policy can have only one primary SAN boot location. • **secondary**—If the server cannot boot from the primary SAN location, it attempts to boot from this location. Each boot policy can have only one secondary SAN boot location. The use of the terms primary or secondary boot devices does not imply a boot order. The effective order of boot devices within the same device class is determined by PCIe bus scan order.

d) If this vHBA points to a bootable SAN image, click the **Add SAN Boot Target** link and, in the **Add SAN Boot Target** dialog box, complete the following fields, then click **OK**:

Name	Description
Boot Target LUN field	The LUN that corresponds to the location of the boot image.
Boot Target WWPN field	The WWPN that corresponds to the location of the boot image.
Type field	This can be: • **primary**—If the server boots using a SAN WWN address, this is the first address it tries. Each boot policy can have only one primary SAN boot location. • **secondary**—If the server cannot boot from the primary SAN location, it attempts to boot from this location. Each boot policy can have only one secondary SAN boot location. The use of the terms primary or secondary boot devices does not imply a boot order. The effective order of boot devices within the same device class is determined by PCIe bus scan order.

e) Add another boot device to the **Boot Order** table, or click **OK** to finish.

Step 14 Click **OK**.

Creating a vNIC for a Service Profile

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization that contains the service profile for which you want to create a vNIC.

Step 4 Expand the service profile for which you want to create a vNIC.

Step 5 Right-click the **vNICs** node and choose **Create vNICs**.

Step 6 In the **Create vNICs** dialog box, do the following:

a) Complete the following fields to specify the identity information for the vNIC:

Name	Description
Name field	Enter a name for this vNIC.

Name	Description
	This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Use LAN Connectivity Template check box	Check this check box if you want to use a template to create the vNIC. Cisco UCS Manager GUI displays the **vNIC Template** drop-down list from which you can select the appropriate template, and the **Adapter Performance Profile** area from which you can select an adapter profile. **Note** You can only select this option if one or more LAN connectivity templates exist in the system.
Create vNIC Template link	Click this link if you want to create a vNIC template.
MAC Address Assignment drop-down list	If you want to: • Use the default MAC address pool, leave this field set to **Select (pool default used by default)**. • Use the MAC address assigned to the server by the manufacturer, select **Hardware Default**. • A specific MAC address, select **02:25:B5:XX:XX:XX** and enter the address in the **MAC Address** field. To verify that this address is available, click the corresponding link. • A MAC address from a pool, select the pool name from the list. Each pool name is followed by a pair of numbers in parentheses. The first number is the number of available MAC addresses in the pool and the second is the total number of MAC addresses in the pool.

b) Complete the following fields to specify the fabric connection information:

Name	Description
Fabric ID field	The fabric interconnect associated with the component. If you want this vNIC to be able to access the second fabric interconnect if the default one is unavailable, check the **Enable Failover** check box. **Note** Do not select **Enable Failover** if you plan to associate this vNIC configuration with a server that has an adapter which does not support fabric failover, such as the Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter. If you do so, Cisco UCS Manager generates a configuration fault when you associate the service profile with the server.
VLANs table	This table lists the VLANs that can be associated with this vNIC. The columns are:

Name	Description
	• **Select**—Check the check box in this column for each VLAN you want to use. • **Name**—The name of the VLAN. • **Native VLAN**—To designate one of the VLANs as the native VLAN, click the radio button in this column.
Create VLAN link	Click this link if you want to create a VLAN.
MTU field	The maximum transmission unit, or packet size, that this vNIC accepts. Enter an integer between 1500 and 9216.
Pin Group drop-down list	Choose the LAN pin group you want associated with this vNIC.
Create LAN Pin Group link	Click this link if you want to create a LAN pin group.
Operational Parameters Section	
Stats Threshold Policy drop-down list	The statistics collection policy with which this vNIC is associated.

c) In the **Adapter Performance Profile** area, complete the following fields:

Name	Description
Adapter Policy drop-down list	The Ethernet adapter policy with which this vNIC is associated.
Create Ethernet Adapter Policy link	Click this link if you want to create an Ethernet adapter policy.
QoS drop-down list	The quality of service policy with which this vNIC is associated.
Create QoS Policy link	Click this link if you want to create a quality of service policy.
Network Control Policy drop-down list	The network control policy with which this vNIC is associated.
Create Network Control Policy Policy link	Click this link if you want to create a network control policy.

d) Click **OK**.

Resetting the MAC Address Assigned to a vNIC from a Pool in a Service Profile Template

If you change the MAC pool assigned to an updating service profile template, Cisco UCS Manager does not change the MAC address assigned to a service profile created with that template. If you want Cisco UCS Manager to assign a MAC address from the newly assigned pool to the service profile, and therefore to the associated server, you must reset the MAC address. You can only reset the MAC address assigned to a service profile and its associated server under the following circumstances:

- The service profile was created from an updating service profile template and includes a MAC address assigned from a MAC pool.
- The MAC pool name is specified in the service profile. For example, the pool name is not empty.
- The MAC address value is not 0, and is therefore not derived from the server hardware.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization that contains the service profile for which you want to reset the MAC address.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Expand ***Service_Profile_Name*** **➤ vNICs**.

Step 5 Click the vNIC for which you want to reset the MAC address.

Step 6 In the **Work** pane, click the **General** tab.

Step 7 In the **Actions** area, click **Reset MAC Address**.

Step 8 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 9 Click **OK**.

Deleting a vNIC from a Service Profile

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization that contains the service profile from which you want to delete a vNIC.

Step 4 Expand the service profile from which you want to delete a vNIC.

Step 5 Expand the **vNICs** node.

Step 6 Right-click the vNIC you want to delete and choose **Delete**.

Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Creating a vHBA for a Service Profile

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization that contains the service profile for which you want to create a vHBA.

Step 4 Expand the service profile for which you want to create a vHBA.

Step 5 Right-click the **vHBAs** node and choose **Create vHBAs**.

Step 6 In the **Create vHBAs** dialog box, do the following:

a) Complete the following fields to specify the identity information for the vHBA:

Name	Description
Name field	The name of this vHBA. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Use SAN Connectivity Template check box	Check this check box if you want to use a template to create the vHBA. Cisco UCS Manager GUI displays the **vHBA Template** drop-down list from which you can select the appropriate template, and the **Adapter Performance Profile** area from which you can select an adapter profile. **Note** You can only select this option if one or more SAN connectivity templates exist in the system.
Create vHBA Template link	Click this link if you want to create a vHBA template.
WWPN Assignment drop-down list	If you want to: • Use the default WWPN pool, leave this field set to **Select (pool default used by default)**. • Use the WWPN assigned to the server by the manufacturer, select **Hardware Default**. • A specific WWPN, select **20:00:00:25:B5:00:00:00**, **20:XX:XX:XX:XX:XX:XX:XX**, or **5X:XX:XX:XX:XX:XX:XX:XX** and enter the WWPN in the **WWPN** field. To verify that this WWPN is available, click the corresponding link. • A WWPN from a pool, select the pool name from the list. Each pool name is followed by a pair of numbers in parentheses. The first number is the number of available WWN addresses in the pool and the second is the total number of WWPN addresses in the pool. To create a new WWPN pool, click **WWPN Pool**.

b) In the **VSAN** area, complete the following fields:

Name	Description
Fabric ID field	The fabric interconnect associated with the component.
Select VSAN drop-down list box	The VSAN with which this vHBA is associated.
Create VSAN link	Click this link if you want to create a VSAN.
Pin Group drop-down list box	The pin group with which this vHBA is associated.
Create SAN Pin Group link	Click this link if you want to create a pin group.
Persistent Binding field	This can be: • **disabled** • **enabled**
Max Data Field Size field	The maximum size of the Fibre Channel frame payload bytes that the vHBA supports. Enter an integer between 256 and 2112. The default is 2048.
Operational Parameters Section	
Stats Threshold Policy drop-down list box	The threshold policy with which this vHBA is associated.

c) In the **Adapter Performance Profile** area, complete the following fields:

Name	Description
Adapter Policy drop-down list box	The Fibre Channel adapter policy with which this vHBA is associated.
Create Fibre Channel Adapter Policy link	Click this link if you want to create a Fibre Channel adapter policy.
QoS drop-down list box	The quality of service policy with which this vHBA is associated.
Create QoS Policy link	Click this link if you want to create a QoS policy.

d) Click **OK**.

Changing the WWPN for a vHBA

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization that contains the service profile for which you want to change the WWPN.

Step 4 Expand ***Service_Profile_Name*** **➤ vHBAs**.

Step 5 Click the vHBA for which you want to change the WWPN.

Step 6 In the **Work** pane, click the **General** tab.

Step 7 In the **Actions** area, click **Change World Wide Name**.

Step 8 In the **Change World Wide Port Name** dialog box, do the following:

a) From the **WWPN Assignment** drop-down list , do one of the following:

- Use the default WWPN pool, choose **Select (pool default used by default)**.
- Use a WWPN derived from the manufacturers specifications, choose **Hardware Default**.
- A specific WWPN, choose **20:00:00:25:B5:00:00:00** and enter the WWNN in the **WWPN** field.
- A WWPN from a pool, select the pool name from the list. Each pool name is followed by number of available/total WWPNs in the pool.

b) Click **OK**.

Resetting the WWPN Assigned to a vHBA from a Pool in a Service Profile Template

If you change the WWPN pool assigned to an updating service profile template, Cisco UCS Manager does not change the WWPN assigned to a service profile created with that template. If you want Cisco UCS Manager to assign a WWPN from the newly assigned pool to the service profile, and therefore to the associated server, you must reset the WWPN. You can only reset the WWPN assigned to a service profile and its associated server under the following circumstances:

- The service profile was created from an updating service profile template and includes a WWPN assigned from a WWPN pool.
- The WWPN pool name is specified in the service profile. For example, the pool name is not empty.
- The WWPN value is not 0, and is therefore not derived from the server hardware.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization that contains the service profile for which you want to reset the WWPN. If the system does not include multi-tenancy, expand the **root** node.

Step 4 Expand ***Service_Profile_Name*** **➤ vHBAs**.

Step 5 Click the vHBA for which you want to reset the WWPN.

Step 6 In the **Work** pane, click the **General** tab.

Step 7 In the **Actions** area, click **Reset WWPN**.

Step 8 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 9 Click **OK**.

Clearing Persistent Binding for a vHBA

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization that contains the service profile for which you want to modify the vHBA.

Step 4 Expand ***Service_Profile_Name*** **➤ vHBAs**.

Step 5 Click the vHBA for which you want to clear the persistent binding.

Step 6 In the **Work** pane, click the **General** tab.

Step 7 In the **Actions** area, click **Clear Persistent Binding**.

Step 8 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Deleting a vHBA from a Service Profile

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization that contains the service profile from which you want to delete a vHBA.

Step 4 Expand the service profile from which you want to delete a vHBA.

Step 5 Expand the **vHBAs** node.

Step 6 Right-click the vHBA you want to delete and choose **Delete**.

Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Binding a Service Profile to a Service Profile Template

You can bind a service profile to a service profile template. When you bind the service profile to a template, Cisco UCS Manager configures the service profile with the values defined in the service profile template. If the existing service profile configuration does not match the template, Cisco UCS Manager reconfigures the service profile. You can only change the configuration of a bound service profile through the associated template.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization that includes the service profile you want to bind.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Click the service profile you want to bind.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Actions** area, click **Bind to a Template**.

Step 7 In the **Bind to a Service Profile Template** dialog box, do the following:

a) From the **Service Profile Template** drop-down list, choose the template to which you want to bind the service profile.

b) Click **OK**.

Unbinding a Service Profile from a Service Profile Template

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization that includes the service profile you want to unbind.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Click the service profile you want to unbind.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Actions** area, click **Unbind from the Template**.

Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Deleting a Service Profile

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 In the **Servers** tab, expand **Servers ➤ Service Profiles ➤** ***Organization_Name*** .

Step 3 Right-click the service profile you want to delete and select **Delete**.

Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 5 Click **OK**.

CHAPTER 29

Managing Power in Cisco UCS

This chapter includes the following sections:

Power Management in Cisco UCS

You can manage power through Cisco UCS Manager by configuring any of the following features:

- Power supply redundancy for all chassis in a Cisco UCS instance
- Policy-driven chassis-level power capping
- Manual blade-level power capping

Rack Server Power Management

Power capping is not supported for rack servers.

Configuring the Power Policy

Power Policy

The power policy is a global policy that specifies the redundancy for power supplies in all chassis in the Cisco UCS instance. This policy is also known as the PSU policy.

For more information about power supply redundancy, see *Cisco UCS 5108 Server Chassis Hardware Installation Guide*.

Configuring the Power Policy

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, click the **Equipment** node.

Step 3 In the **Work** pane, click the **Policies** tab.

Step 4 Click the **Global Policies** subtab.

Step 5 In the **Power Policy** area, click one of the following radio buttons in the **Redundancy** field:

- **non-redundant**—All installed power supplies are turned on and the load is evenly balanced. Only smaller configurations (requiring less than 2500W) can be powered by a single power supply.
- **n+1**—The total number of power supplies to satisfy non-redundancy, plus one additional power supply for redundancy, are turned on and equally share the power load for the chassis. If any additional power supplies are installed, Cisco UCS Manager sets them to a "turned-off" state.
- **grid**—Two power sources are turned on, or the chassis requires greater than N+1 redundancy. If one source fails (which causes a loss of power to one or two power supplies), the surviving power supplies on the other power circuit continue to provide power to the chassis.

For more information about power supply redundancy, see *Cisco UCS 5108 Server Chassis Hardware Installation Guide*.

Step 6 Click **Save Changes**.

Configuring the Global Cap Policy

Global Cap Policy

The global cap policy is a global policy that specifies whether policy-driven chassis group power capping or manual blade-level power capping will be applied to all servers in a chassis.

We recommend that you use the default power capping method: policy-driven chassis group power capping.

Important Any change to the manual blade-level power cap configuration will result in the loss of any groups or configuration options set for policy-driven chassis group power capping.

Configuring the Global Cap Policy

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, click the **Equipment** node.

Step 3 In the **Work** pane, click the **Policies** tab.

Step 4 Click the **Global Policies** subtab.

Step 5 In the **Global Cap Policy** area, click one of the following radio buttons in the **Allocation Method** field to determine the power cap management mode used in the Cisco UCS instance:

- **Manual Blade Level Cap**—Power allocation is configured on each individual blade server in all chassis. If you select this option, you cannot create power groups.
- **Policy Driven Chassis Group Cap**—Power allocation is configured at the chassis level through power control policies included in the associated service profiles. If you select this option, you can also create power groups that contain one or more chassis in the Cisco UCS instance.

By default, power allocation is done for each chassis through a power control policy.

Step 6 Click **Save Changes**.

Configuring Policy-Driven Chassis Group Power Capping

Policy-Driven Chassis Group Power Capping

When policy-driven power chassis group power capping is selected in the global cap policy, Cisco UCS can maintain the oversubscription of servers without risking costly power failures. This is achieved through a two-tier process. At the chassis level, Cisco UCS divides the amount of power available between members of the power group. At the blade level, the amount of power allotted to a chassis is divided between blades based on priority.

Each time a service profile is associated or disassociated, UCS Manager recalculates the power allotment for each blade server within the chassis. If necessary, power from lower-priority service profiles is redistributed to higher-priority service profiles.

Note The system reserves enough power to boot a server in each slot, even if that slot is empty. This reserved power cannot be leveraged by servers requiring more power. Blades that fail to comply with the power cap are penalized or shut down.

Configuring Power Groups

Power Groups

A power group is a set of chassis that all draw power from the same power distribution unit (PDU). In Cisco UCS Manager, you can create power groups that include one or more chassis and then set a peak power cap in AC watts for that power grouping.

Instituting power capping at the chassis level requires the following:

- IOM, CIMC, and BIOS version 1.4 or higher
- 2 PSUs

The peak power cap is a static value that represents the maximum power available to all blade servers within a given power group. If you add or remove a blade from a power group, but do not manually modify the peak power value, the power group adjusts the peak power cap to accommodate the basic power-on requirements of all blades within that power group.

A minimum of 3788 AC watts should be set for each chassis. This converts to 3400 watts of DC power, which is the minimum amount of power required to power a fully-populated chassis.

If insufficient power is available, Cisco UCS Manager raises an alert.

Once a chassis is added to a power group, every service profile associated with that chassis also becomes part of that power group. Similarly, if you add a new blade to a chassis, that blade inherently becomes part of the chassis' power group.

Note Creating a power group is not the same as creating a server pool. However, you can populate a server pool with members of the same power group by creating a power qualifier and adding it to server pool policy.

Creating a Power Group

Before You Begin

Make sure the global power allocation policy is set to **Policy Driven Chassis Group Cap** on the **Global Policies** tab.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, click the **Equipment** node.

Step 3 In the **Work** pane, click the **Policies** tab.

Step 4 Click the **Power Groups** subtab.

Step 5 On the icon bar to the right of the table, click +.
If the + icon is disabled, click an entry in the table to enable it.

Step 6 On the first page of the **Create Power Group** wizard, complete the following fields:

a) Enter a unique name and description for the power group.

This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

b) Click **Next**.

Step 7 On the **Add Chassis Members** page of the **Create Power Group** wizard, do the following:

a) In the **Chassis** table, choose one or more chassis to include in the power group.

b) Click the >> button to add the chassis to the **Selected Chassis** table that displays all chassis included in the power group.
You can use the << button to remove one or more chassis from the power group.

c) Click **Next**.

Step 8 On the **Power Group Attributes** page of the **Create Power Group** wizard, do the following:

a) Complete the following fields:

Name	Description
AC Power Cap field	The maximum peak power (in watts) available to the power group. Enter an integer between 0 and 10000000.
Enable Dynamic Reallocation field	This can be: • **none**—Blade allocations are not adjusted dynamically. • **chassis**—Cisco UCS monitors power usage and changes the blade allocations as required to maximize power utilization.

b) Click **Finish**.

Adding a Chassis to a Power Group

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, click the **Equipment** node.

Step 3 In the **Work** pane, click the **Power Groups** tab.

Step 4 Right-click the power group to which you want to add a chassis and choose **Add Chassis Members**.

Step 5 In the **Add Chassis Members** dialog box, do the following:

a) In the **Chassis** table, choose one or more chassis to include in the power group.

b) Click the >> button to add the chassis to the **Selected Chassis** table that displays all chassis included in the power group.
You can use the << button to remove one or more chassis from the power group.

c) Click **OK**.

Removing a Chassis from a Power Group

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, click the **Equipment** node.
Step 3 In the **Work** pane, click the **Power Groups** tab.
Step 4 Expand the power group from which you want to remove a chassis.
Step 5 Right-click the chassis that you want to remove from the power group and choose **Delete**.
Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Deleting a Power Group

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, click the **Equipment** node.
Step 3 In the **Work** pane, click the **Power Groups** tab.
Step 4 Right-click the power group that you want to delete and choose **Delete**.
Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring Power Control Policies

Power Control Policy

Cisco UCS uses the priority set in the power control policy, along with the blade type and configuration, to calculate the initial power allocation for each blade within a chassis. During normal operation, the active blades within a chassis can borrow power from idle blades within the same chassis. If all blades are active and reach the power cap, service profiles with higher priority power control policies take precedence over service profiles with lower priority power control policies.

Priority is ranked on a scale of 1-10, where 1 indicates the highest priority and 10 indicates lowest priority. The default priority is 5.

For mission-critical application a special priority called no-cap is also available. Setting the priority to no-cap prevents Cisco UCS from leveraging unused power from that particular blade server. The server is allocated the maximum amount of power that that blade can reach.

Note You must include this policy in a service profile and that service profile must be associated with a server for it to take effect.

Creating a Power Control Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **Power Control Policies** and choose **Create Power Control Policy**.

Step 5 In the **Create Power Control Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Power Capping field	What happens to a server when the demand for power within a power group exceeds the power supply. This can be: • **no-cap**—The server runs at full capacity regardless of the power requirements of the other servers in its power group. • **cap**—The server is allocated a minimum amount of power capacity based on the the server's priority relative to the other servers in its server group. If more power becomes available, Cisco UCS allows the capped servers to exceed their original allocations. It only lowers the allocations if there is a drop in the total power available to the power group.
Priority field	The priority the server has within its power group when power capping is in effect. Enter an integer between 1 and 10, where 1 is the highest priority.

Step 6 Click **OK**.

What to Do Next

Include the policy in a service profile or service profile template.

Deleting a Power Control Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.
Step 2 On the **Servers** tab, expand **Servers ➤ Policies ➤** ***Organization_Name***.
Step 3 Expand the **Power Control Policies** node.
Step 4 Right-click the policy you want to delete and select **Delete**.
Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring Manual Blade-Level Power Capping

Manual Blade-Level Power Capping

When manual blade-level power capping is configured in the global cap policy, you can set a power cap for each blade server in a Cisco UCS instance.

The following configuration options are available:

Enabled	You can specify the maximum amount of power that the server can consume at one time. This maximum can be any amount between 0 watts and 1100 watts.
Disabled	No power usage limitations are imposed upon the server. The server can use as much power as it requires.

If the server encounters a spike in power usage that meets or exceeds the maximum configured for the server, Cisco UCS Manager does not disconnect or shut down the server. Instead, Cisco UCS Manager reduces the power that is made available to the server. This reduction can slow down the server, including a reduction in CPU speed.

Setting the Blade-Level Power Cap for a Server

Before You Begin

Make sure the global power allocation policy is set to **Manual Blade Level Cap** on the **Global Policies** tab.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.
Step 3 Choose the server for which you want to set the power budget.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Power Budget** area, do the following:

a) Click the **Expand** icon to the right of the heading to display the fields.
b) Complete the following fields:

Global PoliciesName	Description
Admin Status field	Whether this server is power capped. This can be: • **Unbounded**—The server is not power capped under any circumstances. • **Enabled**—Cisco UCS Manager GUI displays the **Watts** field. **Note** Power capping only goes into effect if there is insufficient power available to the chassis to meet the demand. If there is sufficient power, the server can use as many watts as it requires.
Watts field	The maximum number of watts the server can use if there is not enough power to the chassis to meet the demand. Enter an integer between 0 and 10000000.

Step 6 Click **Save Changes**.

Viewing the Blade-Level Power Cap

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis**.
Step 3 Choose the chassis for which you want to view the server power usage.
Step 4 Do one of the following:

- To view the power usage for all servers in the chassis, click the **Power** tab in the **Work** pane.
- To view the power usage for one server in the chassis, expand the chassis and click the server. Then click the **Power** tab in the **Work** pane.

Step 5 If necessary, expand the **Motherboards** node to view the power counters.

PART VI

VN-Link Configuration

CHAPTER 30

Overview of VN-Link in Cisco UCS

This chapter includes the following sections:

Virtualization with a Virtual Interface Card Adapter

Virtual interface card (VIC) adapters support virtualized environments with VMware. These environments support the standard VMware integration with ESX installed on the server and all virtual machine management performed through the VMware vCenter.

This virtualized adapter supports the following:

- Dynamic vNICs in a virtualized environment with VM software, such as vSphere. This solution enables you to divide a single physical blade server into multiple logical PCIE instances.
- Static vNICs in a single operating system installed on a server.

With a VIC adapter, the solution you choose determines how communication works. This type of adapter supports the following communication solutions:

- Cisco VN-Link in hardware, which is a hardware-based method of handling traffic to and from a virtual machine. Details of how to configure this solution are available in this document.
- Cisco VN-Link in software, which is a software-based method of handling traffic to and from a virtual machine and uses the Nexus 1000v virtual switch. Details of how to configure this solution are available in the Nexus 1000v documentation.
- Single operating system installed on the server without virtualization, which uses the same methods of handling traffic as the other Cisco UCS adapters.

Cisco VN-Link

Cisco Virtual Network Link (VN-Link) is a set of features and capabilities that enable you to individually identify, configure, monitor, migrate, and diagnose virtual machine interfaces in a way that is consistent with the current network operation models for physical servers. VN-Link literally indicates the creation of a logical

link between a vNIC on a virtual machine and a Cisco UCS fabric interconnect. This mapping is the logical equivalent of using a cable to connect a NIC with a network port on an access-layer switch.

VN-Link in Hardware

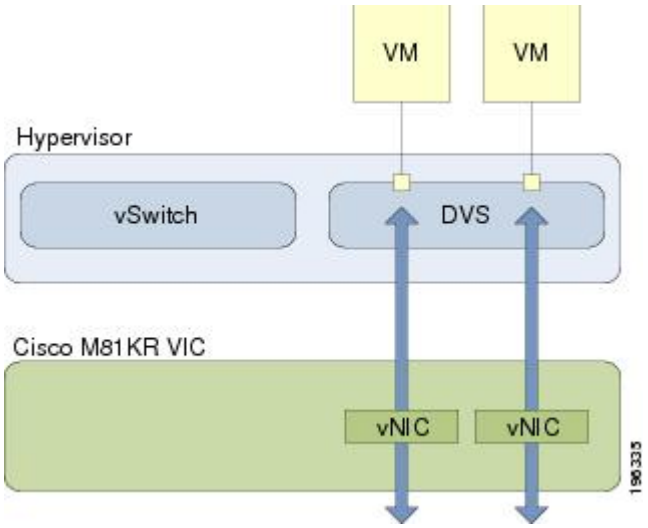
Cisco VN-Link in hardware is a hardware-based method of handling traffic to and from a virtual machine on a server with a VIC adapter. This method is sometimes referred to as pass-through switching. This solution replaces software-based switching with ASIC-based hardware switching and improves performance.

The distributed virtual switch (DVS) framework delivers VN-Link in hardware features and capabilities for virtual machines on Cisco UCS servers with VIC adapters. This approach provides an end-to-end network solution to meet the new requirements created by server virtualization.

With VN-Link in hardware, all traffic to and from a virtual machine passes through the DVS and the hypervisor. and then returns to the virtual machine on the server. Switching occurs in the fabric interconnect (hardware). As a result, network policies can be applied to traffic between virtual machines. This capability provides consistency between physical and virtual servers.

The following figure shows the traffic paths taken by VM traffic on a Cisco UCS server with a VIC adapter:

Figure 2: Traffic Paths for VM traffic with VN-Link in Hardware



Extension File for Communication with VMware vCenter

For Cisco UCS instances that use VIC adapters to implement VN-Link in hardware, you must create and install an extension file to establish the relationship and communications between Cisco UCS Manager and the VMware vCenter. This extension file is an XML file that contains vital information, including the following:

- Extension key
- Public SSL certificate

If you need to have two Cisco UCS instances share the same set of distributed virtual switches in a vCenter, you can create a custom extension key and import the same SSL certificate in the Cisco UCS Manager for each Cisco UCS instance.

Extension Key

The extension key includes the identity of the Cisco UCS instance. By default, this key has the value Cisco UCS GUID, as this value is identical across both fabric interconnects in a cluster configuration.

When you install the extension, vCenter uses the extension key to create a distributed virtual switch (DVS).

Public SSL Certificate

Cisco UCS Manager generates a default, self-signed SSL certificate to support communication with vCenter. You can also provide your own custom certificate.

Custom Extension Files

You can create a custom extension file for a Cisco UCS instance that does not use either or both of the default extension key or SSL certificate. For example, you can create the same custom key in two different Cisco UCS instances when they are managed by the same VMware vCenter instance.

Important You cannot change an extension key that is being used by a DVS or vCenter. If you want to use a custom extension key, we recommend that you create and register the custom key before you create the DVS in Cisco UCS Manager to avoid any possibility of having to delete and recreate the associated DVS.

Distributed Virtual Switches

Each VMware ESX host has its own software-based virtual switch (vSwitch) in its hypervisor that performs the switching operations between its virtual machines (VMs). The Cisco UCS distributed virtual switch (DVS) is a software-based virtual switch that runs alongside the vSwitch in the ESX hypervisor, and can be distributed across multiple ESX hosts. Unlike vSwitch, which uses its own local port configuration, a DVS associated with multiple ESX hosts uses the same port configuration across all ESX hosts.

After associating an ESX host to a DVS, you can migrate existing VMs from the vSwitch to the DVS, and you can create VMs to use the DVS instead of the vSwitch. With the hardware-based VN-Link implementation, when a VM uses the DVS, all VM traffic passes through the DVS and ASIC-based switching is performed by the fabric interconnect.

In Cisco UCS Manager, DVSes are organized in the following hierarchy:

```
vCenter
    Folder (optional)
        Datacenter
            Folder (required)
                DVS
```

At the top of the hierarchy is the vCenter, which represents a VMware vCenter instance. Each vCenter contains one or more datacenters, and optionally vCenter folders with which you can organize the datacenters. Each datacenter contains one or more required datacenter folders. Datacenter folders contain the DVSes.

Port Profiles

Port profiles contain the properties and settings used to configure virtual interfaces in Cisco UCS for VN-Link in hardware. The port profiles are created and administered in Cisco UCS Manager. There is no clear visibility into the properties of a port profile from VMware vCenter.

In VMware vCenter, a port profile is represented as a port group. Cisco UCS Manager pushes the port profile names to vCenter, which displays the names as port groups. None of the specific networking properties or settings in the port profile are visible in VMware vCenter.

After a port profile is created, assigned to, and actively used by one or more DVSes, any changes made to the networking properties of the port profile in Cisco UCS Manager are immediately applied to those DVSes.

You must configure at least one port profile client for a port profile, if you want Cisco UCS Manager to push the port profile to VMware vCenter.

Port Profile Clients

The port profile client determines the DVSes to which a port profile is applied. By default, the port profile client specifies that the associated port profile applies to all DVSes in the vCenter. However, you can configure the client to apply the port profile to all DVSes in a specific datacenter or datacenter folder, or only to one DVS.

VN-Link in Hardware Considerations

How you configure a Cisco UCS instance for VN-Link in hardware has several dependencies. The information you need to consider before you configure VN-Link in hardware includes the following:

- A Cisco UCS instance can have a maximum of 4 vCenters
- Each vCenter can have a maximum of 8 distributed virtual switches
- Each distributed virtual switch can have a maximum of 4096 ports
- Each port profile can have a maximum of 4096 ports
- Each Cisco UCS instance can have a maximum of 256 port profiles

Configuring Cisco UCS for VN-Link in Hardware

You must perform some of the following high-level steps in the VMware Virtual Center (vCenter). For more information about those steps, see the VMware documentation.

Procedure

	Command or Action	Purpose
Step 1	Configure the VN-Link components and connectivity.	For more information, see the following chapter: Configuring VN-Link Components and Connectivity, page 449.
Step 2	In VMware vCenter, create a vCenter and datacenter.	For more information, see the VMware documentation.
Step 3	In Cisco UCS Manager create distributed virtual switches.	To create a distributed virtual switch (DVS), you must first create a vCenter, a datacenter under the vCenter, and a datacenter folder under the datacenter. You can then create a DVS in the datacenter folder. The vCenter name you specify in Cisco UCS Manager does not need to match the vCenter name specified in VMware vCenter; however, the datacenter name you specify in Cisco UCS Manager must match the

	Command or Action	Purpose
		datacenter name specified in VMware vCenter. The datacenter folder and DVS you create in Cisco UCS Manager are pushed to VMware vCenter. For more information, see the following chapter: Configuring Distributed Virtual Switches in Cisco UCS, page 465.
Step 4	In Cisco UCS Manager, create the port profile and profile clients.	The port profiles are pushed to their clients in VMware vCenter. They appear in VMware vCenter as port groups, not port profiles. For more information, see the following chapter: Configuring Port Profiles, page 477.
Step 5	In VMware vCenter, add an ESX host to the DVS.	Configure the ESX host with the option to migrate to PTS/DVS.
Step 6	In vCenter, create the virtual machines required for the VMs on the server.	As part of this configuration, ensure you select the port profiles (port groups) configured in Cisco UCS Manager.

CHAPTER 31

Configuring VN-Link Components and Connectivity

This chapter includes the following sections:

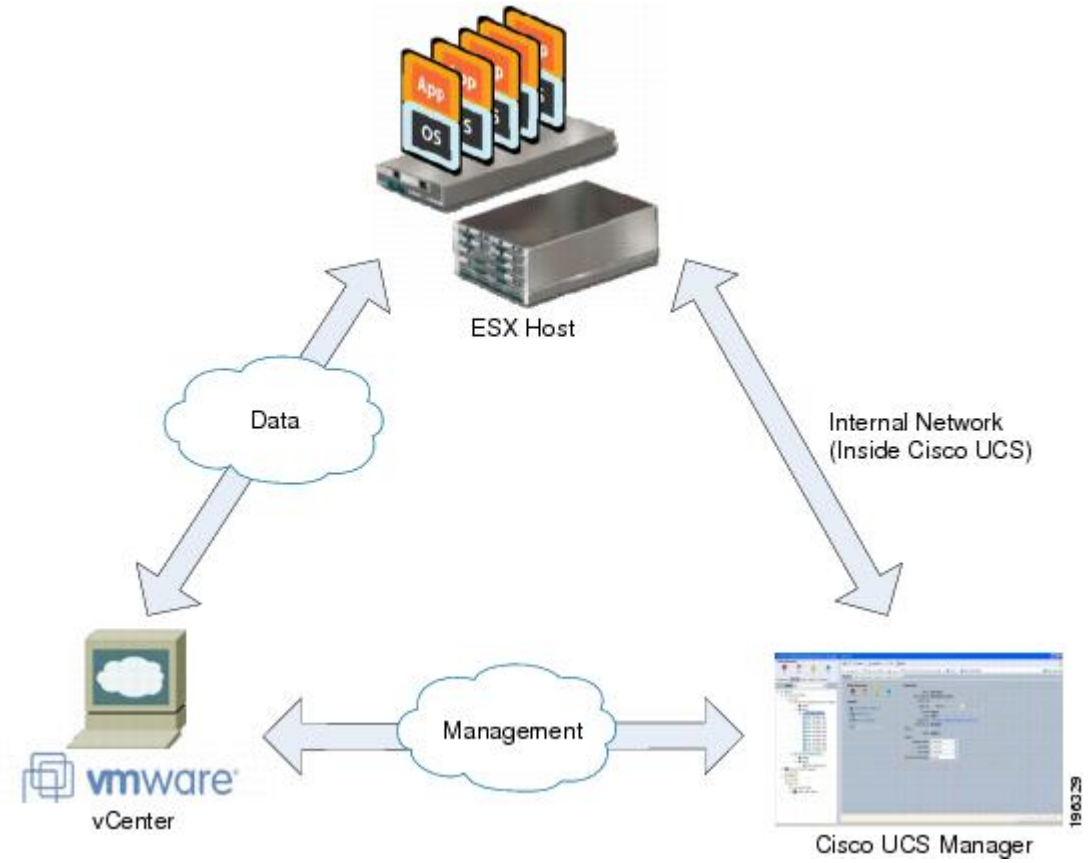
Components of VN-Link in Hardware

The following three main components must be connected for VN-Link in hardware to work:

VMware ESX Host	A server with the VMware ESX installed. It contains a datastore and the virtual machines. The ESX host must have a Cisco M81KR VIC installed, and it must have uplink data connectivity to the network for communication with VMware vCenter.
VMware vCenter	Windows-based software used to manage one or more ESX hosts. VMware vCenter must have connectivity to the UCS management port for management plane integration, and uplink data connectivity to the network for communication with the ESX Host. A vCenter extension key provided by Cisco UCS Manager must be registered with VMware vCenter before the Cisco UCS instance can be acknowledged.
Cisco UCS Manager	The Cisco UCS management software that integrates with VMware vCenter to handle some of the network-based management tasks. Cisco UCS Manager must have management port connectivity to VMware vCenter for management plane integration. It also provides a vCenter extension key that represents the Cisco UCS identity. The extension key must be registered with VMware vCenter before the Cisco UCS instance can be acknowledged.

The following figure shows the three main components of VN-Link in hardware and the methods by which they are connected:

Figure 3: Component Connectivity for VN-Link in Hardware



Configuring a VMware ESX Host for VN-Link

Before You Begin

Ensure that Virtualization Technology is enabled in BIOS of the UCS server if you intend to run 64-bit VMs on the ESX host. An ESX host will not run 64-bit VMs unless Virtualization Technology is enabled.

Procedure

Step 1 If not already present, install a Cisco M81KR VIC in the server you intend to use as the VMware ESX host. For more information about installing a Cisco M81KR VIC, see the *Cisco UCS 5108 Server Chassis Hardware Installation Guide*.

Step 2 Configure and associate a service profile to the server. The service profile configuration must include the following:

- A Dynamic vNIC Connection policy that determines how the VN-link connectivity between VMs and dynamic vNICs is configured.
- Two static vNICs for each adapter on the ESX host. For ESX hosts with multiple adapters, your service profile must use either vCons or have an associated vNIC/vHBA placement profile that ensures the static vNICs are assigned to the appropriate adapters.

For more information, see the following chapter: Configuring Service Profiles, page 363.

Step 3 Install VMware ESX 4.0 or later on the blade server. No additional drivers are required during the installation.

Configuring a VMware vCenter Instance for VN-Link

Procedure

Step 1 Configure a Window-based machine to use a static IP address. Take note of the IP address. You will use it to connect to vCenter Server.
The Windows-based machine must have network connectivity to the the Cisco UCS management port and to the uplink Ethernet port(s) being used by the ESX host. The management port connectivity is used for management plane integration between VMware vCenter and Cisco UCS Manager; the uplink Ethernet port connectivity is used for communication between VMware vCenter and the ESX host.

Step 2 Install VMware vCenter (vCenter Server and vSphere Client 4.0 or later) on the Windows-based machine.

Step 3 Launch vSphere Client.

Step 4 On the vSphere Client launch page, enter the following information to connect to vCenter Server:

a) Static IP address of the Windows-based machine.
b) Username and password specified while installing vCenter Server. If, during the vCenter Server installation, you chose to use the Windows login credentials, you can check the **Use Windows session credentials** check box.

Step 5 If a Security Warning dialog box appears, click **Ignore**.

What to Do Next

Do one of the following:

- (Optional) If you plan to use a custom certificate for VN-Link in hardware, configure the certificate for VN-Link in hardware.
- Connect Cisco UCS Manager to VMware vCenter using the extension key.

Configuring a Certificate for VN-Link in Hardware

Certificate for VN-Link in Hardware

Cisco UCS Manager generates a default, self-signed SSL certificate to support communication with vCenter. You can also create your own custom certificate to communicate with multiple vCenter instances. When you create a custom certificate, Cisco UCS Manager recreates the extension files to include the new certificate. If you subsequently delete the custom certificate, Cisco UCS Manager recreates the extension files to include the default, self-signed SSL certificate.

To create a custom certificate, you must obtain and copy an external certificate into Cisco UCS, and then create a certificate for VN-Link in hardware that uses the certificate you copied into Cisco UCS.

Copying a Certificate to the Fabric Interconnect

Before You Begin

Obtain a certificate.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **connect local-mgmt**	Enters local management mode.
Step 2	UCS-A(local-mgmt)# **copy** *from-filesystem:*[*from-path*]*filename* *to-filesystem:*[*to-path*]*filename*	Copies the certificate from its source location to its destination location. For the *from-filesystem:* argument, use one of the following syntax: • **ftp:**//*server-ip-addr* • **scp:**//*username@server-ip-addr* • **sftp:**//*username@server-ip-addr* • **tftp:**//*server-ip-addr* **:***port-num* For the *to-filesystem:* argument, use one of the following syntax: • **Volatile:** • **Workspace:**

The following example uses FTP to copy a certificate (certificate.txt) to the temp folder in the workspace:

```
UCS-A # connect local-mgmt
Cisco UCS 6100 Series Fabric Interconnect

TAC support: http://www.cisco.com/tac

Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.

The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
```

```
Some parts of this software may be covered under the GNU Public
License or the GNU Lesser General Public License. A copy of
each such license is available at
http://www.gnu.org/licenses/gpl.html and
http://www.gnu.org/licenses/lgpl.html

UCS-A(local-mgmt)# copy ftp://192.168.10.10/certs/certificate.txt
workspace:/temp/certificate.txt
UCS-A(local-mgmt)#
```

What to Do Next

Create a certificate for VN-Link in hardware.

Creating a Certificate for VN-Link in Hardware

Before You Begin

Copy a certificate to the fabric interconnect.

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.

Step 2 On the **VM** tab, expand the **All** node.

Step 3 On the **VM** tab, click **VMWare**.

Step 4 In the **Work** pane, click the **Certificates** tab.

Step 5 On the icon bar to the right of the table, click +.
If the + icon is disabled, click an entry in the table to enable it.

Step 6 In the **Create Key Ring** dialog box, complete the following fields:

Name	Description
Name field	The name of the key ring. Enter up to 510 characters.
Protocol field	This can be: • **workspace** • **volatile**
Certificate File field	The name of the certificate file associated with this key ring.
Path field	The path to the certificate file on the server.

Step 7 Click **OK**.

Deleting a Certificate for VN-Link in Hardware

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.
Step 2 On the **VM** tab, expand the **All** node.
Step 3 On the **VM** tab, click **VMWare**.
Step 4 In the **Work** pane, click the **Certificates** tab.
Step 5 In the **Key Rings** table, click the certificate you want to delete.
Step 6 Right-click the certificate you want to delete and select **Delete**.
Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Connecting Cisco UCS Manager to VMware vCenter Using the Extension Key

(Optional) Modifying the vCenter Extension Key

You can modify the vCenter extension key for the following reasons:

- To provide better system identification, you can name the vCenter extension key something more meaningful than the default ID string.
- If two Cisco UCS instances want to connect to the same VMware vCenter instance, they must use the same extension key and certificate.

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.
Step 2 On the **VM** tab, expand the **All** node.
Step 3 On the **VM** tab, click **VMWare**.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Actions** area, click **Modify Extension Key**.
Step 6 In the **Modify Extension Key** dialog box, do the following:
a) In the **Key** field, modify the key as needed.
A vCenter extension key can have a maximum length of 33 characters. These characters can be letters, numbers, or hyphens. No other characters or spaces are permitted in the extension key.
b) Click **OK**.

What to Do Next

Export the vCenter extension file or files from Cisco UCS Manager.

Exporting a vCenter Extension File from Cisco UCS Manager

Depending on the version of VMware vCenter you are using, you can either generate one extension file or a set of nine extension files.

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.

Step 2 On the **VM** tab, expand the **All** node.

Step 3 On the **VM** tab, click **VMWare**.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click one of the following links:

Option	Description
Export vCenter Extension	For vCenter version 4.0 update 1 and later.
Export Multiple vCenter Extensions	For vCenter version 4.0.

Step 6 In the **Export vCenter Extension** dialog box, do the following:

a) In the **Save Location** field, enter the path to the directory where you want to save the extension file or files.
If you do not know the path, click the **...** button and browse to the location.

b) Click **OK**.

Cisco UCS Manager generates the extension file(s) and saves them to the specified location.

What to Do Next

Register the vCenter extension file or files in VMware vCenter.

Registering a vCenter Extension File in VMware vCenter

In VMware vCenter, the vCenter extension files are called plug-ins.

Before You Begin

Export the vCenter extension file(s) from Cisco UCS Manager. Ensure that the exported vCenter extension files are saved to a location that can be reached by VMware vCenter.

Procedure

Step 1 In VMware vCenter, choose **Plug-ins ➤ Manage Plug-ins**.

Step 2 Right-click any empty space below the Available Plug-ins section of the **Plug-in Manager** dialog box and click **New Plug-in**.

Step 3 Click **Browse** and navigate to the location where the vCenter extension file(s) are saved.

Step 4 Choose a vCenter extension file and click **Open**.

Step 5 Click **Register Plug-in**.

Step 6 If the **Security Warning** dialog box appears, click **Ignore**.

Step 7 Click **OK**.
The vCenter extension file registers as an available VMware vCenter plug-in. You do not need to install the plug-in, leave it in the available state. If you are registering multiple vCenter extension files, repeat this procedure until all files are registered.

CHAPTER 32

Using the Configure VMware Integration Wizard

This chapter includes the following sections:

Configure VMware Integration Wizard

The **Configure VMware Integration** wizard provides a single access to perform the configuration steps that are specific to Cisco UCS Manager. You cannot use this wizard to complete the configuration steps that must be performed in VMware vCenter to complete the integration.

Through the **Configure VMware Integration** wizard, you can perform the following configuration steps:

1. Export the vCenter extension files to establish a connection to VMware vCenter.

   You must register the vCenter extension key as a plug-in in VMware vCenter. You cannot perform that step in the **Configure VMware Integration** wizard.

2. Define the structure for a VMware vCenter Distributed Virtual Switch (DVS), including the vCenter server, datacenter, DVS folder, and DVS.

   A DVS structure created with this wizard does not include a vCenter server folder that contains the datacenter. If you want a folder between the vCenter server and the datacenter, do not use this wizard to configure the integration with VMware vCenter.

3. Define the port profile and profile client.

4. Apply the configuration to VMware vCenter.

When you have completed the integration steps through the wizard, you must log in to VMware vCenter and associate the VMs and port profiles with the DVS. The port profiles are shown as port groups in VMware vCenter.

Configuring the VMware Integration with the Wizard

If you prefer not to use this wizard, you can perform each of these steps individually.

Before You Begin

Before you use the **Configure VMware Integration** wizard, complete the following:

- Configure the VMware ESX host for VN-Link.
- Configure a VMware vCenter Instance for VN-Link
- Configure a certificate for VN-Link in Hardware

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.
Step 2 On the **VM** tab, expand the **All** node.
Step 3 In the **Work** pane, click the **General** tab.
Step 4 In the **Actions** area, click **Configure VMware Integration**.
Step 5 In the **Configure VMware Integration** wizard, complete the following:

- Page 1: Establishing the Connection to vCenter Server, page 458
- Page 2: Defining a VMware vCenter Distributed Virtual Switch, page 459
- Page 3: Defining a Port Profile, page 461
- Page 4: Applying Port Profiles and Configuration to vCenter Server, page 463

Page 1: Establishing the Connection to vCenter Server

This procedure directly follows the steps in Configuring the VMware Integration with the Wizard, page 457. It describes how to establish a connection to VMware vCenter through the **Configure VMware Integration** wizard.

You can skip this page and move onto the next page if you have already exported and registered the vCenter extension key files.

Before You Begin

If you want to use a custom extension key, you must modify the extension key before performing this step as described in (Optional) Modifying the vCenter Extension Key, page 454.

Procedure

Step 1 To export the vCenter extension files, click one of the following:

Option	Description
Export	For VMware vCenter version 4.0 update 1 and later. Exports a single vCenter Extension Key file.

Option	Description
Export Multiple	For VMware vCenter version 4.0. Exports nine vCenter Extension Key files.

Step 2 In the **Export vCenter Extension** dialog box, do the following:

a) In the **Save Location** field, enter the path to the directory where you want to save the extension file or files.
If you do not know the path, click the **...** button and browse to the location.

b) Click **OK**.

Cisco UCS Manager generates the extension file(s) and saves them to the specified location.

Step 3 Copy the downloaded file to a location on the VMware vCenter.

Step 4 Register the vCenter extension file(s) in VMware vCenter.
For more information, see Registering a vCenter Extension File in VMware vCenter, page 455, and the instructions on this page in the **Configure VMware Integration** wizard.

Step 5 Click **Next**.

What to Do Next

Complete the steps in Page 2: Defining a VMware vCenter Distributed Virtual Switch, page 459.

Page 2: Defining a VMware vCenter Distributed Virtual Switch

This procedure directly follows the steps in Page 1: Establishing the Connection to vCenter Server, page 458. It describes how to define the components of a distributed virtual switch in VMware vCenter through the **Configure VMware Integration** wizard.

Procedure

Step 1 In the **vCenter Server** area, complete the following fields to define the connection to VMware vCenter:

Name	Description
vCenter Server Name field	The user-defined name for the vCenter server. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	The description of the vCenter server. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
vCenter Server Hostname or IP Address field	The hostname or IP address of the vCenter server.

Name	Description
	Note If you use a hostname rather than an IP address, you must configure a DNS server in Cisco UCS Manager.

Step 2 In the **Datacenter** area, complete the following fields to create the datacenter in VMware vCenter:

Name	Description
vCenter Datacenter Name field	The name of the vCenter Datacenter. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	The user-defined description of the Datacenter. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).

Step 3 In the **DVS Folder** area, complete the following fields to create a folder to contain the distributed virtual switch in VMware vCenter:

Name	Description
Folder Name field	The name of the folder that contains the distributed virtual switch (DVS). This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	The user-defined description of the folder. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).

Step 4 In the **DVS** area, complete the following fields to create the distributed virtual switch in VMware vCenter:

Name	Description
DVS Name field	The name of the DVS. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	The user-defined description of the DVS. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
DVS field	This can be:

Name	Description
	• **disable** • **enable** If you disable the DVS, Cisco UCS Manager does not push any configuration changes related to the DVS to VMware vCenter.

b

Step 5 Click **Next**.

What to Do Next

Complete the steps in Page 3: Defining a Port Profile, page 461.

Page 3: Defining a Port Profile

This procedure directly follows the steps in Page 2: Defining a VMware vCenter Distributed Virtual Switch, page 459. It describes how to define the components of a distributed virtual switch in VMware vCenter through the **Configure VMware Integration** wizard.

Procedure

Step 1 In the **Port Profile** area, complete the following fields to define the port profile:

Name	Description
Name field	The user-defined name for the port profile. This name can be between 1 and 31 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	The user-defined description for the port profile. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
QoS Policy drop-down list	The quality of service policy associated with this port profile.
Network Control Policy drop-down list	The network control policy associated with this port profile.
Max Ports field	The maximum number of ports that can be associated with this port profile. The default is 64 ports. The maximum number of ports that can be associated with a single distributed virtual switch (DVS) is 4096. If the DVS has only one associated port profile, that port profile can be configured with up to

Name	Description
	4096 ports. However, if the DVS has more than one associated port profile, the total number of ports associated with all of those port profiles combined cannot exceed 4096.
Host Network IO Performance field	This can be: • **None** • **High Performance**
Pin Group drop-down list	The pin group associated with this port profile.

Step 2 In the **VLANs** area, do the following to assign one or more VLANs to the port profile:

a) In the **Select** column, check the check box in the appropriate row for each VLAN you want to use in the port profile.

b) In the **Native VLAN** column, click the radio button in the appropriate row for the VLAN you want to designate as the native VLAN.

Step 3 In the **Client Profile** area, do the following to create a profile client for the port profile:

Name	Description
Name field	The user-defined name for the profile client. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	The user-defined description of the client. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Datacenter drop-down list	Select a Datacenter from the drop-down list or select **All** if this profile client applies to all Datacenters.
Folder drop-down list	Select a folder from the drop-down list or select **All** if this profile client applies to all folders.
Distributed Virtual Switch drop-down list	Select a virtual switch from the drop-down list or select **All** if this profile client applies to all virtual switches.

Step 4 Click **Next**.

What to Do Next

Complete the configuration of the virtual machines in VMware vCenter.

Page 4: Applying Port Profiles and Configuration to vCenter Server

This procedure directly follows the steps in Page 3: Defining a Port Profile, page 461. It describes how to apply the port profiles to vCenter Server through the **Configure VMware Integration** wizard.

Procedure

Step 1 Review the text on the page in the **Configure VMware Integration** wizard.

Step 2 Click **Finish**.
Cisco UCS Manager connects to the vCenter Server, creates the specified DVS, and applies the port profiles.

What to Do Next

In VMware vCenter, associate the VMs and port profiles with the DVS. The port profiles are shown as port groups in VMware vCenter.

CHAPTER 33

Configuring Distributed Virtual Switches in Cisco UCS

This chapter includes the following sections:

Distributed Virtual Switches

Each VMware ESX host has its own software-based virtual switch (vSwitch) in its hypervisor that performs the switching operations between its virtual machines (VMs). The Cisco UCS distributed virtual switch (DVS) is a software-based virtual switch that runs alongside the vSwitch in the ESX hypervisor, and can be distributed across multiple ESX hosts. Unlike vSwitch, which uses its own local port configuration, a DVS associated with multiple ESX hosts uses the same port configuration across all ESX hosts.

After associating an ESX host to a DVS, you can migrate existing VMs from the vSwitch to the DVS, and you can create VMs to use the DVS instead of the vSwitch. With the hardware-based VN-Link implementation, when a VM uses the DVS, all VM traffic passes through the DVS and ASIC-based switching is performed by the fabric interconnect.

In Cisco UCS Manager, DVSes are organized in the following hierarchy:

```
vCenter
    Folder (optional)
        Datacenter
            Folder (required)
                DVS
```

At the top of the hierarchy is the vCenter, which represents a VMware vCenter instance. Each vCenter contains one or more datacenters, and optionally vCenter folders with which you can organize the datacenters. Each datacenter contains one or more required datacenter folders. Datacenter folders contain the DVSes.

Configuring a Distributed Virtual Switch

Before You Begin

You must first create a datacenter in VMware vCenter. Do not create the folder inside the datacenter or the DVS in VMware vCenter.

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.

Step 2 On the **VM** tab, expand the **All** node.

Step 3 Right-click the **VMWare** node and choose **Configure vCenter**.

Step 4 On the **Configure vCenter** page, do the following:

a) Complete the following fields:

Name	Description
Name field	The user-defined name for the VMware Virtual Center (vCenter). This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	The user-defined description of VMware vCenter. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Hostname field	The hostname or IP address of the machine that hosts VMware vCenter. **Note** If you use a hostname rather than an IP address, you must configure a DNS server in Cisco UCS Manager.

b) Click **Next**.

Step 5 On the **Create Folder** page, click one of the following:

Option	Description
Next	Moves to the next page. Choose this option if the vCenter structure does not require you to include the datacenter in a high-level folder. If you choose this option, continue with Step 7.
Add	Opens the **Create Folder** dialog box, where you can add a high-level folder above the datacenter. If you choose this option, continue with Step 6.

Step 6 (Optional) In the **Create Folder** dialog box, do the following:

a) Complete the following fields:

Name	Description
Name field	The name of the vCenter folder. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A user-defined description of the folder. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).

b) Click **Next**.

Step 7 On the **Create Datacenter** page, do the following:

a) Click **Add**.

b) In the **Create Datacenter** dialog box, complete the following fields:

Name	Description
Name field	The name of the Datacenter. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved. The datacenter name that you specify in Cisco UCS Manager must exactly match the name of the datacenter previously created in VMware vCenter.
Description field	The user-defined description of the Datacenter. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).

c) Click **Next**.

Step 8 In the **Create Folder** page, do the following to create a folder in the datacenter:

a) Click **Add**.

b) In the **Create Folder** dialog box, complete the following fields:

Name	Description
Name field	The name of the vCenter folder. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A user-defined description of the folder.

Name	Description
	Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).

c) Click **Next**.

Step 9 On the **Create Distributed Virtual Switches** page, do the following to create a distributed virtual switch in the folder:

a) Click **Add** to add a distributed virtual switch to the folder.

b) In the **Create Distributed Virtual Switches** dialog box, complete the following fields:

Name	Description
Name field	The name of the distributed virtual switch. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	The user-defined description of the distributed virtual switch. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Admin State field	This can be: • **enabled** • **disabled** If you disable the DVS, Cisco UCS Manager does not push any configuration changes related to the DVS to VMware vCenter.

c) Click **OK**

Step 10 Click **Finish** if you have finished adding all datacenters, folders, and DVSes to the vCenter.
You may need to click **Finish** more than once to exit the wizard. You can stop at any page to add another datacenter, folder, or DVS.

Managing Distributed Virtual Switches

Adding a Folder to a vCenter

You can add a folder inside a vCenter and place your datacenters inside the folder. However, this folder is optional.

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.

Step 2 On the **VM** tab, expand the **VMWare** node.

Step 3 Right-click the vCenter to which you want to add a datacenter and choose **Create Folder**.

Step 4 (Optional) In the **Create Folder** dialog box, do the following:

a) Complete the following fields:

Name	Description
Name field	The name of the vCenter folder. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A user-defined description of the folder. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).

b) Click **Next**.

Step 5 On the **Create Datacenter** page, do the following:

a) Click **Add**.

b) In the **Create Datacenter** dialog box, complete the following fields:

Name	Description
Name field	The name of the Datacenter. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved. The datacenter name that you specify in Cisco UCS Manager must exactly match the name of the datacenter previously created in VMware vCenter.
Description field	The user-defined description of the Datacenter. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).

c) Click **Next**.

Step 6 In the **Create Folder** page, do the following to create a folder in the datacenter:

a) Click **Add**.

b) In the **Create Folder** dialog box, complete the following fields:

Name	Description
Name field	The name of the vCenter folder. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A user-defined description of the folder. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).

c) Click **Next**.

Step 7 On the **Create Distributed Virtual Switches** page, do the following to create a distributed virtual switch in the folder:

a) Click **Add** to add a distributed virtual switch to the folder.

b) In the **Create Distributed Virtual Switches** dialog box, complete the following fields:

Name	Description
Name field	The name of the distributed virtual switch. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	The user-defined description of the distributed virtual switch. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Admin State field	This can be: • **enabled** • **disabled** If you disable the DVS, Cisco UCS Manager does not push any configuration changes related to the DVS to VMware vCenter.

c) Click **OK**

Step 8 Click **Finish** if you have finished adding all fdatacenters, folders, and DVSes to the folder.
You may need to click **Finish** more than once to exit the wizard. You can stop at any page to add another datacenter, folder, or DVS.

Adding a Datacenter to a vCenter

Before You Begin

You must first create a datacenter in VMware vCenter. Do not create the folder inside the datacenter or the DVS in VMware vCenter.

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.

Step 2 On the **VM** tab, expand the **VMWare** node.

Step 3 Right-click the vCenter to which you want to add a datacenter and choose **Create Datacenter**.

Step 4 On the **Create Datacenter** page, do the following:

a) Click **Add**.

b) In the **Create Datacenter** dialog box, complete the following fields:

Name	Description
Name field	The name of the Datacenter. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved. The datacenter name that you specify in Cisco UCS Manager must exactly match the name of the datacenter previously created in VMware vCenter.
Description field	The user-defined description of the Datacenter. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).

c) Click **Next**.

Step 5 In the **Create Folder** page, do the following to create a folder in the datacenter:

a) Click **Add**.

b) In the **Create Folder** dialog box, complete the following fields:

Name	Description
Name field	The name of the vCenter folder. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A user-defined description of the folder. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).

c) Click **Next**.

Step 6 On the **Create Distributed Virtual Switches** page, do the following to create a distributed virtual switch in the folder:

a) Click **Add** to add a distributed virtual switch to the folder.

b) In the **Create Distributed Virtual Switches** dialog box, complete the following fields:

Name	Description
Name field	The name of the distributed virtual switch. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	The user-defined description of the distributed virtual switch. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Admin State field	This can be: • **enabled** • **disabled** If you disable the DVS, Cisco UCS Manager does not push any configuration changes related to the DVS to VMware vCenter.

c) Click **OK**

Step 7 Click **Finish** if you have finished adding all folders and distributed virtual switches to the Datacenter. You may need to click **Finish** more than once to exit the wizard. You can stop at any page to add another folder or DVS to the datacenter.

Adding a Folder to a Datacenter

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.

Step 2 On the **VM** tab, expand the **VMWare** node.

Step 3 Expand the vCenter that includes the datacenter to which you want to add a folder.

Step 4 Right-click the datacenter to which you want to add a folder and choose **Create Folder**.

Step 5 In the **Create Folder** page, do the following to add a folder to the datacenter:

a) Complete the following fields:

Name	Description
Name field	The name of the vCenter folder. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A user-defined description of the folder. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).

b) • Click **Next** to create a DVS in the folder and continue with Step 6.
• Continue with Step 7 if you do not want to create a DVS in the folder.

Step 6 On the **Create Distributed Virtual Switches** page, do the following to create a distributed virtual switch in the folder:

a) Click **Add** to add a distributed virtual switch to the folder.

b) In the **Create Distributed Virtual Switches** dialog box, complete the following fields:

Name	Description
Name field	The name of the distributed virtual switch. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	The user-defined description of the distributed virtual switch. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Admin State field	This can be: • **enabled** • **disabled** If you disable the DVS, Cisco UCS Manager does not push any configuration changes related to the DVS to VMware vCenter.

c) Click **OK**

Step 7 Click **Finish** if you have finished adding all folders and DVSes to the datacenter.
You may need to click **Finish** more than once to exit the wizard. You can stop at any page to add another folder or DVS.

Deleting a Folder from a vCenter

If the folder contains a datacenter, Cisco UCS Manager also deletes that datacenter and any folders and DVSes it contains.

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.
Step 2 On the **VM** tab, expand **All ➤ VMWare** .
Step 3 Expand the node for the vcenter that contains the folder you want to delete.
Step 4 Right-click the folder and choose **Delete**.
Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Deleting a Datacenter

If the datacenter contains a folder, Cisco UCS Manager also deletes that folder and any DVS it contains.

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.
Step 2 On the **VM** tab, expand **All ➤ VMWare** .
Step 3 If the datacenter that you want to delete is contained in a higher level folder, expand the node for that folder.
Step 4 Right-click the datacenter and choose **Delete**.
Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Deleting a Folder from a Datacenter

If the folder contains a DVS, Cisco UCS Manager also deletes that DVS.

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.
Step 2 On the **VM** tab, expand **All ➤ VMWare** .
Step 3 If the datacenter that you want to modify is contained in a higher level folder, expand the node for that folder.
Step 4 Expand the node for the datacenter which contains the folder you want to delete.
Step 5 Right-click the folder and choose **Delete**.
Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Deleting a Distributed Virtual Switch from a Folder

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.

Step 2 On the **VM** tab, expand **All ➤ VMWare** .

Step 3 If the datacenter that you want to modify is contained in a higher level folder, expand the node for that folder.

Step 4 Expand the node for the datacenter and the folder which contains the DVS you want to delete.

Step 5 Right-click the DVS and choose **Delete**.

Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

CHAPTER 34

Configuring Port Profiles

This chapter includes the following sections:

Port Profiles

Port profiles contain the properties and settings used to configure virtual interfaces in Cisco UCS for VN-Link in hardware. The port profiles are created and administered in Cisco UCS Manager. There is no clear visibility into the properties of a port profile from VMware vCenter.

In VMware vCenter, a port profile is represented as a port group. Cisco UCS Manager pushes the port profile names to vCenter, which displays the names as port groups. None of the specific networking properties or settings in the port profile are visible in VMware vCenter.

After a port profile is created, assigned to, and actively used by one or more DVSes, any changes made to the networking properties of the port profile in Cisco UCS Manager are immediately applied to those DVSes.

You must configure at least one port profile client for a port profile, if you want Cisco UCS Manager to push the port profile to VMware vCenter.

Port Profile Clients

The port profile client determines the DVSes to which a port profile is applied. By default, the port profile client specifies that the associated port profile applies to all DVSes in the vCenter. However, you can configure the client to apply the port profile to all DVSes in a specific datacenter or datacenter folder, or only to one DVS.

Creating a Port Profile

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.

Step 2 On the **VM** tab, expand **All ➤ VMWare** .

Step 3 Right-click the **Port Profiles** node and choose **Create Port Profile**.

Step 4 In the **Create Port Profile** dialog box, complete the following fields:

Name	Description
Name field	The user-defined name for the port profile. This name can be between 1 and 31 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	The user-defined description for the port profile. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
QoS Policy drop-down list	The quality of service policy associated with this port profile.
Network Control Policy drop-down list	The network control policy associated with this port profile.
Max Ports field	The maximum number of ports that can be associated with this port profile. The default is 64 ports. The maximum number of ports that can be associated with a single distributed virtual switch (DVS) is 4096. If the DVS has only one associated port profile, that port profile can be configured with up to 4096 ports. However, if the DVS has more than one associated port profile, the total number of ports associated with all of those port profiles combined cannot exceed 4096.
Host Network IO Performance field	This can be: • **None** • **High Performance**

Name	Description
Pin Group drop-down list	The pin group associated with this port profile.

Step 5 In the **VLANs** area, complete the following fields:

Name	Description
Select column	Check the check box in this column for each VLAN you want to use.
Name column	The name of the VLAN.
Native VLAN column	To designate one of the VLANs as the native VLAN, click the radio button in this column.

Step 6 Click **Finish**.

Modifying the VLANs in a Port Profile

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.

Step 2 On the **VM** tab, expand **All ➤ VMWare ➤ Port Profiles**.

Step 3 Right-click the port profile for which you want to modify the VLANs and choose **Modify VLANs**.

Step 4 In the **Modify VLANs** dialog box, change one or more of the following:

Name	Description
Select column	Check the check box in this column for each VLAN you want to use.
Name column	The name of the VLAN.
Native VLAN column	To designate one of the VLANs as the native VLAN, click the radio button in this column.
Create VLAN link	Click this link if you want to create a VLAN.

Step 5 Click **OK**.

Changing the Native VLAN for a Port Profile

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.

Step 2 On the **VM** tab, expand **All ➤ VMWare ➤ Port Profiles**.

Step 3 Right-click the port profile for which you want to change the native VLAN and choose **Modify VLANs**.

Step 4 In the **Modify VLANs** dialog box, do the following:

a) In the **Native VLAN** column, click the radio button in the row for the VLAN that you want to become the native VLAN.

b) Click **OK**.

Adding a VLAN to a Port Profile

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.

Step 2 On the **VM** tab, expand **All ➤ VMWare ➤ Port Profiles**.

Step 3 Right-click the port profile to which you want to add a VLAN and choose **Modify VLANs**.

Step 4 In the **Modify VLANs** dialog box, do the following:

a) In the **Select** column, check the check box in the row for the VLAN that you want to add to the port profile.

b) (Optional) If you want this VLAN to be the native VLAN, click the radio button in the **Native VLAN** column.

c) Click **OK**.

Removing a VLAN from a Port Profile

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.

Step 2 On the **VM** tab, expand **All ➤ VMWare ➤ Port Profiles**.

Step 3 Right-click the port profile from which you want to remove a VLAN and choose **Modify VLANs**.

Step 4 In the **Modify VLANs** dialog box, do the following:

a) In the **Select** column, uncheck the check box in the row for the VLAN that you want to remove from the port profile.

b) (Optional) If the VLAN was the native VLAN, click the radio button in the **Native VLAN** column for a different VLAN assocated with the port profile to make that the native VLAN.
c) Click **OK**.

Deleting a Port Profile

You cannot delete a port profile if a VM is actively using that port profile.

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.
Step 2 On the **VM** tab, expand **All ➤ VMWare ➤ Port Profiles**.
Step 3 Right-click the port profile you want to delete and choose **Delete**.
Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
Step 5 Click **OK**.
Cisco UCS Manager deletes the port profile and all associated port profile clients.

Creating a Profile Client

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.
Step 2 On the **VM** tab, expand **All ➤ VMWare ➤ Port Profiles**.
Step 3 Right-click the port profile for which you want to create a profile client and choose **Create Profile Client**.
Step 4 In the **Create Profile Client** dialog box, complete the following fields:

Name	Description
Name field	The user-defined name for the profile client. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	The user-defined description of the client. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Datacenter drop-down list	Select a Datacenter from the drop-down list or select **All** if this profile client applies to all Datacenters.

Name	Description
Folder drop-down list	Select a folder from the drop-down list or select **All** if this profile client applies to all folders.
Distributed Virtual Switch drop-down list	Select a virtual switch from the drop-down list or select **All** if this profile client applies to all virtual switches.

Step 5 Click **OK**.

What to Do Next

Complete the configuration of the virtual machines in VMware vCenter.

Modifying a Profile Client

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.

Step 2 On the **VM** tab, expand **All ➤ VMWare ➤ Port Profiles**.

Step 3 Click the port profile for which you want to modify the profile client.

Step 4 In the **Work** pane, click the **Profile Clients** tab.

Step 5 Right-click the profile client you want to modify and choose **Show Navigator**.

Step 6 In the Navigator for the profile client, change the values for one or more of the following fields:

Name	Description
Name field	The user-defined name for the profile client.
Description field	The user-defined description of the client.
Datacenter field	A regular expression used to select the appropriate Datacenter.
Folder field	A regular expression used to select the appropriate Datacenter folder.
Distributed Virtual Switch field	A regular expression used to select the appropriate virtual switch.

Step 7 Click **OK**.

Deleting a Profile Client

You cannot delete a port profile client if a VM is actively using the port profile with which the client is associated.

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.

Step 2 On the **VM** tab, expand **All ➤ VMWare ➤ Port Profiles**.

Step 3 Click the port profile from which you want to delete a profile client.

Step 4 In the **Work** pane, click the **Profile Clients** tab.

Step 5 Right-click the profile client you want to delete and choose **Delete**.

Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 7 Click **Save Changes**.

CHAPTER 35

Configuring VN-Link Related Policies

This chapter includes the following sections:

Configuring Dynamic vNIC Connection Policies

Dynamic vNIC Connection Policy

This policy determines how the VN-link connectivity between VMs and dynamic vNICs is configured. This policy is required for Cisco UCS instances that include servers with virtual interface card adapters on which you have installed VMs and configured dynamic vNICs.

Note If you Vmotion a server that is configured with dynamic vNICs, the dynamic interface used by the vNICs fails and Cisco UCS Manager raises a fault to notify you of that failure.

When the server comes back up, Cisco UCS Manager assigns new dynamic vNICs to the server. If you are monitoring traffic on the dynamic vNIC, you must reconfigure the monitoring source.

Each Dynamic vNIC connection policy must include an adapter policy and designate the number of vNICs that can be configured for any server associated with a service profile that includes the policy.

Creating a Dynamic vNIC Connection Policy

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the **Dynamic vNIC Connection Policies** node and select **Create Dynamic vNIC Connection Policy**.

Step 5 In the **Create Dynamic vNIC Connection Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Number of Dynamic vNICs field	The number of dynamic vNICs that this policy affects.
Adapter Policy drop-down list	The adapter profile associated with this policy. The profile must already exist to be included in the drop-down list.
Protection field	vNICs are always protected in Cisco UCS, but this field allows you to to select a prefered fabric, if any. You can choose: • **protected-pref-a**—Cisco UCS attempts to use fabric A, but will fail over to fabric B if necessary • **protected-pref-b**—Cisco UCS attempts to use fabric B, but will fail over to fabric A if necessary • **protected**—Cisco UCS uses whichever fabic is available

Step 6 Click **OK**.

Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Changing a Dynamic vNIC Connection Policy

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN ➤ Policies**.

Step 3 Expand the node for the organization that contains the policy you want to change.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Expand the **Dynamic vNIC Connection Policies** node and click the policy that you want to change.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 Change one or more of the following fields:

Name	Description
Description field	A description of the policy. We recommend including information about where and when the policy should be used.
Number of Dynamic vNICs field	The number of dynamic vNICs that this policy affects.
Adapter Policy drop-down list	The adapter profile associated with this policy. The profile must already exist to be included in the drop-down list.

You cannot change the other properties of the policy, such as the **Name** field.

Step 7 Click **Save Changes**.

Step 8 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Deleting a Dynamic vNIC Connection Policy

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN ➤ Policies ➤** ***Organization_Name***.

Step 3 Expand the **Dynamic vNIC Connection Policies** node.

Step 4 Right-click the policy you want to delete and select **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring the VM Lifecycle Policy

VM Lifecycle Policy

The VM lifecycle policy determines how long Cisco UCS Manager retains offline VMs and offline dynamic vNICs in its database. If a VM or dynamic vNIC remains offline after that period, Cisco UCS Manager deletes the object from its database.

All virtual machines (VMs) on Cisco UCS servers are managed by vCenter. Cisco UCS Manager cannot determine whether an inactive VM is temporarily shutdown, has been deleted, or is in some other state that renders it inaccessible. Therefore, Cisco UCS Manager considers all inactive VMs to be in an offline state.

Cisco UCS Manager considers a dynamic vNIC to be offline when the associated VM is shutdown, or the link between the fabric interconnect and the I/O module fails. On rare occasions, an internal error can also cause Cisco UCS Manager to consider a dynamic vNIC to be offline.

The default VM and dynamic vNIC retention period is 15 minutes. You can set that for any period of time between 1 minute and 7200 minutes (or 5 days).

Note The VMs that Cisco UCS Manager displays are for information and monitoring only. You cannot manage VMs through Cisco UCS Manager. Therefore, when you delete a VM from the Cisco UCS Manager database, you do not delete the VM from the server or from vCenter.

Configuring the VM Lifecycle Policy

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.

Step 2 On the **VM** tab, expand the **All** node.

Step 3 On the **VM** tab, click **VMWare**.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Lifecycle Policy** area, complete the following fields:

Name	Description
VM Retention field	The period of time, in minutes, that Cisco UCS Manager retains an offline VM in its database. If a VM remains offline after that period, Cisco UCS Manager deletes the VM from its database. The default VM retention period is 15 minutes. You can configure this for any period of time between 1 minute and 7200 minutes (or 5 days).
vNIC Retention field	The period of time, in minutes, that Cisco UCS Manager retains an offline dynamic vNIC in its database. If a dynamic vNIC remains offline after that period, Cisco UCS Manager deletes the dynamic vNIC from its database. The default vNIC retention period is 15 minutes. You can configure this for any period of time between 1 minute and 7200 minutes (or 5 days).

Step 6 Click **Save Changes**.

Viewing Dynamic vNIC Properties in a VM

Before You Begin

The VM must be running.

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.

Step 2 On the **VM** tab, expand **All ➤ VMWare** .

Step 3 Expand **Virtual Machines**.

Step 4 Expand the virtual machine that contains the dynamic vNIC.

Step 5 Choose the dynamic vNIC.

Step 6 In the **Work** pane, click the **General** tab.
In the **Properties** area, the vNIC properties appear.

CHAPTER 36

Managing Pending Deletions

This chapter includes the following sections:

Pending Deletions for VN-Link Tasks

When you delete a DVS from Cisco UCS Manager, either explicitly or by deleting any parent object in the hierarchy, Cisco UCS Manager initiates a connection with VMware vCenter to start the process of deleting the DVS. Until the DVS is successfully deleted from VMware vCenter, Cisco UCS Manager places the DVS in a pending deletion list.

However, Cisco UCS Manager cannot successfully delete a DVS from VMware vCenter if certain situations occur, including the following:

- VMware vCenter database was corrupted
- VMware vCenter was uninstalled
- The IP address for VMware vCenter was changed

If the DVS cannot be successfully deleted from VMware vCenter, the DVS remains in the pending deletion list until the pending deletion is deleted in Cisco UCS Manager or the properties for that pending deletion are changed in a way that allows the DVS to be successfully deleted from VMware vCenter. When you delete a pending deletion, the DVS is deleted from Cisco UCS Manager but is not deleted from VMware vCenter. If the DVS remains in VMware vCenter, you must delete the DVS manually.

You can view the pending deletion list, delete a pending deletion, or change the properties for a pending deletion in Cisco UCS Manager. For example, you can correct the VMware vCenter IP address for a pending deletion so that Cisco UCS Manager can successfully initiate a connection and delete the DVS from VMware vCenter. You cannot cancel the deletion of a DVS from Cisco UCS Manager.

Viewing Pending Deletions

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.

Step 2 On the **VM** tab, expand the **All** node.

Step 3 On the **VM** tab, click **VMWare**.

Step 4 In the **Work** pane, click the **Deletion Tasks** tab.

Changing the Properties of a Pending Deletion

You can change the properties of a pending deletion, if necessary, to ensure that Cisco UCS Manager can successfully initiate a connection and delete the DVS from VMware vCenter.

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.

Step 2 On the **VM** tab, expand the **All** node.

Step 3 On the **VM** tab, click **VMWare**.

Step 4 In the **Work** pane, click the **Deletion Tasks** tab.

Step 5 Click the pending deletion for which you want to change the properties.

Step 6 Right-click the pending deletion and choose **Show Navigator**.

Step 7 In the **Properties** dialog box, change one or more of the following properties to ensure that Cisco UCS Manager can connect to VMware vCenter:

Name	Description
Hostname field	The host on which the Datacenter resides.
Datacenter field	The name of the Datacenter.
Protocol field	The Datacenter protocol.
Folder field	The folder that is to be deleted.

Step 8 Click **OK**.
Cisco UCS Manager attempts to connect with VMware vCenter and delete the DVS.

Deleting a Pending Deletion

When you delete a pending deletion, the DVS is deleted from Cisco UCS Manager but is not deleted from VMware vCenter. If the DVS remains in VMware vCenter, you must delete the DVS manually.

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.

Step 2 On the **VM** tab, expand the **All** node.

Step 3 On the **VM** tab, click **VMWare**.

Step 4 In the **Work** pane, click the **Deletion Tasks** tab.

Step 5 Click the pending deletion that you want to delete.

Step 6 Right-click the pending deletion and select **Delete**.

Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

PART VII

System Management

CHAPTER 37

Managing Time Zones

This chapter includes the following sections:

Time Zones

Cisco UCS requires an instance-specific time zone setting and an NTP server to ensure the correct time display in Cisco UCS Manager. If you do not configure both of these settings in a Cisco UCS instance, the time does not display correctly.

Setting the Time Zone

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 In the **Admin** tab, expand **All**.
Step 3 Click **Timezone Management**.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 From the **Timezone** drop-down list, select the time zone you want to use for the Cisco UCS instance.
Step 6 Click **Save Changes**.

Adding an NTP Server

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All**.

Step 3 Click **Timezone Management**.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **NTP Servers** area, click the + button on the table icon bar.

Step 6 In the **Add NTP Server** dialog box, do the following:

a) In the **NTP Server** field, enter the IP address or hostname of the NTP server you want to use for this Cisco UCS instance.

b) Click **OK**.

Deleting an NTP Server

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All**.

Step 3 Click **Timezone Management**.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **NTP Servers** area, right-click the server you want to delete and select **Delete**.

Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 7 Click **Save Changes**.

CHAPTER 38

Managing the Chassis

This chapter includes the following sections:

Chassis Management in Cisco UCS Manager GUI

You can manage and monitor all chassis in a Cisco UCS instance through Cisco UCS Manager GUI.

Acknowledging a Chassis

Perform the following procedure if you increase or decrease the number of links that connect the chassis to the fabric interconnect. Acknowledging the chassis ensures that Cisco UCS Manager is aware of the change in the number of links and that traffics flows along all available links.

After you enable or disable a port on a fabric interconnect, wait for at least 1 minute before you reacknowledge the chassis. If you reacknowledge the chassis too soon, the pinning of server traffic from the chassis may not be updated with the changes to the port that you enabled or disabled.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis**.

Step 3 Choose the chassis that you want to acknowledge.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Acknowledge Chassis**.

Step 6 If Cisco UCS Manager displays a confirmation dialog box, click **Yes**.
Cisco UCS Manager disconnects the chassis and then rebuilds the connections between the chassis and the fabric interconnect or fabric interconnects in the system.

Removing a Chassis

Before You Begin

Physically remove the chassis before performing the following procedure.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis**.

Step 3 Choose the chassis that you want to remove.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Remove Chassis**.

Step 6 If Cisco UCS Manager displays a confirmation dialog box, click **Yes**.
The removal may take several minutes to complete.

Decommissioning a Chassis

This procedure decommissions the chassis and deletes it from the Cisco UCS configuration. The chassis hardware physically remains in the Cisco UCS instance. However, Cisco UCS ignores it and does not list it with the other commissioned chassis.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis**.

Step 3 Choose the chassis that you want to decommission.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Decommission Chassis**.

Step 6 If Cisco UCS Manager displays a confirmation dialog box, click **Yes**.
The decommission may take several minutes to complete. After the chassis has been removed from the configuration, Cisco UCS Manager adds the chassis to the **Decommissioned** tab.

Recommissioning a Chassis

This procedure returns the chassis to the configuration and applies the chassis discovery policy to the chassis. After this procedure, you can access the chassis and any servers in it.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 In the **Equipment** tab, expand the **Equipment** node.

Step 3 Click the **Chassis** node.

Step 4 In the **Work** pane, click the **Decommissioned** tab.

Step 5 Right-click the chassis you want to enable and choose **Recommission**.

Step 6 If Cisco UCS Manager displays a confirmation dialog box, click **Yes**.
This procedure may take several minutes to complete. After the chassis has been recommissioned, Cisco UCS Manager runs the chassis discovery policy and adds the chassis to the list in the **Navigation** pane.

Toggling the Locator LED

Turning on the Locator LED for a Chassis

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis**.

Step 3 Click the chassis that you need to locate.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Turn on Locator LED**.
This action is not available if the locator LED is already turned on.

The LED on the chassis starts flashing.

Turning off the Locator LED for a Chassis

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis**.

Step 3 Choose the chassis for which you want to turn off the locator LED.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Turn off Locator LED**.
This action is not available if the locator LED is already turned off.

The LED on the chassis stops flashing.

Viewing the POST Results for a Chassis

You can view any errors collected during the Power On Self-Test process for all servers and adapters in a chassis.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis**.

Step 3 Choose the chassis for which you want to view the POST results.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **View POST Results**.
The **POST Results** dialog box lists the POST results for each server in the chassis and its adapters.

Step 6 (Optional) Click the link in the **Affected Object** column to view the properties of that adapter.

Step 7 Click **OK** to close the **POST Results** dialog box.

CHAPTER 39

Managing Blade Servers

This chapter includes the following sections:

Blade Server Management

You can manage and monitor all blade servers in a Cisco UCS instance through Cisco UCS Manager. Some blade server management tasks, such as changes to the power state, can be performed from the server and service profile.

The remaining management tasks can only be performed on the server.

If a blade server slot in a chassis is empty, Cisco UCS Manager provides information, errors, and faults for that slot. You can also reacknowledge the slot to resolve server mismatch errors and to have Cisco UCS Manager rediscover the blade server in the slot.

Booting Blade Servers

Booting a Blade Server

If the **Boot Server** link is dimmed in the **Actions** area, you must shut down the server first.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.
Step 3 Choose the server that you want to boot.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Actions** area, click **Boot Server**.
Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

After the server has booted, the **Overall Status** field on the **General** tab displays an OK status.

Booting a Server from the Service Profile

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.
Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.
Step 3 Expand the node for the organization where you want to create the service profile.
If the system does not include multi-tenancy, expand the **root** node.
Step 4 Choose the service profile that requires the associated server to be booted.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 In the **Actions** area, click **Boot Server**.
Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
Step 8 Click **OK** in the **Boot Server** dialog box.
After the server has booted, the **Overall Status** field on the **General** tab displays an ok status or an up status.

Determining the Boot Order of a Blade Server

Tip You can also view the boot order tabs from the **General** tab of the service profile associated with a server.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.

Step 3 Click the server for which you want to determine the boot order.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 If the **Boot Order Details** area is not expanded, click the **Expand** icon to the right of the heading.

Step 6 To view the boot order assigned to the server, click the **Configured Boot Order** tab.

Step 7 To view what will boot from the various devices in the physical server configuration, click the **Actual Boot Order** tab.

Note The **Actual Boot Order** tab always shows "Internal EFI Shell" at the bottom of the boot order list.

Shutting Down Blade Servers

Shutting Down a Blade Server

When you use this procedure to shut down a server with an installed operating system, Cisco UCS Manager triggers the OS into a graceful shutdown sequence.

If the **Shutdown Server** link is dimmed in the **Actions** area, the server is not running.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.

Step 3 Choose the server that you want to shut down.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Shutdown Server**.

Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

After the server has been successfully shut down, the **Overall Status** field on the **General** tab displays a power-off status.

Shutting Down a Server from the Service Profile

When you use this procedure to shut down a server with an installed operating system, Cisco UCS Manager triggers the OS into a graceful shutdown sequence.

If the **Shutdown Server** link is dimmed in the **Actions** area, the server is not running.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization where you want to create the service profile.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Choose the service profile that requires the associated server to be shut down.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Actions** area, click **Shutdown Server**.

Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

After the server has been successfully shut down, the **Overall Status** field on the **General** tab displays a down status or a power-off status.

Resetting a Blade Server

When you reset a server, Cisco UCS Manager sends a pulse on the reset line. You can choose to gracefully shut down the operating system. If the operating system does not support a graceful shut down, the server is power cycled. The option to have Cisco UCS Manager complete all management operations before it resets the server does not guarantee that these operations will be completed before the server is reset.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.

Step 3 Choose the server that you want to reset.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Reset**.

Step 6 In the **Reset Server** dialog box, do the following:

a) Click the **Power Cycle** option.

b) (Optional) Check the check box if you want Cisco UCS Manager to complete all management operations that are pending on this server.

c) Click **OK**.

The reset may take several minutes to complete. After the server has been reset, the **Overall Status** field on the **General** tab displays an ok status.

Reacknowledging a Blade Server

Perform the following procedure if you need to have Cisco UCS Manager rediscover the server and all endpoints in the server. For example, you can use this procedure if a server is stuck in an unexpected state, such as the discovery state.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤ *Chassis Number* ➤ Servers**.

Step 3 Choose the server that you want to acknowledge.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Server Maintenance**.

Step 6 In the **Maintenance** dialog box, do the following:

a) Click **Re-acknowledge**.

b) Click **OK**.

Cisco UCS Manager disconnects the server and then builds the connections between the server and the fabric interconnect or fabric interconnects in the system. The acknowledgment may take several minutes to complete. After the server has been acknowledged, the **Overall Status** field on the **General** tab displays an OK status.

Removing a Server from a Chassis

Before You Begin

Physically remove the server from its chassis before performing the following procedure.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤ *Chassis Number* ➤ Servers**.

Step 3 Choose the server that you want to remove from the chassis.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Server Maintenance**.

Step 6 In the **Maintenance** dialog box, do the following:

a) Click **Decommission**.

b) Click **OK**.

The server is removed from the Cisco UCS configuration.

Step 7 Go to the physical location of the chassis and remove the server hardware from the slot.
For instructions on how to remove the server hardware, see the *Cisco UCS Hardware Installation Guide* for your chassis.

What to Do Next

If you physically re-install the blade server, you must re-acknowledge the slot to have Cisco UCS Manager rediscover the server.

For more information, see Reacknowledging a Server Slot in a Chassis, page 510.

Decommissioning a Blade Server

This procedure decommissions a server and deletes it from the Cisco UCS configuration. The server hardware physically remains in the Cisco UCS instance. However, Cisco UCS Manager ignores it and does not list it with the other servers.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤ *Chassis Number* ➤ Servers**.

Step 3 Choose the server that you want to decommission.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Server Maintenance**.

Step 6 In the **Maintenance** dialog box, do the following:

a) Click **Decommission**.

b) Click **OK**.

The server is removed from the Cisco UCS configuration.

What to Do Next

If you physically re-install the blade server, you must re-acknowledge the slot to have Cisco UCS Manager rediscover the server.

For more information, see Reacknowledging a Server Slot in a Chassis, page 510.

Reacknowledging a Server Slot in a Chassis

Perform the following procedure if you decommissioned a blade server without removing the physical hardware from the chassis and you want Cisco UCS Manager to rediscover and recommission the server.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤ *Chassis Number* ➤ Servers**.

Step 3 Choose the server whose slot you want to reacknowledge.

Step 4 If Cisco UCS Manager displays a **Resolve Slot Issue** dialog box, do one of the following:

Option	Description
The **here** link in the **Situation** area	Click this link and then click **Yes** in the confirmation dialog box. Cisco UCS Manager reacknowledges the slot and discovers the server in the slot.
OK	Click this button if you want to proceed to the **General** tab. You can use the **Reacknowledge Slot** link in the **Actions** area to have Cisco UCS Manager reacknowledge the slot and discover the server in the slot.

Removing a Non-Existent Blade Server from the Configuration Database

Perform the following procedure if you physically removed the server hardware without first decommissioning the server. You cannot perform this procedure if the server is physically present.

If you want to physically remove a server, see Removing a Server from a Chassis, page 509.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤ *Chassis Number* ➤ Servers**.

Step 3 Choose the server that you want to remove from the configuration database.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Server Maintenance**.

Step 6 In the **Maintenance** dialog box, do the following:

a) Click **Remove**.

b) Click **OK**.

Cisco UCS Manager removes all data about the server from its configuration database. The server slot is now available for you to insert new server hardware.

Turning the Locator LED for a Blade Server On and Off

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤ *Chassis Number* ➤ Servers**.

Step 3 Choose the server for which you want to turn the locator LED on or off.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click one of the following:

- **Turn on Locator LED**
- **Turn off Locator LED**

Resetting the CMOS for a Blade Server

On rare occasions, troubleshooting a server may require you to reset the CMOS. This procedure is not part of the normal maintenance of a server.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.
Step 3 Choose the server for which you want to reset the CMOS.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Actions** area, click **Recover Server**.
Step 6 In the **Recover Server** dialog box, do the following:
a) Click **Reset CMOS**.
b) Click **OK**.

Resetting the CIMC for a Blade Server

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reset the CIMC. This procedure is not part of the normal maintenance of a server. After you reset the CIMC, the server boots with the running version of the firmware for that server.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.
Step 3 Choose the server for which you want to reset the CIMC.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Actions** area, click **Recover Server**.
Step 6 In the **Recover Server** dialog box, do the following:
a) Click **Reset CIMC (Server Controller)**.
b) Click **OK**.

Recovering the Corrupt BIOS on a Blade Server

On rare occasions, an issue with a server may require you to recover the corrupted BIOS. This procedure is not part of the normal maintenance of a server. After you recover the BIOS, the server boots with the running version of the firmware for that server. This radio button may be dimmed if the BIOS does not require recovery or the option is not available for a particular server.

Before You Begin

Important Remove all attached or mapped USB storage from a server before you attempt to recover the corrupt BIOS on that server. If an external USB drive is attached or mapped from vMedia to the server, BIOS recovery fails.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.

Step 3 Choose the server for which you want to recover the BIOS.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Recover Server**.

Step 6 In the **Recover Server** dialog box, do the following:

a) Click **Recover Corrupt BIOS**.

b) Click **OK**.

Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 8 In the **Recover Corrupt BIOS** dialog box, do the following:

a) Complete the following fields:

Name	Description
Version To Be Activated drop-down list	Choose the firmware version that you want to activate from the drop-down list.
Ignore Compatibility Check check box	By default, Cisco UCS makes sure that the firmware version is compatible with everything running on the server before it activates that version. Check this check box if you want Cisco UCS to activate the firmware without making sure that it is compatible first. **Note** We recommend that you use this option only when explicitly directed to do so by a technical support representative.

b) Click **OK**.

Viewing the POST Results for a Blade Server

You can view any errors collected during the Power On Self-Test process for a server and its adapters.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.

Step 3 Choose the server for which you want to view the POST results.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **View POST Results**.
The **POST Results** dialog box lists the POST results for the server and its adapters.

Step 6 (Optional) Click the link in the **Affected Object** column to view the properties of that adapter.

Step 7 Click **OK** to close the **POST Results** dialog box.

CHAPTER 40

Managing Rack-Mount Servers

This chapter includes the following sections:

Rack-Mount Server Management

You can manage and monitor all rack-mount servers that have been integrated with a Cisco UCS instance through Cisco UCS Manager. All management and monitoring features are supported for rack-mount servers except power capping. Some rack-mount server management tasks, such as changes to the power state, can be performed from both the server and service profile. The remaining management tasks can only be performed on the server.

Cisco UCS Manager provides information, errors, and faults for each rack-mount server that it has discovered.

Tip For information about how to integrate a supported Cisco UCS rack-mount server with Cisco UCS Manager, see the hardware installation guide for that server.

Booting Rack-Mount Servers

Booting a Rack-Mount Server

If the **Boot Server** link is dimmed in the **Actions** area, you must shut down the server first.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, expand **Equipment ➤ Rack Mounts ➤ Servers**.
Step 3 Choose the server that you want to boot.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Actions** area, click **Boot Server**.
Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

After the server has booted, the **Overall Status** field on the **General** tab displays an OK status.

Booting a Server from the Service Profile

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.
Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.
Step 3 Expand the node for the organization where you want to create the service profile.
If the system does not include multi-tenancy, expand the **root** node.
Step 4 Choose the service profile that requires the associated server to be booted.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 In the **Actions** area, click **Boot Server**.
Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
Step 8 Click **OK** in the **Boot Server** dialog box.
After the server has booted, the **Overall Status** field on the **General** tab displays an ok status or an up status.

Determining the Boot Order of a Rack-Mount Server

Tip You can also view the boot order tabs from the **General** tab of the service profile associated with a server.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Rack Mounts ➤ Servers**.

Step 3 Click the server for which you want to determine the boot order.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 If the **Boot Order Details** area is not expanded, click the **Expand** icon to the right of the heading.

Step 6 To view the boot order assigned to the server, click the **Configured Boot Order** tab.

Step 7 To view what will boot from the various devices in the physical server configuration, click the **Actual Boot Order** tab.

Note The **Actual Boot Order** tab always shows "Internal EFI Shell" at the bottom of the boot order list.

Shutting Down Rack-Mount Servers

Shutting Down a Rack-Mount Server

When you use this procedure to shut down a server with an installed operating system, Cisco UCS Manager triggers the OS into a graceful shutdown sequence.

If the **Shutdown server** link is dimmed in the **Actions** area, the server is not running.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Rack Mounts ➤ Servers**.

Step 3 Choose the server that you want to shut down.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Shutdown Server**.

Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

After the server has been successfully shut down, the **Overall Status** field on the **General** tab displays a power-off status.

Shutting Down a Server from the Service Profile

When you use this procedure to shut down a server with an installed operating system, Cisco UCS Manager triggers the OS into a graceful shutdown sequence.

If the **Shutdown Server** link is dimmed in the **Actions** area, the server is not running.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization where you want to create the service profile.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Choose the service profile that requires the associated server to be shut down.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Actions** area, click **Shutdown Server**.

Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

After the server has been successfully shut down, the **Overall Status** field on the **General** tab displays a down status or a power-off status.

Resetting a Rack-Mount Server

When you reset a server, Cisco UCS Manager sends a pulse on the reset line. You can choose to gracefully shut down the operating system. If the operating system does not support a graceful shut down, the server is power cycled. The option to have Cisco UCS Manager complete all management operations before it resets the server does not guarantee that these operations will be completed before the server is reset.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Rack Mounts ➤ Servers**.

Step 3 Choose the server that you want to reset.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Reset**.

Step 6 In the **Reset Server** dialog box, do the following:

a) Click the **Power Cycle** option.

b) (Optional) Check the check box if you want Cisco UCS Manager to complete all management operations that are pending on this server.

c) Click **OK**.

The reset may take several minutes to complete. After the server has been reset, the **Overall Status** field on the **General** tab displays an ok status.

Reacknowledging a Rack-Mount Server

Perform the following procedure if you need to have Cisco UCS Manager rediscover the server and all endpoints in the server. For example, you can use this procedure if a server is stuck in an unexpected state, such as the discovery state.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Rack Mounts ➤ Servers**.

Step 3 Choose the server that you want to acknowledge.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Server Maintenance**.

Step 6 In the **Maintenance** dialog box, do the following:

a) Click **Re-acknowledge**.

b) Click **OK**.

Cisco UCS Manager disconnects the server and then builds the connections between the server and the fabric interconnect or fabric interconnects in the system. The acknowledgment may take several minutes to complete. After the server has been acknowledged, the **Overall Status** field on the **General** tab displays an OK status.

Decommissioning a Rack-Mount Server

This procedure decommissions a server and deletes it from the Cisco UCS configuration. The server hardware physically remains in the Cisco UCS instance. However, Cisco UCS Manager ignores it and does not list it with the other servers.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Rack Mounts ➤ Servers**.

Step 3 Choose the server that you want to decommission.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Server Maintenance**.

Step 6 In the **Maintenance** dialog box, do the following:

a) Click **Decommission**.

b) Click **OK**.

The server is removed from the Cisco UCS configuration.

Removing a Non-Existent Rack-Mount Server from the Configuration Database

Perform the following procedure if you physically removed the server hardware without first decommissioning the server. You cannot perform this procedure if the server is physically present.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Rack Mounts ➤ Servers**.

Step 3 Choose the server that you want to remove from the configuration database.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Server Maintenance**.

Step 6 In the **Maintenance** dialog box, do the following:

a) Click **Remove**.

b) Click **OK**.

Cisco UCS Manager removes all data about the server from its configuration database. The server slot is now available for you to insert new server hardware.

Turning the Locator LED for a Rack-Mount Server On and Off

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Rack Mounts ➤ Servers**.

Step 3 Choose the server for which you want to turn the locator LED on or off.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click one of the following:

- **Turn on Locator LED**
- **Turn off Locator LED**

Resetting the CMOS for a Rack-Mount Server

On rare occasions, troubleshooting a server may require you to reset the CMOS. This procedure is not part of the normal maintenance of a server.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, expand **Equipment ➤ Rack Mounts ➤ Servers**.
Step 3 Choose the server for which you want to reset the CMOS.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Actions** area, click **Recover Server**.
Step 6 In the **Recover Server** dialog box, do the following:
a) Click **Reset CMOS**.
b) Click **OK**.

Resetting the CIMC for a Rack-Mount Server

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reset the CIMC. This procedure is not part of the normal maintenance of a server. After you reset the CIMC, the server boots with the running version of the firmware for that server.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, expand **Equipment ➤ Rack Mounts ➤ Servers**.
Step 3 Choose the server for which you want to reset the CIMC.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Actions** area, click **Recover Server**.
Step 6 In the **Recover Server** dialog box, do the following:
a) Click **Reset CIMC (Server Controller)**.
b) Click **OK**.

Recovering the Corrupt BIOS on a Rack-Mount Server

On rare occasions, an issue with a server may require you to recover the corrupted BIOS. This procedure is not part of the normal maintenance of a server. After you recover the BIOS, the server boots with the running version of the firmware for that server. This radio button may be dimmed if the BIOS does not require recovery or the option is not available for a particular server.

Before You Begin

Important Remove all attached or mapped USB storage from a server before you attempt to recover the corrupt BIOS on that server. If an external USB drive is attached or mapped from vMedia to the server, BIOS recovery fails.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Rack Mounts ➤ Servers**.

Step 3 Choose the server for which you want to recover the BIOS.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Recover Server**.

Step 6 In the **Recover Server** dialog box, do the following:

a) Click **Recover Corrupt BIOS**.

b) Click **OK**.

Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 8 In the **Recover Corrupt BIOS** dialog box, do the following:

a) Complete the following fields:

Name	Description
Version To Be Activated drop-down list	Choose the firmware version that you want to activate from the drop-down list.
Ignore Compatibility Check check box	By default, Cisco UCS makes sure that the firmware version is compatible with everything running on the server before it activates that version. Check this check box if you want Cisco UCS to activate the firmware without making sure that it is compatible first. **Note** We recommend that you use this option only when explicitly directed to do so by a technical support representative.

b) Click **OK**.

Viewing the POST Results for a Rack-Mount Server

You can view any errors collected during the Power On Self-Test process for a server and its adapters.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Rack Mounts ➤ Servers**.

Step 3 Choose the server for which you want to view the POST results.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **View POST Results**.
The **POST Results** dialog box lists the POST results for the server and its adapters.

Step 6 (Optional) Click the link in the **Affected Object** column to view the properties of that adapter.

Step 7 Click **OK** to close the **POST Results** dialog box.

CHAPTER 41

Starting the KVM Console

This chapter includes the following sections:

KVM Console

The KVM console is an interface accessible from the Cisco UCS Manager GUI or the KVM Launch Manager that emulates a direct KVM connection. Unlike the KVM dongle, which requires you to be physically connected to the server, the KVM console allows you to connect to the server from a remote location across the network.

You must ensure that either the server or the service profile associated with the server is configured with a CIMC IP address if you want to use the KVM console to access the server. The KVM console uses the CIMC IP address assigned to a server or a service profile to identify and connect with the correct server in a Cisco UCS.

Instead of using CD/DVD or floppy drives directly connected to the server, the KVM console uses virtual media, which are actual disk drives or disk image files that are mapped to virtual CD/DVD or floppy drives. You can map any of the following to virtual drives:

- CD/DVD or floppy drives on your computer
- Disk image files on your computer
- CD/DVD or floppy drives on the network
- Disk image files on the network

Recommendations for Using the KVM Console to Install a Server OS

To install an OS from a virtual CD/DVD or floppy drive, you must ensure that the virtual CD/DVD or floppy drive is set as the first boot device in the service profile.

Installing an OS using the KVM console may be slower than using the KVM dongle because the installation files must be downloaded across the network to the server. If you map a disk drive or disk image file from a

network share to a virtual drive, the installation may be even slower because the installation files must be downloaded from the network to the KVM console (your computer) and then from the KVM console to the server. When using this installation method, we recommend that you have the installation media as close as possible to the system with the KVM console.

Virtual KVM Console

The KVM console is an interface accessible from CIMC that emulates a direct keyboard, video, and mouse (KVM) connection to the server. It allows you to connect to and control the server from a remote location.

File Menu

Menu Item	Description
Capture to File	Opens the **Save** dialog box that lets you save the current screen as a JPG image.
Exit	Closes the KVM console.

View Menu

Menu Item	Description
Refresh	Updates the console display with the server's current video output.
Full Screen	Expands the KVM console so that it fills the entire screen.
Windowed	Returns the KVM console to Windowed mode where it can be resized.
Fit	Resizes the console window to the minimum size needed to display the video image from the server. This option is only available if the console is in Windowed mode.

Macros Menu

Select the keyboard shortcut you want to execute on the remote system.

Tools Menu

Menu Item	Description
Session Options	Opens the **Session Options** dialog box that lets you specify: • Whether all keystrokes are passed to the target system when the console is in Windowed mode. The default is no. • The termination key when in single cursor mode. The default is **F12**. • The mouse acceleration to use on the target system. The default is **Windows**.

Menu Item	Description
Single Cursor	Turns on the single cursor feature, which offsets mouse alignment issues encountered on some remote operating systems. When you turn this feature on, the mouse pointer is trapped within the viewer window. To turn the feature off, press the termination key specified in the **Session Options** dialog box.
Stats	Opens the **Stats** dialog box, which displays the: • Frame rate measured in number of frames per second • Bandwidth measured in number of KBs per second • Compression measured in the percentage of compression being used • Packet rate measured in number of packets per second
Launch Virtual Media	Opens the **Virtual Media Session** dialog box that lets you map physical locations to virtual drives that can by accessed by the server. **Note** In order to use virtual media, the **Enabled** check box must be checked on the **Virtual Media** tab.

Virtual Media Session Dialog Box

Instead of using CD/DVD or floppy drives physically connected to the server, the KVM console uses virtual media, which are actual disk drives or disk image files that are mapped to virtual CD/DVD or floppy drives on the server. The **Client View** table displays the floppy images, floppy drives, CD/DVD drives, and ISO images that are available to the server. For each type of media, the table displays:

Name	Description
Mapped column	If the check box in this column is checked, the associated disk drive or image file can be accessed by the server. Clear the check box to disconnect the server from the drive or image file. Each drive or image file can exist either on the users local computer or on the network, and each falls into one of three categories: • Virtual CD/DVD • Removable Media • Floppy—This category includes USB keys or flash drives. You can enable Virtual Media for one drive or image in each of the three categories, but you cannot virtualize multiple drives or images in the same category.
Read Only column	If checked, the server cannot write to the Virtual Media device even if the device has write capability.
Drive column	Displays the path to the device used by the server.

Name	Description
Exit button	Closes the **Virtual Media Session** dialog box.
Add Image button	Opens the **Open** dialog box that lets you navigate to the drive or image file you want to virtualize.
Details button	Toggles the display of the **Details** area. This area contains a table showing the three device categories, their mapped status, read and write statistics, and the length of time that the device has been mapped. It also contains the **USB Reset** button that lets you reset all USB devices connected to the server.

Starting the KVM Console from a Server

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.

Step 3 Choose the server that you want to access through the KVM console.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **KVM Console**.
The KVM console opens in a separate window.

Tip If the Caps Lock key on your keyboard is on when you open a KVM session, and you subsequently turn off your Caps Lock key, the KVM console may continue to act as if Caps Lock is turned on. To synchronize the KVM console and your keyboard, press Caps Lock once without the KVM console in focus and then press Caps Lock again with the KVM console in focus.

Starting the KVM Console from a Service Profile

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the node for the organization which contains the service profile for which you want to launch the KVM console.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Choose the service profile for which you need KVM access to the associated server.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Actions** area, click **KVM Console**.

The KVM console opens in a separate window.

Tip If the Caps Lock key on your keyboard is on when you open a KVM session, and you subsequently turn off your Caps Lock key, the KVM console may continue to act as if Caps Lock is turned on. To synchronize the KVM console and your keyboard, press Caps Lock once without the KVM console in focus and then press Caps Lock again with the KVM console in focus.

Starting the KVM Console from the KVM Launch Manager

The KVM Launch Manager enables you to access a server through the KVM console without logging in to Cisco UCS Manager.

Before You Begin

To access the KVM console for a server through the KVM Launch Manager, you need the following:

- Cisco UCS username and password.
- Name of the service profile associated with the server for which you want KVM access.

Procedure

Step 1 In your web browser, type or select the web link for Cisco UCS Manager GUI.

Example:
The default web link is `http://UCSManager_IP` or `https://UCSManager_IP`. In a standalone configuration, *`UCSManager_IP`* is the IP address for the management port on the fabric interconnect. In a cluster configuration, *`UCSManager_IP`* is the IP address assigned to Cisco UCS Manager.

Step 2 On the Cisco UCS Manager page, click **KVM Launch Manager**.

Step 3 On the **UCS - KVM Launch Manager Login** page, do the following:

a) Enter your Cisco UCS username and password.
b) Click **OK**.

Step 4 In the **Service Profiles** table of the KVM Launch Manager, do the following:

a) Choose the service profile for which you need KVM access to the associated server.
b) In the **Launch KVM** row for that service profile, click **Launch**.
The KVM console opens in a separate window.

Tip If the Caps Lock key on your keyboard is on when you open a KVM session, and you subsequently turn off your Caps Lock key, the KVM console may continue to act as if Caps Lock is turned on. To synchronize the KVM console and your keyboard, press Caps Lock once without the KVM console in focus and then press Caps Lock again with the KVM console in focus.

CHAPTER 42

Managing the I/O Modules

This chapter includes the following sections:

I/O Module Management in Cisco UCS Manager GUI

You can manage and monitor all I/O modules in a Cisco UCS instance through Cisco UCS Manager GUI.

Resetting an I/O Module

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment** ➤ **Chassis** ➤ ***Chassis Number*** ➤ **IO Modules**.

Step 3 Choose the I/O module that you want to reset.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Reset IO Module**.

Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Viewing the POST Results for an I/O Module

You can view any errors collected during the Power On Self-Test process for an I/O module.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ IO Modules**.

Step 3 Choose the I/O module for which you want to view the POST results.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **View POST Results**.
The **POST Results** dialog box lists the POST results for the I/O module.

Step 6 Click **OK** to close the **POST Results** dialog box.

CHAPTER 43

Backing Up and Restoring the Configuration

This chapter includes the following sections:

Backup and Export Configuration

When you perform a backup through Cisco UCS Manager, you take a snapshot of all or part of the system configuration and export the file to a location on your network. You cannot use Cisco UCS Manager to back up data on the servers.

You can perform a backup while the system is up and running. The backup operation only saves information from the management plane. It does not have any impact on the server or network traffic.

Backup Types

You can perform one or more of the following types of backups through Cisco UCS Manager:

- **Full state**—A binary file that includes a snapshot of the entire system. You can use the file generated from this backup to restore the system during disaster recovery. This file can restore or rebuild the configuration on the original fabric interconnect, or recreate the configuration on a different fabric interconnect. You cannot use this file for an import.

- **All configuration**—An XML file that includes all system and logical configuration settings. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore.
- **System configuration**—An XML file that includes all system configuration settings such as usernames, roles, and locales. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore.
- **Logical configuration**—An XML file that includes all logical configuration settings such as service profiles, VLANs, VSANs, pools, and policies. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore.

Considerations and Recommendations for Backup Operations

Before you create a backup operation, consider the following:

Backup Locations	The backup location is the destination or folder on the network where you want Cisco UCS Manager to export the backup file. You can maintain only one backup operation for each location where you plan to save a backup file.
Potential to Overwrite Backup Files	If you rerun a backup operation without changing the filename, Cisco UCS Manager overwrites the existing file on the server. To avoid overwriting existing backup files, change the filename in the backup operation or copy the existing file to another location.
Multiple Types of Backups	You can run and export more than one type of backup to the same location. You need to change the backup type before you rerun the backup operation. We recommend that you change the filename for easier identification of the backup type and to avoid overwriting the existing backup file.
Scheduled Backups	You cannot schedule a backup operation. You can, however, create a backup operation in advance and leave the admin state disabled until you are ready to run the backup. Cisco UCS Manager does not run the backup operation, save, or export the configuration file until you set the admin state of the backup operation to enabled.
Incremental Backups	You cannot perform incremental backups of the Cisco UCS Manager system configuration.
Backwards Compatibility	Starting with Release 1.1(1) of the Cisco UCS Manager, full state backups are encrypted so that passwords and other sensitive information are not exported as clear text. As a result, full state backups made from Release 1.1(1) or later cannot be restored to a Cisco UCS instance running an earlier software release.

Import Configuration

You can import any configuration file that was exported from Cisco UCS Manager. The file does not need to have been exported from the same Cisco UCS Manager.

The import function is available for all configuration, system configuration, and logical configuration files. You can perform an import while the system is up and running. An import operation modifies information on the management plane only. Some modifications caused by an import operation, such as a change to a vNIC assigned to a server, can cause a server reboot or other operations that disrupt traffic.

You cannot schedule an import operation. You can, however, create an import operation in advance and leave the admin state disabled until you are ready to run the import. Cisco UCS Manager will not run the import operation on the configuration file until you set the admin state to enabled.

You can maintain only one import operation for each location where you saved a configuration backup file.

Import Methods

You can use one of the following methods to import and update a system configuration through Cisco UCS Manager:

- **Merge**—The information in the imported configuration file is compared with the existing configuration information. If there are conflicts, the import operation overwrites the information on the Cisco UCS instance with the information in the import configuration file.
- **Replace**—The current configuration information is replaced with the information in the imported configuration file one object at a time.

System Restore

You can restore a system configuration from any full state backup file that was exported from Cisco UCS Manager. The file does not need to have been exported from the Cisco UCS Manager on the system that you are restoring.

The restore function is only available for a full state backup file. You cannot import a full state backup file. You perform a restore through the initial system setup.

You can use the restore function for disaster recovery.

Required User Role for Backup and Import Operations

You must have a user account that includes the admin role to create and run backup and import operations.

Backup Operations

Creating a Backup Operation

Before You Begin

Obtain the backup server IP address and authentication credentials.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 Click the **All** node.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area, click **Backup Configuration**.

Step 5 In the **Backup Configuration** dialog box, click **Create Backup Operation**.

Step 6 In the **Create Backup Operation** dialog box, complete the following fields:

Name	Description
Admin State field	This can be: • **enabled**—Cisco UCS Manager runs the backup operation as soon as you click **OK**. • **disabled**—Cisco UCS Manager does not run the backup operation when you click **OK**. If you select this option, all fields in the dialog box remain visible. However, you must manually run the backup from the **Backup Configuration** dialog box.
Type field	The information saved in the backup configuration file. This can be: • **Full state**—A binary file that includes a snapshot of the entire system. You can use the file generated from this backup to restore the system during disaster recovery. This file can restore or rebuild the configuration on the original fabric interconnect, or recreate the configuration on a different fabric interconnect. You cannot use this file for an import. • **All configuration**—An XML file that includes all system and logical configuration settings. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore. • **System configuration**—An XML file that includes all system configuration settings such as usernames, roles, and locales. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore. • **Logical configuration**—An XML file that includes all logical configuration settings such as service profiles, VLANs, VSANs, pools, and policies. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore.

Name	Description
Preserve Identities check box	If this check box is checked, the backup file preserves all identities derived from pools, including the MAC addresses, WWPN, WWNN, and UUIDs.
Location of the Backup File field	Where the backup file should be saved. This can be: • **Remote File System**—The backup XML file is saved to a remote server. Cisco UCS Manager GUI displays the fields described below that allow you to specify the protocol, host, filename, username, and password for the remote system. • **Local File System**—The backup XML file is saved locally. Cisco UCS Manager GUI displays the **Filename** field with an associated **Browse** button that let you specify the name and location for the backup file. **Note** Once you click **OK**, the location cannot be changed.
Protocol field	The protocol to use when communicating with the remote server. This can be: • **FTP** • **TFTP** • **SCP** • **SFTP**
Hostname field	The hostname or IP address of the location where the backup file is stored. This can be a server, storage array, local drive, or any read/write media that the fabric interconnect can access through the network. **Note** If you use a hostname rather than an IP address, you must configure a DNS server in Cisco UCS Manager.
Remote File field	The full path to the backup configuration file. This field can contain the filename as well as the path. If you omit the filename, the backup procedure assigns a name to the file.
User field	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP.
Password field	The password for the remote server username. This field does not apply if the protocol is TFTP. Cisco UCS Manager does not store this password. Therefore, you do not need to enter this password unless you intend to enable and run the backup operation immediately.

Step 7 Click **OK**.

Step 8 If Cisco UCS Manager displays a confirmation dialog box, click **OK**.
If you set the **Admin State** field to enabled, Cisco UCS Manager takes a snapshot of the configuration type that you selected and exports the file to the network location. The backup operation displays in the **Backup Operations** table in the **Backup Configuration** dialog box.

Step 9 (Optional) To view the progress of the backup operation, do the following:

a) If the operation does not display in the **Properties** area, click the operation in the **Backup Operations** table.

b) In the **Properties** area, click the down arrows on the **FSM Details** bar.

The **FSM Details** area expands and displays the operation status.

Step 10 Click **OK** to close the **Backup Configuration** dialog box.
The backup operation continues to run until it is completed. To view the progress, re-open the **Backup Configuration** dialog box.

Running a Backup Operation

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 Click the **All** node.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area, click **Backup Configuration**.

Step 5 In the **Backup Operations** table of the **Backup Configuration** dialog box, click the backup operation that you want to run.
The details of the selected backup operation display in the **Properties** area.

Step 6 In the **Properties** area, complete the following fields:

a) In the **Admin State** field, click the **Enabled** radio button.

b) For all protocols except TFTP, enter the password for the username in the **Password** field.

c) (Optional) Change the content of the other available fields.

Step 7 Click **Apply**.
Cisco UCS Manager takes a snapshot of the configuration type that you selected and exports the file to the network location. The backup operation displays in the **Backup Operations** table in the **Backup Configuration** dialog box.

Step 8 (Optional) To view the progress of the backup operation, click the down arrows on the **FSM Details** bar.
The **FSM Details** area expands and displays the operation status.

Step 9 Click **OK** to close the **Backup Configuration** dialog box.
The backup operation continues to run until it is completed. To view the progress, re-open the **Backup Configuration** dialog box.

Modifying a Backup Operation

You can modify a backup operation to save a file of another backup type to that location or to change the filename and avoid overwriting previous backup files.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 Click the **All** node.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area, click **Backup Configuration**.

Step 5 In the **Backup Operations** area of the **Backup Configuration** dialog box, click the backup operation that you want to modify.
The details of the selected backup operation display in the **Properties** area. If the backup operation is in a disabled state, the fields are dimmed.

Step 6 In the **Admin State** field, click the **enabled** radio button.

Step 7 Modify the appropriate fields.
You do not have to enter the password unless you want to run the backup operation immediately.

Step 8 (Optional) If you do not want to run the backup operation immediately, click the **disabled** radio button in the **Admin State** field.

Step 9 Click **OK**.

Deleting One or More Backup Operations

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 Click the **All** node.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area, click **Backup Configuration**.

Step 5 In the **Backup Operations** table of the **Backup Configuration** dialog box, click the backup operations that you want to delete.

Tip You cannot click a backup operation in the table if the admin state of the operation is set to **Enabled.**

Step 6 Click the **Delete** icon in the icon bar of the **Backup Operations** table.

Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 8 In the **Backup Configuration** dialog box, click one of the following:

Option	Description
Apply	Deletes the selected backup operations without closing the dialog box.

Option	Description
OK	Deletes the selected backup operations and closes the dialog box.

Import Operations

Creating an Import Operation

You cannot import a Full State configuration file. You can import any of the following configuration files:

- All configuration
- System configuration
- Logical configuration

Before You Begin

Collect the following information that you will need to import a configuration file:

- Backup server IP address and authentication credentials
- Fully qualified name of a backup file

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 Click the **All** node.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area, click **Import Configuration**.

Step 5 In the **Import Configuration** dialog box, click **Create Import Operation**.

Step 6 In the **Create Import Operation** dialog box, complete the following fields:

Name	Description
Admin State field	This can be: • **enabled**—Cisco UCS runs the import operation as soon as you click **OK**. • **disabled**—Cisco UCS does not run the import operation when you click **OK**. If you select this option, all fields in the dialog box remain visible. However, you must manually run the import from the **Import Configuration** dialog box.
Action field	You can select:

Name	Description
	• **Merge**—The configuration information is merged with the existing information. If there are conflicts, the system replaces the information on the current system with the information in the import configuration file. • **Replace**—The system takes each object in the import configuration file and overwrites the corresponding object in the current configuration.
Location of the Import File field	Where the backup file that you want to import is located. This can be: • **Remote File System**—The backup XML file is stored on a remote server. Cisco UCS Manager GUI displays the fields described below that allow you to specify the protocol, host, filename, username, and password for the remote system. • **Local File System**—The backup XML file is stored locally. Cisco UCS Manager GUI displays the **Filename** field with an associated **Browse** button that let you specify the name and location for the backup file to be imported.
Protocol field	The protocol to use when communicating with the remote server. This can be: • **FTP** • **TFTP** • **SCP** • **SFTP**
Hostname field	The hostname or IP address from which the configuration file should be imported. **Note** If you use a hostname rather than an IP address, you must configure a DNS server in Cisco UCS Manager.
Remote File field	The name of the XML configuration file.
User field	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP.
Password field	The password for the remote server username. This field does not apply if the protocol is TFTP. Cisco UCS Manager does not store this password. Therefore, you do not need to enter this password unless you intend to enable and run the import operation immediately.

Step 7 Click **OK**.

Step 8 In the confirmation dialog box, click **OK**.
If you set the **Admin State** to enabled, Cisco UCS Manager imports the configuration file from the network location. Depending upon which action you selected, the information in the file is either merged with the existing configuration or replaces the existing configuration. The import operation displays in the **Import Operations** table of the **Import Configuration** dialog box.

Step 9 (Optional) To view the progress of the import operation, do the following:

a) If the operation does not automatically display in the **Properties** area, click the operation in the **Import Operations** table.

b) In the **Properties** area, click the down arrows on the **FSM Details** bar.

The **FSM Details** area expands and displays the operation status.

Step 10 Click **OK** to close the **Import Configuration** dialog box.
The import operation continues to run until it is completed. To view the progress, re-open the **Import Configuration** dialog box.

Running an Import Operation

You cannot import a Full State configuration file. You can import any of the following configuration files:

- All configuration
- System configuration
- Logical configuration

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 Click the **All** node.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area, click **Import Configuration**.

Step 5 In the **Import Operations** table of the **Import Configuration** dialog box, click the operation that you want to run.
The details of the selected import operation display in the **Properties** area.

Step 6 In the **Properties** area, complete the following fields:

a) In the **Admin State** field, click the **Enabled** radio button.

b) For all protocols except TFTP, enter the password for the username In the **Password** field.

c) (Optional) Change the content of the other available fields.

Step 7 Click **Apply**.
Cisco UCS Manager imports the configuration file from the network location. Depending upon which action you selected, the information in the file is either merged with the existing configuration or replaces the existing

configuration. The import operation displays in the **Import Operations** table of the **Import Configuration** dialog box.

Step 8 (Optional) To view the progress of the import operation, click the down arrows on the **FSM Details** bar. The **FSM Details** area expands and displays the operation status.

Step 9 Click **OK** to close the **Import Configuration** dialog box.
The import operation continues to run until it is completed. To view the progress, re-open the **Import Configuration** dialog box.

Modifying an Import Operation

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 Click the **All** node.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area, click **Import Configuration**.

Step 5 In the **Import Operations** area of the **Import Configuration** dialog box, click the import operation that you want to modify.
The details of the selected import operation display in the **Properties** area. If the import operation is in a disabled state, the fields are dimmed.

Step 6 In the **Admin State** field, click the **enabled** radio button.

Step 7 Modify the appropriate fields.
You do not have to enter the password unless you want to run the import operation immediately.

Step 8 (Optional) If you do not want to run the import operation immediately, click the **disabled** radio button in the **Admin State** field.

Step 9 Click **OK**.

Deleting One or More Import Operations

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 Click the **All** node.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area, click **Import Configuration**.

Step 5 In the **Import Operations** table of the **Backup Configuration** dialog box, click the import operations that you want to delete.

Tip You cannot click an import operation in the table if the admin state of the operation is set to **Enabled.**

Step 6 Click the **Delete** icon in the icon bar of the **Import Operations** table.

Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 8 In the **Import Configuration** dialog box, click one of the following:

Option	Description
Apply	Deletes the selected import operations without closing the dialog box.
OK	Deletes the selected import operations and closes the dialog box.

Restoring the Configuration for a Fabric Interconnect

Before You Begin

Collect the following information that you will need to restore the system configuration:

- Fabric interconnect management port IP address and subnet mask
- Default gateway IP address
- Backup server IP address and authentication credentials
- Fully qualified name of a Full State backup file

Note You must have access to a Full State configuration file to perform a system restore. You cannot perform a system restore with any other type of configuration or backup file.

Procedure

Step 1 Connect to the console port.

Step 2 If the fabric interconnect is off, power on the fabric interconnect.
You will see the power on self-test message as the fabric interconnect boots.

Step 3 At the installation method prompt, enter gui.

Step 4 If the system cannot access a DHCP server, you may be prompted to enter the following information:

- IP address for the management port on the fabric interconnect
- Subnet mask for the management port on the fabric interconnect
- IP address for the default gateway assigned to the fabric interconnect

Step 5 Copy the web link from the prompt into a web browser and go to the Cisco UCS Manager GUI launch page.

Step 6 On the launch page, select **Express Setup**.

Step 7 On the **Express Setup** page, select **Restore From Backup** and click **Submit**.

Step 8 In the **Protocol** area of the **Cisco UCS Manager Initial Setup** page, select the protocol you want to use to upload the full state backup file:

- **SCP**
- **TFTP**
- **FTP**
- **SFTP**

Step 9 In the **Server Information** area, complete the following fields:

Name	Description
Server IP	The IP address of the computer where the full state backup file is located. This can be a server, storage array, local drive, or any read/write media that the fabric interconnect can access through the network.
Backup File Path	The file path where the full state backup file is located, including the folder names and filename.
User ID	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP.

Step 10 Click **Submit**.

You can return to the console to watch the progress of the system restore.

The fabric interconnect logs in to the backup server, retrieves a copy of the specified full-state backup file, and restores the system configuration.

For a cluster configuration, you do not need to restore the secondary fabric interconnect. As soon as the secondary fabric interconnect reboots, Cisco UCS Manager sychronizes the configuration with the primary fabric interconnect.

CHAPTER 44

Recovering a Lost Password

This chapter includes the following sections:

Recovering a Lost Password

Password Recovery for the Admin Account

The admin account is the system administrator or superuser account. If an administrator loses the password to this account, you can have a serious security issue. As a result, the procedure to recover the password for the admin account requires you to power cycle all fabric interconnects in a Cisco UCS instance.

When you recover the password for the admin account, you actually change the password for that account. You cannot retrieve the original password for that account.

You can reset the password for all other local accounts through Cisco UCS Manager. However, you must log in to Cisco UCS Manager with an account that includes aaa or admin privileges.

Caution This procedure requires you to power down all fabric interconnects in a Cisco UCS instance. As a result, all data transmission in the instance is stopped until you restart the fabric interconnects.

Determining the Leadership Role of a Fabric Interconnect

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 In the **Equipment** tab, expand **Equipment ➤ Fabric Interconnects**.
Step 3 Click the fabric interconnect for which you want to identify the role.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **General** tab, click the down arrows on the **High Availability Details** bar to expand that area.
Step 6 View the **Leadership** field to determine whether the fabric interconnect is the primary or subordinate.

Verifying the Firmware Versions on a Fabric Interconnect

You can use the following procedure to verify the firmware versions on all fabric interconnects in a Cisco UCS instance. You can verify the firmware for a single fabric interconnect through the **Installed Firmware** tab for that fabric interconnect.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 In the **Equipment** tab, click the **Equipment** node.
Step 3 In the **Work** pane, click the **Firmware Management** tab.
Step 4 In the **Installed Firmware** tab, verify that the following firmware versions for each fabric interconnect match the version to which you updated the firmware:

- Kernel version
- System version

Recovering the Admin Account Password in a Standalone Configuration

This procedure will help you to recover the password that you set for the admin account when you performed an initial system setup on the fabric interconnect. The admin account is the system administrator or superuser account.

Before You Begin

1 Physically connect the console port on the fabric interconnect to a computer terminal or console server
2 Determine the running versions of the following firmware:

- The firmware kernel version on the fabric interconnect

- The firmware system version

Tip To find this information, you can log in with any user account on the Cisco UCS instance.

Procedure

Step 1 Connect to the console port.

Step 2 Power cycle the fabric interconnect:

a) Turn off the power to the fabric interconnect.

b) Turn on the power to the fabric interconnect.

Step 3 In the console, press one of the following key combinations as it boots to get the `loader` prompt:

- Ctrl+l
- Ctrl+Shift+r

You may need to press the selected key combination multiple times before your screen displays the `loader` prompt.

Step 4 Boot the kernel firmware version on the fabric interconnect.

`loader >` **boot /installables/switch/***kernel_firmware_version*

Example:

`loader >` **boot /installables/switch/**`ucs-6100-k9-kickstart.4.1.3.N2.1.0.11.gbin`

Step 5 Enter config terminal mode.

`Fabric(boot)#` **config terminal**

Step 6 Reset the admin password.

`Fabric(boot)(config)#` **admin-password***password*

Choose a strong password that includes at least one capital letter and one number. The password cannot be blank.

The new password displays in clear text mode.

Step 7 Exit config terminal mode and return to the boot prompt.

Step 8 Boot the system firmware version on the fabric interconnect.

`Fabric(boot)#` **load /installables/switch/***system_firmware_version*

Example:

`Fabric(boot)#` **load /installables/switch/**`ucs-6100-k9-system.4.1.3.N2.1.0.211.bin`

Step 9 After the system image loads, log in to Cisco UCS Manager.

Recovering the Admin Account Password in a Cluster Configuration

This procedure will help you to recover the password that you set for the admin account when you performed an initial system setup on the fabric interconnects.The admin account is the system administrator or superuser account.

Before You Begin

1. Physically connect a console port on one of the fabric interconnects to a computer terminal or console server
2. Obtain the following information:
   - The firmware kernel version on the fabric interconnect
   - The firmware system version
   - Which fabric interconnect has the primary leadership role and which is the subordinate

Tip To find this information, you can log in with any user account on the Cisco UCS instance.

Procedure

Step 1 Connect to the console port.

Step 2 For the subordinate fabric interconnect:

a) Turn off the power to the fabric interconnect.
b) Turn on the power to the fabric interconnect.
c) In the console, press one of the following key combinations as it boots to get the `loader` prompt:
   - Ctrl+l
   - Ctrl+Shift+r

   You may need to press the selected key combination multiple times before your screen displays the `loader` prompt.

Step 3 Power cycle the primary fabric interconnect:

a) Turn off the power to the fabric interconnect.
b) Turn on the power to the fabric interconnect.

Step 4 In the console, press one of the following key combinations as it boots to get the `loader` prompt:

- Ctrl+l
- Ctrl+Shift+r

You may need to press the selected key combination multiple times before your screen displays the `loader` prompt.

Step 5 Boot the kernel firmware version on the primary fabric interconnect.

```
loader > boot /installables/switch/kernel_firmware_version
```

Example:

```
loader > boot /installables/switch/ucs-6100-k9-kickstart.4.1.3.N2.1.0.11.gbin
```

Step 6 Enter config terminal mode.

```
Fabric(boot)# config terminal
```

Step 7 Reset the admin password.

```
Fabric(boot)(config)# admin-password password
```

Choose a strong password that includes at least one capital letter and one number. The password cannot be blank.

The new password displays in clear text mode.

Step 8 Exit config terminal mode and return to the boot prompt.

Step 9 Boot the system firmware version on the primary fabric interconnect.

```
Fabric(boot)# load /installables/switch/system_firmware_version
```

Example:

```
Fabric(boot)# load /installables/switch/ucs-6100-k9-system.4.1.3.N2.1.0.211.bin
```

Step 10 After the system image loads, log in to Cisco UCS Manager.

Step 11 In the console for the subordinate fabric interconnect, do the following to bring it up:

a) Boot the kernel firmware version on the subordinate fabric interconnect.

```
loader > boot /installables/switch/kernel_firmware_version
```

b) Boot the system firmware version on the subordinate fabric interconnect.

```
Fabric(boot)# load /installables/switch/system_firmware_version
```

PART VIII

System Monitoring

CHAPTER 45

Monitoring Traffic

This chapter includes the following sections:

Traffic Monitoring

Traffic monitoring copies traffic from one or more sources and sends the copied traffic to a dedicated destination port for analysis by a network analyzer. This feature is also known as Switched Port Analyzer (SPAN).

Type of Session

When you create a traffic monitoring session, you can choose either an Ethernet or Fibre Channel destination port to receive the traffic. The type of destination port determines the type of session, which in turn determines the types of available traffic sources. For an Ethernet traffic monitoring session, the destination port must be an unconfigured physical port. For a Fibre Channel traffic monitoring session, the destination port must be a Fibre Channel uplink port.

Traffic Sources

An Ethernet traffic monitoring session can monitor any of the following traffic sources:

- Uplink Ethernet port
- Ethernet port channel
- VLAN
- Service profile vNIC
- Service profile vHBA

- FCoE port
- Port channels
- Server port

A Fibre Channel traffic monitoring session can monitor any of the following traffic sources:

- Uplink Fibre Channel port
- SAN port channel
- VSAN
- Service profile vHBA
- Fibre Channel storage port

Guidelines and Recommendations for Traffic Monitoring

When configuring or activating traffic monitoring, consider the following guidelines:

- You can create and store up to 16 traffic monitoring sessions, but only two can be active at the same time.
- A traffic monitoring session is disabled by default when created. To begin monitoring traffic, you must activate the session.
- To monitor traffic from a server, add all vNICs from the service profile corresponding to the server.
- To monitor traffic from a VM, you must first determine the identity of the dynamic vNIC assigned to the VM. Follow the procedure in Viewing Dynamic vNIC Properties in a VM, page 488 to find the vNIC and view its identity properties, then add the vNIC as a source for the monitoring session. If you later move the VM using VMotion, a new dynamic vNIC is assigned and you must reconfigure the monitoring source.
- You can monitor Fibre Channel traffic using either a Fibre Channel traffic analyzer or an Ethernet traffic analyzer. When Fibre Channel traffic is monitored using an Ethernet traffic monitoring session, with an Ethernet destination port, the destination traffic will be FCoE.
- Because a traffic monitoring destination is a single physical port, a traffic monitoring session can monitor only a single fabric. To monitor uninterrupted vNIC traffic across a fabric failover, you must create two sessions—one per fabric—and connect two analyzers. Add the vNIC as the traffic source for both sessions.
- All traffic sources must be located within the same switch as the destination port.
- A port configured as a destination port cannot also be configured as a source port.
- A member port of a port channel cannot be configured individually as a source. If the port channel is configured as a source, all member ports are source ports.
- A vHBA can be a source for either an Ethernet or Fibre Channel monitoring session, but it cannot be a source for both simultaneously.
- A server port can be a source only if it is a non-virtualized rack server adapter-facing port.

- Traffic monitoring can impose a significant load on your system resources. To minimize the load, select sources that carry as little unwanted traffic as possible and disable traffic monitoring when it is not needed.

Creating a Traffic Monitoring Session

Note This procedure describes how to create an Ethernet traffic monitoring session. To create a Fibre Channel monitoring session, select the **SAN** tab instead of the **LAN** tab in Step 2.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN ➤ Traffic Monitoring Sessions ➤** ***Fabric_Interconnect_Name***.

Step 3 Right-click ***Fabric_Interconnect_Name*** and choose **Create Traffic Monitoring Session**.

Step 4 In the **Create Traffic Monitoring Session** dialog box, complete the following fields:

Name	Description
Name field	The name of the traffic monitoring session. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Admin State field	Whether traffic will be monitored for the physical port selected in the **Destination** field. This can be: • **enabled**—Cisco UCS begins monitoring the port activity as soon as some source components are added to the session. • **disabled**—Cisco UCS does not monitor the port activity.
Destination drop-down list	Select the physical port whose communication traffic you want to monitor from the navigation tree.

Step 5 Click **OK**.

What to Do Next

- Add traffic sources to the traffic monitoring session.
- Activate the traffic monitoring session.

Adding Sources for Traffic Monitoring

You can choose multiple sources from more than one source type to be monitored by a traffic monitoring session. The available sources depend on the components configured in the Cisco UCS instance.

Note This procedure describes how to add sources for Ethernet traffic monitoring sessions. To add sources for a Fibre Channel monitoring session, select the **SAN** tab instead of the **LAN** tab in Step 2.

Before You Begin

A traffic monitoring session must be created.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN ➤ Traffic Monitoring Sessions ➤** ***Fabric_Interconnect_Name***.

Step 3 Expand ***Fabric_Interconnect_Name*** and click the monitor session that you want to configure.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Sources** area, expand the section for the type of traffic source that you want to add.

Step 6 To see the components that are available for monitoring, click the + button in the right-hand edge of the table to open the **Create Monitoring Session Source** dialog box.

Step 7 Select a source component and click **OK**.
You can repeat the preceding three steps as needed to add multiple sources from multiple source types.

Step 8 Click **Save Changes**.

What to Do Next

Activate the traffic monitoring session. If the session is already activated, traffic will be forwarded to the monitoring destination when you add a source.

Activating a Traffic Monitoring Session

Note This procedure describes how to activate an Ethernet traffic monitoring session. To activate a Fibre Channel monitoring session, select the **SAN** tab instead of the **LAN** tab in Step 2.

Before You Begin

A traffic monitoring session must be created.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.
Step 2 On the **LAN** tab, expand **LAN ➤ Traffic Monitoring Sessions ➤** ***Fabric_Interconnect_Name***.
Step 3 Expand ***Fabric_Interconnect_Name*** and click the monitor session that you want to activate.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Properties** area, click the **enabled** radio button for **Admin State**.
Step 6 Click **Save Changes**.

If a traffic monitoring source is configured, traffic begins to flow to the traffic monitoring destination port.

Deleting a Traffic Monitoring Session

Note This procedure describes how to delete an Ethernet traffic monitoring session. To delete a Fibre Channel monitoring session, select the **SAN** tab instead of the **LAN** tab in Step 2.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.
Step 2 On the **LAN** tab, expand **LAN ➤ Traffic Monitoring Sessions ➤** ***Fabric_Interconnect_Name***.
Step 3 Expand ***Fabric_Interconnect_Name*** and click the monitor session that you want to delete.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Actions** area, click the **Delete** icon.
Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

CHAPTER 46

Monitoring Hardware

This chapter includes the following sections:

Monitoring a Fabric Interconnect

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Fabric Interconnects**.

Step 3 Click the node for the fabric interconnect that you want to monitor.

Step 4 In the **Work** pane, click one of the following tabs to view the status of the fabric interconnect:

Option	Description
General tab	Provides an overview of the status of the fabric interconnect, including a summary of any faults, a summary of the fabric interconnect properties, and a physical display of the fabric interconnect and its components.

Option	Description
Physical Ports tab	Displays the status of all ports on the fabric interconnect. This tab includes the following subtabs: • **Uplink Ports** tab • **Server Ports** tab • **Fibre Channel Ports** tab • **Unconfigured Ports** tab
Fans tab	Displays the status of all fan modules in the fabric interconnect.
PSUs tab	Displays the status of all power supply units in the fabric interconnect.
Physical Display tab	Provides a graphical view of the fabric interconnect and all ports and other components. If a component has a fault, the fault icon is displayed next to that component.
Faults tab	Provides details of faults generated by the fabric interconnect.
Events tab	Provides details of events generated by the fabric interconnect.
Statistics tab	Provides statistics about the fabric interconnect and its components. You can view these statistics in tabular or chart format.

Monitoring a Chassis

Tip To monitor an individual component in a chassis, expand the node for that component.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis**.

Step 3 Click the chassis that you want to monitor.

Step 4 Click one of the following tabs to view the status of the chassis:

Option	Description
General tab	Provides an overview of the status of the chassis, including a summary of any faults, a summary of the chassis properties, and a physical display of the chassis and its components.

Option	Description
Servers tab	Displays the status and selected properties of all servers in the chassis.
Service Profiles tab	Displays the status of the service profiles associated with servers in the chassis.
IO Modules tab	Displays the status and selected properties of all IO modules in the chassis.
Fans tab	Displays the status of all fan modules in the chassis.
PSUs	Displays the status of all power supply units in the chassis.
Hybrid Display tab	Displays detailed information about the connections between the chassis and the fabric interconnects. The display has an icon for the following: • Each fabric interconnect in the system • The I/O module (IOM) in the selected component, which is shown as an independent unit to make the connection paths easier to see • The selected chassis showing the servers and PSUs
Slots tab	Displays the status of all slots in the chassis.
Installed Firmware tab	Displays the current firmware versions on the IO modules and servers in the chassis. You can also use this tab to update and activate the firmware on those components.
Management Logs tab	Displays and provides access to the system event logs for the servers in the chassis.
Faults tab	Provides details of faults generated by the chassis.
Events tab	Provides details of events generated by the chassis.
FSM tab	Provides details about and the status of FSM tasks related to the chassis. You can use this information to diagnose errors with those tasks.
Statistics tab	Provides statistics about the chassis and its components. You can view these statistics in tabular or chart format.
Temperatures tab	Provides temperature statistics for the components of the chassis. You can view these statistics in tabular or chart format.
Power tab	Provides power statistics for the components of the chassis. You can view these statistics in tabular or chart format.

Monitoring a Blade Server

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.

Step 3 Click the server that you want to monitor.

Step 4 In the **Work** pane, click one of the following tabs to view the status of the server:

Option	Description
General tab	Provides an overview of the status of the server, including a summary of any faults, a summary of the server properties, and a physical display of the server and its components.
Inventory tab	Provides details about the properties and status of the components of the server on the following subtabs: • **Motherboard**—Information about the motherboard and information about the server BIOS settings. You can also recover corrupt BIOS firmware from this subtab. • **CIMC**—Information about the CIMC and its firmware, and provides access to the SEL for the server. You can also assign a static or pooled management IP address, and update and activate the CIMC firmware from this subtab. • **CPU**—Information about each CPU in the server. • **Memory**—Information about each memory slot in the server and the DIMM in that slot. • **Interface cards**—Information about each adapter installed in the server. • **HBAs**—Properties of each HBA and the configuration of that HBA in the service profile associated with the server. • **NICs**—Properties of each NIC and the configuration of that NIC in the service profile associated with the server. You can expand each row to view information about the associated VIFs and vNICs. • **Storage**—Properties of the storage controller, the local disk configuration policy in the service profile associated with the server, and for each hard disk in the server. **Tip** If the server contains one or more SATA devices, such as a hard disk drive or solid state drive, Cisco UCS Manager GUI displays the vendor name for the SATA device in the **Vendor** field. However, Cisco UCS Manager CLI displays ATA in the **Vendor** field and includes the vendor information, such as the vendor name, in a **Vendor Description** field. This second field does not exist in Cisco UCS Manager GUI.

Option	Description
Virtual Machines tab	Displays details about any virtual machines hosted on the server.
Installed Firmware tab	Displays the firmware versions on the CIMC, adapters, and other server components. You can also use this tab to update and activate the firmware on those components.
Management Logs tab	Displays the system event log for the server.
VIF Paths tab	Displays the VIF paths for the adapters on the server.
Faults tab	Displays an overview of the faults generated by the server. You can click any fault to view additional information.
Events tab	Displays an overview of the events generated by the server. You can click any event to view additional information.
FSM tab	Provides details about the current FSM task running on the server, including the status of that task. You can use this information to diagnose errors with those tasks.
Statistics tab	Displays statistics about the server and its components. You can view these statistics in tabular or chart format.
Temperatures tab	Displays temperature statistics for the components of the server. You can view these statistics in tabular or chart format.
Power tab	Displays power statistics for the components of the server. You can view these statistics in tabular or chart format.

Step 5 In the **Navigation** pane, expand ***Server_ID*** ➤ **Interface Cards** ➤ ***Interface_Card_ID***.

Step 6 In the **Work** pane, right-click one or more of the following components of the interface card to open the navigator and view the status of the component:

- Interface card
- DCE interfaces
- HBAs
- NICs

Tip Expand the nodes in the table to view the child nodes. For example, if you expand a NIC node, you can view each VIF created on that NIC.

Monitoring a Rack-Mount Server

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Rack Mounts ➤ Servers**.

Step 3 Click the server that you want to monitor.

Step 4 In the **Work** pane, click one of the following tabs to view the status of the server:

Option	Description
General tab	Provides an overview of the status of the server, including a summary of any faults, a summary of the server properties, and a physical display of the server and its components.
Inventory tab	Provides details about the properties and status of the components of the server on the following subtabs: • **Motherboard**—Information about the motherboard and information about the server BIOS settings. You can also recover corrupt BIOS firmware from this subtab. • **CIMC**—Information about the CIMC and its firmware, and provides access to the SEL for the server. You can also assign a static or pooled management IP address, and update and activate the CIMC firmware from this subtab. • **CPU**—Information about each CPU in the server. • **Memory**—Information about each memory slot in the server and the DIMM in that slot. • **Interface cards**—Information about each adapter installed in the server. • **HBAs**—Properties of each HBA and the configuration of that HBA in the service profile associated with the server. • **NICs**—Properties of each NIC and the configuration of that NIC in the service profile associated with the server. You can expand each row to view information about the associated VIFs and vNICs. • **Storage**—Properties of the storage controller, the local disk configuration policy in the service profile associated with the server, and for each hard disk in the server. **Tip** If the server contains one or more SATA devices, such as a hard disk drive or solid state drive, Cisco UCS Manager GUI displays the vendor name for the SATA device in the **Vendor** field. However, Cisco UCS Manager CLI displays ATA in the **Vendor** field and includes the vendor information, such as the vendor name, in a **Vendor Description** field. This second field does not exist in Cisco UCS Manager GUI.

Option	Description
Virtual Machines tab	Displays details about any virtual machines hosted on the server.
Installed Firmware tab	Displays the firmware versions on the CIMC, adapters, and other server components. You can also use this tab to update and activate the firmware on those components.
Management Logs tab	Displays the system event log for the server.
VIF Paths tab	Displays the VIF paths for the adapters on the server.
Faults tab	Displays an overview of the faults generated by the server. You can click any fault to view additional information.
Events tab	Displays an overview of the events generated by the server. You can click any event to view additional information.
FSM tab	Provides details about the current FSM task running on the server, including the status of that task. You can use this information to diagnose errors with those tasks.
Statistics tab	Displays statistics about the server and its components. You can view these statistics in tabular or chart format.
Temperatures tab	Displays temperature statistics for the components of the server. You can view these statistics in tabular or chart format.
Power tab	Displays power statistics for the components of the server. You can view these statistics in tabular or chart format.

Step 5 In the **Navigation** pane, expand ***Server_ID*** ➤ **Interface Cards** ➤ ***Interface_Card_ID***.

Step 6 In the **Work** pane, right-click one or more of the following components of the interface card to open the navigator and view the status of the component:

- Interface card
- DCE interfaces
- HBAs
- NICs

Tip Expand the nodes in the table to view the child nodes. For example, if you expand a NIC node, you can view each VIF created on that NIC.

Monitoring an I/O Module

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ IO Modules**.

Step 3 Click the I/O module that you want to monitor.

Step 4 Click one of the following tabs to view the status of the I/O module:

Option	Description
General tab	Provides an overview of the status of the I/O module, including a summary of any faults, a summary of the module properties, and a physical display of the module and its components.
Fabric Ports tab	Displays the status and selected properties of all fabric ports in the I/O module.
Backplane Ports tab	Displays the status and selected properties of all backplane ports in the I/O module.
Faults tab	Provides details of faults generated by the I/O module.
Events tab	Provides details of events generated by the I/O module.
FSM tab	Provides details about and the status of FSM tasks related to the I/O module. You can use this information to diagnose errors with those tasks.
Statistics tab	Provides statistics about the I/O module and its components. You can view these statistics in tabular or chart format.

Monitoring Management Interfaces

Management Interfaces Monitoring Policy

This policy defines how the mgmt0 Ethernet interface on the fabric interconnect should be monitored. If Cisco UCS detects a management interface failure, a failure report is generated. If the configured number of failure reports is reached, the system assumes that the management interface is unavailable and generates a fault. By default, the management interfaces monitoring policy is disabled.

If the affected management interface belongs to a fabric interconnect which is the managing instance, Cisco UCS confirms that the subordinate fabric interconnect's status is up, that there are no current failure reports logged against it, and then modifies the managing instance for the end-points.

If the affected fabric interconnect is currently the primary inside of a high availability setup, a failover of the management plane is triggered. The data plane is not affected by this failover.

You can set the following properties related to monitoring the management interface:

- Type of mechanism used to monitor the management interface.
- Interval at which the management interface's status is monitored.
- Maximum number of monitoring attempts that can fail before the system assumes that the management is unavailable and generates a fault message.

Important In the event of a management interface failure on a fabric interconnect, the managing instance may not change if one of the following occurs:

- A path to the end-point through the subordinate fabric interconnect does not exist.
- The management interface for the subordinate fabric interconnect has failed.
- The path to the end-point through the subordinate fabric interconnect has failed.

Configuring the Management Interfaces Monitoring Policy

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Management**.

Step 3 Click **Management Interfaces**.

Step 4 In the **Work** pane, click the **Management Interfaces Monitoring Policy** tab.

Step 5 Complete the following fields:

Name	Description
Admin Status field	Whether the monitoring policy is enabled or disabled for the management interfaces.
Poll Interval field	The number of seconds the system should wait between data recordings. Enter an integer between 90 and 300.
Max Fail Report Count field	The maximum number of monitoring attempts that can fail before the system assumes that the management interface is unavailable and generates a fault message.
Monitoring Mechanism field	The type of monitoring you want the system to use. You can select: • **MII Status**—The system monitors the availability of the Media Independent Interface (MII). If you select this option, Cisco UCS Manager GUI displays the **Media Independent Interface Monitoring** area. • **Ping ARP Targets**—The system pings designated targets using the Address Resolution Protocol (ARP). If you select this option,

Name	Description
	Cisco UCS Manager GUI displays the **ARP Target Monitoring** area. • **Ping Gateway**—The system pings the default gateway address specified for this Cisco UCS instance on the **Management Interfaces** tab. If you select this option, Cisco UCS Manager GUI displays the **Gateway Ping Monitoring** area.

Step 6 If you chose **MII Status** for the monitoring mechanism, complete the following fields in the **Media Independent Interface Monitoring** area:

Name	Description
Retry Interval field	The number of seconds the system should wait before requesting another response from the MII if a previous attempt fails. Enter an integer between 3 and 10.
Max Retry Count field	The number of times the system polls the MII until the system assumes the interface is unavailable. Enter an integer between 1 and 3.

Step 7 If you chose **Ping ARP Targets** for the monitoring mechanism, complete the following fields in the **ARP Target Monitoring** area:

Name	Description
Target IP 1 field	The first IP address the system pings.
Target IP 2 field	The second IP address the system pings.
Target IP 3 field	The third IP address the system pings.
Number of ARP Requests field	The number of ARP requests to send to the target IP addresses. Enter an integer between 1 and 5.
Max Deadline Timeout field	The number of seconds to wait for responses from the ARP targets until the system assumes they are unavailable. Enter an integer between 5 and 15.

Type 0.0.0.0 to remove the ARP target.

Step 8 If you chose **Ping Gateway** for the monitoring mechanism, complete the following fields in the **Gateway Ping Monitoring** area:

Name	Description
Number of Ping Requests field	The number of times the system should ping the gateway. Enter an integer between 1 and 5.

Name	Description
Max Deadline Timeout field	The number of seconds to wait for a response from the gateway until the system assumes the address is unavailable. Enter an integer between 5 and 15.

Step 9 Click **Save Changes**.

CHAPTER 47

Configuring Statistics-Related Policies

This chapter includes the following sections:

Configuring Statistics Collection Policies

Statistics Collection Policy

A statistics collection policy defines how frequently statistics are to be collected (collection interval) and how frequently the statistics are to be reported (reporting interval). Reporting intervals are longer than collection intervals so that multiple statistical data points can be collected during the reporting interval, which provides Cisco UCS Manager with sufficient data to calculate and report minimum, maximum, and average values.

For NIC statistics, Cisco UCS Manager displays the average, minimum, and maximum of the change since the last collection of statistics. If the values are 0, there has been no change since the last collection.

Statistics can be collected and reported for the following five functional areas of the Cisco UCS system:

- Adapter—statistics related to the adapters
- Chassis—statistics related to the blade chassis
- Host—this policy is a placeholder for future support
- Port—statistics related to the ports, including server ports, uplink Ethernet ports, and uplink Fibre Channel ports
- Server—statistics related to servers

Note Cisco UCS Manager has one default statistics collection policy for each of the five functional areas. You cannot create additional statistics collection policies and you cannot delete the existing default policies. You can only modify the default policies.

Modifying a Statistics Collection Policy

Note Cisco UCS Manager has one default statistics collection policy for each of the five functional areas. You cannot create additional statistics collection policies and you cannot delete the existing default policies. You can only modify the default policies.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Stats Management ➤ Stats**.

Step 3 Right-click the policy that you want to modify and select **Modify Collection Policy**.

Step 4 In the **Modify Collection Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the collection policy. This name is assigned by Cisco UCS and cannot be changed.
Collection Interval field	The length of time the fabric interconnect should wait between data recordings. This can be: • **30 Seconds** • **1 Minute** • **2 Minutes** • **5 Minutes**
Reporting Interval field	The length of time the fabric interconnect should wait before sending any data collected for the counter to Cisco UCS Manager GUI. This can be: • **2 Minutes** • **15 Minutes** • **30 Minutes** • **60 Minutes** • **2 Hours** • **4 Hours** • **8 Hours** When this time has elapsed, the fabric interconnect groups all data collected since the last time it sent information to Cisco UCS Manager GUI, and it extracts four pieces of information from that group and sends them to Cisco UCS Manager GUI:

Name	Description
	• The most recent statistic collected • The average of this group of statistics • The maximum value within this group • The minimum value within this group For example, if the collection interval is set to 1 minute and the reporting interval is 15 minutes, the fabric interconnect collects 15 samples in that 15 minute reporting interval. Instead of sending 15 statistics to Cisco UCS Manager GUI, it sends only the most recent recording along with the average, minimum, and maximum values for the entire group.
States Section	
Current Task field	This field shows the task that is executing on behalf of this component. For details, see the associated **FSM** tab. **Note** If there is no current task, this field is not displayed.

Step 5 Click **OK**.

Configuring Statistics Threshold Policies

Statistics Threshold Policy

A statistics threshold policy monitors statistics about certain aspects of the system and generates an event if the threshold is crossed. You can set both minimum and maximum thresholds. For example, you can configure the policy to raise an alarm if the CPU temperature exceeds a certain value, or if a server is overutilized or underutilized.

These threshold policies do not control the hardware or device-level thresholds enforced by endpoints, such as the CIMC. Those thresholds are burned in to the hardware components at manufacture.

Cisco UCS enables you to configure statistics threshold policies for the following components:

- Servers and server components
- Uplink Ethernet ports
- Ethernet server ports, chassis, and fabric interconnects
- Fibre Channel port

Note You cannot create or delete a statistics threshold policy for Ethernet server ports, uplink Ethernet ports, or uplink Fibre Channel ports. You can only configure the existing default policy.

Creating a Server and Server Component Threshold Policy

Tip This procedure documents how to create a server and server component threshold policy on the **Server** tab. You can also create and configure these threshold policies within the appropriate organization in the **Policies** node on the **LAN** tab, **SAN** tab, and under the **Stats Management** node of the **Admin** tab.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **Threshold Policies** and choose **Create Threshold Policy**.

Step 5 In the **Define Name and Description** page of the **Create Threshold Policy** wizard, do the following:

a) Complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).

b) Click **Next**.

Step 6 In the **Threshold Classes** page of the **Create Threshold Policy** wizard, do the following:

a) Click **Add**.

b) In the **Choose Statistics Class** dialog box, choose the statistics class for which you want to configure a custom threshold from the **Stat Class** drop-down list.

c) Click **Next**.

Step 7 In the **Threshold Definitions** page, do the following:

a) Click **Add**.
The **Create Threshold Definition** dialog box opens.

b) From the **Property Type** field, choose the threshold property that you want to define for the class.
c) In the **Normal Value** field, enter the desired value for the property type.
d) In the **Alarm Triggers (Above Normal Value)** fields, check one or more of the following check boxes:

- **Critical**
- **Major**
- **Minor**
- **Warning**
- **Condition**
- **Info**

e) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.
f) In the **Alarm Triggers (Below Normal Value)** fields, check one or more of the following check boxes:

- **Info**
- **Condition**
- **Warning**
- **Minor**
- **Major**
- **Critical**

g) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.
h) Click **Finish Stage**.
i) Do one of the following:

- To define another threshold property for the class, repeat Step 7.
- If you have defined all required properties for the class, click **Finish Stage**.

Step 8 In the **Threshold Classes** page of the **Create Threshold Policy** wizard, do one the following:

- To configure another threshold class for the policy, repeat Steps 6 and 7.
- If you have configured all required threshold classes for the policy, click **Finish**.

Step 9 Click **OK**.

Adding a Threshold Class to an Existing Server and Server Component Threshold Policy

Tip This procedure documents how to add a threshold class to a server and server component threshold policy in the **Server** tab. You can also create and configure these threshold policies within the appropriate organization in the **Policies** node on the **LAN** tab, **SAN** tab, and under the **Stats Management** node of the **Admin** tab.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers** ➤ **Policies** ➤ ***Organization_Name***.

Step 3 Expand the **Threshold Policies** node.

Step 4 Right-click the policy to which you want to add a threshold class and choose **Create Threshold Class**.

Step 5 In the **Choose Statistics Class** page of the **Create Threshold Class** wizard, do the following:

a) From the **Stat Class** drop-down list, choose the statistics class for which you want to configure a custom threshold.

b) Click **Next**.

Step 6 In the **Threshold Definitions** page, do the following:

a) Click **Add**.
The **Create Threshold Definition** dialog box opens.

b) From the **Property Type** field, choose the threshold property that you want to define for the class.

c) In the **Normal Value** field, enter the desired value for the property type.

d) In the **Alarm Triggers (Above Normal Value)** field, check one or more of the following check boxes:

- **Critical**
- **Major**
- **Minor**
- **Warning**
- **Condition**
- **Info**

e) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.

f) In the **Alarm Triggers (Below Normal Value)** field, check one or more of the following check boxes:

- **Info**
- **Condition**
- **Warning**
- **Minor**
- **Major**

- **Critical**

g) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.
h) Click **Finish Stage**.
i) Do one of the following:
   - To define another threshold property for the class, repeat Step 6.
   - If you have defined all required properties for the class, click **Finish Stage**.

Step 7 In the **Choose Statistics Class** page of the **Create Threshold Class** wizard, do one the following:
- To configure another threshold class for the policy, repeat Steps 5 and 6.
- If you have configured all required threshold classes for the policy, click **Finish**.

Step 8 Click **OK**.

Deleting a Server and Server Component Threshold Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.
Step 2 On the **Servers** tab, expand **Servers ➤ Policies ➤ *Organization_Name***.
Step 3 Expand the **Threshold Policies** node.
Step 4 Right-click the policy you want to delete and select **Delete**.
Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Adding a Threshold Class to the Uplink Ethernet Port Threshold Policy

Tip You cannot create an uplink Ethernet port threshold policy. You can only modify or delete the default policy.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.
Step 2 On the **LAN** tab, expand **LAN ➤ LAN Cloud**.
Step 3 Expand the **Threshold Policies** node.
Step 4 Right-click **Thr-policy-default** and choose the **Create Threshold Class**.
Step 5 In the **Choose Statistics Class** page of the **Create Threshold Class** wizard, do the following:

a) From the **Stat Class** drop-down list, choose the statistics class for which you want to configure a custom threshold.
b) Click **Next**.

Step 6 In the **Threshold Definitions** page, do the following:

a) Click **Add**.
The **Create Threshold Definition** dialog box opens.
b) From the **Property Type** field, choose the threshold property that you want to define for the class.
c) In the **Normal Value** field, enter the desired value for the property type.
d) In the **Alarm Triggers (Above Normal Value)** field, check one or more of the following check boxes:

- **Critical**
- **Major**
- **Minor**
- **Warning**
- **Condition**
- **Info**

e) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.
f) In the **Alarm Triggers (Below Normal Value)** field, check one or more of the following check boxes:

- **Info**
- **Condition**
- **Warning**
- **Minor**
- **Major**
- **Critical**

g) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.
h) Click **Finish Stage**.
i) Do one of the following:

- To define another threshold property for the class, repeat Step 6.
- If you have defined all required properties for the class, click **Finish Stage**.

Step 7 In the **Create Threshold Class** page of the **Create Threshold Policy** wizard, do one the following:

- To configure another threshold class for the policy, repeat Steps 5 and 6.
- If you have configured all required threshold classes for the policy, click **Finish**.

Adding a Threshold Class to the Ethernet Server Port, Chassis, and Fabric Interconnect Threshold Policy

Tip You cannot create an Ethernet server port, chassis, and fabric interconnect threshold policy. You can only modify or delete the default policy.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 In the **LAN** tab, expand **LAN ➤ Internal LAN**.

Step 3 Expand the **Threshold Policies** node.

Step 4 Right-click **Thr-policy-default** and choose the **Create Threshold Class**.

Step 5 In the **Choose Statistics Class** page of the **Create Threshold Class** wizard, do the following:

a) From the **Stat Class** drop-down list, choose the statistics class for which you want to configure a custom threshold.

b) Click **Next**.

Step 6 In the **Threshold Definitions** page, do the following:

a) Click **Add**.
The **Create Threshold Definition** dialog box opens.

b) From the **Property Type** field, choose the threshold property that you want to define for the class.

c) In the **Normal Value** field, enter the desired value for the property type.

d) In the **Alarm Triggers (Above Normal Value)** field, check one or more of the following check boxes:

- **Critical**
- **Major**
- **Minor**
- **Warning**
- **Condition**
- **Info**

e) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.

f) In the **Alarm Triggers (Below Normal Value)** field, check one or more of the following check boxes:

- **Info**
- **Condition**
- **Warning**
- **Minor**
- **Major**
- **Critical**

g) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.
h) Click **Finish Stage**.
i) Do one of the following:

- To define another threshold property for the class, repeat Step 6.
- If you have defined all required properties for the class, click **Finish Stage**.

Step 7 In the **Create Threshold Class** page of the **Create Threshold Policy** wizard, do one the following:

- To configure another threshold class for the policy, repeat Steps 5 and 6.
- If you have configured all required threshold classes for the policy, click **Finish**.

Adding a Threshold Class to the Fibre Channel Port Threshold Policy

You cannot create a Fibre Channel port threshold policy. You can only modify or delete the default policy.

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.
Step 2 On the **SAN** tab, expand **SAN ➤ SAN Cloud**.
Step 3 Expand the **Threshold Policies** node.
Step 4 Right-click **Thr-policy-default** and choose the **Create Threshold Class**.
Step 5 In the **Choose Statistics Class** page of the **Create Threshold Class** wizard, do the following:
a) From the **Stat Class** drop-down list, choose the statistics class for which you want to configure a custom threshold.
b) Click **Next**.
Step 6 In the **Threshold Definitions** page, do the following:
a) Click **Add**.
The **Create Threshold Definition** dialog box opens.
b) From the **Property Type** field, choose the threshold property that you want to define for the class.
c) In the **Normal Value** field, enter the desired value for the property type.
d) In the **Alarm Triggers (Above Normal Value)** field, check one or more of the following check boxes:

- **Critical**
- **Major**
- **Minor**
- **Warning**
- **Condition**
- **Info**

e) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.
f) In the **Alarm Triggers (Below Normal Value)** field, check one or more of the following check boxes:

- **Info**
- **Condition**
- **Warning**
- **Minor**
- **Major**
- **Critical**

g) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.
h) Click **Finish Stage**.
i) Do one of the following:

- To define another threshold property for the class, repeat Step 6.
- If you have defined all required properties for the class, click **Finish Stage**.

Step 7 In the **Create Threshold Class** page of the **Create Threshold Policy** wizard, do one the following:

- To configure another threshold class for the policy, repeat Steps 5 and 6.
- If you have configured all required threshold classes for the policy, click **Finish**.

CHAPTER 48

Configuring Call Home

This chapter includes the following sections:

Call Home

Call Home provides an email-based notification for critical system policies. A range of message formats are available for compatibility with pager services or XML-based automated parsing applications. You can use this feature to page a network support engineer, email a Network Operations Center, or use Cisco Smart Call Home services to generate a case with the Technical Assistance Center.

The Call Home feature can deliver alert messages containing information about diagnostics and environmental faults and events.

The Call Home feature can deliver alerts to multiple recipients, referred to as Call Home destination profiles. Each profile includes configurable message formats and content categories. A predefined destination profile is provided for sending alerts to the Cisco TAC, but you also can define your own destination profiles.

When you configure Call Home to send messages, Cisco UCS Manager executes the appropriate CLI **show** command and attaches the command output to the message.

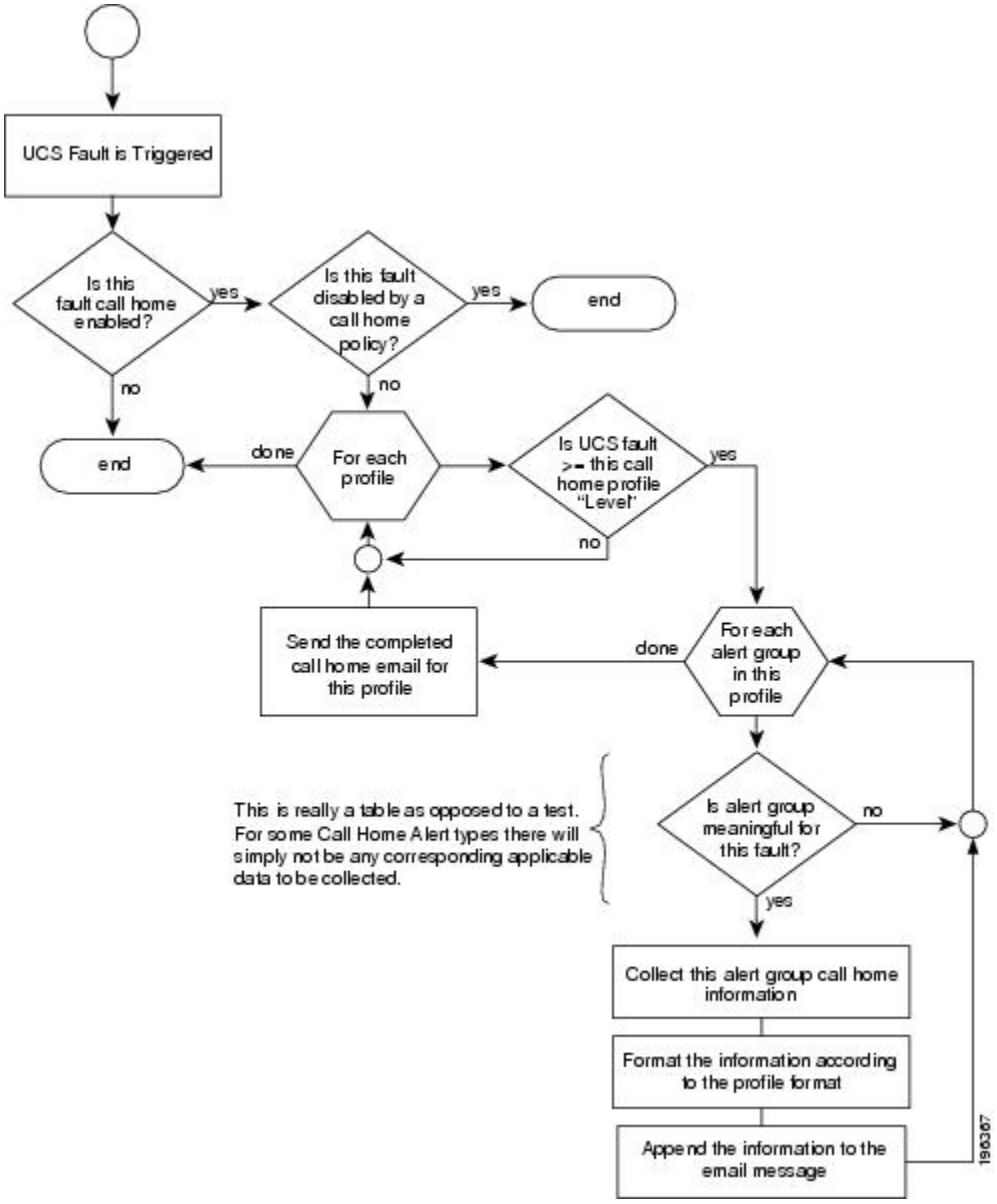
Cisco UCS delivers Call Home messages in the following formats:

- Short text format which provides a one or two line description of the fault that is suitable for pagers or printed reports.
- Full text format which provides fully formatted message with detailed information that is suitable for human reading.
- XML machine readable format that uses Extensible Markup Language (XML) and Adaptive Messaging Language (AML) XML schema definition (XSD). The AML XSD is published on the Cisco.com website at http://www.cisco.com/. The XML format enables communication with the Cisco Systems Technical Assistance Center.

For information about the faults that can trigger Call Home email alerts, see the *Cisco UCS Faults Reference*.

The following figure shows the flow of events after a Cisco UCS is triggered in a system with Call Home configured:

Figure 4: Flow of Events after a Fault is Triggered



Call Home Considerations and Guidelines

How you configure Call Home depends on how you intend to use the feature. The information you need to consider before you configure Call Home includes the following:

Destination Profile

You must configure at least one destination profile. The destination profile or profiles that you use depend upon whether the receiving entity is a pager, email, or automated service such as Cisco Smart Call Home.

If the destination profile uses email message delivery, you must specify a Simple Mail Transfer Protocol (SMTP) server when you configure Call Home.

Contact Information

The contact email, phone, and street address information should be configured so that the receiver can determine the origin of messages received.

IP Connectivity to Email Server or HTTP Server

The fabric interconnect must have IP connectivity to an email server or the destination HTTP server. In a cluster configuration, both fabric interconnects must have IP connectivity. This connectivity ensures that the current, active fabric interconnect can send Call Home email messages. The source of these email messages is always the IP address of a fabric interconnect. The virtual IP address assigned Cisco UCS Manager in a cluster configuration is never the source of the email.

Smart Call Home

If Cisco Smart Call Home is used, the following are required:

- An active service contract must cover the device being configured
- The customer ID associated with the Smart Call Home configuration in Cisco UCS must be the CCO (Cisco.com) account name associated with a support contract that includes Smart Call Home

Cisco UCS Faults and Call Home Severity Levels

Because Call Home is present across several Cisco product lines, Call Home has developed its own standardized severity levels. The following table describes how the underlying Cisco UCS fault levels map to the Call Home severity levels. You need to understand this mapping when you configure the Level setting for Call Home profiles.

Table 9: Mapping of Faults and Call Home Severity Levels

Call Home Severity	Cisco UCS Fault	Call Home Meaning
(9) Catastrophic	N/A	Network-wide catastrophic failure.
(8) Disaster	N/A	Significant network impact.
(7) Fatal	N/A	System is unusable.
(6) Critical	Critical	Critical conditions, immediate attention needed.
(5) Major	Major	Major conditions.
(4) Minor	Minor	Minor conditions.

Call Home Severity	Cisco UCS Fault	Call Home Meaning
(3) Warning	Warning	Warning conditions.
(2) Notification	Info	Basic notifications and informational messages. Possibly independently insignificant.
(1) Normal	Clear	Normal event, signifying a return to normal state.
(0) debug	N/A	Debugging messages.

Cisco Smart Call Home

Cisco Smart Call Home is a web application which leverages the Call Home feature of Cisco UCS. Smart Call Home offers proactive diagnostics and real-time email alerts of critical system events, which results in higher network availability and increased operational efficiency. Smart Call Home is a secure connected service offered by Cisco Unified Computing Support Service and Cisco Unified Computing Mission Critical Support Service for Cisco UCS.

Note Using Smart Call Home requires the following:

- A CCO ID associated with a corresponding Cisco Unified Computing Support Service or Cisco Unified Computing Mission Critical Support Service contract for your company.
- Cisco Unified Computing Support Service or Cisco Unified Computing Mission Critical Support Service for the device to be registered.

You can configure and register Cisco UCS Manager to send Smart Call Home email alerts to either the Smart Call Home System or the secure Transport Gateway. Email alerts sent to the secure Transport Gateway are forwarded to the Smart Call Home System using HTTPS.

Note For security reasons, we recommend using the Transport Gateway option. The Transport Gateway can be downloaded from Cisco.

To configure Smart Call Home, you must do the following:

- Enable the Smart Call Home feature.
- Configure the contact information.
- Configure the email information.
- Configure the SMTP server information.
- Configure the default CiscoTAC-1 profile.
- Send a Smart Call Home inventory message to start the registration process.

- Ensure that the CCO ID you plan to use as the Call Home Customer ID for the Cisco UCS instance has the contract numbers from the registration added to its entitlements. You can update the ID in the account properties under Additional Access in the Profile Manager on CCO.

Configuring Call Home

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.

Step 3 Click **Call Home**.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Admin** area, do the following to enable Call Home:

a) In the **State** field, click **on**.

Note If this field is set to **on**, Cisco UCS Manager GUI displays the rest of the fields on this tab.

b) From the **Switch Priority** drop-down list, select one of the following levels:

- **alerts**
- **critical**
- **debugging**
- **emergencies**
- **errors**
- **information**
- **notifications**
- **warnings**

For a large Cisco UCS deployment with several pairs of fabric interconnects, this field enables you to attach significance to messages from one particular Cisco UCS instance, so that message recipients can gauge the priority of the message. This field may not be as useful for a small Cisco UCS deployment, such as a single Cisco UCS instance.

Step 6 In the **Contact Information** area, complete the following fields with the required contact information:

Name	Description
Contact field	The main Call Home contact person.
Phone field	The telephone number for the main contact. Enter the number in international format, starting with a + (plus sign) and a country code.
Email field	The email address for the main contact.

Name	Description
Address field	The mailing address for the main contact.

Step 7 In the **Ids** area, complete the following fields with the identification information that Call Home should use:

Tip If you are not configuring Smart Call Home, this step is optional.

Name	Description
Customer Id field	The CCO ID that includes the contract numbers for the support contract in its entitlements.
Contract Id field	The Call Home contract number for the customer.
Site Id field	The unique Call Home identification number for the customer site.

Step 8 In the **Email Addresses** area, complete the following fields with email information for Call Home alert messages:

Name	Description
From field	The email address that should appear in the From field on Call Home alert messages sent by the system.
Reply To field	The return email address that should appear in the From field on Call Home alert messages sent by the system.

Step 9 In the **SMTP Server** area, complete the following fields with information about the SMTP server where Call Home should send email messages:

Name	Description
Host field	The IP address or hostname of the SMTP server. **Note** If you use a hostname rather than an IP address, you must configure a DNS server in Cisco UCS Manager.
Port field	The port number the system should use to talk to the SMTP server.

Step 10 Click **Save Changes**.

Disabling Call Home

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.

Step 3 Click **Call Home**.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Admin** area, click **off** in the **State** field.

Note If this field is set to **off**, Cisco UCS Manager hides the rest of the fields on this tab.

Step 6 Click **Save Changes**.

Enabling Call Home

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.

Step 3 Click **Call Home**.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Admin** area, click **on** in the **State** field.

Note If this field is set to **on**, Cisco UCS Manager GUI displays the rest of the fields on this tab.

Step 6 Click **Save Changes**.

What to Do Next

Ensure that Call Home is fully configured.

Configuring System Inventory Messages

Configuring System Inventory Messages

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.

Step 3 Click **Call Home**.

Step 4 In the **Work** pane, click the **System Inventory** tab.

Step 5 In the **Properties** area, complete the following fields:

Name	Description
Send Periodically field	If this field is set to on, Cisco UCS sends the system inventory to the Call Home database. When the information is sent depends on the other fields in this area.
Send Interval field	The number of days that should pass between automatic system inventory data collection.
Hour of Day to Send field	The hour that the data should be sent using the 24-hour clock format.
Minute of Hour field	The number of minutes after the hour that the data should be sent.
Time Last Sent field	The date and time the information was last sent. **Note** This field is displayed after the first inventory has been sent.
Next Scheduled field	The date and time for the upcoming data collection. **Note** This field is displayed after the first inventory has been sent.

Step 6 Click **Save Changes**.

Sending a System Inventory Message

Use this procedure if you need to manually send a system inventory message outside of the scheduled messages.

Note The system inventory message is sent only to those recipients defined in CiscoTAC-1 profile.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.

Step 3 Click **Call Home**.

Step 4 In the **Work** pane, click the **System Inventory** tab.

Step 5 In the **Actions** area, click **Send System Inventory Now**.
Cisco UCS Manager immediately sends a system inventory message to the recipient configured for Call Home.

Configuring Call Home Profiles

Call Home Profiles

Call Home profiles determine which alert groups and recipients receive email alerts for events that occur at a specific severity. You can also use these profiles to specify the format of the alert for a specific set of recipients and alert groups.

By default, you must configure the Cisco TAC-1 profile. However, you can also create additional profiles to send email alerts to one or more specified groups when events occur at the level that you specify.

For example, you may want to configure two profiles for faults with a major severity:

- A profile that sends an alert to the Supervisor alert group in the short text format. Members of this group receive a one- or two-line description of the fault that they can use to track the issue.
- A profile that sends an alert to the CiscoTAC alert group in the XML format. Members of this group receive a detailed message in the machine readable format preferred by the Cisco Systems Technical Assistance Center.

Creating a Call Home Profile

By default, you must configure the Cisco TAC-1 profile. However, you can also create additional profiles to send email alerts to one or more specified groups when events occur at the level that you specify.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.

Step 3 Click **Call Home**.

Step 4 In the **Work** pane, click the **Profiles** tab.

Step 5 On the icon bar to the right of the table, click +.
If the + icon is disabled, click an entry in the table to enable it.

Step 6 In the **Create Call Home Profile** dialog box, complete the following information fields:

Name	Description
Name field	A user-defined name for this profile. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Level field	Cisco UCS faults that are greater than or equal to this level trigger the profile. This can be: • **critical** • **debug** • **disaster** • **fatal** • **major** • **minor** • **normal** • **notification** • **warning**
Alert Groups field	The group or groups that are alerted based on this Call Home profile. This can be one or more of the following: • **ciscoTac** • **diagnostic** • **environmental** • **inventory** • **license** • **lifeCycle** • **linecard** • **supervisor** • **syslogPort** • **system** • **test**

Step 7 In the **Email Configuration** area, complete the following fields to configure the email alerts:

Name	Description
Format field	This can be:

Name	Description
	• **xml**—A machine readable format that uses Extensible Markup Language (XML) and Adaptive Messaging Language (AML) XML schema definition (XSD). This format enables communication with the Cisco Systems Technical Assistance Center. • **fullTxt**—A fully formatted message with detailed information that is suitable for human reading. • **shortTxt**—A one or two line description of the fault that is suitable for pagers or printed reports.
Max Message Size field	The maximum message size that is sent to the designated Call Home recipients. The default is 1000000. For full-txt and xml messages, the maximum recommended size is 5000000. For short-txt messages, the maximum recommended size is 100000. For the CiscoTAC-1, the maximum message size must be 5000000.

Step 8 In the **Recipients** area, do the following to add one or more email recipients for the email alerts:

a) On the icon bar to the right of the table, click +.

b) In the **Add Email Recipients** dialog box, enter the email address to which Call Home alerts should be sent in the **Email** field.
After you save this email address, it can be deleted but it cannot be changed.

c) Click **OK**.

Step 9 Click **OK**.

Deleting a Call Home Profile

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.

Step 3 Click **Call Home**.

Step 4 In the **Work** pane, click the **Profiles** tab.

Step 5 Right-click the profile you want to delete and choose **Delete**.

Step 6 Click **Save Changes**.

Configuring Call Home Policies

Call Home Policies

Call Home policies determine whether or not Call Home alerts are sent for a specific type of fault or system event. By default, Call Home is enabled to send alerts for certain types of faults and system events. However, you can configure Cisco UCS not to process certain types.

To disable alerts for a type of fault or events, you must create a Call Home policy for that type, and you must first create a policy for that type and then disable the policy.

By default, Cisco UCS sends Call Home alerts for each of the following types of faults and system events:

- **association-failed**
- **configuration-failure**
- **connectivity-problem**
- **election-failure**
- **equipment-inaccessible**
- **equipment-inoperable**
- **equipment-problem**
- **fru-problem**
- **identity-unestablishable**
- **link-down**
- **management-services-failure**
- **management-services-unresponsive**
- **power-problem**
- **thermal-problem**
- **unspecified**
- **version-incompatible**
- **voltage-problem**

Configuring a Call Home Policy

Tip By default, all Call Home policies are enabled to ensure that email alerts are sent for all critical system events.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.

Step 3 Click **Call Home**.

Step 4 In the **Work** pane, click the **Policies** tab.

Step 5 On the icon bar to the right of the table, click +.
If the + icon is disabled, click an entry in the table to enable it.

Step 6 In the **Create Call Home Policy** dialog box, complete the following fields:

Name	Description
State field	If this field is **enabled**, the system uses this policy when an error matching the associated cause is encountered. Otherwise, the system ignores this policy even if a matching error occurs. By default, all policies are enabled.
Cause field	The event that triggers the alert. Each policy defines whether an alert is sent for one type of event. This can be: • **association-failed** • **configuration-failure** • **connectivity-problem** • **election-failure** • **equipment-inaccessible** • **equipment-inoperable** • **equipment-problem** • **fru-problem** • **identity-unestablishable** • **link-down** • **management-services-failure** • **management-services-unresponsive** • **power-problem** • **thermal-problem** • **unspecified** • **version-incompatible** • **voltage-problem**

Step 7 Click **OK**.

Step 8 Repeat Steps 6 and 7 if you want to configure a Call Home policy for a different type of fault or event.

Disabling a Call Home Policy

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.

Step 3 Click **Call Home**.

Step 4 In the **Work** pane, click the **Policies** tab.

Step 5 Click the policy that you want to disable and choose **Show Navigator**.

Step 6 In the **State** field, click **Disabled**.

Step 7 Click **OK**.

Enabling a Call Home Policy

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.

Step 3 Click **Call Home**.

Step 4 In the **Work** pane, click the **Policies** tab.

Step 5 Click the policy that you want to enable and choose **Show Navigator**.

Step 6 In the **State** field, click **Enabled**.

Step 7 Click **OK**.

Deleting a Call Home Policy

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.
Step 3 Click **Call Home**.
Step 4 In the **Work** pane, click the **Policies** tab.
Step 5 Right-click the policy that you want to disable and choose **Delete**.
Step 6 Click **Save Changes**.

Example: Configuring Call Home for Smart Call Home

Configuring Smart Call Home

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.
Step 3 Click **Call Home**.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Admin** area, do the following to enable Call Home:
a) In the **State** field, click **on**.
Note If this field is set to **on**, Cisco UCS Manager GUI displays the rest of the fields on this tab.
b) From the **Switch Priority** drop-down list, select one of the following urgency levels:
- **alerts**
- **critical**
- **debugging**
- **emergencies**
- **errors**
- **information**
- **notifications**
- **warnings**

Step 6 In the **Contact Information** area, complete the following fields with the required contact information:

Name	Description
Contact field	The main Call Home contact person.
Phone field	The telephone number for the main contact. Enter the number in international format, starting with a + (plus sign) and a country code.
Email field	The email address for the main contact.
Address field	The mailing address for the main contact.

Step 7 In the **Ids** area, complete the following fields with the Smart Call Home identification information:

Name	Description
Customer Id field	The CCO ID that includes the contract numbers for the support contract in its entitlements.
Contract Id field	The Call Home contract number for the customer.
Site Id field	The unique Call Home identification number for the customer site.

Step 8 In the **Email Addresses** area, complete the following fields with the email information for Smart Call Home alert messages:

Name	Description
From field	The email address that should appear in the From field on Call Home alert messages sent by the system.
Reply To field	The return email address that should appear in the From field on Call Home alert messages sent by the system.

Step 9 In the **SMTP Server** area, complete the following fields with information about the SMTP server that Call Home should use to send email messages:

Name	Description
Host field	The IP address or hostname of the SMTP server. **Note** If you use a hostname rather than an IP address, you must configure a DNS server in Cisco UCS Manager.
Port field	The port number the system should use to talk to the SMTP server.

Step 10 Click **Save Changes**.

Configuring the Default Cisco TAC-1 Profile

The following are the default settings for the CiscoTAC-1 profile:

- Level is normal
- Only the CiscoTAC alert group is selected
- Format is xml
- Maximum message size is 5000000

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.

Step 3 Click **Call Home**.

Step 4 In the **Work** pane, click the **Profiles** tab.

Step 5 Right-click the Cisco TAC-1 profile and choose **Recipient**.

Step 6 In the **Add Email Recipients** dialog box, do the following:

a) In the **Email** field, enter the email address to which Call Home alerts should be sent. For example, enter callhome@cisco.com.

After you save this email address, it can be deleted but it cannot be changed.

b) Click **OK**.

Configuring System Inventory Messages for Smart Call Home

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.

Step 3 Click **Call Home**.

Step 4 In the **Work** pane, click the **System Inventory** tab.

Step 5 In the **Properties** area, complete the following fields to specify how system inventory messages will be sent to Smart Call Home:

Name	Description
Send Periodically field	If this field is set to on, Cisco UCS sends the system inventory to the Call Home database. When the information is sent depends on the other fields in this area.
Send Interval field	The number of days that should pass between automatic system inventory data collection.

Name	Description
Hour of Day to Send field	The hour that the data should be sent using the 24-hour clock format.
Minute of Hour field	The number of minutes after the hour that the data should be sent.
Time Last Sent field	The date and time the information was last sent. **Note** This field is displayed after the first inventory has been sent.
Next Scheduled field	The date and time for the upcoming data collection. **Note** This field is displayed after the first inventory has been sent.

Step 6 Click **Save Changes**.

Registering Smart Call Home

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.

Step 3 Click **Call Home**.

Step 4 In the **Work** pane, click the **System Inventory** tab.

Step 5 In the **Actions** area, click **Send System Inventory Now** to start the registration process.

Step 6 When you receive the email response from Cisco, click the link in the email to complete registration for Smart Call Home.

CHAPTER 49

Managing the System Event Log

This chapter includes the following sections:

System Event Log

The system event log (SEL) resides on the CIMC in NVRAM. It records most server-related events, such as over and under voltage, temperature events, fan events, and events from BIOS. The SEL is mainly used for troubleshooting purposes.

SEL file is approximately 40KB in size, and no further events can be recorded when it is full. It must be cleared before additional events can be recorded.

You can use the SEL policy to backup the SEL to a remote server, and optionally clear the SEL after a backup operation occurs. Backup operations can be triggered based on specific actions, or they can occur at regular intervals. You can also manually backup or clear the SEL.

The backup file is automatically generated. The filename format is sel-*SystemName-ChassisID-ServerID-ServerSerialNumber-Timestamp*; for example, sel-UCS-A-ch01-serv01-QCI12522939-20091121160736.

Viewing the System Event Log for an Individual Server

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.

Step 3 Click the server for which you want to view the system event log.

Step 4 In the **Work** pane, click the **Management Logs** tab.
Cisco UCS Manager retrieves the system event log for the server and displays the the list of events.

Viewing the System Event Log for the Servers in a Chassis

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis_Name***.

Step 3 In the **Work** pane, click the **Management Logs** tab.

Step 4 In the Server table, click the server for which you want to view the system event log.
Cisco UCS Manager retrieves the system event log for the server and displays the the list of events.

Configuring the SEL Policy

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, click the **Equipment** node.

Step 3 In the **Work** pane, click the **Policies** tab.

Step 4 Click the **SEL Policy** subtab.

Step 5 (Optional) In the **General** area, type a description of the policy in the **Description** field.
The other fields in this area are read-only.

Step 6 In the **Backup Configuration** area, complete the following fields:

Name	Description
Protocol field	The protocol to use when communicating with the remote server. This can be:

Name	Description
	• **FTP** • **TFTP** • **SCP** • **SFTP**
Hostname field	The hostname or IP address of the server on which the backup configuration resides. If you use a hostname rather than an IP address, you must configure a DNS server in Cisco UCS Manager. **Note** The name of the backup file is generated by Cisco UCS. The name is in `sel-system-name-chchassis-id-servblade-id-blade-se`
Remote Path field	The absolute path to the file on the remote server, if required. If you use SCP, the absolute path is always required. If you use any other protocol, you may not need to specify a remote path if the file resides in the default download folder. For details about how your file server is configured, contact your system administrator.
Backup Interval drop-down list	The time to wait between automatic backups. This can be: • **Never**—Do not perform any automatic SEL data backups. • **1 Hour** • **2 Hours** • **4 Hours** • **8 Hours** • **24 Hours** **Note** If you want the system to create automatic backups, make sure you check the **Timer** check box in the **Action** option box.
Format field	The format to use for the backup file. This can be: • **ASCII** • **Binary**
Clear on Backup check box	If checked, Cisco UCS clears all system event logs after the backup.
User field	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP.
Password field	The password for the remote server username. This field does not apply if the protocol is TFTP.

Name	Description
Action option box	For each box that is checked, then the system creates a SEL backup when that event is encountered : • **Log Full**—The log reaches the maximum size allowed. • **On Change of Association**—The association between a server and its service profile changes. • **On Clear**—The user manually clears a system event log. • **Timer**—The time interval specified in the **Backup Interval** drop-down list is reached.

Step 7 Click **Save Changes**.

Managing the System Event Log for a Server

Copying One or More Entries in the System Event Log

This task assumes that you are viewing the system event log for a server from the **Management Logs** tab for a server or a chassis.

Procedure

Step 1 After Cisco UCS Manager GUI displays the system event log in the **Management Logs** tab, use your mouse to highlight the entry or entries that you want to copy from the system event log.

Step 2 Click **Copy** to copy the highlighted text to the clipboard.

Step 3 Paste the highlighted text into a text editor or other document.

Printing the System Event Log

This task assumes that you are viewing the system event log for a server from the **Management Logs** tab for a server or a chassis.

Procedure

Step 1 After Cisco UCS Manager GUI displays the system event log in the **Management Logs** tab, click **Print**.

Step 2 In the **Print** dialog box, do the following:

a) (Optional) Modify the default printer or any other fields or options.

b) Click **Print**.

Refreshing the System Event Log

This task assumes that you are viewing the system event log for a server from the **Management Logs** tab for a server or a chassis.

Procedure

After Cisco UCS Manager GUI displays the system event log in the **Management Logs** tab, click **Refresh**. Cisco UCS Manager retrieves the system event log for the server and displays the updated list of events.

Manually Backing Up the System Event Log

This task assumes that you are viewing the system event log for a server from the **Management Logs** tab for a server or a chassis.

Before You Begin

Configure the system event log policy. The manual backup operation uses the remote destination configured in the system event log policy.

Procedure

After Cisco UCS Manager GUI displays the system event log in the **Management Logs** tab, click **Backup**. Cisco UCS Manager backs up the system event log to the location specified in the SEL policy.

Manually Clearing the System Event Log

This task assumes that you are viewing the system event log for a server from the **Management Logs** tab for a server or a chassis.

Procedure

After Cisco UCS Manager GUI displays the system event log in the **Management Logs** tab, click **Clear**.

Note This action triggers an automatic backup if **Clear** is enabled in the SEL policy **Action** option box.

CHAPTER 50

Configuring Settings for Faults, Events, and Logs

This chapter includes the following sections:

Configuring Settings for the Fault Collection Policy

Fault Collection Policy

The fault collection policy controls the lifecycle of a fault in a Cisco UCS instance, including when faults are cleared, the flapping interval (the length of time between the fault being raised and the condition being cleared), and the retention interval (the length of time a fault is retained in the system).

A fault in Cisco UCS has the following lifecycle:

1. A condition occurs in the system and Cisco UCS Manager raises a fault. This is the active state.
2. When the fault is alleviated, it is cleared if the time between the fault being raised and the condition being cleared is greater than the flapping interval, otherwise, the fault remains raised but its status changes to soaking-clear. Flapping occurs when a fault is raised and cleared several times in rapid succession. During the flapping interval the fault retains its severity for the length of time specified in the fault collection policy.
3. If the condition reoccurs during the flapping interval, the fault remains raised and its status changes to flapping. If the condition does not reoccur during the flapping interval, the fault is cleared.
4. When a fault is cleared, it is deleted if the clear action is set to delete, or if the fault was previously acknowledged; otherwise, it is retained until either the retention interval expires, or if the fault is acknowledged.
5. If the condition reoccurs during the retention interval, the fault returns to the active state. If the condition does not reoccur, the fault is deleted.

Configuring the Fault Collection Policy

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All ➤ Faults, Events, and Audit Log**.

Step 3 Click **Settings**.

Step 4 In the **Work** pane, complete the following fields in the **Fault Collection Policy** area:

Name	Description
Flapping Interval field	Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, the system does not allow a fault to change its state until this amount of time has elapsed since the last state change. If the condition reoccurs during the flapping interval, the fault returns to the active state. If the condition does not reoccur during the flapping interval, the fault is cleared. What happens at that point depends on the setting in the **Clear Action** field. Enter an integer between 5 and 3,600. The default is 10.
Clear Action field	This can be: • **retain**—Cisco UCS Manager GUI displays the **Length of time to retain cleared faults** section. • **delete**—The system immediately deletes all fault messages as soon as they are marked as cleared.
Length of Time to Retain Cleared Faults Section	
Retention Interval field	This can be: • **forever**—The system leaves all cleared fault messages on the fabric interconnect regardless of how long they have been in the system. • **other**—Cisco UCS Manager GUI displays the **dd:hh:mm:ss** field.
dd:hh:mm:ss field	The number of days, hours, minutes, and seconds that should pass before the system deletes a cleared fault message.

Step 5 Click **Save Changes**.

Configuring Settings for the Core File Exporter

Core File Exporter

Cisco UCS Manager uses the Core File Exporter to export core files as soon as they occur to a specified location on the network through TFTP. This functionality allows you to export the tar file with the contents of the core file.

Configuring the Core File Exporter

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All ➤ Faults, Events, and Audit Log**.

Step 3 Click **Settings**.

Step 4 In the **Work** pane, complete the following fields in the **TFTP Core Exporter** area:

Name	Description
Admin State field	This can be: • **enabled**—If an error causes the server to perform a core dump, the system sends the core dump file via FTP to a given location. When this option is selected, Cisco UCS Manager GUI displays the other fields in this area that enable you to specify the FTP export options. • **disabled**—Core dump files are not automatically exported.
Description field	A user-defined description of the core file.
Port field	The port number to use when exporting the core dump file via TFTP.
Hostname field	The hostname or IP address to connect with via TFTP. **Note** If you use a hostname rather than an IP address, you must configure a DNS server in Cisco UCS Manager.
Path field	The path to use when storing the core dump file on the remote system.

Step 5 Click **Save Changes**.

Disabling the Core File Exporter

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, expand **All ➤ Faults, Events, and Audit Log**.
Step 3 Click **Settings**.
Step 4 In the **Work** pane, click the **Settings** tab.
Step 5 In the **TFTP Core Exporter** area, click the **disabled** radio button in the **Admin State** field.
Step 6 Click **Save Changes**.

Configuring the Syslog

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, expand **All ➤ Faults, Events, and Audit Log**.
Step 3 Click **Syslog**.
Step 4 In the **Work** pane, click the **Syslog** tab.
Step 5 In the **Local Destinations** area, complete the following fields:

Name	Description
Console Section	
Admin State field	This can be: • **enabled** • **disabled**
Level field	If the **Admin State** field is **enabled**, select the lowest message level that you want displayed. The system displays that level and above on the console. • **emergencies** • **alerts** • **critical**
Monitor Section	
Admin State field	This can be:

Name	Description
	• **enabled** • **disabled** If **Admin State** is enabled, Cisco UCS Manager GUI displays the rest of the fields in this section.
Level drop-down list	If the **Admin State** field is **enabled**, select the lowest message level that you want displayed. The system displays that level and above on the monitor. • **emergencies** • **alerts** • **critical** • **errors** • **warnings** • **notifications** • **information** • **debugging**
File Section	
Admin State field	This can be: • **enabled** • **disabled** If **Admin State** is enabled, Cisco UCS Manager GUI displays the rest of the fields in this section.
Level drop-down list	Select the lowest message level that you want the system to store. The system stores that level and above in a file on the fabric interconnect. • **emergencies** • **alerts** • **critical** • **errors** • **warnings** • **notifications** • **information** • **debugging**

Name	Description
Name field	The name of the file in which the messages are logged. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or special characters.
Size field	The maximum size, in bytes, the file can be before Cisco UCS Manager GUI begins to write over the oldest messages with the newest ones. Enter an integer between 4096 and 4194304.

Step 6 In the **Remote Destinations** area, complete the following fields to configure up to three external logs that can store messages generated by the Cisco UCS components:

Name	Description
Admin State field	This can be: • **enabled** • **disabled** If **Admin State** is enabled, Cisco UCS Manager GUI displays the rest of the fields in this section.
Level drop-down list	Select the lowest message level that you want the system to store. The system stores that level and above in the remote file. • **emergencies** • **alerts** • **critical** • **errors** • **warnings** • **notifications** • **information** • **debugging**
Hostname field	The hostname or IP address on which the remote log file resides. **Note** If you use a hostname rather than an IP address, you must configure a DNS server in Cisco UCS Manager.
Facility drop-down list	This can be: • **local0** • **local1** • **local2** • **local3**

Name	Description
	• local4 • local5 • local6 • local7

Step 7 Click **Save Changes**.

INDEX

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z