Cisco UCS Manager GUI Configuration Guide, Release 1.2(1)

First Published: 03/31/2010

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:

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

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

Part	Title	Description
		authentication, and role-based access control configuration, and how to manage firmware 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, and service profiles, and how to install an OS on a server.
Part 6	System Management	Contains chapters that describe how to manage 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 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.

Convention	Indication
!, #	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 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 BMC
- 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 Cisco UCS CNA M71KR 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 Cisco UCS CNA M71KR has two HBAs, which means you can create a maximum of two vHBAs for each of those adapters. In contrast, a Cisco UCS 82598KR-CI 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

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 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 the Cisco UCS CNA M71KR adapters, 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.
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

This discovery policy determines how the system reacts when you add a new chassis. If you create a chassis discovery policy, Cisco UCS Manager configures the chassis for the number of links between the chassis and the fabric interconnect specified in the policy.

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 Cisco M81KR VIC adapters that host VMs and dynamic vNICs.

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

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 firmware images
- Storage controller firmware images
- Fibre Channel adapter firmware images
- BIOS firmware images
- HBA Option ROM firmware images

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 BMC. 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:

- **Any Configuration**—For a server configuration that carries forward the local disk configuration without any changes.
- **No Local Storage**—For a diskless workstation 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.
- **No RAID**—For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered.
- **RAID Mirrored**—For a 2-disk RAID 1 server configuration.
- **RAID Stripes**—For a 2-disk RAID 0 server configuration.

You must include this policy in a service profile, and that service profile must be associated with a server for it 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 only includes the baseboard management controller (BMC) on the server. You do not need to use this package if you upgrade the BMC directly.

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

This policy ensures that the BMC 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.

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.

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

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 Policies

QoS policies assign a system class to the outgoing traffic for a vNIC or vHBA. This system class determines the quality of service for that traffic.

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.

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.

f 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.

Depending upon the implementation, you may include server pool policy qualifications in the following policies:

- 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 Profiles

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

Scrub Policy

This policy determines what happens to local data on a server during the discovery process and when the server is disassociated from a service profile. This policy can ensure that the data on local drives is erased at those times.

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.

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 BMC. 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, is 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.

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 baseboard management controller (BMC) on a server.

Cisco UCS Manager uses the IP addresses in a management IP pool for external access to a server through the following:

- KVM console
- Serial over LAN
- IPMI

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:

The 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.

The number of uplink ports from the fabric interconnect to the 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.

The number of uplink ports from the I/O module to the 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.

The number of active links from the server to the 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.
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 1: 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.

Quality of Service Policies

QoS policies assign a system class to the outgoing traffic for a vNIC or vHBA. This system class determines the quality of service for that traffic.

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

In Cisco UCS, you can use multi-tenancy 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

The 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 adapter. The Cisco M81KR 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 the Cisco UCS CNA M71KR and Cisco UCS 82598KR-CI Adapters

The Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter, Cisco UCS M71KR - E Emulex Converged Network Adapter, and Cisco UCS M71KR - Q QLogic Converged Network Adapter support virtualized environments with the following VMware versions:

- VMware 3.5 update 4
- VMware 4.0

These environments support 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, quality of service 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 the Cisco M81KR VIC Adapter

The Cisco M81KR VIC adapter supports virtualized environments with VMware 4.0 Update 1. 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 the Cisco M81KR VIC adapter, how communication works depends upon which solution you choose. This 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

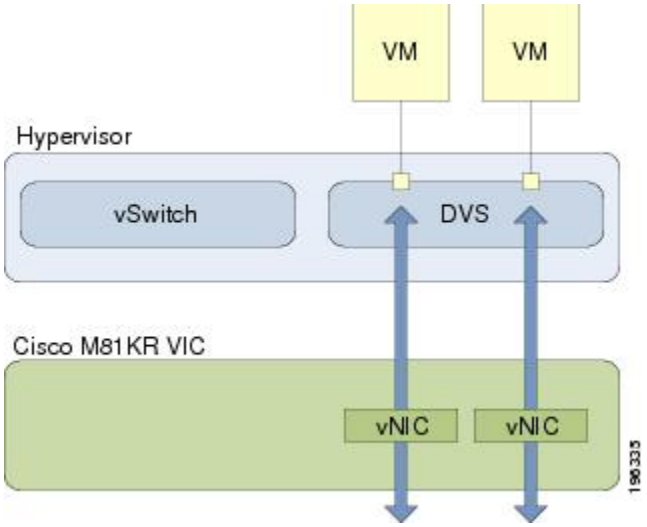
Cisco VN-Link in hardware is a hardware-based method of handling traffic to and from a virtual machine on a server with a Cisco M81KR VIC adapter. This method is sometimes referred to as pass-through switching. This solution replaces software-based switching with ASIC-based hardware switching and improves performance.

The distributed virtual switch (DVS) framework delivers VN-Link in hardware features and capabilities for virtual machines on Cisco UCS servers with Cisco M81KR 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 Cisco M81KR 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 Cisco M81KR 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 along side 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 consistent 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 new 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 service 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

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 Ethernet NICs and Fibre Channel HBAs
- 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 the Cisco M81KR 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

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

- Cards
- Slots
- 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 Cluster Environment

In a cluster Cisco UCS instance 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.

The following table describes the tabs in the **Navigation** pane:

Tab name	Description
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.
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.

Tab name	Description
LAN tab	This tab contains the components related to LAN configuration, such as LAN pin groups, quality of service classes, VLANs, policies, pools, the internal domain, and VM systems. A network administrator typically accesses and manages the components on this tab.
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.
VM tab	This tab contains the components required to configure VN-Link in Hardware for servers with the Cisco M81KR 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.
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.

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.

Name	Description
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.
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 chassis, 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 On 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, enter your username and password.

Step 6 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, enter your username and password.

Step 4 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 setup 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.

Note The cluster configuration only provides redundancy 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 setup must be enabled for a cluster configuration, then when the second fabric interconnect is setup, 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

Tip After the initial configuration, you can change the management IP port and the related subnet mask in the Cisco UCS Manager CLI. You cannot make this change in the Cisco UCS Manager GUI.

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 with at least one capital letter and one number. 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. Use a strong password with at least one capital letter and one number. The 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 with at least one capital letter and one number. 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. Use a strong password with at least one capital letter and one number. The 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.

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 the 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 Switching Mode**
- **Set End-Host Mode**

The link for the current Ethernet switching 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.

Step 6 Launch Cisco UCS Manager GUI and log back in to continue configuring your system.

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.
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 displays 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.

Changing the Properties of a Fabric Interconnect

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 **Change System Name/IP Address**.

Step 5 In the **Properties for: UCS Manager** dialog box, change one or more of the following fields:

Name	Description
System Name field	The name assigned to this Cisco UCS system.
System IP Address field	The IP address assigned to the Cisco UCS Manager GUI.
HA Configuration field	How this system is configured for high availability. This can be: • **cluster** • **stand-alone**

Step 6 Click **OK**.

Step 7 Log out of Cisco UCS Manager GUI and log back in again to see your changes.

Changing Access to a Fabric Interconnect

In-band access cannot be changed from Cisco UCS Manager GUI.

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 **Change *Fabric_Interconnect_Name* Access**.

Step 5 In the **Properties for: *Fabric_Interconnect_Name*** dialog box, click the **Communication Services** tab.

Step 6 Change one or more of 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 7 Click **OK**.

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.

	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. 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 Ports** 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.

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

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

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.

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 for the purpose of providing 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 **Add Ports**.

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.
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 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**.

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 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 to which you want to add ports.
Step 4 Right-click the port channel and choose **Add Ports**.
Step 5 In the **Add Ports** dialog box:
a) In the **Ports** table, chose one or more ports to include 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.
c) Click **Finish**.

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**.
Step 3 Expand ***Fabric_Interconnect_Name*** **➤ Port Channels ➤** ***Port_Channel_ID*** .
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 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**.

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.
HTTPS	This service is enabled on port 443 by default. You must enable either HTTP or HTTPS to run Cisco UCS Manager GUI. If you select HTTPS, all data is exchanged in encrypted mode through a secure server.

Communication Service	Description
	For security purposes, we recommend that you enable HTTPS and disable HTTP.
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. Only enable this service 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 Select 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 will use for HTTP.
The default port is 80.

Step 6 Click **Save Changes**.

Configuring HTTPS

Creating a Key Ring

Procedure

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

Step 2 On the **Admin** tab, expand **All ➤ Key Management ➤ Root**.

Step 3 Right-click **Root** 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:

- **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 ➤ Root**.

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 ➤ Root**.

Step 3 Right-click **Root** 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.
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 ➤ Root**.

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

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 will use for HTTPS. The default port is 443.

Step 6 (Optional) In the **Key Ring** field, enter the name of the key ring you created for HTTPS.

Caution If you update the **Key Ring** field, all current HTTP and HTTPS sessions will be closed without warning after you click **Save Changes**.

Step 7 Click **Save Changes**.

Step 8 Click **OK**.

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 ➤ Root**.

Step 3 Right-click the key ring you want to delete and select **Delete**.

Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Deleting a Trusted Point

Procedure

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

Step 2 On the **Admin** tab, expand **All ➤ Key Management ➤ Root**.

Step 3 Right-click the trusted point 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**.

Configuring SNMP

Enabling SNMP

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 In the **Community** field, enter the default community name that Cisco UCS Manager GUI should include with any trap messages it sends to the SNMP server.
The default community is public.

Step 6 Click **Save Changes**.

Configuring Trap Hosts

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 the fabric interconnect should send the trap.
Community field	The community name the fabric interconnect includes when it sends the trap to the SNMP host. This must be the same community as you configured for the SNMP service. Enter an alphanumeric string between 1 and 32 characters.
Port field	The port on which the fabric interconnect communicates with the SNMP host. The default port is 162.

Step 6 Click **OK**.

Step 7 Click **Save Changes**.

Configuring SNMPv3 users

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.
Auth Type field	The authorization type. This can be: • **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**.

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 Primary Authentication

This chapter includes the following sections:

Primary Authentication

Cisco UCS supports two methods to authenticate user logins:

- Local to Cisco UCS Manager
- Remote through one of the following protocols:
  - LDAP
  - RADIUS
  - TACACS+

Note You can only use one authentication method. For example, if you select LDAP as your authentication provider, you cannot use RADIUS or TACACS+ for authentication. However, if the user account in the remote authentication provider does not have at least one Cisco UCS role, Cisco UCS Manager checks the local database to determine whether an account with the same name exists in the local database.

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

You can create user accounts 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. If an account does not have the required roles, the user is granted only read-only privileges.

User Attribute for LDAP

If a Cisco UCS instance uses LDAP as the remote authentication provider, you can do one of the following:

- Map an existing attribute to the user roles and locale for the Cisco UCS instance.
- Create a CiscoAVPair or other unique attribute in the LDAP service and map that attribute to the user roles and locale for the Cisco UCS instance.

You must configure the LDAP provider in Cisco UCS Manager with the attribute that holds the user roles and locales. When a user logs in, Cisco UCS Manager checks for the value of this attribute when it queries the remote authentication service and validates the user.

If you create a CiscoAVPair attribute for the Cisco UCS instance, use the following definition for the OID:

```
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
```

Required User Attribute for RADIUS and TACACS+

If a Cisco UCS instance uses either RADIUS or TACACS+ as the remote authentication provider, you must create a cisco-av-pair attribute in the remote authentication service and map that attribute to the user roles and locale for the Cisco UCS instance. When a user logs in, Cisco UCS Manager checks for the value of this attribute when it queries the remote authentication service and validates the user.

Note You cannot use any other attribute in RADIUS or TACAC+ for the Cisco UCS roles. You must create the attribute required for that specific remote authentication service.

Configuring LDAP Providers

Configuring Properties for LDAP Providers

The properties that you configure in this task apply to all LDAP provider connections defined in Cisco UCS Manager.

Procedure

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

Step 2 In the Admin tab, expand **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. The valid range is from 1 to 60 seconds. The default value is 5 seconds. This property is optional.
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 map an existing LDAP attribute to the Cisco UCS roles and locales, 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 **Note** If you do not specify this property, user access is restricted to read-only.
Base DN field	The specific distinguished name in the LDAP hierarchy where the server should begin a search when it receives an authorization request. The maximum supported string length is 128 characters. This property is required.
Filter field	If specified, the LDAP search is restricted to those usernames that match the defined filter. This property is optional.

Step 4 Click **Save Changes**.

What to Do Next

Create an LDAP provider.

Creating an LDAP Provider

Before You Begin

Perform the following configuration in the LDAP server:

- Configure users with the attribute that holds the user role and locale information for Cisco UCS Manager. You can use an existing LDAP attribute that is mapped to the Cisco UCS user roles and locales or create a custom attribute, such as the CiscoAVPair attribute, which has an attribute ID of 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 log-in requests are sourced from these IP addresses, not the virtual IP address used by Cisco UCS Manager.

If you have not already done so, configure the properties for the LDAP provider connections in Cisco UCS Manager.

Procedure

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

Step 2 In the Admin tab, expand **User Management ➤ LDAP**.

Step 3 In the **Actions** area of the **General** tab, click **Create LDAP Provider**.

Step 4 In the **Create LDAP Provider** dialog box:

a) Complete the following fields with the information about the LDAP service you want to use:

Name	Description
Hostname field	The hostname or IP address on which the LDAP 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 0 and 16.
Bind DN field	The distinguished name (DN) for the LDAP database superuser account. The maximum supported string length is 128 characters.
Port field	The port through which Cisco UCS communicates with the LDAP database.

Name	Description
Enable SSL check box	If checked, communications to the LDAP database require SSL encryption.
Key field	If **Enable SSL** is checked, the SSL encryption key for the database.
Confirm Key field	The SSL encryption key repeated for confirmation purposes.

b) Click **OK**.

Step 5 Click **Save Changes**.

What to Do Next

Select LDAP as the primary authentication service. For more information, see Selecting a Primary Authentication Service, page 89.

Deleting an LDAP Provider

Procedure

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

Step 2 In the **Admin** tab, expand **User Management ➤ LDAP** .

Step 3 Right-click the LDAP provider you want to delete and choose **Delete**.

Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring RADIUS Providers

Configuring Properties for RADIUS Providers

The properties that you configure in this task apply to all RADIUS provider connections defined in Cisco UCS Manager.

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 a value from 1 to 60 seconds. The default value is 5 seconds.
Retries field	The number of times to retry the connection before the re3quest is considered to have failed.

Step 4 Click **Save Changes**.

What to Do Next

Create a RADIUS provider.

Creating a RADIUS Provider

Before You Begin

Perform the following configuration in the RADIUS server:

- Create the cisco-av-pairs attribute. You cannot use an existing RADIUS attribute.
- 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 log-in requests are sourced from these IP addresses, not the virtual IP address used by Cisco UCS Manager.

If you have not already done so, configure the properties for the RADIUS provider connections in Cisco UCS Manager.

Procedure

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

Step 2 In the **Admin** tab, expand **User Management ➤ RADIUS** .

Step 3 In the **Actions** area of the **General** tab, click **Create RADIUS Provider**.

Step 4 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 0 and 16.

Name	Description
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.

b) Click **OK**.

Step 5 Click **Save Changes**.

What to Do Next

Select RADIUS as the primary authentication service. For more information, see Selecting a Primary Authentication Service, page 89.

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 Properties for TACACS+ Providers

The properties that you configure in this task apply to all RADIUS provider connections defined in Cisco UCS Manager.

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 a value from 1 to 60 seconds. The default is 5 seconds.

Step 4 Click **Save Changes**.

What to Do Next

Create an TACACS+ provider.

Creating a TACACS+ Provider

Before You Begin

Perform the following configuration in the TACACS+ server:

- Create the cisco-av-pairs attribute. You cannot use an existing TACACS+ attribute.
- 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 log-in requests are sourced from these IP addresses, not the virtual IP address used by Cisco UCS Manager.

If you have not already done so, configure the properties for the TACACS+ provider connections in Cisco UCS Manager.

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 **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 0 and 16.
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.

b) Click **OK**.

Step 5 Click **Save Changes**.

What to Do Next

Select TACACS as the primary authentication service. For more information, see Selecting a Primary Authentication Service, page 89.

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**.

Selecting a Primary Authentication Service

Before You Begin

If the system uses a remote authentication service, create a provider for that authentication service. If you chose console, 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 **User Management ➤ Authorization** .

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

Step 4 On the **General** tab, complete the following fields:

Name	Description
Console field	The method by which a user logging into the console is authenticated. This can be: • **ldap**—The user must be defined on the LDAP server specified for this Cisco UCS instance. • **local**—The user account must be defined locally in 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.

Name	Description
	• **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.
Default field	The default method by which a user is authenticated during remote login. This can be: • **ldap**—The user must be defined on the LDAP server specified for this Cisco UCS instance. • **local**—The user account must be defined locally in 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. • **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.
Role Policy for Remote Users field	The action to take when a user attempts to log in and the LDAP, RADIUS, or TACACS+ server does not supply a user role with the authentication information. This can be: • **no-login**—The user is not allowed to log into the system, even if the user name and password are correct. • **assign-default-role**—The user is allowed to log in with a read-only user role.

Step 5 Click **Save Changes**.

CHAPTER 8

Configuring Organizations

This chapter includes the following sections:

Organizations in a Multi-Tenancy Environment

In Cisco UCS, you can use multi-tenancy 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 an Organization that is not Root

Procedure

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

Step 2 In the **Servers** tab, navigate to the organization under which you want to create the organization.

Step 3 Right-click the organization under which you want to create the 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

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.

Guidelines for Usernames

The unique username for each user account cannot be all-numeric and cannot start with a number.

If an all-numeric username exists on an AAA server (RADIUS or TACACS+) and is entered during login, Cisco UCS Manager cannot log in the user. You cannot create a local user with an all-numeric username.

Guidelines for Passwords

For authentication purposes, a password is required for each user account. To prevent users from choosing insecure passwords, each password should meet the following requirements and guidelines:

- Must be least 8 characters long
- Must not contain more than 3 consecutive characters, such as abcd
- Must not contain more than 3 repeating characters, such as aaabbb
- Should not be based on standard dictionary words
- Should not contain common proper names
- Should contain at least 5 uppercase letters, such as N, or 5 lowercase letters, such as t, or a combination of both
- Should contain at least 2 numerical characters, such as 5
- Should contain at least 1 special character, such as $
- Should not be blank for local user accounts

If the Cisco UCS instance is configured to use remote authentication with LDAP, RADIUS, or TACACS+, passwords for those remote accounts can be blank. With this configuration, the remote credentials store is used just for authentication, not authorization. The definition of the local user role definition applies to the remotely authenticated user.

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.

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.

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.

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.
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.

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 cisco-av-pair vendor-specific 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.

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 2: 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
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
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

Privilege	Description	Default Role Assignment
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
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 Security 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.

Users with AAA Administrator 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.

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**.

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 Adding a Locale to a Locally Authenticated User Account, page 105.

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.

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. The login ID can contain between 1 and 32 characters, including the following: • Any alphabetic character • Any digit • _ (underscore) • - (dash) • @ After you save the user, the login ID cannot be changed. **Note** You can create up to 48 user accounts in a Cisco UCS instance.
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. The password must contain at least 8 characters and it must pass a basic strength check. A strong password contains a mix of the alphanumeric characters, including uppercase and lowercase letters. It can also contain special characters such as !, @, or #. Passwords cannot contain the characters $ (dollar sign) or ? (question mark).
Confirm Password field	The password a second time for confirmation purposes.
Password Expires check box	If checked, this password expires and must be changed on a given date.

Name	Description
Expiration Date field	If **Password Expires** is checked, this field specifies the date on which the password 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.

Step 5 In the **Roles** area, check one or more boxes to assign roles and privileges to the user account.

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**.

Adding a Locale to 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 ➤ 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, check the appropriate check boxes to assign the user to those locales.

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.

CHAPTER 10

Firmware Management

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 baseboard management controller (BMC)
- Endpoints physically located on adapters, including NIC and HBA firmware, and Option ROM (where applicable)
- I/O modules
- Fabric interconnects
- Cisco UCS Manager

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.

Image Management

Cisco delivers all firmware updates or packages to Cisco UCS components in images. These images can be the following:

- Component image, which contains the firmware for one component
- Package, which is a collection of component images

Cisco also provides release notes with each image, which you can obtain from the same website from which you obtained the image.

Cisco UCS Manager provides mechanisms to download both component images and packages to the fabric interconnect.

Image Headers

Every 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

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 packages 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 (were) in each downloaded package.
Images	The images view lists the component images available on the system. You cannot use this view to see packages. 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 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 BMC, 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 BMC for those servers through the firmware package.

Upgrades of a BMC 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

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.

Cannot Upgrade Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter

The firmware on the Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter (N20-AI0002) is burned into the hardware at manufacture. You cannot upgrade the firmware on this adapter.

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 BMC, I/O Modules, and Adapters

Each BMC, 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 recent activate. 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 BMC 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.

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
- BMC
- I/O modules
- Cisco UCS Manager
- Fabric interconnects

Note Upgrades of a BMC 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
- BMCs
- 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.

For Cisco UCS Manager and the fabric interconnects, only the activate stage occurs because the specified firmware image already exists on the fabric interconnect. During activation, 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.

Recommended Order of Components for Firmware Activation

If you upgrade firmware by individual components in a Cisco UCS instance, we recommend that you activate the updates in the required order for quicker activation and to avoid potential issues with conflicting firmware versions.

Recommended Order when Updating from Cisco UCS, Release 1.0(2)

1. Adapter (interface card)
2. BMC
3. I/O module
4. Cisco UCS Manager
5. Fabric interconnect

Recommended Order when Updating from Cisco UCS, Release 1.0(1)

1. Adapter (interface card)
2. BMC
3. I/O module
4. Fabric interconnect
5. Cisco UCS Manager

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 BMC Firmware Upgrade

When you upgrade the firmware for a BMC in a server, you impact only the BMC and internal processes. You do not interrupt server traffic. This firmware upgrade causes the following outage impacts and disruptions to the BMC:

- 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 firmware images
- Storage controller firmware images
- Fibre Channel adapter firmware images
- BIOS firmware images
- HBA Option ROM firmware images

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 only includes the baseboard management controller (BMC) on the server. You do not need to use this package if you upgrade the BMC directly.

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

This policy ensures that the BMC 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.

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.

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.

Downloading and Managing Images

Obtaining Images 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 Enter your Cisco.com username and password to log in.

Step 5 Click **Cisco Unified Computing System**.

Step 6 Click **Unified Computing System (UCS) Complete Software Bundle**.

Step 7 Under the **Latest Releases** folder, click the link for the latest release of Cisco UCS. Images for earlier releases are archived under the **All Releases** link.

Step 8 Click the Release Notes link to download the latest version of the Release Notes.

Step 9 Click one of the following buttons and follow the instructions provided:

- **Download Now**—Allows you to download the firmware image immediately
- **Add to Cart**—Adds the firmware image to your cart to be downloaded at a later time

Step 10 Follow the prompts to complete your download of the image.

Step 11 Read the Release Notes before upgrading Cisco UCS.

What to Do Next

Download the firmware image to the fabric interconnect.

Downloading Images to the Fabric Interconnect

Note In a cluster setup, the firmware image is downloaded to both fabric interconnects, regardless of which fabric interconnect is used to initiate the download. Cisco UCS Manager always keeps the 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 firmware images from Cisco.

Procedure

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

Step 2 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, 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** **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	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 firmware executable you want to download.
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.
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 GUI begins downloading the firmware bundle to the fabric interconnect.

Step 7 Click **OK**.

Step 8 (Optional) Monitor the status of the image download on the **Download Tasks** tab.

Note If Cisco UCS Manager reports that the bootflash is out of space, delete obsolete images 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.

What to Do Next

Update the firmware on the endpoints.

Determining the Contents of a Firmware Package

Procedure

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

Step 2 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.

Canceling an Image Download

You can cancel an image download only while it is in progress. After the image has downloaded, deleting the download task does not delete the image that was downloaded.

Procedure

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

Step 2 Expand the **Equipment** node.

Step 3 In the **Work** pane, select the **Firmware Management** tab.

Step 4 On the **Download Tasks** tab, right-click the task you want to cancel and select **Delete**.

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 from a Fabric Interconnect

You cannot delete firmware packages from the **Packages** tab. Cisco UCS Manager removes the packages after you have deleted all images in the package.

Before You Begin

We recommend that you determine the contents of a firmware package before you delete the package and its contents.

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**.

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 **dicovery-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**
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.

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
- BMCs
- 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 on 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 Firmware on a BMC

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 BMC.

Step 4 In the **General** tab, click the **Inventory** tab.

Step 5 Click the **BMC** 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**.

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 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 Firmware on a BMC

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 BMC for which you want to activate the updated firmware.

Step 4 On the **General** tab, click the **Inventory** tab.

Step 5 Click the **BMC** 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.
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 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**.
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 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.
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**.

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 disconnects all active sessions, logs out all users, and then activates the software. When the upgrade is complete, you are prompted to log back in.

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 then 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 Status** 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**

Field Name	Required Value
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 132 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 then 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 Status** 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 then 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

Creating a Host 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 **Host Firmware Packages** and select **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 Click the down arrows to expand one or more of the following sections on the left of the dialog box:

- **Adapter Firmware Packages**
- **Storage Controller Firmware Packages**
- **Fibre Channel Adapters Firmware Packages**
- **BIOS Firmware Packages**
- **HBA Option ROM Packages**

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.

Step 7 In each section for the endpoint to which you want to include firmware in the pack, do the following:

a) Select the line in the table which lists the firmware version that you want to add to the pack.
By default, the entries are sorted by vendor name. To sort the entries, click on a column heading.

b) Drag the line to the table on the right.

c) Click **Yes** to confirm that you selected the correct version.

Step 8 When you have added all the desired firmware to the pack, click **OK**.

What to Do Next

Include the policy in a service profile and/or template.

Updating a Host Firmware Pack

If the policy is included in one or more service profiles associated with a server, as soon as you save the host firmware package policy, Cisco UCS Manager updates and activates the firmware in the server and adapter with the new versions and reboots the server.

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 select the policy you want to update.

Step 5 In the table on the right, delete the existing entries for the firmware you want to update:

a) Select the line in the table for the firmware version that you want to change.
b) Right-click and select **Delete**.
c) Click **Yes** to confirm that you want to delete that entry.

Step 6 On the **General** tab, click the down arrows to expand one or more of the following sections on the left:

- **Adapter Firmware Packages**
- **Storage Controller Firmware Packages**
- **Fibre Channel Adapters Firmware Packages**
- **BIOS Firmware Packages**
- **HBA Option ROM Packages**

Step 7 In each section for the endpoint to which you want to include firmware in the pack:

a) Select the line in the table for the firmware version that you want to add to the pack.
By default, the entries are sorted by vendor name. To sort the entries, click on a column heading.
b) Drag the line to the table on the right.
c) Click **Yes** to confirm that you selected the correct version.

Step 8 Click **Save Changes**.

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 **BMC Firmware Packages** section on the left of the dialog box, do the following:

a) Click the down arrows to expand the section.
By default, the entries are sorted by vendor name. To sort the entries, click on a column heading.

b) Select the line in the table which lists the firmware version that you want to add to the package.
The firmware version must match the model numbers (PID) on the servers that are associated with this firmware pack. If you select a firmware version with the wrong model number, Cisco UCS Manager cannot install the firmware update.

c) Drag the line to the table on the right.

d) Click **Yes** to confirm that you selected the correct version.

Step 7 If you need to include BMC firmware for servers with different model numbers (PIDs) in this management firmware package, repeat Step 6.

Step 8 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 a one or more service profiles associated with a server, as soon as you save the management firmware package policy, Cisco UCS Manager updates and activates the BMC firmware in the server with the new version.

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 select the policy you want to update.

Step 5 In the table on the right, delete the existing entry for the firmware you want to update:

a) Select the line in the table for the firmware version that you want to change.
b) Right-click and select **Delete**.
c) Click **Yes** to confirm that you want to delete that entry.

Step 6 In the **BMC Firmware Packages** section on the left:

a) Click the down arrows to expand the section.
By default, the entries in a section are sorted by vendor name. To sort the entries, click on a column heading.

b) Select the line in the table which lists the firmware version that you want to add to the pack.
The firmware version must match the model numbers (PID) on the servers that are associated with this firmware pack. If you select a firmware version with the wrong model number, Cisco UCS Manager cannot install the firmware update.

c) Drag the line to the table on the right.
d) Click **Yes** to confirm that you selected the correct version.

Step 7 If you need to include BMC firmware for servers with different model numbers (PIDs) in this management firmware package, repeat Step 6.

Step 8 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.

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.

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

This discovery policy determines how the system reacts when you add a new chassis. If you create a chassis discovery policy, Cisco UCS Manager configures the chassis for the number of links between the chassis and the fabric interconnect specified in the policy.

Configuring the Chassis Discovery Policy

Procedure

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

Step 2 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 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.

Step 7 Click **Save Changes**.

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 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 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 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 7,200 seconds. If it is set to switching mode, the default is 300 seconds. • **other**—Cisco UCS Manager GUI displays the **Seconds** field which allows you to enter a custom value.
Seconds field	The number of seconds 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 an integer between 1 and 1,000,001.

Step 6 Click **Save Changes**.

Configuring the Aging Time for the MAC Address Table

CHAPTER 13

Managing Port Licenses

This chapter includes the following sections:

Port 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 licenses pre-installed:

- Cisco UCS 6120XP fabric interconnect—pre-installed licenses for the first eight Ethernet ports and any Fibre Channel ports on expansion modules
- Cisco UCS 6140XP fabric interconnect—pre-installed licenses for the first sixteen Ethernet ports and any Fibre Channel ports on expansion modules

If you purchase additional expansion modules or want to use additional ports in the fixed module, you must purchase and install licenses for those ports.

At this time, you can only install port licenses through Cisco UCS Manager CLI.

Obtaining the Host ID for a Fabric Interconnect

The host ID is also known as the serial number. You can also view the serial number in the Cisco UCS Manager GUI on the **General** tab for the fabric interconnect.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **connect local-mgmt**	Enters local management mode.
Step 2	UCS-A(local-mgmt)# **show license host-id**	Obtains the host ID or serial number for the fabric interconnect. **Tip** Use the entire host ID that displays after the equal (=) sign.

The following example obtains the host ID for a fabric interconnect:

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# show license host-id
License hostid: VDH=FLC12121212
```

What to Do Next

Obtain the port license from Cisco.

Obtaining a Port 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 port license on the fabric interconnect.

Installing a Port License on a Fabric Interconnect

You must use Cisco UCS Manager CLI to install a port license.

Before You Begin

Obtain the port license from Cisco.

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*]/*license_filename* **Workspace:***license_filename*	Copies the port license 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*
Step 3	UCS-A(local-mgmt)# **install-license workspace:***license_filename*	Installs the port license.

The following example uses FTP to copy a port license to the workspace and then installs that port license:

```
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/license/port9.lic workspace:/port9.lic
UCS-A(local-mgmt)# install-license workspace:port9.lic
```

Viewing the Port Licenses Installed on a Fabric Interconnect

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **connect local-mgmt**	Enters local management mode.
Step 2	UCS-A(local-mgmt)# **show license** [**brief** | **file** [*license_filename*]]	Displays the port licenses installed on the fabric interconnect with the level of detail specified in the command.

The following example displays full details of the port licenses installed on a fabric interconnect:

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# show license file

enter.lic:
SERVER this_host ANY
VENDOR cisco
INCREMENT ENTERPRISE_PKG cisco 1.0 permanent uncounted \
        VENDOR_STRING=<LIC_SOURCE>UCS_SWIFT</LIC_SOURCE><SKU>ENTERPRISE_PKG=</SKU> \
        HOSTID=VDH=FLC12360025 \
        NOTICE="<LicFileID>20090519230254773</LicFileID><LicLineID>1</LicLineID> \
        <PAK></PAK>" SIGN=134D2848E9B0

port1.lic:
SERVER this_host ANY
VENDOR cisco
INCREMENT ETH_PORT_ACTIVATION_PKG cisco 1.0 permanent 1 \
        VENDOR_STRING=<LIC_SOURCE>UCS_SWIFT</LIC_SOURCE><SKU>N10-L001=</SKU> \
        HOSTID=VDH=FLC12360025 \
        NOTICE="<LicFileID>20090519200954833</LicFileID><LicLineID>1</LicLineID> \
        <PAK></PAK>" SIGN=C01FAE4E87FA

port2.lic:
SERVER this_host ANY
VENDOR cisco
INCREMENT ETH_PORT_ACTIVATION_PKG cisco 1.0 permanent 8 \
       VENDOR_STRING=<LIC_SOURCE>UCS_SWIFT</LIC_SOURCE><SKU>ETH_PORT_ACTIVATION_PKG=</SKU>

\
        HOSTID=VDH=FLC12360025 \
        NOTICE="<LicFileID>20090519231228131</LicFileID><LicLineID>1</LicLineID> \
        <PAK></PAK>" SIGN=DF6A586C43C6
UCS-A(local-mgmt)#
```

Viewing Port License Usage for a Fabric Interconnect

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **connect local-mgmt**	Enters local management mode.

	Command or Action	Purpose
Step 2	UCS-A(local-mgmt)# **show license usage**	Displays the license usage table for all license files installed on the fabric interconnect.

The following example displays full details of the licenses installed on a fabric interconnect:

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# show license usage
Feature                      Ins  Lic   Status Expiry Date Comments
                                 Count
--------------------------------------------------------------------------------
FM_SERVER_PKG                 No    -   Unused             -
ENTERPRISE_PKG                No    -   Unused             -
FC_FEATURES_PKG               No    -   Unused             Grace expired
ETH_PORT_ACTIVATION_PKG       No    8   Unused Never       -
ETH_MODULE_ACTIVATION_PKG     No    0   Unused             -
--------------------------------------------------------------------------------
UCS-A(local-mgmt)#
```

Uninstalling a Port License from a Fabric Interconnect

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.

If you attempt to use a port that does not have an installed license, Cisco UCS initiates a grace period. The grace period is measured from the first use of the feature without a license and is reset when a valid license file is installed. After the grace period expires, the ports are not functional. Contact your Cisco representative for information about the length of the grace period for your fabric interconnect.

Note Permanent licenses cannot be uninstalled if they are in use.

Before You Begin

- Back up the Cisco UCS Manager configuration
- Disable the port associated with the port license you want to uninstall

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **connect local-mgmt**	Enters local management mode.
Step 2	UCS-A(local-mgmt)# **clear license** *license_filename*	Uninstalls the port license that you specify by name.

The following example shows the uninstallation of port9.lic:

```
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)# clear license port9.lic
Clearing license port9.lic:
SERVER this_host ANY
VENDOR cisco
INCREMENT ETH_PORT_ACTIVATION_PKG cisco 1.0 permanent 1 \
        VENDOR_STRING=<LIC_SOURCE>UCS_SWIFT</LIC_SOURCE><SKU>N10-L001=</SKU> \
        HOSTID=VDH=FLC12360025 \
        NOTICE="<LicFileID>20090519200954833</LicFileID><LicLineID>1</LicLineID> \
        <PAK></PAK>" SIGN=C01FAE4E87FA

Clearing license ........done
UCS-A(local-mgmt)#
```

What to Do Next

For a cluster configuration, uninstall the port license for the same port on 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 Switching Mode**
- **Set 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.

Step 4 Launch Cisco UCS Manager GUI and log back in to continue configuring your system.

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 Right-click the port that you want to configure and choose one of the following:

- **Configure as Server Port**
- **Configure as Uplink Port**

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

Configuring Server Ports

Enabling 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 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

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.
Step 2 In the **Ports and Port Channels** area, expand **Ports** ➤ **Fabric Interconnects** ➤ *Fabric_Interconnect_Name*.
Step 3 Right-click the port that you want to enable and choose **Enable Port**.
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 **Ports** ➤ **Fabric Interconnects** ➤ *Fabric_Interconnect_Name*.
Step 3 Right-click the port that you want to disable and choose **Disable Port**.
Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

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 **Ports** ➤ **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 **Unconfigure**.

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

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.
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 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 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. • **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 to 3967 • Be between 4049 to 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.
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 impacts the maximum MTU supported. Network MTU above the maximums may cause the packet to be dropped for the following adapters:

- The Cisco UCS CNA M71KR adapter supports a maximum MTU of 9216.
- The Cisco UCS 82598KR-CI adapter 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. 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

Name	Description
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**.
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 fabric interconnects, you can create a named VLAN that is accessible to both fabric interconnects or to only one fabric interconnect.

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 to 3967 • Be between 4049 to 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.
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.

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.
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**.

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

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.
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 Policies

QoS policies assign a system class to the outgoing traffic for a vNIC or vHBA. This system class determines the quality of service for that traffic.

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.

Configuring QoS System Classes

The type of adapter in a server impacts the maximum MTU supported. Network MTU above the maximums may cause the packet to be dropped for the following adapters:

- The Cisco UCS CNA M71KR adapter supports a maximum MTU of 9216.
- The Cisco UCS 82598KR-CI adapter 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. 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:

Name	Description
	• 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**.
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**.

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: • **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. • **bronze**—Use this priority for QoS policies that control vNIC traffic only. • **fc**—Use this priority for QoS policies that control vHBA traffic only • **gold**—Use this priority for QoS policies that control vNIC traffic only. • **platinum**—Use this priority for QoS policies that control vNIC traffic only. • **silver**—Use this priority for QoS policies that control vNIC traffic only.
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.
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.
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.

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 which 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**.

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.
Description field	A user-defined description of the template.
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 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.

Name	Description
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.

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.

Name	Description
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.

Name	Description
	• **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: • **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

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.

Name	Description
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**
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**.

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.

In a cluster configuration, a named VSAN can be configured to be accessible only to the FC uplinks on one fabric interconnect or to the FC Uplinks on both fabric interconnects.

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

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.
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.

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 VSAN accessible to both fabric interconnects.
- The **FC Uplinks - *Switch_Name* ➤ VSANs** node for a VSAN accessible to only one fabric interconnect.

Deleting a Named 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 select **Delete**.

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

Step 8 Click **OK**.

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.

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.

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.

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.

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**.

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.

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.

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**.

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.
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.

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 the Cisco M81KR VIC adapter 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 the Cisco M81KR VIC adapter 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 the Cisco M81KR VIC adapter 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 the Cisco M81KR VIC adapter 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 the Cisco M81KR VIC adapter 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 to a server with the Cisco M81KR VIC adapter running the ESX host, the recommended value is 10000.
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.

Name	Description
	Enter an integer between 0 and 255. **Note** This option only applies to a server with the Cisco M81KR VIC adapter 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 the Cisco M81KR VIC adapter 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 the Cisco M81KR VIC adapter 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 the Cisco M81KR VIC adapter 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 the Cisco M81KR VIC adapter.

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 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 server pool.

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, is 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 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 pool.
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**.

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 baseboard management controller (BMC) on a server.

Cisco UCS Manager uses the IP addresses in a management IP pool for external access to a server through the following:

- KVM console
- Serial over LAN
- IPMI

Creating an IP Address Block in 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** .

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**.

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 25

Configuring Server-Related Policies

This chapter includes the following sections:

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. 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.
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.

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.

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.

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.

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 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 BMC. 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 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	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 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:

- **Any Configuration**—For a server configuration that carries forward the local disk configuration without any changes.
- **No Local Storage**—For a diskless workstation 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.
- **No RAID**—For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered.
- **RAID Mirrored**—For a 2-disk RAID 1 server configuration.
- **RAID Stripes**—For a 2-disk RAID 0 server configuration.

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 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 select **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.
Mode drop-down list	This can be one of the following local disk policy modes:

Name	Description
	• **Any Configuration**—For a server configuration that carries forward the local disk configuration without any changes. • **No Local Storage**—For a diskless workstation 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. • **No RAID**—For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered. • **RAID Mirrored**—For a 2-disk RAID 1 server configuration. • **RAID Stripes**—For a 2-disk RAID 0 server configuration. **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.

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 on a server during the discovery process and when the server is disassociated from a service profile. This policy can ensure that the data on local drives is erased at those times.

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.
Disk Scrub field	If this field is set to **yes**, when a service profile containing this scrub policy is associated with a server, the disks on that server are completely erased. If this field is set to **no**, the contents of the disks 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.
Admin State field	This can be: • **enabled** • **disabled**
Speed drop-down list	This can be: • **115200** • **19200** • **38400** • **57600** • **9600**

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 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.
Qualification drop-down list	The server pool policy qualification associated with this autoconfiguration 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 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.

f 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 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 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 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.
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 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.
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.

Depending upon the implementation, you may include server pool policy qualifications in the following policies:

- 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.

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.
Max Number of Cores field	The maximum number of CPU cores allowed.
Min Number of Threads field	The minimum number of CPU threads required.
Max Number of Threads field	The maximum number of CPU threads allowed.
CPU Speed field	The minimum CPU speed required.
CPU Stepping field	The minimum CPU version required.

c) Click **OK**.

Step 11 (Optional) To use this policy to qualify servers according to their storage configuration and capacity:
a) Click **Create Storage Qualifications**.
b) In the **Create Storage Qualifications** dialog box, complete the following fields:

Name	Description
Number of Blocks field	The minimum number of blocks required.
Block Size field	The minimum block size required, in bytes.
Min Cap field	The minimum storage capacity required, in megabytes.
Max Cap field	The maximum storage capacity allowed, in megabytes.
Per Disk Cap field	The minimum storage capacity per disk required, in gigabytes.
Units field	The number of units.

c) Click **OK**.

Step 12 Verify the qualifications in the table and correct if necessary.
Step 13 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 Profiles

vNIC/vHBA Placement Profiles

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

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 Profiles** and choose **Create Placement Profile**.

Step 5 In the **Create Placement Profile** dialog box, do the following:

a) In the **Name** field, enter a unique name for the 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.

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 Profile

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 Profiles** node.

Step 4 Right-click the profile you want to delete and choose **Delete**.

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

CHAPTER 26

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

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 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 the Cisco UCS CNA M71KR adapters, 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.

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 251
- Page 2: Configuring the Storage Options, page 252
- Page 3: Configuring the Networking Options, page 257
- Page 4: Setting the vNIC/vHBA Placement, page 260
- Page 5: Setting the Server Boot Order, page 262
- Page 6: Specifying the Server Assignment, page 264
- Page 7: Adding Operational Policies, page 266

Page 1: Identifying the Service Profile

This procedure directly follows the steps in Creating a Service Profile with the Expert Wizard, page 251. It describes how to set the identity of a service profile 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 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 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 4.

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 4.
XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX	Uses the UUID that you manually assign. Continue with Step 3.
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 4.

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) In the text box, enter a description of this service profile.
The description can contain up to 256 characters.

Step 5 Click **Next**.

What to Do Next

Complete the steps in Page 2: Configuring the Storage Options, page 252.

Page 2: Configuring the Storage Options

This procedure directly follows Page 1: Identifying the Service Profile , page 251. 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.
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**, do the following:

a) From the **Mode** drop-down list, choose one of the following:

- **Any Configuration**—For a server configuration that carries forward the local disk configuration without any changes.
- **No Local Storage**—For a diskless workstation 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.
- **No RAID**—For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered.
- **RAID Mirrored**—For a 2-disk RAID 1 server configuration.
- **RAID Stripes**—For a 2-disk RAID 0 server configuration.

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) 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 231.

c) Click **OK**.

d) From the **Local Storage** drop-down list, choose the policy you created.

Step 4 From the **Scrub Policy** drop-down list , choose one of the following:

Option	Description
<not set>	Does not include a scrub policy in the service profile.
Policy_Name	Assigns an existing scrub 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 5. Otherwise, continue with Step 6.

Step 5 (Optional) To create a scrub policy that will be available to all service profiles, do the following:

a) Click the **Create Scrub Policy** link .

b) In the **Create Scrub Policy** dialog box, complete the fields.
For more information, see Creating a Scrub Policy, page 233.

c) Click **OK**.

d) From the **Scrub Policy** drop-down list , choose the policy you created.

Step 6 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 7 (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 **Derived from vHBA** to use a WWN derived from the first vHBA you specify.
- 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 195.

c) Repeat Step 7b in the **vHBA 1 (Fabric B)** area to create a VSAN for that vHBA.

d) Continue with Step 9.

Step 8 (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 **Derived from vHBA** to use a WWN derived from the first vHBA you specify.
- 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.

Name	Description
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.
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 9 Click **Next**.

What to Do Next

Complete Page 3: Configuring the Networking Options, page 257.

Page 3: Configuring the Networking Options

This procedure directly follows Page 2: Configuring the Storage Options, page 252. 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 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 2.
Expert	Allows you to create an unlimited number of vNICs for this service profile. Continue with Step 3.
No vNICs	Does not include any vNICs for connections to a LAN in the service profile. Any server associated with this service profile will not be able to communicate with a LAN unless you modify the service profile to add vNICs. Continue with Step 4.

Option	Description
Hardware Inherited	Uses the vNICs assigned to the Ethernet adapter profile associated with the server. Continue with Step 4.

Step 2 (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 165.

b) Repeat Step 2a in the **vNIC 1 (Fabric B)** area to create a VLAN for that vNIC.

c) Continue with Step 4.

Step 3 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.
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

Name	Description
	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 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.
VLAN Trunking field	If you want to use VLAN trunking, click **Yes**. Otherwise, select **No**.
Select VLAN drop-down list	The VLAN with which this vNIC is associated.
Create VLAN link	Click this link if you want to create a VLAN.
Native VLAN check box	Check this check box if this vNIC is associated with the native 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.

Name	Description
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 4 Click **Next**.

What to Do Next

Complete Page 4: Setting the vNIC/vHBA Placement, page 260.

Page 4: Setting the vNIC/vHBA Placement

This procedure directly follows Page 3: Configuring the Networking Options, page 257. 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.
vNIC/vHBA Placement Profiles ***Placement Profile Name***	Assigns an existing vNIC/vHBA placement profile to the service profile. If you choose this option, Cisco UCS Manager displays the details of the profile. If you do not want use any of the existing profiles, but instead want to create a profile that all service profiles can access, click **Create Placement Profile** 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 Profile**, do the following in the **Create Placement Profile** dialog box:

a) In the **Name** field, enter a unique name for the 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.

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 262

Page 5: Setting the Server Boot Order

This procedure directly follows Page 4: Setting the vNIC/vHBA Placement, page 260. 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 7.
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.
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 7.

Step 2 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 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.

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.

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.

Name	Description
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.

e) Add another boot device to the **Boot Order** table, or click **OK** to finish.

Step 8 Click **Next**.

What to Do Next

Complete Page 6: Specifying the Server Assignment, page 264

Page 6: Specifying the Server Assignment

This procedure directly follows Page 5: Setting the Server Boot Order, page 262. It describes how to specify the way a server is assigned to 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.
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.

Option	Description
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 7: Adding Operational Policies, page 266.

Page 7: Adding Operational Policies

This procedure directly follows Page 6: Specifying the Server Assignment, page 264. 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 provide external access to the BMC on the server, click the down arrows on 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 2 To add an IPMI profile to the service profile, do one of the following:

a) To add an existing policy, select the desired IPMI profile from the **IPMI Profile** drop-down list.
b) If the **IPMI Profile** drop-down list does not include an IPMI profile with the desired user access, click the **Create IPMI Profile** link to create an IPMI profile that is available to all service profiles.
For more information about how to create an IPMI profile, see Creating an IPMI Profile, page 229.
c) If you chose to create an IPMI profile, select that profile from the **IPMI Profile** drop-down list.

Step 3 To add a Serial over LAN policy to the service profile, do one of the following:

a) To add an existing policy, select the desired Serial over LAN policy from the **SoL Configuration Profile** drop-down list.
b) To create a Serial over LAN policy that is only available to this service profile, 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.
c) To create a Serial over LAN policy that is available to all service profiles, click the **Create Serial over LAN Policy** link and complete the fields in the dialog box.
d) If you chose to create a Serial over LAN policy that is available to all service profiles, select that policy from the **SoL Configuration Profile** drop-down list.

Step 4 To monitor thresholds and collect statistics for the associated server, do the following:

a) Click the down arrows on the **Monitoring Configuration** bar.
b) To add an existing policy, select the desired threshold policy from the **Threshold Policy** drop-down list.
c) To create a threshold policy that is available to all service profiles, click the **Create Threshold Policy** link and complete the fields in the dialog box.
d) If you chose to create a threshold policy that is available to all service profiles, select that policy from the **Threshold Policy** drop-down list.

Step 5 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 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 **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.
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	

Name	Description
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.
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.

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. • **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. • **virtual CD-ROM**—The server boots from a virtual CD-ROM. • **virtual 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.
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. • **virtual CD-ROM**—The server boots from a virtual CD-ROM. • **virtual 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.

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 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 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.

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 271
- Page 2: Specifying the Template Storage Options, page 272
- Page 3: Specifying the Template Networking Options, page 276
- Page 4: Setting the vNIC/vHBA Placement, page 279
- Page 5: Specifying the Template Server Boot Order Options, page 281

• Page 6: Specifying the Template Server Assignment Options, page 283
• Page 7: Specifying Template Policy Options, page 285

Page 1: Identifying the Service Profile Template

This procedure directly follows the steps in Creating a Service Profile Template, page 270. 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 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 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.
The description can contain up to 256 characters.

Step 5 Click **Next**.

What to Do Next

Complete the steps in Page 2: Specifying the Template Storage Options, page 272.

Page 2: Specifying the Template Storage Options

This procedure directly follows Page 1: Identifying the Service Profile Template, page 271. 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**, do the following:

a) From the **Mode** drop-down list, choose one of the following:

- **Any Configuration**—For a server configuration that carries forward the local disk configuration without any changes.
- **No Local Storage**—For a diskless workstation 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.
- **No RAID**—For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered.
- **RAID Mirrored**—For a 2-disk RAID 1 server configuration.
- **RAID Stripes**—For a 2-disk RAID 0 server configuration.

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) 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 231.

c) Click **OK**.

d) From the **Local Storage** drop-down list, choose the policy you created.

Step 4 From the **Scrub Policy** drop-down list, choose one of the following:

Option	Description
<not set>	Does not include a scrub policy in a service profile created from this template.
Policy_Name	Assigns an existing scrub 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 5. Otherwise, continue with Step 6.

Step 5 (Optional) To create a scrub policy that will be available to all service profiles and templates, do the following:

a) Click the **Create Scrub Policy** link.

b) In the **Create Scrub Policy** dialog box, complete the fields.
For more information, see Creating a Scrub Policy, page 233.

c) Click **OK**.

d) From the **Scrub Policy** drop-down list, choose the policy you created.

Step 6 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 7.
Expert	Allows you to create an unlimited number of vHBAs for every service profile created from this template. Continue with Step 8.

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 9.

Step 7 (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 **Derived from vHBA** to use a WWN derived from the first vHBA you specify.
- 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 195.

c) Repeat Step 7b in the **vHBA 1 (Fabric B)** area to create a VSAN for that vHBA.

d) Continue with Step 9.

Step 8 (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 **Derived from vHBA** to use a WWN derived from the first vHBA you specify.
- 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.

Name	Description
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 9 Click **Next**.

What to Do Next

Complete Page 3: Specifying the Template Networking Options, page 276.

Page 3: Specifying the Template Networking Options

This procedure directly follows Page 2: Specifying the Template Storage Options, page 272. 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 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 2.
Expert	Allows you to create an unlimited number of vNICs for every service profile created from this template. Continue with Step 3.
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 4.

Step 2 (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 165.

b) Repeat Step 2a in the **vNIC 1 (Fabric B)** area to create a VLAN for that vNIC.

c) Continue with Step 4.

Step 3 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.
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 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.
VLAN Trunking field	If you want to use VLAN trunking, click **Yes**. Otherwise, select **No**.
Select VLAN drop-down list	The VLAN with which this vNIC is associated.
Create VLAN link	Click this link if you want to create a VLAN.
Native VLAN check box	Check this check box if this vNIC is associated with the native 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	

Name	Description
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 4 Click **Next**.

What to Do Next

Complete Page 4: Setting the vNIC/vHBA Placement, page 279.

Page 4: Setting the vNIC/vHBA Placement

This procedure directly follows Page 3: Specifying the Template Networking Options, page 276. 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.

Option	Description
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 profile to a service profile created from this template. If you choose this option, Cisco UCS Manager displays the details of the profile. If you do not want use any of the existing profiles, but instead want to create a profile that all service profiles and templates can access, click **Create Placement Profile** 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 Profile**, do the following in the **Create Placement Profile** dialog box:

a) In the **Name** field, enter a unique name for the 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.

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: Specifying the Template Server Boot Order Options, page 281

Page 5: Specifying the Template Server Boot Order Options

This procedure directly follows Page 4: Setting the vNIC/vHBA Placement, page 279. 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 7.
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, continue with Step 7.

Step 2 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 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.

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.

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.

e) Add another boot device to the **Boot Order** table, or click **OK** to finish.

Step 8 Click **Next**.

What to Do Next

Complete Page 6: Specifying the Template Server Assignment Options, page 283.

Page 6: Specifying the Template Server Assignment Options

This procedure directly follows Page 5: Specifying the Template Server Boot Order Options, page 281. It describes how to specify the way a server is assigned to 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 7: Specifying Template Policy Options, page 285.

Page 7: Specifying Template Policy Options

This procedure directly follows Page 6: Specifying the Template Server Assignment Options, page 283. 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 provide external access to the BMC on the server, click the down arrows on 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 2 To add an IPMI profile to service profile created from this template, do one of the following:

- To add an existing policy, select the desired IPMI profile from the **IPMI Profile** drop-down list.
- If the **IPMI Profile** drop-down list does not include an IPMI profile with the desired user access, click the **Create IPMI Profile** link to create an IPMI profile that is available to all service profiles templates and then select that profile from the **IPMI Profile** drop-down list.

For more information about how to create an IPMI profile, see Creating an IPMI Profile, page 229.

Step 3 To add a Serial over LAN policy to service profile 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..

Step 4 To monitor thresholds and collect statistics for the associated server, do the following:

a) Click the down arrows on the **Monitoring Configuration** bar.
b) 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 profile templates, click the **Create Threshold Policy** link and complete the fields in the dialog box and then select that policy from the **Threshold Policy** drop-down list.

Step 5 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 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 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 **Template Based Service Profile** radio button.

b) In the **Name** field, enter a unique name for the service 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.

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 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.
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**.

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**.

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 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**.

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.

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 server or server pool when you created it, or to change the 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.

Option	Description
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.

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.
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**.

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.

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.

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.

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.
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) In the **Fabric Interconnect** area, complete the following fields:

Name	Description
Fabric ID field	The fabric interconnect associated with the component.

Name	Description
	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 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.
VLAN Trunking field	If you want to use VLAN trunking, click **Yes**. Otherwise, select **No**.
Select VLAN drop-down list	The VLAN with which this vNIC is associated.
Create VLAN link	Click this link if you want to create a VLAN.
Native VLAN check box	Check this check box if this vNIC is associated with the native 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.

Name	Description
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 27

Installing an OS on a Server

This chapter includes the following sections:

OS Installation Methods

Servers in the Cisco UCS support several operating systems, including Windows- and Linux-based operating systems. Regardless of the OS being installed, you can install it on a server using one of the following methods:

- PXE install server
- KVM dongle directly connected to the server
- KVM console in the UCS Manager GUI
- Third-party tool (not covered in this document)

PXE Install Server

A Preboot Execution Environment (PXE) install server allows clients (servers) to boot and install an OS over the network. To use this method, a PXE environment must be configured and available on a VLAN, typically a dedicated provisioning VLAN, and a client server must be set to boot from the network. When a client server boots, it sends a PXE request across the network, and the PXE install server acknowledges the request and starts a sequence of events that installs the OS on the client server.

PXE servers can use installation disks, disk images, and scripts to install the OS. Proprietary disk images can also be used install an OS and additional components or applications.

PXE installation is an efficient method for consistently installing an OS on a large number of servers. However, considering that this method requires configuring a PXE environment, if you do not already have an PXE

install server set up, it might be easier to use one of the other installation methods if you are installing an OS on only one or two servers,

KVM Dongle

The KVM dongle plugs into the front of a server and allows you to directly connect a keyboard, video monitor, mouse, and USB CD/DVD or floppy drive to the server. This direct access to the server allows you to locally install an OS.

To install an OS from a CD/DVD or floppy drive connected to the USB port, you must ensure that the CD/DVD or floppy drive is set as the first boot device in the service profile.

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.

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

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.

Installation Targets

The installation target is the location where you install the OS. The UCS server has two possible installation targets: a local hard drive or a SAN LUN. During the OS installation process, drivers for the local disk controller or HBA must be loaded so that the installer can find the drives. If the installer cannot find any drives, the drivers were probably not loaded. Newer OS installation disks should have the drivers; however, older OS installation disks may not have them.

If your OS installation disk does not have the needed drivers, you must provide them during the installation process. For local drives, you need LSI controller drivers, and for HBAs you need Emulex or Qlogic drivers.

Installing an OS Using a PXE Installation Server

Before You Begin

- Verify that a PXE installation environment has been configured to install the appropriate OS, and that the client server can be reached over a VLAN.
- Verify that a service profile is associated with the server onto which the OS is being installed.

Procedure

Step 1 Depending on whether the service profile is associated with a boot policy, or contains the definition for a local boot policy, perform one of the following:

- For a service profile with a boot policy, set the boot order for the boot policy to boot from the LAN first as described in Creating a Boot Policy, page 227.
- For a service profile which contains the definition for a local boot policy, set the boot order for the local boot definition to boot from the LAN first.

Step 2 Reboot the server.
For more information, see Booting a Server from the Service Profile , page 362.

If a PXE install server is available on a VLAN, the installation process begins when the server reboots. PXE installations are typically automated and require no additional user input. Refer to the installation guide for the OS being installed to guide you through the rest of the installation process.

What to Do Next

After the OS installation is complete, reset the LAN boot order to its original setting.

Installing an OS Using the KVM Dongle

Before You Begin

- Locate the following items:
  - USB keyboard and mouse
  - Video monitor
  - USB CD/DVD drive
  - USB floppy drive (optional)
  - OS installation disk or disk image file
- Verify that a service profile is associated with the server onto which the OS is being installed.

Procedure

Step 1 Connect the KVM dongle to the front of the server.

Step 2 Connect the keyboard, video monitor, mouse, USB CD/DVD drive, and optionally a USB floppy drive to the KVM console.

Note The USB dongle contains only two USB ports. To connect more than two USB devices to the dongle, first connect a USB hub to the dongle and then connect your USB devices to the hub.

Step 3 Load the OS installation disk into the USB CD/DVD drive connected to the dongle.

Step 4 If Cisco UCS Manager GUI is not open, log in.

Step 5 Depending on whether the service profile is associated with a boot policy, or contains the definition for a local boot policy, perform one of the following:

- For a service profile with a boot policy, set the boot order for the boot policy to boot from the virtual media first.

  For more information, see Creating a Boot Policy, page 227.

- For a service profile which contains the definition for a local boot policy, set the boot order for the local boot definition to boot from the virtual media first.

Step 6 Reboot the server.
For more information, see Booting a Server from the Service Profile , page 362

When the server reboots, it begins the installation process from the CD/DVD drive. Refer to the installation guide for the OS being installed to guide you through the rest of the installation process.

What to Do Next

After the OS installation is complete, reset the virtual media boot order to its original setting.

Installing an OS Using the KVM Console

Before You Begin

- Locate the OS installation disk or disk image file.
- Verify that a service profile is associated with the server onto which the OS is being installed.

Procedure

Step 1 Load the OS installation disk into your CD/DVD drive, or copy the disk image files to your computer.

Step 2 If Cisco UCS Manager GUI is not open, log in.

Step 3 In the **Navigation** pane, click the **Servers** tab.

Step 4 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 5 Expand the node for the organization that contains the service profile associated with the server on which the OS is being installed and click the service profile.

If the system does not include multi-tenancy, expand the **root** node and click the service profile.

Step 6 In the **Work** pane, click the **General** tab.

Step 7 In the **Actions** area, click **KVM Console**.
The KVM Console opens in a separate window.

Step 8 From the KVM console, choose **Tools ➤ Launch Virtual Media** to open the Virtual Media Session dialog box.

Step 9 In the Virtual Media Session dialog box, map the virtual media using either of the following methods:

- Check the **Mapped** check box for the CD/DVD drive containing the OS installation disk.
- Click **Add Image**, navigate to and select the OS installation disk image, click **Open** to mount the disk image, and then check the **Mapped** check box for the mounted disk image.

Note You must keep the **Virtual Media Session** dialog box open during the OS installation process; closing the dialog box unmaps all virtual media.

Step 10 Depending on whether the service profile is associated with a boot policy, or contains the definition for a local boot policy, perform one of the following in Cisco UCS Manager GUI:

- For a service profile with a boot policy, set the boot order for the boot policy to boot from the virtual media first.

  For more information, see Creating a Boot Policy, page 227.
- For a service profile which contains the definition for a local boot policy, set the boot order for the local boot definition to boot from the virtual media first.

Step 11 Reboot the server.
For more information, see Booting a Server from the Service Profile , page 362.

When the server reboots, it begins the installation process from the virtual CD/DVD drive. Refer to the installation guide for the OS being installed to guide you through the rest of the installation process.

What to Do Next

After the OS installation is complete, reset the virtual media boot order to its original setting.

PART VI

VN-Link Configuration

CHAPTER 28

Overview of VN-Link in Cisco UCS

This chapter includes the following sections:

Virtualization with the Cisco M81KR VIC Adapter

The Cisco M81KR VIC adapter supports virtualized environments with VMware 4.0 Update 1. 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 the Cisco M81KR VIC adapter, how communication works depends upon which solution you choose. This 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

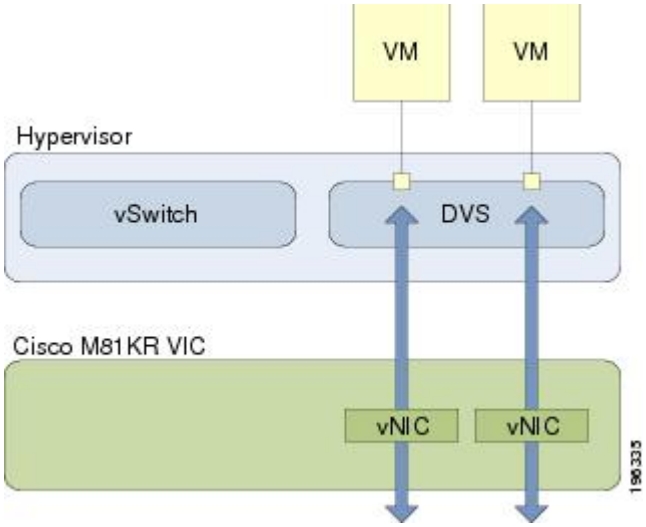
Cisco VN-Link in hardware is a hardware-based method of handling traffic to and from a virtual machine on a server with a Cisco M81KR VIC adapter. This method is sometimes referred to as pass-through switching. This solution replaces software-based switching with ASIC-based hardware switching and improves performance.

The distributed virtual switch (DVS) framework delivers VN-Link in hardware features and capabilities for virtual machines on Cisco UCS servers with Cisco M81KR 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 Cisco M81KR 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 Cisco M81KR 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 along side 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 consistent 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 new 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 319
Step 2	In VMware vCenter, create a vCenter and datacenter.	For more information, see the VMware documentation.

	Command or Action	Purpose
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 datacenter name specified in VMware vCenter. The datacenter folder and DVS you create in Cisco UCS Manager are pushed to WMware vCenter. For more information, see the following chapter: Configuring Distributed Virtual Switches in Cisco UCS, page 327
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 337
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 29

Configuring VN-Link Components and Connectivity

This chapter includes the following sections:

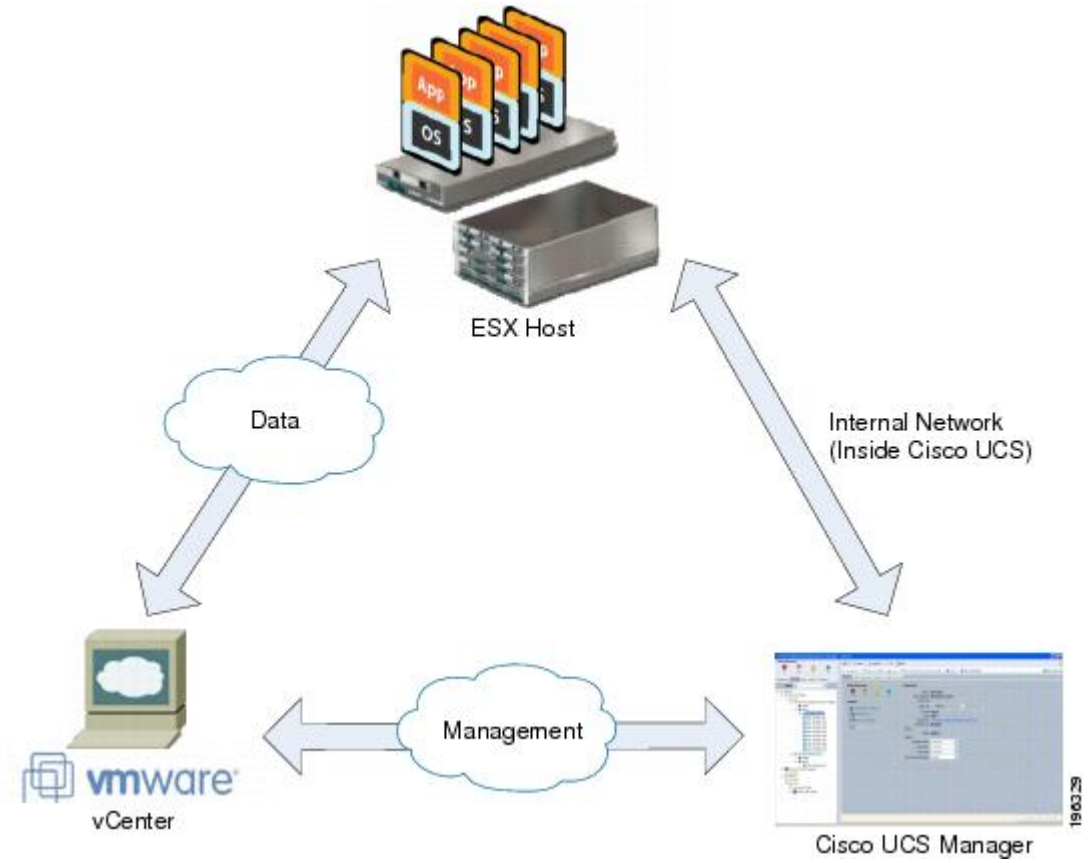
Components of VN-Link in Hardware

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 249.

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 WMware vCenter and the ESX host.

Step 2 Install WMware 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) User name and password specified while installing vCenter Server. During the vCenter Server installation you chose to use the Windows logon credentials, then 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. 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.
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 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 WMware 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 reachable by VMware vCenter.

Procedure

Step 1 In WMware 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 WMware 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 30

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 along side 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 consistent 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 new 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 of the **Configure vCenter** wizard, 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.
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 of the **Configure vCenter** wizard, 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.

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.

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.

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.
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 on 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.

Name	Description
Description field	A user-defined description of the folder.

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.

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.

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.

Name	Description
Description field	The user-defined description of the distributed virtual switch.
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.

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.

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.
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.

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.
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 31

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 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
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.
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.

Name	Description
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.
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 5 Click **OK**.

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 32

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 Cisco M81KR VIC adapters that host VMs and dynamic vNICs.

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.

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.
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	This field is always set to "protected" because failover mode is always enabled for virtual NICs.

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**.

CHAPTER 33

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 34

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 35

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.

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

This procedure removes the chassis from the configuration. As long as the chassis physically remains in the Cisco UCS instance, Cisco UCS Manager considers the chassis to be decommissioned and ignores it.

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. 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.

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.

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.
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 chassis, 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.

Option	Description
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.

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 36

Managing the Servers

This chapter includes the following sections:

Server Management in Cisco UCS Manager GUI

You can manage and monitor all servers in a Cisco UCS instance through Cisco UCS Manager GUI. Some server management tasks, such as changes to the power state, can be performed from the following locations:

- **General** tab for the server
- **General** tab for the service profile associated with the server

The remaining management tasks can only be performed on the server.

If a 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 server in the slot.

Booting Servers

Booting a 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.

Shutting Down Servers

Shutting Down a 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 **Shut Down** 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 **Shut Down**.
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

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 **Shut Down**.
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 Server

When you reset a server, Cisco UCS Manager sends a pulse on the reset line. You can choose to gracefully shutdown the operating system. If the operating system does not support a graceful shutdown, the server will

be 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 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 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 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 366.

Decommissioning a Server

This procedure removes the server from the configuration. As long as the server physically remains in the Cisco UCS instance, Cisco UCS Manager considers the server to be decommissioned and ignores it.

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 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 366.

Reacknowledging a Server Slot in a Chassis

Perform the following procedure if you decommission a server without removing the physical hardware 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 Server from the Configuration Database

Perform the following procedure if you physically removed a server from its slot in a chassis without first decommissioning the server. You cannot perform this procedure if the server is physically present in the chassis slot.

If you want to physically remove a server, see Removing a Server from a Chassis, page 365.

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.

Toggling the Locator LED

Turning on the Locator LED for 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 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 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 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 server stops flashing.

Starting the KVM Console

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.

Resetting the CMOS for a 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 BMC for a Server

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reset the BMC. This procedure is not part of the normal maintenance of a server. After you reset the BMC, 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 BMC.

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 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**.

Recovering the Corrupt BIOS on a 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 **Reset iBMC (Server Controller)**.

b) Click **OK**.

Monitoring 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 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	The subtabs display the properties and status of the components of the server.
Virtual Machines	Provides details of the virtual machines hosted on the server.
Installed Firmware tab	Displays the firmware versions on the BMC and interface cards in the server. 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.
Faults tab	Provides details of faults generated by the server.
Events tab	Provides details of events generated by the server.
FSM tab	Provides details about and the status of FSM tasks related to the server. You can use this information to diagnose errors with those tasks.
Statistics tab	Provides statistics about the server and its components. You can view these statistics in tabular or chart format.
Temperatures tab	Provides temperature statistics for the components of the server. You can view these statistics in tabular or chart format.
Power tab	Provides 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.

Viewing the POST Results for a 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 37

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**.

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.

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 38

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.

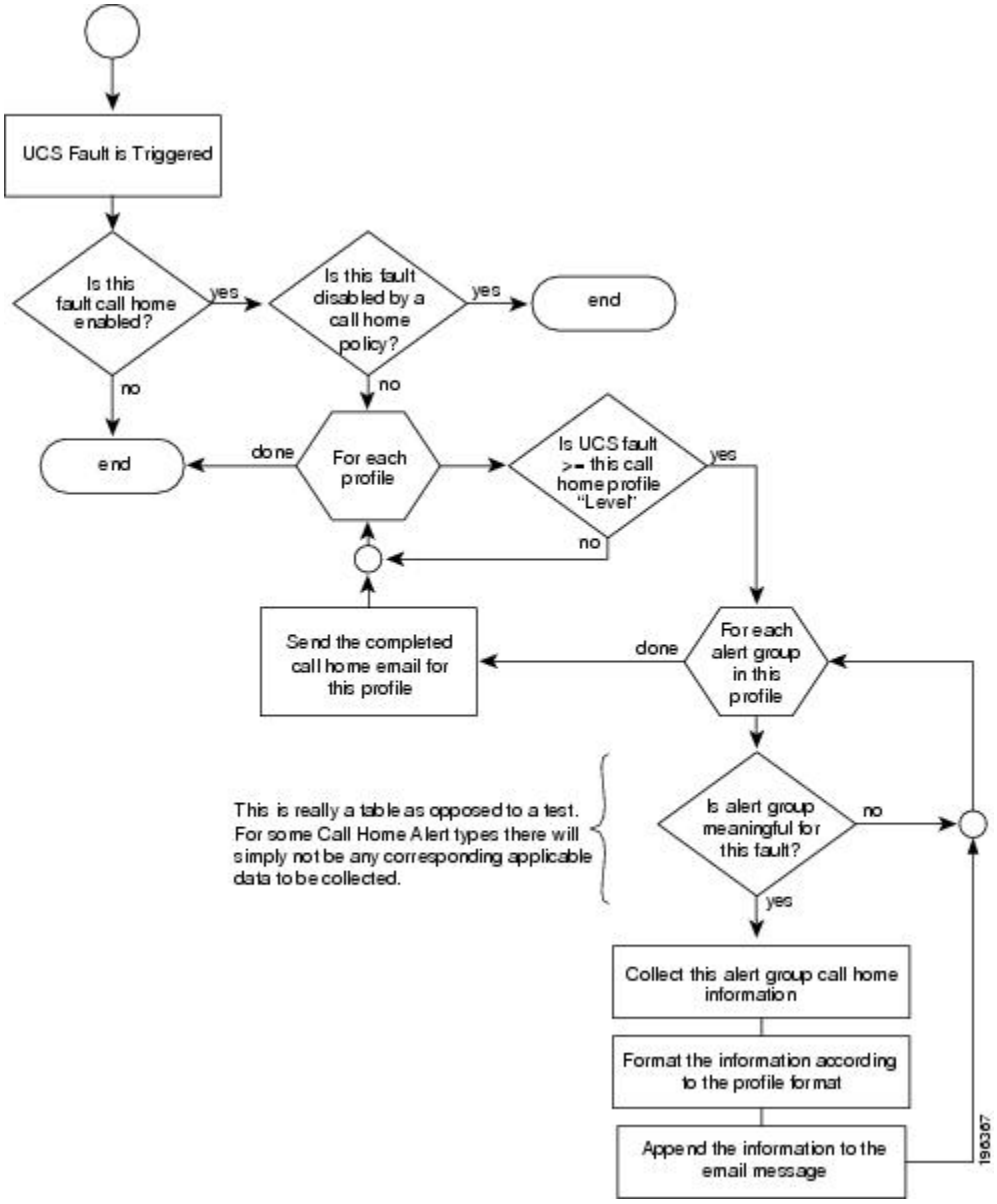
When you configure Call Home to send messages, Cisco UCS Manager executes the appropriate CLI **show** command and attaches the command output to the message.

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.

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

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:

- 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.
- The contact email, phone, and street address information should be configured so that the receiver can determine the origin of messages received.
- 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.
- 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 Homet configuration in Cisco UCS must be the CCO account name that is associated with a support contract that includes Smart Call Home

Cisco UCS Faults that Trigger Call Home Alerts

The following table describes the faults that trigger a Call Home alert to be sent.

Note If Smart Call Home is configured in the Cisco UCS instance, every fault listed in the following table triggers a Smart Call Home event to the Cisco Smart Call Home system. In addition, if the value in the Case Created column for the event is "yes", then a Cisco Technical Support case is created and sent to the queue for a customer call-back.

Table 4: Cisco UCS Faults that Trigger Call Home Alerts

Cisco UCS Faults	Cisco UCS Severity	Call Home Severity	Call Home Alert Type	Call Home Cause	Case Created?
compute:Blade:biosPostTimeout	Critical	Critical	Diagnostic	equipment-inoperable	yes
equipment:FanModule:identity unestablishable	Critical	—	Diagnostic	identity-unestablishable	—
equipment:Chassis:identity unestablishable	Critical	Critical	Diagnostic	identity-unestablishable	yes
equipment:Chassis:thermal ThresholdNonRecoverable	Critical	Critical	Environmental	thermal-problem	—

Cisco UCS Faults	Cisco UCS Severity	Call Home Severity	Call Home Alert Type	Call Home Cause	Case Created?
equipment:IOCard:identity-unestablishable	Critical	Critical	Diagnostic	identity-unestablishable	yes
equipment:Psu:identity unestablishable	Critical	Critical	Diagnostic	identity-unestablishable	yes
equipment:Psu:thermal ThresholdNonRecoverable	Critical	Critical	Environmental	thermal-problem	—
equipment:Psu:voltage ThresholdNonRecoverable	Critical	Critical	Environmental	voltage-problem	—
memory:Unit:thermal ThresholdNonRecoverable	Critical	Critical	Environmental	thermal-problem	—
processor:Unit:thermal ThresholdNonRecoverable	Critical	Critical	Environmental	thermal-problem	—
compute:Blade:inoperable	Major	Major	Diagnostic	equipment-inoperable	yes
equipment:Chassis:thermal ThresholdCritical	Major	Major	Environmental	thermal-problem	—
equipment:Fan:inoperable	Major	Major	Environmental	equipment-inoperable	yes
equipment:IOCard:thermal Problem	Major	Major	Environmental	thermal-problem	—
equipment:Psu:inoperable	Major	Major	Environmental	equipment-inoperable	yes
equipment:Psu:voltage ThresholdCritical	Major	Major	Environmental	voltage-problem	—
memory:Unit:inoperable	Major	Major	Diagnostic	equipment-inoperable	—
memory:Unit:thermal ThresholdCritical	Major	Major	Environmental	thermal-problem	—
processor:Unit:inoperable	Major	Major	Diagnostic	equipment-inoperable	yes
processor:Unit:thermal ThresholdCritical	Major	Major	Environmental	thermal-problem	—

Cisco UCS Faults	Cisco UCS Severity	Call Home Severity	Call Home Alert Type	Call Home Cause	Case Created?
equipment:Psu:thermal ThresholdCritical	Major	Major	Environmental	thermal-problem	—
compute:Blade:Degraded	Major	Major	Diagnostic	equipment-degraded	—
compute:Blade:identity Unestablishable	Minor	Minor	Diagnostic	identity-unestablishable	yes

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 5: 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.
(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.
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

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.

Name	Description
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 System Inventory Messages

Use this procedure if you need to manually send a system inventory message outside of the scheduled 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 **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**

Name	Description
	• **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: • **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 UCSsends 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**

Name	Description
	• **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 39

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**—Includes a snapshot of the entire system. You can use this file for disaster recovery if you need to recreate every configuration on a fabric interconnect or rebuild a fabric interconnect. • **All configuration**—Includes all system and logical configuration information. • **System configuration**—Includes all system configuration settings such as user names, roles, and locales. • **Logical configuration**—Includes all logical configuration settings such as service profiles, LAN configuration settings, SAN configuration settings, pools, and policies.
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.
Protocol field	The protocol to use when communicating with the remote server. This can be: • **FTP** • **TFTP** • **SCP** • **SFTP**

Name	Description
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.
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: • **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.
Protocol field	The protocol to use when communicating with the remote server. This can be: • **FTP** • **TFTP** • **SCP** • **SFTP**

Name	Description
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 configuration file that is being imported.
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 40

Managing the System Event Log

This chapter includes the following sections:

System Event Log

The system event log (SEL) resides on the BMC in NVRAM. It records most server-related events, such as over and under voltage, temperature events, fan events, events from BIOS, etc. 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 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: • **1 Hour** • **24 Hours** • **2 Hours** • **4 Hours** • **8 Hours** • **Never**—Do not perform any automatic SEL data backups. **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. • **none**—Automatic backups are never triggered by any events. • **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 41

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. • **alerts** • **critical** • **debugging** • **emergencies** • **errors** • **information** • **notifications** • **warnings**
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. • **alerts** • **critical** • **debugging** • **emergencies** • **errors** • **information** • **notifications** • **warnings**

Name	Description
Name field	The name of the file in which the messages are logged.
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.

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. • **alerts** • **critical** • **debugging** • **emergencies** • **errors** • **information** • **notifications** • **warnings**
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** • **local4** • **local5**

Name	Description
	• local6 • local7

Step 7 Click **Save Changes**.

CHAPTER 42

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 acounts 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 is designed to assist you in recovering 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 The running versions of the following firmware:

- The firmware kernel version on the fabric interconnect

- The firmware system version

Tip To find out 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 is designed to assist you in recovering 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 out 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
```

CHAPTER 43

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.

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
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: • **15 Minutes** • **30 Minutes** • **60 Minutes** 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: • 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

Name	Description
	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 BMC. 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 select **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 assigned to the threshold 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 threshold policy.

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, select one of the following classes to configure from the **Stat Class** drop-down list:

- **ethernet-port-stats-by-size-large-packets**
- **ethernet-port-stats-by-size-small-packets**
- **ethernet-port-err-stats**
- **ethernet-port-multicast-stats**
- **ethernet-port-over-under-sized-stats**
- **ethernet-port-stats**
- **fc-port-stats**
- **vnic-stats**
- **cpu-stats**

- **dimm-stats**
- **mb-power-stats**
- **mb-temp-stats**

Note If you see a different list of statistics classes, verify that you are creating the threshold policy in an organization.

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, select 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 a 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 select **Create Threshold Class**.

Step 5 In the **Create Threshold Class** page of the **Create Threshold Policy** wizard, do the following:

a) Click **Add**.

b) In the **Statistics Class** dialog box, select one of the following classes to configure from the **Stat Class** drop-down list:

- **ethernet-port-stats-by-size-large-packets**
- **ethernet-port-stats-by-size-small-packets**
- **ethernet-port-err-stats**
- **ethernet-port-multicast-stats**
- **ethernet-port-over-under-sized-stats**
- **ethernet-port-stats**
- **fc-port-stats**
- **vnic-stats**
- **cpu-stats**
- **dimm-stats**
- **mb-power-stats**
- **mb-temp-stats**

Note If you see a different list of statistics classes, verify that you are creating the threshold policy in an organization.

c) 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, select 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:
st fo the
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**.

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 select the **Create Threshold Class**.

Step 5 In the **Create Threshold Class** page, do the following:

a) Click **Add**.

b) In the **Statistics Class** dialog box, select one of the following classes to configure from the **Stat Class** drop-down list:

- **ether-error-stats**
- **ether-loss-stats**
- **ether-rx-stats**
- **ether-tx-stats**

Note If you see a different list of statistics classes, verify that you are creating the threshold policy in the **LAN Cloud** node.

c) 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, select 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: st fo the
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 select the **Create Threshold Class**.
Step 5 In the **Create Threshold Class** page, do the following:
a) Click **Add**.
b) In the **Statistics Class** dialog box, select one of the following classes to configure from the **Stat Class** drop-down list:
   - **chassis-stats**
   - **fan-module-stats**
   - **fan-stats**
   - **io-card-stats**
   - **psu-input-stats**
   - **psu-stats**
   - **ether-error-stats**

- **ether-loss-stats**
- **ether-rx-stats**
- **ether-tx-stats**
- **env-stats**
- **system-stats**

Note If you see a different list of statistics classes, verify that you are creating the threshold policy in the **Internal LAN** node.

c) 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, select 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: st fo the
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 select the **Create Threshold Class**.

Step 5 In the **Create Threshold Class** page, do the following:

a) Click **Add**.

b) In the **Statistics Class** dialog box, select one of the following classes to configure from the **Stat Class** drop-down list:

- **fc-error-stats**
- **fc-stats**

Note If you see a different list of statistics classes, verify that you are creating the threshold policy in the **SAN Cloud** node.

c) 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, select 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: st fo the

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**.

INDEX

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X