CONTENTS

Preface xviii

Audience xviii
Organization xviii
Conventions xix
Related Documentation xx
Documentation Feedback xxi
Obtaining Documentation and Submitting a Service Request xxi

Introduction 1

Overview of Cisco Unified Computing System 3

About Cisco Unified Computing System 3
Unified Fabric 4
Fibre Channel over Ethernet 5
Link-Level Flow Control 5
Priority Flow Control 5

Server Architecture and Connectivity 6

Overview of Service Profiles 6
Network Connectivity through Service Profiles 6
Configuration through Service Profiles 6
Service Profiles that Override Server Identity 7
Service Profiles that Inherit Server Identity 8
Service Profile Templates 8

Policies 9
Configuration Policies 9
Boot Policy 9
Chassis Discovery Policy 10
Ethernet and Fibre Channel Adapter Policies 10
Contents

Host Firmware Pack 11
IPMI Access Profile 11
Local Disk Configuration Policy 11
Management Firmware Pack 11
Quality of Service Policies 12
Server Autoconfiguration Policy 12
Server Discovery Policy 12
Server Inheritance Policy 12
Server Pool Policy 12
Server Pool Policy Qualifications 13
vHBA Template 13
vNIC Template 13
Operational Policies 13
   Fault Collection Policy 13
   Scrub Policy 14
   Serial over LAN Policy 14
   Statistics Collection Policy 14
   Statistics Threshold Policy 14
Pools 15
   Server Pools 15
   MAC Pools 15
   UUID Suffix Pools 16
   WWN Pools 16
   Management IP Pool 16
Traffic Management 17
   Oversubscription 17
   Oversubscription Considerations 17
   Guidelines for Estimating Oversubscription 18
Pinning 18
   Pinning Server Traffic to Server Ports 19
   Guidelines for Pinning 20
Quality of Service 20
   System Classes 20
   Quality of Service Policies 21
   Flow Control Policies 21
Opt-In Features 21
  Stateless Computing 21
  Multi-Tenancy 22
Virtualization 23
  Virtualization with the Cisco UCS CNA M71KR and Cisco UCS 82598KR-CI Adapters 23

Overview of Cisco UCS Manager 25
  About Cisco UCS Manager 25
  Tasks You Can Perform in Cisco UCS Manager 26
  Tasks You Cannot Perform in Cisco UCS Manager 28
  Cisco UCS Manager in a Cluster Environment 28

Overview of Cisco UCS Manager GUI 29
  Overview of Cisco UCS Manager GUI 29
    Fault Summary Area 29
    Navigation Pane 30
    Toolbar 31
    Work Pane 31
    Status Bar 31
    Table Customization 32
    LAN Uplinks Manager 33
    Hybrid Display 33
  Logging in to Cisco UCS Manager GUI through HTTPS 34
  Logging in to Cisco UCS Manager GUI through HTTP 34
  Logging Off Cisco UCS Manager GUI 35
  Changing the Cisco UCS Manager GUI Properties 35

System Configuration 39
  Configuring the Fabric Interconnects 41
    Initial System Setup 41
      Setup Mode 42
      System Configuration Type 42
      Management Port IP Address 42
    Performing an Initial System Setup for a Standalone Configuration 42
    Initial System Setup for a Cluster Configuration 44
      Performing an Initial System Setup on the First fabric interconnect 44
      Performing an Initial System Setup on the Second Fabric Interconnect 46
Enabling a Standalone Fabric Interconnect for Cluster Configuration 47
Ethernet Switching Mode 48
Configuring the Ethernet Switching Mode 49
Monitoring a Fabric Interconnect 49

Configuring Ports 51
Server and Uplink Ports on the Fabric Interconnect 51
Configuring Server Ports 52
Configuring Uplink Ethernet Ports 52
Reconfiguring a Port on a Fabric Interconnect 53
Enabling a Port on a Fabric Interconnect 53
Disabling a Port on a Fabric Interconnect 54
Unconfiguring a Port on a Fabric Interconnect 54
Configuring Uplink Ethernet Port Channels 55
Creating an Uplink Ethernet Port Channel 55
Enabling an Uplink Ethernet Port Channel 56
Disabling an Uplink Ethernet Port Channel 56
Adding Ports to an Uplink Ethernet Port Channel 56
Removing Ports from an Uplink Ethernet Port Channel 57
Deleting an Uplink Ethernet Port Channel 57

Configuring Communication Services 59
Communication Services 59
Configuring CIM-XML 60
Configuring HTTP 61
Configuring HTTPS 61
Creating a Key Ring 61
Creating a Certificate Request for a Key Ring 62
Creating a Trusted Point 62
Importing a Certificate into a Key Ring 63
Configuring HTTPS 63
Deleting a Key Ring 64
Deleting a Trusted Point 64
Configuring SNMP 65
Enabling SNMP 65
Configuring Trap Hosts 65
Configuring SNMPv3 users 66
Enabling Telnet 67
Disabling Communication Services 67

**Configuring Primary Authentication** 69
Primary Authentication 69
Remote Authentication Providers 69
Creating a Remote Authentication Provider 70
  Creating an LDAP Provider 70
  Creating a RADIUS Provider 72
  Creating a TACACS+ Provider 73
Deleting a Remote Authentication Provider 75
  Deleting an LDAP Provider 75
  Deleting a RADIUS Provider 75
  Deleting a TACACS+ Provider 75
Selecting a Primary Authentication Service 75

**Configuring Organizations** 77
Organizations in a Multi-Tenancy Environment 77
Hierarchical Name Resolution in a Multi-Tenancy Environment 78
Creating an Organization under the Root Organization 79
Creating an Organization under an Organization that is not Root 80
Deleting an Organization 80

**Configuring Role-Based Access Control** 81
Role-Based Access Control 81
User Accounts 81
User Roles 82
Privileges 83
User Locales 85
Configuring User Roles 85
  Creating a User Role 85
  Adding Privileges to a User Role 86
  Removing Privileges from a User Role 86
  Deleting a User Role 86
Configuring Locales 87
  Creating a Locale 87
  Adding an Organization to a Locale 88
  Deleting an Organization from a Locale 88
Deleting a Locale 88
Configuring User Accounts 89
  Creating a User Account 89
  Deleting a Locally Authenticated User Account 91
Monitoring User Sessions 91
Firmware Management 93
  Overview of Firmware 93
  Image Management 93
    Image Headers 94
    Image Catalog 94
  Firmware Updates 94
    Firmware Versions 95
    Direct Firmware Update at Endpoints 95
      Stages of a Direct Firmware Update 96
      Recommended Order of Components for Firmware Activation 96
    Firmware Updates through Service Profiles 97
      Host Firmware Pack 97
      Management Firmware Pack 98
      Stages of a Firmware Update through Service Profiles 98
Firmware Downgrades 98
Downloading and Managing Images 99
  Obtaining Images from Cisco 99
  Checking the Available Space on a Fabric Interconnect 99
  Downloading Images to the Fabric Interconnect 99
  Canceling an Image Download 101
Directly Updating Firmware at Endpoints 101
  Updating the Firmware on Multiple Components 101
  Activating the Firmware on Multiple Components 101
  Updating the Firmware on an Adapter 102
  Activating the Firmware on an Adapter 103
  Updating the Firmware on a BMC 103
  Activating the Firmware on a BMC 104
  Updating the Firmware on an IOM 104
  Activating the Firmware on an IOM 105
  Updating and Activating the Firmware on a Fabric Interconnect 105
Updating and Activating the Cisco UCS Manager Software 106
Updating Firmware through Service Profiles 106
Creating a Host Firmware Package 106
Updating a Host Firmware Pack 107
Creating a Management Firmware Package 108
Updating a Management Firmware Pack 108
Verifying Firmware Versions on Components 109

Configuring DNS Servers 111
DNS Servers in Cisco UCS 111
Adding a DNS Server 111
Deleting a DNS Server 112

Network Configuration 113

Using the LAN Uplinks Manager 115
Launching the LAN Uplinks Manager 115
Changing the Ethernet Switching Mode with the LAN Uplinks Manager 116
Configuring a Port with the LAN Uplinks Manager 116
Configuring Server Ports 117
- Enabling a Server Port with the LAN Uplinks Manager 117
- Disabling a Server Port with the LAN Uplinks Manager 117
- Unconfiguring a Server Port with the LAN Uplinks Manager 117
Configuring Uplink Ethernet Ports 118
- Enabling an Uplink Ethernet Port with the LAN Uplinks Manager 118
- Disabling an Uplink Ethernet Port with the LAN Uplinks Manager 118
- Unconfiguring an Uplink Ethernet Port with the LAN Uplinks Manager 118
Configuring Uplink Ethernet Port Channels 119
- Creating a Port Channel with the LAN Uplinks Manager 119
- Enabling a Port Channel with the LAN Uplinks Manager 120
- Disabling a Port Channel with the LAN Uplinks Manager 120
- Adding Ports to a Port Channel with the LAN Uplinks Manager 120
- Removing Ports from a Port Channel with the LAN Uplinks Manager 121
- Deleting a Port Channel with the LAN Uplinks Manager 121
Configuring LAN Pin Groups 121
- Creating a Pin Group with the LAN Uplinks Manager 121
- Deleting a Pin Group with the LAN Uplinks Manager 122
Configuring Named VLANs 122
Creating a UUID Suffix Pool 173
Deleting a UUID Suffix Pool 174
Configuring the Management IP Pool 174
Management IP Pool 174
Creating an IP Address Block in the Management IP Pool 174
Deleting an IP Address Block from the Management IP Pool 175

Configuring Server-Related Policies 177
Configuring Boot Policies 177
Boot Policy 177
Creating a Boot Policy 179
Deleting a Boot Policy 180
Configuring Chassis Discovery Policies 181
Chassis Discovery Policy 181
Configuring a Chassis Discovery Policy 181
Configuring IPMI Profiles 181
IPMI Access Profile 181
Creating an IPMI Profile 182
Deleting an IPMI Profile 183
Configuring Local Disk Configuration Policies 183
Local Disk Configuration Policy 183
Creating a Local Disk Configuration Policy 183
Changing a Local Disk Configuration Policy 184
Deleting a Local Disk Configuration Policy 185
Configuring Scrub Policies 185
Scrub Policy 185
Creating a Scrub Policy 186
Deleting a Scrub Policy 186
Configuring Serial over LAN Policies 187
Serial over LAN Policy 187
Creating a Serial over LAN Policy 187
Deleting a Serial over LAN Policy 188
Configuring Server Autoconfiguration Policies 188
Server Autoconfiguration Policy 188
Creating an Autoconfiguration Policy 188
Deleting an Autoconfiguration Policy 189
Contents

Turning on the Locator LED for a Chassis 249
Turning off the Locator LED for a Chassis 249
Monitoring a Chassis 249
View the POST Results for a Chassis 251

Managing the Servers 253
Server Management in Cisco UCS Manager GUI 253
Booting Servers 254
  Booting a Server 254
  Booting a Server from the Service Profile 254
Shutting Down Servers 255
  Shutting down a Server from the Service Profile 255
Resetting a Server 255
Reacknowledging a Server 256
Removing a Server from a Chassis 257
Decommissioning a Server 257
Reacknowledging a Server Slot in a Chassis 258
Removing a Non-Existent Server from the Configuration Database 258
Toggling the Locator LED 259
  Turning on the Locator LED for a Server 259
  Turning off the Locator LED for a Server 259
Starting the KVM Console 260
  Starting the KVM Console from a Server 260
  Starting the KVM Console from a Service Profile 260
Resetting the CMOS for a Server 261
Resetting the BMC for a Server 261
Monitoring a Server 262
Viewing the POST Results for a Server 263

Managing the IO Modules 265
I/O Module Management in Cisco UCS Manager GUI 265
Resetting an I/O Module 265
Monitoring an I/O Module 266
Viewing the POST Results for an I/O Module 266

Configuring Call Home 269
  Call Home 269
Contents

Restoring the Configuration for a Fabric Interconnect 293

Configuring Settings for Faults and Events 295
  Configuring Settings for the Fault Collection Policy 295
    Fault Collection Policy 295
    Configuring the Fault Collection Policy 296
  Configuring Settings for the Core File Exporter 297
    Core File Exporter 297
    Configuring the Core File Exporter 297

Recovering a Lost Password 299
  Password Recovery for the Admin Account 299
  Determining the Leadership Role of a Fabric Interconnect 300
  Verifying the Firmware Versions on a Fabric Interconnect 300
  Recovering the Admin Account Password in a Standalone Configuration 300
  Recovering the Admin Account Password in a Cluster Configuration 301

Configuring Statistics-Related Policies 303
  Statistics Collection Policy 303
  Statistics Threshold Policy 304
  Modifying a Statistics Collection Policy 304
  Configuring Statistics Threshold Policies 306
    Creating a Server and Server Component Threshold Policy 306
    Adding a Threshold Class to a Server and Server Component Threshold Policy 308
    Deleting a Server and Server Component Threshold Policy 310
    Adding a Threshold Class to the Uplink Ethernet Port Threshold Policy 310
    Adding a Threshold Class to the Ethernet Server Port, Chassis, and Fabric Interconnect Threshold Policy 311
    Adding a Threshold Class to the Fibre Channel Port Threshold Policy 313
Preface

This preface includes the following:

- Audience, page xviii
- Organization, page xviii
- Conventions, page xix
- Related Documentation, page xx
- Documentation Feedback, page xxi
- Obtaining Documentation and Submitting a Service Request, page xxi

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 sections:

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part 1</td>
<td>Introduction</td>
<td>Describes the Cisco Unified Computing System (UCS), UCS Manager, and UCS Manager GUI.</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Part 2</td>
<td>System Configuration</td>
<td>Describes configuring fabric interconnects, ports, communication services, primary authentication, and role-based access control configuration, and also describes managing firmware.</td>
</tr>
<tr>
<td>Part 3</td>
<td>Network Configuration</td>
<td>Describes configuring named VLANs, LAN pin groups, MAC pools, and Quality of Service (QoS).</td>
</tr>
<tr>
<td>Part 4</td>
<td>Storage Configuration</td>
<td>Describes configuring named VSANs, SAN pin groups, and WWN pools.</td>
</tr>
<tr>
<td>Part 5</td>
<td>Server Configuration</td>
<td>Describes configuring server-related policies, server-related pools, and service profiles, and also describes installing an OS on servers.</td>
</tr>
<tr>
<td>Part 6</td>
<td>System Management</td>
<td>Describes managing chassis, servers, and I/O modules, and also describes backing up and restoring the configuration.</td>
</tr>
</tbody>
</table>

## Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold font</strong></td>
<td>Commands, keywords, GUI elements, and user-entered text appear in <strong>bold font</strong>.</td>
</tr>
<tr>
<td><em>italic font</em></td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in <em>italic font</em>.</td>
</tr>
<tr>
<td>[]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td><strong>courier font</strong></td>
<td>Terminal sessions and information the system displays appear in <strong>courier font</strong>.</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>Convention</td>
<td>Indication</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

**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

Documentation for Cisco UCS is available at the following URL:

http://www.cisco.com

The following are related Cisco UCS documents:

- Cisco UCS Documentation Roadmap
- Cisco UCS Manager CLI Configuration Guide
- Cisco UCS Manager XML API Programmer's Guide
- Cisco UCS Manager Troubleshooting Guide
- Cisco UCS Site Planning Guide
- Cisco UCS 6100 Series Fabric Interconnect Hardware Installation Guide
- Cisco UCS 5108 Server Chassis Hardware Installation Guide
- Regulatory Compliance and Safety Information for Cisco UCS
- Release Notes for Cisco UCS Manager
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:


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

- Overview of Cisco Unified Computing System, page 3
- Overview of Cisco UCS Manager, page 25
- Overview of Cisco UCS Manager GUI, page 29
Overview of Cisco Unified Computing System

This chapter includes:

- About Cisco Unified Computing System, page 3
- Unified Fabric, page 4
- Server Architecture and Connectivity, page 6
- Traffic Management, page 17
- Opt-In Features, page 21
- Virtualization, page 23

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.

The result of this radical simplification is a reduction by up to two-thirds of the switches, cables, adapters, and management points. 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 will support 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:

• 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 Interconnect
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:

- 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 of those adapters.

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:

- 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 type of service profile is the simplest to use and create. This profile 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 automatically applies the identity and configuration information that is present at the time of association, such as:

- 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 have been subsequently changed before this profile is associated with the server.

---

**Service Profile Templates**

Service profile templates enable you to create a large number of similar service profiles. 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 of 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 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 which configure the servers and other components.
- Operational policies which control certain management, monitoring, and access control functions.

Configuration Policies

Boot Policy

This 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 virtual 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:

<table>
<thead>
<tr>
<th>Boot type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAN boot</td>
<td>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.</td>
</tr>
<tr>
<td>LAN boot</td>
<td>Boots from a centralized provisioning server. It is frequently used to install operating systems on a server from that server.</td>
</tr>
<tr>
<td>Local disk boot</td>
<td>If the server has a local drive, boots from that drive.</td>
</tr>
<tr>
<td>Virtual media boot</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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, the system does the following:

- Automatically configures the chassis for the number of links between the chassis and the fabric interconnect specified in the policy.
- Specifies the power policy to be used by the chassis.

**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

Operating systems are sensitive to the settings in these policies. The configuration and selection of the policy is driven by the type of operating system.

**Host Firmware Pack**

This policy enables you to specify a common set of firmware versions that make up the host firmware pack. The host firmware includes the following server and adapter components:

- BIOS
- SAS controller
- Emulex Option ROM (applicable only to Emulex-based Converged Network Adapters [CNAs])
- Emulex firmware (applicable only to Emulex-based CNAs)
- QLogic option ROM (applicable only to QLogic-based CNAs)
- Adapter firmware

The firmware pack 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 of the component in the firmware pack, 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 while associating the service profile, UCSM will just ignore firmware update and complete 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 the RAID mode and the way the drives are partitioned.

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 Pack**

This policy enables you to specify a common set of firmware versions that make up the management firmware pack. The management firmware includes the server controller (BMC) on the server.
The firmware pack 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.

**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**

This policy determines whether one or more of the following is automatically applied to a new server:

- A server pool policy qualification that qualifies the server for one or more server pools
- An organization
- A service profile template that associates the server with a service profile created from that template

**Prerequisites**

**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.

With this policy, an inventory of the server is conducted, then server pool policy qualifications are run to determine whether the new server qualifies for one or more server pools.

**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 policy defines how a vHBA on a server connects to the SAN. This policy 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.

**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.

**Operational Policies**

**Fault Collection Policy**

The fault collection policy controls the lifecycle of a fault in a Cisco UCS instance, including the length of time that each fault remains in the flapping and retention intervals.

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 enters a flapping or soaking interval that is designed to prevent flapping. 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 returns to the active state. If the condition does not reoccur during the flapping interval, the fault is cleared.

4. The cleared fault enters the retention interval. This interval ensures that the fault reaches the attention of an administrator, even if the condition that caused the fault has been alleviated, and that the fault is not deleted prematurely. The retention interval retains the cleared fault for the length of time specified in the fault collection policy.
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.

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 in the fabric Interconnect
- 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

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 identify 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 64GB 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 will use 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:

- 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 which contains only WW node names. If you include a pool of WWNNs in a service profile, the associated server will be assigned a WWNN from that pool.

WWPN Pools

A WWPN pool is a WWN pool which 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 will be 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 server controller (BMC) in a server.

Cisco UCS Manager uses the IP addresses in a management IP pool for external access through serial over LAN and 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:

1. **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.

2. **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.

3. **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
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 the data center. 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.

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

<table>
<thead>
<tr>
<th>Links on Chassis</th>
<th>Servers Pinned to Link 1</th>
<th>Servers Pinned to Link 2</th>
<th>Servers Pinned to Link 3</th>
<th>Servers Pinned to Link 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 link</td>
<td>All server slots.</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>2 links</td>
<td>Slots 1, 3, 5, and 9.</td>
<td>Slots 2, 4, 6, and 8.</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>4 links</td>
<td>Slots 1 and 5.</td>
<td>Slots 2 and 6.</td>
<td>Slots 3 and 7.</td>
<td>Slots 4 and 8.</td>
</tr>
</tbody>
</table>

### Chassis with Two I/O Modules

If a chassis has two I/O modules, then 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.

Adding a second I/O module to a chassis does not improve oversubscription. The server port pinning is the same for a single I/O module. The second I/O module improves the high availability of the system through the vNIC binding to the fabric interconnect.

<table>
<thead>
<tr>
<th>Fabric Interconnect Configured in vNIC</th>
<th>Server Traffic Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Server traffic goes to fabric interconnect A. If A fails, the server traffic does not fail over to B.</td>
</tr>
<tr>
<td>B</td>
<td>All server traffic goes to fabric interconnect B. If B fails, the server traffic does not fail over to A.</td>
</tr>
<tr>
<td>A-B</td>
<td>All server traffic goes to fabric interconnect A. If A fails, the server traffic fails over to B.</td>
</tr>
<tr>
<td>B-A</td>
<td>All server traffic goes to fabric interconnect B. If B fails, the server traffic fails over to A.</td>
</tr>
</tbody>
</table>
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. System classes determine how the DCE bandwidth in these 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:

<table>
<thead>
<tr>
<th>System Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platinum Priority</td>
<td>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.</td>
</tr>
<tr>
<td>Gold Priority</td>
<td>All properties of these system classes are available for you to assign custom settings and policies.</td>
</tr>
<tr>
<td>Silver Priority</td>
<td></td>
</tr>
<tr>
<td>Bronze Priority</td>
<td></td>
</tr>
<tr>
<td>Best Effort Priority</td>
<td>A system class that sets the quality of service for the lane reserved for Basic Ethernet traffic.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Fibre Channel Priority</td>
<td>A system class that sets the quality of service for the lane reserved for Fibre Channel over Ethernet traffic.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
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 Policies

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.

If you enable the send function, then 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, then the uplink Ethernet port will honor 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:

- 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 a new service profile to create a new 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 physical a server 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 Cisco UCS 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 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 will depend 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**

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.

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 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.
Overview of Cisco UCS Manager

This chapter includes:

- About Cisco UCS Manager, page 25
- Tasks You Can Perform in Cisco UCS Manager, page 26
- Tasks You Cannot Perform in Cisco UCS Manager, page 28
- Cisco UCS Manager in a Cluster Environment, page 28

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 a command that has been 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 Palo 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 server, 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:

• 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
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 the 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.
Overview of Cisco UCS Manager GUI

This chapter includes:

• Overview of Cisco UCS Manager GUI, page 29
• Logging in to Cisco UCS Manager GUI through HTTPS, page 34
• Logging in to Cisco UCS Manager GUI through HTTP, page 34
• Logging Off Cisco UCS Manager GUI, page 35
• Changing the Cisco UCS Manager GUI Properties, page 35

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 launch 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 launch 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 on 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:

<table>
<thead>
<tr>
<th>Fault Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical Alarms</td>
<td>Critical problems exist with one or more components. These issues should be researched and fixed immediately.</td>
</tr>
<tr>
<td>Major Alarms</td>
<td>Serious problems exist with one or more components. These issues should be researched and fixed immediately.</td>
</tr>
<tr>
<td>Minor Alarms</td>
<td>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.</td>
</tr>
<tr>
<td>Warning Alarms</td>
<td>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.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Tab name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equipment</td>
<td>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.</td>
</tr>
<tr>
<td>Servers</td>
<td>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.</td>
</tr>
</tbody>
</table>
Overview of Cisco UCS Manager GUI

<table>
<thead>
<tr>
<th>Tab name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LAN tab</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>SAN tab</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Admin tab</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

**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, such as:

- Navigating between previously viewed items in the **Work pane**.
- Creating new elements for the Cisco UCS instance.
- Setting the options for Cisco UCS Manager GUI.
- Accessing the 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 on 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 will depend upon the selected component. You can use these tabs to view information about the component, create new components, and modify properties of the component, and examine the selected object.

**Status Bar**

The status bar displays across the bottom of Cisco UCS Manager GUI. The status bar provides information about the current 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 user name 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:

<table>
<thead>
<tr>
<th>Menu Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Column Name</strong></td>
<td>The menu contains an entry for each column in the table. Click a column name to toggle the display of the column on and off.</td>
</tr>
<tr>
<td><strong>Horizontal Scroll</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Pack All Columns</strong></td>
<td>Resizes all columns to their default width.</td>
</tr>
<tr>
<td><strong>Pack Selected Column</strong></td>
<td>Resizes only the selected column to its default width.</td>
</tr>
</tbody>
</table>

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:

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

**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 perform in the LAN Uplinks Manager can also be performed in nodes on other tabs, such as the Equipment tab or the LAN tab.

**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:

- 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:

- 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

**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, `CalManager_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** 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 checkbox 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

**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, CalManager_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**  
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:

- **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**. The **Properties** dialog box displays.

**Step 2**  
(Optional) To specify whether or not Cisco UCS Manager GUI will require confirmation for certain procedures, do the following: update one or more of the following options:

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

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confirm Deletion</strong> check box</td>
<td>If checked, Cisco UCS Manager GUI requires that you confirm all delete operations.</td>
</tr>
</tbody>
</table>
If checked, Cisco UCS Manager GUI requires that you confirm before the system discards any changes.

If checked, Cisco UCS Manager GUI requires that you confirm before the system modifies or creates objects.

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH field</td>
<td>The application to use for SSH processing.</td>
</tr>
<tr>
<td>SSH Parameters</td>
<td>Any parameters to include in all SSH commands.</td>
</tr>
</tbody>
</table>

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:

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

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right Aligned Labels check box</td>
<td>If checked, all labels are right-aligned with respect to one another. Otherwise all labels are left-aligned.</td>
</tr>
</tbody>
</table>
### 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.

### Visual Theme drop-down list
The color scheme used by the GUI. You can select:

- **Modern**—Pale blue-grey borders, dark blue-grey tab areas, and black text. This is the default theme.
- **Classic**—Blue borders with light grey tabs and black text. This theme offers more contrast between the GUI elements.

**Note**
If you change this option the system requires you to re-log into the GUI.

### 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**.
PART II

System Configuration

• Configuring the Fabric Interconnects, page 41
• Configuring Ports, page 51
• Configuring Communication Services, page 59
• Configuring Primary Authentication, page 69
• Configuring Organizations, page 77
• Configuring Role-Based Access Control, page 81
• Firmware Management, page 93
• Configuring DNS Servers, page 111
This chapter includes:

- Initial System Setup, page 41
- Performing an Initial System Setup for a Standalone Configuration, page 42
- Initial System Setup for a Cluster Configuration, page 44
- Enabling a Standalone Fabric Interconnect for Cluster Configuration, page 47
- Ethernet Switching Mode, page 48
- Configuring the Ethernet Switching Mode, page 49
- Monitoring a Fabric Interconnect, page 49

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 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 automatically 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 will automatically detect the first fabric interconnect as a peer fabric interconnect in the cluster.

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

Management Port IP Address

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

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

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

Performing an Initial System Setup for a Standalone Configuration

Before You Begin

1. Verify the following physical connections on the fabric interconnect:

   - The console port is physically connected to a computer terminal or console server.
   - The management Ethernet port (mgmt0) is connected to an external hub, switch, or router.
For more information, refer to the *Cisco UCS Hardware Installation Guide* for your fabric interconnect.

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

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

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

- System name
- Password for the admin account
- 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 *Springfield 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Name field</td>
<td>The name assigned to the Cisco UCS instance</td>
</tr>
<tr>
<td></td>
<td>In a standalone configuration, the system adds &quot;-A&quot; to the system name. In a cluster configuration, the system adds</td>
</tr>
</tbody>
</table>
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.

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Password field</td>
<td>The password used for the Admin account on the fabric interconnect.</td>
</tr>
<tr>
<td>Confirm Admin Password field</td>
<td>The password used for the Admin account on the fabric interconnect.</td>
</tr>
<tr>
<td>Mgmt IP Address field</td>
<td>The static IP address for the management port on the fabric interconnect.</td>
</tr>
<tr>
<td>Mgmt IP Netmask field</td>
<td>The subnet mask for the management port on the fabric interconnect.</td>
</tr>
<tr>
<td>Default Gateway field</td>
<td>The IP address for the default gateway assigned to the management port on the fabric interconnect.</td>
</tr>
<tr>
<td>DNS Server IP field</td>
<td>The IP address for the DNS server assigned to the fabric interconnect.</td>
</tr>
<tr>
<td>Domain Name field</td>
<td>The name of the domain in which the fabric interconnect resides.</td>
</tr>
</tbody>
</table>

**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.
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

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

- System name
- Password for the admin account
- 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 **Springfield 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.

**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.

You must know
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 **Springfield Express Setup** page, select **Initial Setup** and click **Submit**. The fabric interconnect should automatically 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> UCS-A# <code>connect local-mgmt</code></td>
<td>Enters local management mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> UCS-A(local-mgmt) # <code>enable cluster ip-addr</code></td>
<td>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.</td>
</tr>
</tbody>
</table>
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
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.

**Procedure**

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

**Step 2** In 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 actions:

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

The action 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** In the **Equipment** tab, expand **Equipment ➤ Fabric Interconnects**.

**Step 3** In the **Work** pane, click one of the following tabs to view the status of the fabric interconnect:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General tab</td>
<td>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.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Physical Ports tab</td>
<td>Displays the status of all ports on the fabric interconnect. This tab includes the following sub-tabs:</td>
</tr>
<tr>
<td></td>
<td>• Uplink Ports tab</td>
</tr>
<tr>
<td></td>
<td>• Server Ports tab</td>
</tr>
<tr>
<td></td>
<td>• Fibre Channel Ports tab</td>
</tr>
<tr>
<td></td>
<td>• Unconfigured Ports tab</td>
</tr>
<tr>
<td>Fans tab</td>
<td>Displays the status of all fan modules in the fabric interconnect.</td>
</tr>
<tr>
<td>PSUs tab</td>
<td>Displays the status of all power supply units in the fabric interconnect.</td>
</tr>
<tr>
<td>Physical Display tab</td>
<td>Provides a graphical view of the fabric interconnect and all ports and other components. If a component has a fault, the fault icon is displayed next to that component.</td>
</tr>
<tr>
<td>Faults tab</td>
<td>Provides details of faults generated by the fabric interconnect.</td>
</tr>
<tr>
<td>Events tab</td>
<td>Provides details of events generated by the fabric interconnect.</td>
</tr>
<tr>
<td>Statistics tab</td>
<td>Provides statistics about the fabric interconnect and its components. You can view these statistics in tabular or chart format.</td>
</tr>
</tbody>
</table>
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. None of these ports are 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 In 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** In 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** In the LAN tab, expand LAN ➤ LAN Cloud.

**Step 3** Expand Fabric_Interconnect_Name ➤ Ports.

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

**Step 5** If Cisco UCS Manager 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  In the LAN tab, expand LAN ➤ LAN Cloud.
Step 3  Expand Fabric_Interconnect_Name ➤ Ports
Step 4  Right-click on the port that you want to disable and choose Disable Port.
Step 5  If Cisco UCS Manager 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  In 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.
Configuring Uplink Ethernet Port Channels

Creating an Uplink Ethernet Port Channel

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the LAN tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the LAN tab, expand LAN ➤ LAN Cloud.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Expand the node for the fabric interconnect where you want to add the port channel.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Right-click the Port Channels node and choose Add Ports.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Set Port Channel Name page of the Create Port Channel wizard, do the following:</td>
</tr>
<tr>
<td></td>
<td>a) Complete the following fields:</td>
</tr>
<tr>
<td></td>
<td>Name</td>
</tr>
<tr>
<td></td>
<td>ID field</td>
</tr>
<tr>
<td></td>
<td>Name field</td>
</tr>
<tr>
<td></td>
<td>b) Click Next.</td>
</tr>
<tr>
<td>Step 6</td>
<td>In the Add Ports page of the Create Port Channel wizard, do the following:</td>
</tr>
<tr>
<td></td>
<td>a) In the Ports table, choose one or more ports to include the port channel.</td>
</tr>
<tr>
<td></td>
<td>b) Click the &gt;&gt; button to add the ports to the Ports in the port channel table. You can use the &lt;&lt; button to remove ports from the port channel.</td>
</tr>
<tr>
<td></td>
<td>Note</td>
</tr>
<tr>
<td>Step 7</td>
<td>Click Finish.</td>
</tr>
</tbody>
</table>
Enabling an Uplink Ethernet Port Channel

Procedure

Step 1  In the Navigation pane, click the LAN tab.
Step 2  In 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  In 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  In 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
In 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 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
In 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.
Deleting an Uplink Ethernet Port Channel
CHAPTER 6

Configuring Communication Services

This chapter includes:

- Communication Services, page 59
- Configuring CIM-XML, page 60
- Configuring HTTP, page 61
- Configuring HTTPS, page 61
- Configuring SNMP, page 65
- Enabling Telnet, page 67
- Disabling Communication Services, page 67

Communication Services

You can use the following communication services to interface third-party applications with Cisco UCS:

<table>
<thead>
<tr>
<th>Communication Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIM XML</td>
<td>This service is disabled by default and is only available in read-only mode. If enabled, the default port is 5988. This common information model is one of the standards defined by the Distributed Management Task Force.</td>
</tr>
<tr>
<td>HTTP</td>
<td>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.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Communication Service Description

<table>
<thead>
<tr>
<th>Communication Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>For security purposes, we recommend that you enable HTTPS and disable HTTP.</td>
<td></td>
</tr>
<tr>
<td>SMASH CLP</td>
<td>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.</td>
</tr>
<tr>
<td>SNMP</td>
<td>This service is disabled by default. If enabled, the service uses port 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.</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>SSH</td>
<td>Telnet</td>
</tr>
</tbody>
</table>

### 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  In the Admin tab, expand All ➤ Key Management ➤ Root.
Step 3  Right-click on 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) From the Modulus drop-down list, select one of the following options:
      • mod1024
      • mod1536
      • mod2048
      • mod512
   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 In 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password field</td>
<td>An optional password for the certification request, which is used to</td>
</tr>
<tr>
<td></td>
<td>authenticate the request with the Certificate Authority (CA). This password</td>
</tr>
<tr>
<td></td>
<td>is not used by the Cisco UCS system.</td>
</tr>
<tr>
<td>Tip</td>
<td>If used, make sure you record this password in a safe place. If</td>
</tr>
<tr>
<td></td>
<td>it is lost, you may be required to create a new certificate request</td>
</tr>
<tr>
<td></td>
<td>and send it to the CA if the CA requires password authentication.</td>
</tr>
<tr>
<td>Confirm Password field</td>
<td>The password for the certification request repeated for confirmation</td>
</tr>
<tr>
<td></td>
<td>purposes.</td>
</tr>
<tr>
<td>Subject field</td>
<td>The fully qualified domain name of the fabric interconnect.</td>
</tr>
<tr>
<td>IP Address field</td>
<td>The virtual IP address of the fabric interconnect.</td>
</tr>
</tbody>
</table>

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 In the Admin tab, expand All ➤ Key Management ➤ Root.
Step 3 Right-click on Root and choose Create Trusted Point.
Step 4 In the Create Trusted Point dialog box, complete the following fields:
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>The name of the trusted point.</td>
</tr>
<tr>
<td>Certificate Chain</td>
<td>The certificate information for this trusted point.</td>
</tr>
</tbody>
</table>

**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**  
In 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**  In the Admin tab, expand All ➤ Key Management ➤ Root.

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

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

### Deleting a Trusted Point

**Procedure**

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

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

**Step 3**  Right-click on the trusted point you want to delete and select Delete.

**Step 4**  If Cisco UCS Manager 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.

**Step 5** In the Community field, enter the default community name Cisco UCS Manager GUI will 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address field</td>
<td>The IP address or hostname of the SNMP host to which the fabric interconnect should send the trap.</td>
</tr>
<tr>
<td>Community field</td>
<td>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.</td>
</tr>
<tr>
<td>Port field</td>
<td>The port on which the fabric interconnect communicates with the SNMP host.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>The user name.</td>
</tr>
<tr>
<td>Auth Type field</td>
<td>The authorization type. This can be:</td>
</tr>
<tr>
<td></td>
<td>• MD5</td>
</tr>
<tr>
<td></td>
<td>• SHA</td>
</tr>
<tr>
<td>Use AES-128 check box</td>
<td>If checked, this user uses AES-128 encryption.</td>
</tr>
<tr>
<td>Password field</td>
<td>The password for this user.</td>
</tr>
<tr>
<td>Confirm Password field</td>
<td>The password again for confirmation purposes.</td>
</tr>
<tr>
<td>Privacy Password field</td>
<td>The privacy password for this user.</td>
</tr>
<tr>
<td>Confirm Privacy Password field</td>
<td>The privacy password again for confirmation purposes.</td>
</tr>
</tbody>
</table>

Step 6  Click OK.
Step 7  Click Save Changes.
## Enabling Telnet

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Admin tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Admin tab, expand All ➤ Communication Services.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the Communication Services tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Telnet area, click the enabled radio button.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Save Changes.</td>
</tr>
</tbody>
</table>

## Disabling Communication Services

### Note

We recommend that you disable all communication services that are not required to interface with other network applications.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Admin tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Admin tab, expand All ➤ Communication Services.</td>
</tr>
<tr>
<td>Step 3</td>
<td>On the Communication Services tab, click the disable radio button for each service that you want to disable.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Save Changes.</td>
</tr>
</tbody>
</table>
Disabling Communication Services

Configuring SNMPv3 users
CHAPTER 7

Configuring Primary Authentication

This chapter includes:

• Primary Authentication, page 69
• Remote Authentication Providers, page 69
• Creating a Remote Authentication Provider, page 70
• Deleting a Remote Authentication Provider, page 75
• Selecting a Primary Authentication Service, page 75

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 local, RADIUS, or TACACS+ for authentication.

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 under **Remotely Authenticated Users** in the following location on the Admin tab: **All ➤ User Management ➤ User Services**.

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 will have only read-only privileges.

The following table contains the name of the attribute that contains the value of the roles. Cisco UCS Manager checks for the value of this attribute when it queries the remote authentication service during login.

<table>
<thead>
<tr>
<th>Remote Authentication Protocol</th>
<th>Attribute Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>CiscoAvPair</td>
</tr>
<tr>
<td>RADIUS</td>
<td>cisco-av-pair</td>
</tr>
<tr>
<td>TACACS+</td>
<td>cisco-av-pair</td>
</tr>
</tbody>
</table>

Creating a Remote Authentication Provider

Creating an LDAP Provider

Before You Begin

Perform the following configuration In the LDAP server:

- Create the CiscoAvPair 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.

Procedure

1. In the Navigation pane, click the Admin tab.
2. In the Admin tab, expand User Management ➤ LDAP.
3. Complete the following fields in the Properties area:
### Creating an LDAP Provider

**Name** | **Description**
--- | ---
**Timeout field** | The length of time in seconds Cisco UCS Manager GUI 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 contains the role and locale information for the user. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name.

You must create the an attribute named CiscoAvPair values in the remote authentication service. For example, create an attribute named CiscoAvPair in LDAP and use that attribute to store the values of role and locales for the user.

**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 user names that match the defined filter. This property is optional.

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

**Step 5** In the Create LDAP Provider dialog box:

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hostname (or IP Address) field</strong></td>
<td>The hostname or IP address on which the LDAP provider resides.</td>
</tr>
<tr>
<td><strong>Root DN field</strong></td>
<td>The distinguished name (DN) for the LDAP database superuser account. The maximum supported string length is 128 characters.</td>
</tr>
<tr>
<td><strong>Port field</strong></td>
<td>The port through which Cisco UCS communicates with the LDAP database.</td>
</tr>
</tbody>
</table>
If checked, communications to the LDAP database require SSL encryption.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SSL check box</td>
<td>If checked, communications to the LDAP database require SSL encryption.</td>
</tr>
<tr>
<td>Key field</td>
<td>If Enable SSL is checked, the SSL encryption key for the database.</td>
</tr>
<tr>
<td>Confirm Key field</td>
<td>The SSL encryption key repeated for confirmation purposes.</td>
</tr>
</tbody>
</table>

b) Click OK.

**Step 6** Click Save Changes.

**What to Do Next**
Select LDAP as the primary authentication service. For more information, see Selecting a Primary Authentication Service, page 75.

**Creating a RADIUS Provider**

**Before You Begin**
Perform the following configuration in the RADIUS server:

- Create the cisco-av-pairs 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.

**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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout</td>
<td>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.</td>
</tr>
<tr>
<td>Retries</td>
<td>The number of times to retry the connection before the request is considered to have failed.</td>
</tr>
<tr>
<td>States</td>
<td>Section</td>
</tr>
</tbody>
</table>
Creating a Remote Authentication Provider

Creating a TACACS+ Provider

### Step 4
In the Actions area of the General tab, click **Create RADIUS Provider**.

### Step 5
In the **Create RADIUS Provider** dialog box:

a) Complete the fields with the information about the RADIUS service you want to use.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hostname (or IP Address)</strong> field</td>
<td>The hostname or IP address on which the RADIUS provider resides.</td>
</tr>
<tr>
<td><strong>Key</strong> field</td>
<td>The SSL encryption key for the database.</td>
</tr>
<tr>
<td><strong>Confirm Key</strong> field</td>
<td>The SSL encryption key repeated for confirmation purposes.</td>
</tr>
<tr>
<td><strong>Authorization Port</strong> field</td>
<td>The port through which Cisco UCS communicates with the RADIUS database.</td>
</tr>
</tbody>
</table>

b) Click **OK**.

### Step 6
Click **Save Changes**.

---

### What to Do Next
Select RADIUS as the primary authentication service. For more information, see Selecting a Primary Authentication Service, page 75.

### Creating a TACACS+ Provider

#### Before You Begin
Perform the following configuration in the TACACS+ server:

- Create the cisco-av-pairs 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.
Creating 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 Complete the following field in the Properties area:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout field</td>
<td>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.</td>
</tr>
</tbody>
</table>

Step 4 In the Actions area of the General tab, click Create TACACS Provider.
Step 5 In the Create TACACS+ Provider dialog box:

a) Complete the fields with the information about the TACACS service you want to use.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname (or IP Address) field</td>
<td>The hostname or IP address on which the TACAS provider resides.</td>
</tr>
<tr>
<td>Key field</td>
<td>The SSL encryption key for the database.</td>
</tr>
<tr>
<td>Confirm Key field</td>
<td>The SSL encryption key repeated for confirmation purposes.</td>
</tr>
<tr>
<td>Port field</td>
<td>The port through which the system should communicate with the TACACS+ database.</td>
</tr>
</tbody>
</table>

b) Click OK.

Step 6 Click Save Changes.

What to Do Next

Select TACACS as the primary authentication service. For more information, see Selecting a Primary Authentication Service, page 75.
Deleting a Remote Authentication Provider

Deleting an LDAP Provider

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Navigation pane, click the Admin tab.</td>
</tr>
<tr>
<td>2</td>
<td>In the Admin tab, expand User Management ➤ LDAP.</td>
</tr>
<tr>
<td>3</td>
<td>Right-click the LDAP provider you want to delete and choose Delete.</td>
</tr>
<tr>
<td>4</td>
<td>If Cisco UCS Manager displays a confirmation dialog box, click Yes.</td>
</tr>
</tbody>
</table>

Deleting a RADIUS Provider

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Navigation pane, click the Admin tab.</td>
</tr>
<tr>
<td>2</td>
<td>In the Admin tab, expand User Management ➤ RADIUS.</td>
</tr>
<tr>
<td>3</td>
<td>Right-click the RADIUS provider you want to delete and choose Delete.</td>
</tr>
<tr>
<td>4</td>
<td>If Cisco UCS Manager displays a confirmation dialog box, click Yes.</td>
</tr>
</tbody>
</table>

Deleting a TACACS+ Provider

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Navigation pane, click the Admin tab.</td>
</tr>
<tr>
<td>2</td>
<td>In the Admin tab, expand User Management ➤ TACACS+.</td>
</tr>
<tr>
<td>3</td>
<td>Right-click the TACACS+ provider you want to delete and choose Delete.</td>
</tr>
<tr>
<td>4</td>
<td>If Cisco UCS Manager displays a confirmation dialog box, click Yes.</td>
</tr>
</tbody>
</table>

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 On the General tab, click the radio button for the primary authentication method you want to use.
Step 4 Click Save Changes.
CHAPTER 8

Configuring Organizations

This chapter includes the following sections:

- Organizations in a Multi-Tenancy Environment, page 77
- Hierarchical Name Resolution in a Multi-Tenancy Environment, page 78
- Creating an Organization under the Root Organization, page 79
- Creating an Organization under an Organization that is not Root, page 80
- Deleting an Organization, page 80

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 Cisco UCS user privileges and roles by organization, if you do not want all users to have access to all organizations.

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
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 Create Organization dialog box, perform the following steps:

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

**Step 3** Right-click on the organization under which you want to create the new organization and choose Create Organization.

**Step 4** In the Create Organization dialog box, perform the following steps:

a) In the Name field, 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.

b) 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 on the organization and choose Delete.

**Step 4** If Cisco UCS Manager displays a confirmation dialog box, click Yes.
Configuring Role-Based Access Control

This chapter includes:

- Role-Based Access Control, page 81
- User Accounts, page 81
- User Roles, page 82
- Privileges, page 83
- User Locales, page 85
- Configuring User Roles, page 85
- Configuring Locales, page 87
- Configuring User Accounts, page 89
- Monitoring User Sessions, page 91

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 would not be able to 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 user name and password.
The system 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.

Each user account must have a unique user name that is not all-numeric and does not start with a number. If an all-numeric user name exists on an AAA server (RADIUS or TACACS+) and is entered during login, the user is not logged in. Local users with all numeric names cannot be created.

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

- At least eight characters long
- Does not contain more than three consecutive characters, such as abcd
- Does not contain more than two repeating characters, such as aaabbb
- Does not contain dictionary words
- Does not contain common proper names

A user account can also be set with a SSH public key. The public key can be set in one of the two formats: OpenSSH and SECSH.

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, then users who are assigned to both Role1 and Role2 have storage and server related privileges.

All roles include read access to all configuration on the system. 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.
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 1: Privileges and Default Role Assignments

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>Default Role Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>System security and AAA</td>
<td>AAA Administrator</td>
</tr>
<tr>
<td>admin</td>
<td>System administration</td>
<td>Administrator</td>
</tr>
<tr>
<td>ext-lan-config</td>
<td>External LAN configuration</td>
<td>Network Administrator</td>
</tr>
<tr>
<td>ext-lan-policy</td>
<td>External LAN policy</td>
<td>Network Administrator</td>
</tr>
<tr>
<td>ext-lan-qos</td>
<td>External LAN QoS</td>
<td>Network Administrator</td>
</tr>
<tr>
<td>ext-lan-security</td>
<td>External LAN security</td>
<td>Network Administrator</td>
</tr>
<tr>
<td>ext-san-config</td>
<td>External SAN configuration</td>
<td>Storage Administrator</td>
</tr>
<tr>
<td>ext-san-policy</td>
<td>External SAN policy</td>
<td>Storage Administrator</td>
</tr>
<tr>
<td>ext-san-qos</td>
<td>External SAN QoS</td>
<td>Storage Administrator</td>
</tr>
<tr>
<td>Privilege</td>
<td>Description</td>
<td>Default Role Assignment</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>ext-san-security</td>
<td>External SAN security</td>
<td>Storage Administrator</td>
</tr>
<tr>
<td>fault</td>
<td>Alarms and alarm policies</td>
<td>Operations</td>
</tr>
<tr>
<td>operations</td>
<td>Logs and Smart Call Home</td>
<td>Operations</td>
</tr>
<tr>
<td>pod-config</td>
<td>Pod configuration</td>
<td>Network Administrator</td>
</tr>
<tr>
<td>pod-policy</td>
<td>Pod policy</td>
<td>Network Administrator</td>
</tr>
<tr>
<td>pod-qos</td>
<td>Pod QoS</td>
<td>Network Administrator</td>
</tr>
<tr>
<td>pod-security</td>
<td>Pod security</td>
<td>Network Administrator</td>
</tr>
<tr>
<td>read-only</td>
<td>Read-only access</td>
<td>Read-Only</td>
</tr>
<tr>
<td>server-equipment</td>
<td>Server hardware management</td>
<td>Server Equipment Administrator</td>
</tr>
<tr>
<td>server-maintenance</td>
<td>Server maintenance</td>
<td>Server Equipment Administrator</td>
</tr>
<tr>
<td>server-policy</td>
<td>Server policy</td>
<td>Server Equipment Administrator</td>
</tr>
<tr>
<td>server-security</td>
<td>Server security</td>
<td>Server Security Administrator</td>
</tr>
<tr>
<td>service-profile-config</td>
<td>Service profile configuration</td>
<td>Server Profile Administrator</td>
</tr>
<tr>
<td>service-profile-config-policy</td>
<td>Service profile configuration policy</td>
<td>Server Profile Administrator</td>
</tr>
<tr>
<td>service-profile-ext-access</td>
<td>Service profile end point access</td>
<td>Server Profile Administrator</td>
</tr>
<tr>
<td>service-profile-network</td>
<td>Service profile network</td>
<td>Network Administrator</td>
</tr>
<tr>
<td>service-profile-network-policy</td>
<td>Service profile network policy</td>
<td>Network Administrator</td>
</tr>
<tr>
<td>service-profile-qos</td>
<td>Service profile QoS</td>
<td>Network Administrator</td>
</tr>
<tr>
<td>service-profile-qos-policy</td>
<td>Service profile QoS policy</td>
<td>Network Administrator</td>
</tr>
<tr>
<td>service-profile-security</td>
<td>Service profile security</td>
<td>Server Security Administrator</td>
</tr>
<tr>
<td>service-profile-security-policy</td>
<td>Service profile security policy</td>
<td>Server Security Administrator</td>
</tr>
<tr>
<td>service-profile-server</td>
<td>Service profile server management</td>
<td>Server Security Administrator</td>
</tr>
<tr>
<td>service-profile-server-policy</td>
<td>Service profile pool policy</td>
<td>Server Security Administrator</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Navigation pane, click the Admin tab.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Admin tab, expand All ➤ User Management ➤ User Services.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Right-click User Services and choose Create Role.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Create Role dialog box, complete the following fields:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>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.</td>
</tr>
<tr>
<td>Privileges list box</td>
<td>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.</td>
</tr>
</tbody>
</table>
Adding Privileges to a User Role

Procedure

Step 1 In the Navigation pane, click the Admin tab.
Step 2 In 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 In 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 automatically removes that role from all user accounts to which the role has been assigned.
Configuring Locales

Creating a Locale

Before You Begin

One or more organizations must exist before you create a locale.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Admin tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Admin tab, expand All ➤ User Management ➤ User Services.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Expand the Roles node.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Right-click the role you want to delete and choose Delete.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Delete dialog box, click Yes.</td>
</tr>
</tbody>
</table>

What to Do Next

Add the locale to one or more user accounts.
Adding an Organization to a Locale

Procedure

Step 1 In the Navigation pane, click the Admin tab.
Step 2 In 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 page, do the following:
   a) Expand the Organizations area to view the organizations in the Cisco UCS instance.
   b) Click on an organization that you want to assign to the locale.
   c) Drag the organization from the Organizations area and drop it into the design area on the right.
   d) Repeat Steps b and c until you have assigned all desired organizations to the locale.
Step 7 Click OK.

Deleting an Organization from aLocale

Procedure

Step 1 In the Navigation pane, click the Admin tab.
Step 2 In 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 on 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 In the Admin tab, expand All ➤ User Management ➤ User Services.
Step 3 Expand the Locales node.
Step 4 Right-click on the locale you want to delete and choose Delete.
Step 5 If Cisco UCS Manager 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

If the system includes:

- 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 will be created in root and will have 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
In 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login ID field</td>
<td>The account name that is used when logging into this account. The login ID can contain between 1 and 32 characters, including:</td>
</tr>
<tr>
<td></td>
<td>- Any alphabetic character</td>
</tr>
<tr>
<td></td>
<td>- Any digit</td>
</tr>
<tr>
<td></td>
<td>- _ (underscore)</td>
</tr>
<tr>
<td></td>
<td>- - (dash)</td>
</tr>
<tr>
<td></td>
<td>- @</td>
</tr>
</tbody>
</table>

After you save the user, the login ID cannot be changed.

Note
You can create up to 48 user accounts in a Cisco UCS system.
### Configuring User Accounts

#### Creating a User Account

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>First Name</strong></td>
<td>The first name of the user. This field can contain up to 32 characters.</td>
</tr>
<tr>
<td><strong>Last Name</strong></td>
<td>The last name of the user. This field can contain up to 32 characters.</td>
</tr>
<tr>
<td><strong>Email</strong></td>
<td>The email address for the user.</td>
</tr>
<tr>
<td><strong>Phone</strong></td>
<td>The telephone number for the user.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password associated with this account.</td>
</tr>
<tr>
<td></td>
<td>The password must contain at least 8 characters and it must pass a basic</td>
</tr>
<tr>
<td></td>
<td>strength check. A strong password contains a mix of the alphanumeric</td>
</tr>
<tr>
<td></td>
<td>characters, including uppercase and lowercase letters. It can also contain</td>
</tr>
<tr>
<td></td>
<td>special characters such as !, @, or #.</td>
</tr>
<tr>
<td></td>
<td>Passwords cannot contain the characters $ (dollar sign) or ? (question mark)</td>
</tr>
<tr>
<td><strong>Confirm Password</strong></td>
<td>The password a second time for confirmation purposes.</td>
</tr>
<tr>
<td><strong>Password Expires</strong></td>
<td>If checked, this password expires and must be changed on a given date.</td>
</tr>
<tr>
<td><strong>Expiration Date</strong></td>
<td>If <strong>Password Expires</strong> is checked, this field specifies the date on which</td>
</tr>
<tr>
<td></td>
<td>the password expires. The date should be in the format yyyy-mm-dd.</td>
</tr>
<tr>
<td></td>
<td>Click the down arrow at the end of this field to view a calendar that you</td>
</tr>
<tr>
<td></td>
<td>can use to select the expiration date.</td>
</tr>
</tbody>
</table>

#### 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 boxes in the **Locales** area to assign the user to the appropriate locales.

#### Step 7
(Optional) If the system uses SSH for authentication instead of passwords, complete the following fields in the **SSH** area:

- a) In the **Type** field, check the **Key** option.
- b) In the **SSH data** field, enter the SSH key.

#### Step 8
Click **OK**.
Deleting a Locally Authenticated User Account

Procedure

Step 1 In the Navigation pane, click the Admin tab.
Step 2 In 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name column</td>
<td>The name for the session.</td>
</tr>
<tr>
<td>User column</td>
<td>The username that is involved in the session.</td>
</tr>
<tr>
<td>Fabric ID column</td>
<td>The fabric interconnect that the user logged in to for the session.</td>
</tr>
<tr>
<td>Login Time column</td>
<td>The date and time the session started.</td>
</tr>
<tr>
<td>Terminal Type column</td>
<td>The kind of terminal the user is logged in through.</td>
</tr>
<tr>
<td>Host column</td>
<td>The IP address from which the user is logged in.</td>
</tr>
</tbody>
</table>
Firmware Management

This chapter includes:

- Overview of Firmware, page 93
- Image Management, page 93
- Firmware Updates, page 94
- Firmware Downgrades, page 98
- Downloading and Managing Images, page 99
- Directly Updating Firmware at Endpoints, page 101
- Updating Firmware through Service Profiles, page 106
- Verifying Firmware Versions on Components, page 109

Overview of Firmware

Cisco UCS uses firmware obtained from and certified by Cisco to upgrade firmware on the following components:

- Servers, including the BIOS, storage controller, and server controller (BMC)
- Adapters, including NIC and HBA firmware, and Option ROM (where applicable)
- I/O modules
- Fabric interconnects
- Cisco UCS Manager

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. These views are:

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.

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. A package is automatically deleted after all images in the package are deleted.

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.

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 Updates

You can use any of the Cisco UCS Manager interfaces to update firmware in the system, including Cisco UCS Manager GUI and the Cisco UCS Manager CLI.

You can use either of the following methods to update the firmware:

- Direct update at the endpoints.
• Updates to server components through service profiles that include a host firmware package policy and a management firmware package policy.

Note
Direct update is not available for some server components, such as BIOS and storage controller.

Firmware Versions
The firmware versions on a component depend upon the type of component.

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 the GUI and CLI:

Running Version
The running version is the firmware that is currently active and in use by the component.

Startup Version
The startup version is the firmware that will be used when the component next boots up. Cisco UCS Manager provides the activate operation to change the startup version.

Backup Version
The backup version is the firmware that is sitting in the other slot and is not in use by the component. This can be firmware that you have updated to the component but have not yet activated, or it can be an older firmware version that was replaced by a recent activate. Cisco UCS Manager provides the update operation to replace the image in the backup slot.

If the component cannot boot from the startup version, the component boots from the backup version.

Firmware Versions in the Fabric Interconnect and Cisco UCS Manager
You can update 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 flash memory.

Note
There are running and startup versions of the fabric interconnect and Cisco UCS Manager firmware, but there are no backup versions.

Direct Firmware Update at Endpoints
You can perform direct firmware updates on the following endpoints:

• Fabric interconnects
You cannot update the BIOS firmware directly. You must perform the BIOS firmware update through a host firmware package in a service profile.

**Stages of a Direct Firmware Update**

Cisco UCS Manager separates the direct update process into stages to ensure that you can push the firmware to a component while the system is running without affecting uptime on the server or other components. Because you do not need to reboot the server until after you activate, you can perform that task overnight or during other maintenance periods.

When you manually update firmware, the following stages occur:

**Update**

During this stage, the system pushes the selected firmware version to the component. The update process always overwrites the firmware in the backup slot on the component. The update stage applies only to I/O modules, BMCs, and adapters.

**Activate**

During this stage, the system sets the specified image version (normally the backup version) as active and reboots the endpoint. When the endpoint is rebooted, the backup slot becomes the active slot, and the active slot becomes the backup slot. The firmware in the new active slot becomes the startup version and the running version.

If the component cannot boot from the startup firmware, it defaults to the backup version and raises an alarm.

**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 following order for quicker activation:

1. Adapter
2. BMC
3. I/O module
4. Fabric interconnect
Consider the following when activating the firmware:

- You can update all components in parallel.
- While activating adapter and I/O Modules, you can use the set-startup-only option to set the startup version and skip the reset.
- Activating a fabric interconnect resets all I/O Modules connected to it in addition to resetting itself.

Firmware Updates through Service Profiles

You can use service profiles to update 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 update the firmware on an I/O module, fabric interconnect, or Cisco UCS Manager through service profiles. You must update the firmware on those components directly.

Host Firmware Pack

This policy enables you to specify a common set of firmware versions that make up the host firmware pack. The host firmware includes the following server and adapter components:

- BIOS
- SAS controller
- Emulex Option ROM (applicable only to Emulex-based Converged Network Adapters [CNAs])
- Emulex firmware (applicable only to Emulex-based CNAs)
- QLogic option ROM (applicable only to QLogic-based CNAs)
- Adapter firmware

The firmware pack 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 of the component in the firmware pack, 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 while associating the service profile, UCSM will just ignore firmware update and complete association.

Management Firmware Pack
This policy enables you to specify a common set of firmware versions that make up the management firmware pack. The management firmware includes the server controller (BMC) on the server.
The firmware pack 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 Update through Service Profiles
If you use policies in service profiles to update server and adapter firmware, you must complete 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.

Associate
During this stage, you include a firmware policy in a service profile, and then associate the service profile with a server. The system pushes the selected firmware versions to the endpoints and reboots to ensure that the endpoints are running the versions specified in the firmware pack.
When the firmware versions in the policies change, the system automatically performs firmware updates (wherever necessary), activates, and reboots the endpoints.

Caution
This can be disruptive as endpoints reboot.

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In a web browser, navigate to the web link provided by Cisco to obtain firmware images for Cisco UCS.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select one or more firmware images and copy them to a network server.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Read the release notes provided with the image or images.</td>
</tr>
</tbody>
</table>

What to Do Next

Download the firmware image to the fabric interconnect.

Note

In a cluster setup, the firmware image is automatically 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 while downloading, the download still finishes successfully. The images are synced to the other fabric interconnect when it comes back online.

Checking the Available Space on a Fabric Interconnect

You cannot download new firmware images if the bootflash on the fabric interconnect or fabric interconnects in the Cisco UCS does not have sufficient available space. In a cluster system, the available space is the same on both fabric interconnects because Cisco UCS mirrors the configuration on both fabric interconnects.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Navigation pane, click the Equipment tab.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Equipment tab, expand Equipment ➤ Fabric Interconnects.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Work pane, click the General tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Expand the Local Storage Information area. If the bootflash area does not have sufficient available space, you can delete obsolete images through the Firmware Management tab on the Equipment node.</td>
</tr>
</tbody>
</table>

Downloading Images to the Fabric Interconnect

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol field</td>
<td>The protocol to use when communicating with the remote server. This can be:</td>
</tr>
<tr>
<td></td>
<td>• FTP</td>
</tr>
<tr>
<td></td>
<td>• SCP</td>
</tr>
<tr>
<td></td>
<td>• SFTP</td>
</tr>
<tr>
<td></td>
<td>• TFTP</td>
</tr>
<tr>
<td>Server field</td>
<td>The IP address or hostname of the remote server on which the files resides.</td>
</tr>
<tr>
<td>Filename field</td>
<td>The name of the firmware executable you want to download.</td>
</tr>
<tr>
<td>Remote Path field</td>
<td>The absolute path to the file on the remote server, if required.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>User field</td>
<td>The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP.</td>
</tr>
<tr>
<td>Password field</td>
<td>The password for the remote server username. This field does not apply if the protocol is TFTP.</td>
</tr>
</tbody>
</table>

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 components.

Canceling an Image Download

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

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Navigation pane, click the Equipment tab.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Expand the Equipment node.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Work pane, select the Firmware Management tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>On the Download Tasks tab, right-click the task you want to cancel and select Delete.</td>
</tr>
</tbody>
</table>

Directly Updating Firmware at Endpoints

Updating the Firmware on Multiple Components

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Navigation pane, click the Equipment tab.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Equipment tab, select the Equipment Node.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Work pane, select the Firmware Management tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Installed Firmware tab, select Update Firmware.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Update Firmware dialog box:</td>
</tr>
<tr>
<td></td>
<td>a) For each component whose firmware you want to update, select the appropriate version from the drop-down list in the Backup Version column.</td>
</tr>
<tr>
<td></td>
<td>b) Click OK.</td>
</tr>
</tbody>
</table>

Cisco UCS Manager GUI copies the selected firmware package to the backup memory slot, where it remains until you explicitly activate it.

What to Do Next

Activate the firmware.

Activating the Firmware on Multiple Components

After you activate the firmware, you may need to reboot the server.
Procedure

Step 1  In the Navigation pane, click the Equipment tab.
Step 2  In the Equipment tab, select the Equipment Node.
Step 3  In the Work pane, select the Firmware Management tab.
Step 4  In the Installed Firmware tab, select Activate Firmware.
Step 5  In the Activate Firmware dialog box:
   a)  For each component whose firmware you want to update, select the appropriate version from the drop-down list in the Startup Version column.
   b)  Click OK.

Updating the Firmware on an Adapter

Procedure

Step 1  In the Navigation pane, click the Equipment tab.
Step 2  In 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:
   a)  From the Version drop-down list, select the firmware version to which you want to update the adapter.
   b)  Click OK.

Cisco UCS Manager copies the selected firmware package to the backup memory slot, where it remains until you explicitly activate it.

What to Do Next

Activate the firmware.
Activating the Firmware on an Adapter

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Navigation pane, click the Equipment tab.</td>
</tr>
<tr>
<td>2</td>
<td>In the Equipment tab, expand Equipment ➤ Chassis ➤ Chassis Number ➤ Servers.</td>
</tr>
<tr>
<td>3</td>
<td>Expand the node for the server that includes the adapter for which you want to activate the updated firmware.</td>
</tr>
<tr>
<td>4</td>
<td>Expand Interface Cards and select the interface card for the adapter.</td>
</tr>
<tr>
<td>5</td>
<td>In the General tab, click Activate Firmware.</td>
</tr>
</tbody>
</table>
| 6    | In the Activate Firmware dialog box:  
  a) Select the appropriate version from the Version To Be Activated drop-down list.  
  b) (Optional) If you want to activate the firmware regardless of any possible incompatibilities or currently-executing tasks, check the Ignore Compatibility Check checkbox.  
  c) Click OK. |

Updating the Firmware on a BMC

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Navigation pane, click the Equipment tab.</td>
</tr>
<tr>
<td>2</td>
<td>In the Equipment tab, expand Equipment ➤ Chassis ➤ Chassis Number ➤ Servers.</td>
</tr>
<tr>
<td>3</td>
<td>Expand the node for the server for which you want to update the BMC.</td>
</tr>
<tr>
<td>4</td>
<td>In the General tab, click the Inventory tab.</td>
</tr>
<tr>
<td>5</td>
<td>Click the BMC tab.</td>
</tr>
<tr>
<td>6</td>
<td>In the Actions area, click Update Firmware.</td>
</tr>
</tbody>
</table>
| 7    | In the Update Firmware dialog box:  
  a) From the Version drop-down list, select the firmware version to which you want to update the BMC.  
  b) (Optional) If you want to update the firmware regardless of any possible incompatibilities or currently-executing tasks, check the Force checkbox.  
  c) Click OK. |

Cisco UCS Manager copies the selected firmware package to the backup memory slot, where it remains until you explicitly activate it.

What to Do Next
Activate the firmware.
## Activating the Firmware on a BMC

### Procedure

1. **Step 1** In the Navigation pane, click the Equipment tab.
2. **Step 2** In the Equipment tab, expand Equipment ➤ Chassis ➤ Chassis Number ➤ Servers.
3. **Step 3** Expand the node for the server that includes the BMC for which you want to activate the updated firmware.
4. **Step 4** In the General tab, click the Inventory tab.
5. **Step 5** Click the BMC tab.
6. **Step 6** In the Actions area, click Activate Firmware.
7. **Step 7** In the Activate Firmware dialog box:
   - (a) Select the appropriate version from the Version To Be Activated drop-down list.
   - (b) (Optional) If you want to activate the firmware regardless of any possible incompatibilities or currently-executing tasks, check the Ignore Compatibility Check checkbox.
   - (c) Click OK.

## Updating the Firmware on an IOM

### Procedure

1. **Step 1** In the Navigation pane, click the Equipment tab.
2. **Step 2** In the Equipment tab, expand Equipment ➤ Chassis ➤ Chassis Number ➤ IO Modules.
3. **Step 3** Click the I/O module that you want to update.
4. **Step 4** In the General tab, click Update Firmware.
5. **Step 5** In the Update Firmware dialog box:
   - (a) From the Version drop-down list, select the firmware version to which you want to update the IOM.
   - (b) (Optional) If you want to update the firmware regardless of any possible incompatibilities or currently-executing tasks, check the Force checkbox.
   - (c) Click OK.

Cisco UCS Manager copies the selected firmware package to the backup memory slot, where it remains until you explicitly activate it.

### 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  In 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:
   a) Select the appropriate version from the Version To Be Activated drop-down list.
   b) (Optional) If you want to activate the firmware regardless of any possible incompatibilities or currently-executing tasks, check the Ignore Compatibility Check checkbox.
   c) Click OK.

Updating and Activating the Firmware on a Fabric Interconnect

Procedure

Step 1  In the Navigation pane, click the Equipment tab.
Step 2  In the Equipment tab, expand the Equipment node.
Step 3  Expand the Fabric Interconnects node and click the fabric interconnect for which you want to update and activate the firmware.
Step 4  In the General tab, click Activate Firmware.
Step 5  In the Activate Firmware dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kernel Version drop-down list</td>
<td>Choose the version that you want to use for the kernel.</td>
</tr>
<tr>
<td>System Version drop-down list</td>
<td>Choose the version you want to use for the system.</td>
</tr>
<tr>
<td>Ignore Compatibility Check check box</td>
<td>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.</td>
</tr>
</tbody>
</table>

Step 6  Click OK.
Cisco UCS Manager updates and activates the firmware, and then reboots the fabric interconnect.
Updating and Activating the Cisco UCS Manager Software

You can also update Cisco UCS Manager when you update and activate the fabric interconnect firmware.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Navigation pane, click the Equipment tab.</td>
</tr>
<tr>
<td>2</td>
<td>Click the Equipment tab, expand the Equipment node.</td>
</tr>
<tr>
<td>3</td>
<td>Select the Fabric Interconnects node.</td>
</tr>
<tr>
<td>4</td>
<td>In the Work pane, click the Installed Firmware tab.</td>
</tr>
<tr>
<td>5</td>
<td>Click Activate Firmware.</td>
</tr>
<tr>
<td>6</td>
<td>On the UCS Manager row of the Activate Firmware dialog box:</td>
</tr>
<tr>
<td></td>
<td>a) From the drop-down list in the Startup Version column, select the version to which you want to update the software.</td>
</tr>
<tr>
<td></td>
<td>b) (Optional) If you want to activate the firmware regardless of any possible incompatibilities or currently-executing tasks, check the Ignore Compatibility Check checkbox.</td>
</tr>
<tr>
<td></td>
<td>c) Click OK.</td>
</tr>
</tbody>
</table>

Cisco UCS Manager disconnects, and then updates and activates the software.

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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Navigation pane, click the Servers tab.</td>
</tr>
<tr>
<td>2</td>
<td>In the Servers tab, expand Servers ➤ Policies.</td>
</tr>
<tr>
<td>3</td>
<td>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.</td>
</tr>
<tr>
<td>4</td>
<td>Right-click Host Firmware Packages and select Create Package.</td>
</tr>
<tr>
<td>5</td>
<td>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.</td>
</tr>
<tr>
<td>6</td>
<td>Click the down arrows to expand one or more of the following sections on the left of the dialog box:</td>
</tr>
</tbody>
</table>
• 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 component to which you want to include firmware in the pack:
   a) Select the line in the table which lists the firmware version that you want to add to the pack.
   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 associated with a service profile, 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** In 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** In 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 component 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.
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  In 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:
a) Click the down arrows to expand the section.
b) Select the line in the table which lists the firmware version that you want to add to the package.
c) Drag the line to the table on the right.
d) Click Yes to confirm that you selected the correct version.
Step 7  When you have added the desired firmware to the package, click OK.

What to Do Next

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

Updating a Management Firmware Pack

If the policy is associated with a service profile, 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  In 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.
   b)  Select the line in the table which lists the firmware version that you want to add to the pack.
   c)  Drag the line to the table on the right.
   d)  Click Yes to confirm that you selected the correct version.
Step 7  Click Save Changes.

Verifying Firmware Versions on Components

Procedure

Step 1  In the Navigation pane, click the Equipment tab.
Step 2  In the Equipment tab, select the Equipment Node.
Step 3  In the Work pane, select the Firmware Management tab.
Step 4  In the Installed Firmware tab, review the firmware versions listed for each component.
Configuring DNS Servers

This chapter includes:

- DNS Servers in Cisco UCS, page 111
- Adding a DNS Server, page 111
- Deleting a DNS Server, page 112

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 host names. For example, you cannot use a name such as www.cisco.com on a fabric interconnect if you do not configure a DNS server.

Adding a DNS Server

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Admin tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Admin tab, expand All ➤ Communication Services.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click DNS Management.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Work pane, click the General tab.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the DNS Server area, click +.</td>
</tr>
<tr>
<td>Step 6</td>
<td>In the Specify DNS Server dialog box, enter the IP address of the DNS server.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Click OK.</td>
</tr>
</tbody>
</table>
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 on the DNS server you want to delete and choose Delete.
Step 6 If Cisco UCS Manager displays a confirmation dialog box, click Yes.
Step 7 Click Save Changes.
PART III

Network Configuration

• Using the LAN Uplinks Manager, page 115
• Configuring Named VLANs, page 127
• Configuring LAN Pin Groups, page 131
• Configuring MAC Pools, page 133
• Configuring Quality of Service, page 135
• Configuring Network-Related Policies, page 141
Using the LAN Uplinks Manager

This chapter includes:

- Launching the LAN Uplinks Manager, page 115
- Changing the Ethernet Switching Mode with the LAN Uplinks Manager, page 116
- Configuring a Port with the LAN Uplinks Manager, page 116
- Configuring Server Ports, page 117
- Configuring Uplink Ethernet Ports, page 118
- Configuring Uplink Ethernet Port Channels, page 119
- Configuring LAN Pin Groups, page 121
- Configuring Named VLANs, page 122
- Configuring QoS System Classes with the LAN Uplinks Manager, page 124

Launching the LAN Uplinks Manager

Procedure

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

Step 2
In 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.

**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 displays a confirmation dialog box, click **Yes**.
Configuring Server Ports

Enabling a Server Port with the LAN Uplinks Manager

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the LAN Uplinks Manager, click the LAN Uplinks tab.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Ports area, click the down arrows to expand the Server Ports section.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Expand Fabric Interconnects ➤ Fabric_Interconnect_Name.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Right-click the port that you want to enable and choose Enable.</td>
</tr>
</tbody>
</table>

Disabling a Server Port with the LAN Uplinks Manager

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the LAN Uplinks Manager, click the LAN Uplinks tab.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Ports area, click the down arrows to expand the Server Ports section.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Expand Fabric Interconnects ➤ Fabric_Interconnect_Name.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Right-click the port that you want to disable and choose Disable.</td>
</tr>
<tr>
<td>Step 5</td>
<td>If Cisco UCS Manager displays a confirmation dialog box, click Yes.</td>
</tr>
</tbody>
</table>

Unconfiguring a Server Port with the LAN Uplinks Manager

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the LAN Uplinks Manager, click the LAN Uplinks tab.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Ports area, click the down arrows to expand the Server Ports section.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Expand Fabric Interconnects ➤ Fabric_Interconnect_Name.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Right-click the port that you want to unconfigure and choose Unconfigure.</td>
</tr>
<tr>
<td>Step 5</td>
<td>If Cisco UCS Manager displays a confirmation dialog box, click Yes.</td>
</tr>
</tbody>
</table>
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 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 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 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID field</td>
<td>The identifier for the port channel.</td>
</tr>
<tr>
<td>Name field</td>
<td>A user-defined name for the port channel.</td>
</tr>
<tr>
<td></td>
<td>This name can be between 1 and 16 alphanumeric characters. You cannot use</td>
</tr>
<tr>
<td></td>
<td>spaces or any special characters, and you cannot change this name after</td>
</tr>
<tr>
<td></td>
<td>the object has been saved.</td>
</tr>
</tbody>
</table>

  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 on the port channel that you want to enable and choose **Enable Port Channel**.
Step 4 If Cisco UCS Manager 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 on the port channel that you want to disable and choose **Disable Port Channel**.
Step 4 If Cisco UCS Manager 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 on 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 on the port you want to remove from the port channel and choose Delete.
Step 5 If Cisco UCS Manager 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 on the port channel you want to delete and choose Delete.
Step 4 If Cisco UCS Manager 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the LAN Uplinks Manager, click the LAN Uplinks tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Pin Groups area, right-click the pin group you want to delete and choose Delete.</td>
</tr>
<tr>
<td>Step 3</td>
<td>If Cisco UCS Manager displays a confirmation dialog box, click Yes.</td>
</tr>
</tbody>
</table>

---

### 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 4048. This range of VLAN IDs is reserved.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the LAN Uplinks Manager, click the VLANs tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>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.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Create VLAN dialog box, complete the following fields:</td>
</tr>
<tr>
<td></td>
<td><strong>Name</strong></td>
</tr>
<tr>
<td>Name field</td>
<td>The name of the virtual LAN.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
<tr>
<td>Configuration options</td>
<td>You can select:</td>
</tr>
<tr>
<td></td>
<td>• Common/Global—This VLAN applies to both fabrics and uses the same configuration parameters in both cases</td>
</tr>
<tr>
<td></td>
<td>• Fabric A—The VLAN only applies to fabric A</td>
</tr>
<tr>
<td></td>
<td>• Fabric B—The VLAN only applies to fabric B</td>
</tr>
<tr>
<td></td>
<td>• Both Fabrics Configured Differently—This VLAN applies to both fabrics but it enables you to specify a different VLAN ID for each fabric.</td>
</tr>
<tr>
<td>VLAN ID field</td>
<td>Enter a numeric ID for this VLAN. This value can:</td>
</tr>
<tr>
<td></td>
<td>• Be in the range from 1 to 3967</td>
</tr>
<tr>
<td></td>
<td>• Be in the range from 4049 to 4093</td>
</tr>
<tr>
<td></td>
<td>• Overlap with other VLAN IDs already defined on the system</td>
</tr>
<tr>
<td>Important</td>
<td>The VLAN IDs from 3968 to 4048 are reserved. You cannot specify an ID within this range.</td>
</tr>
<tr>
<td>Check Overlap button</td>
<td>Click this button to determine whether the VLAN ID overlaps with any other IDs on the system.</td>
</tr>
</tbody>
</table>

**Step 4**

Click **OK**.
Cisco UCS Manager GUI 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 includes a named VLAN with the same VLAN ID as the one you delete, the VLAN will not be 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:

<table>
<thead>
<tr>
<th>Subtab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Displays all VLANs in the Cisco UCS instance.</td>
</tr>
<tr>
<td>Dual Mode</td>
<td>Displays the VLANs that are accessible to both fabric interconnects.</td>
</tr>
<tr>
<td>Fabric A</td>
<td>Displays the VLANs that are accessible to only fabric interconnect A.</td>
</tr>
<tr>
<td>Fabric B</td>
<td>Displays the VLANs that are accessible to only fabric interconnect B.</td>
</tr>
</tbody>
</table>

**Step 3** In the table, click the VLAN you want to delete. You can use the Shift or Ctrl keys to select multiple entries.

**Step 4** Right-click the highlighted VLAN or VLANs and select Delete.

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

### Configuring QoS System Classes with the LAN Uplinks Manager

#### 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 Priority.  
**Note** This field is always checked for Best Effort Priority and Fibre Channel Priority. |
| 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.  
**Note** This field is set to 7 for internal traffic and to any for Best Effort Priority. Both of these values are reserved and cannot be assigned to any other priority. |
### Name | Description
--- | ---
Packet Drop check box | If checked, packet drop is allowed for this class. If unchecked, packets cannot be dropped during transmission. Besides the Fibre Channel Priority class, which never allows dropped packets, only one other class can have this field unchecked.

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 of 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 1538 and 9216. This value corresponds to the maximum packet size.
- fc—A predefined packet size of 2240.
- normal—A predefined packet size of 1359.

Note | This field is always set to fc for Fibre Channel Priority.

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 Priority.

### 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.
Configuring Named VLANs

This chapter includes:

- Named VLANs, page 127
- Creating a Named VLAN, page 127
- Deleting a Named VLAN, page 129

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 4048. This range of VLAN IDs is reserved.
Procedure

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

**Step 2** In 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name field</strong></td>
<td>The name of the virtual LAN. 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.</td>
</tr>
<tr>
<td><strong>Configuration options</strong></td>
<td>You can select:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Common/Global</strong>—This VLAN applies to both fabrics and uses the same configuration parameters in both cases</td>
</tr>
<tr>
<td></td>
<td>• <strong>Fabric A</strong>—The VLAN only applies to fabric A</td>
</tr>
<tr>
<td></td>
<td>• <strong>Fabric B</strong>—The VLAN only applies to fabric B</td>
</tr>
<tr>
<td></td>
<td>• <strong>Both Fabrics Configured Differently</strong>—This VLAN applies to both fabrics but it enables you to specify a different VLAN ID for each fabric.</td>
</tr>
<tr>
<td><strong>VLAN ID field</strong></td>
<td>Enter a numeric ID for this VLAN. This value can:</td>
</tr>
<tr>
<td></td>
<td>• Be in the range from 1 to 3967</td>
</tr>
<tr>
<td></td>
<td>• Be in the range from 4049 to 4093</td>
</tr>
<tr>
<td></td>
<td>• Overlap with other VLAN IDs already defined on the system</td>
</tr>
<tr>
<td><strong>Check Overlap button</strong></td>
<td>Click this button to determine whether the VLAN ID overlaps with any other IDs on the system.</td>
</tr>
</tbody>
</table>

**Step 6** Click **OK**.
Cisco UCS Manager GUI 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 includes a named VLAN with the same VLAN ID as the one you delete, the VLAN will not be removed from the fabric interconnect configuration until all named VLANs with that ID are deleted.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Navigation pane, click the LAN tab.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the LAN tab, click the LAN node.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Work pane, click the VLANs tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click one of the following subtabs, depending upon what type of VLAN you want to delete:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subtab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Displays all VLANs in the Cisco UCS instance.</td>
</tr>
<tr>
<td>Dual Mode</td>
<td>Displays the VLANs that are accessible to both fabric interconnects.</td>
</tr>
<tr>
<td>Fabric A</td>
<td>Displays the VLANs that are accessible to only fabric interconnect A.</td>
</tr>
<tr>
<td>Fabric B</td>
<td>Displays the VLANs that are accessible to only fabric interconnect B.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>In the table, click the VLAN you want to delete. You can use the Shift or Ctrl keys to select multiple entries.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td>Right-click the highlighted VLAN or VLANs and select <strong>Delete</strong>.</td>
</tr>
<tr>
<td>Step 7</td>
<td>If Cisco UCS Manager displays a confirmation dialog box, click <strong>Yes</strong>.</td>
</tr>
</tbody>
</table>
Configuring LAN Pin Groups

This chapter includes:

• LAN Pin Groups, page 131
• Creating a LAN Pin Group, page 131
• Deleting a LAN Pin Group, page 132

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.

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.
**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**.

**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.
Configuring MAC Pools

This chapter includes:

- MAC Pools, page 133
- Creating a MAC Pool, page 133
- Deleting a MAC Pool, page 134

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 will use 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 displays a confirmation dialog box, click Yes.
Configuring Quality of Service

This chapter includes:

- Quality of Service, page 135
- System Classes, page 135
- Quality of Service Policies, page 136
- Flow Control Policies, page 136
- Configuring QoS System Classes, page 137
- Creating a QoS Policy, page 138
- Deleting a QoS Policy, page 139
- Creating a Flow Control Policy, page 139
- Deleting a Flow Control Policy, page 140

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. System classes determine how the DCE bandwidth in these 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:

<table>
<thead>
<tr>
<th>System Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platinum Priority</td>
<td>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.</td>
</tr>
<tr>
<td>Gold Priority</td>
<td></td>
</tr>
<tr>
<td>Silver Priority</td>
<td></td>
</tr>
<tr>
<td>Bronze Priority</td>
<td></td>
</tr>
<tr>
<td>Best Effort Priority</td>
<td>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.</td>
</tr>
<tr>
<td>Fibre Channel Priority</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 Policies

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.

If you enable the send function, then 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, then the uplink Ethernet port will honor 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

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 General tab, 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 Priority.  
  **Note** This field is always checked for Best Effort Priority and Fibre Channel Priority. |
| 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.  
  **Note** This field is set to 7 for internal traffic and to any for Best Effort Priority. 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.  
  Besides the Fibre Channel Priority class, which never allows dropped packets, only one other class can have this field unchecked. |
| 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 of the channels.  
  2  Divides the channel weight by the sum of all weights to get a percentage. |
### Creating a QoS Policy

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>In the Navigation pane, click the LAN tab.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>In the LAN tab, expand LAN ➤ Policies.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Right-click QoS Policy and select Create QoS Policy.</td>
</tr>
</tbody>
</table>
| **Step 5** | In the Create QoS Policy dialog box:  
   a) In the Name field, enter a unique name for the policy.  
   b) From the Priority drop-down list, select the system class you want to assign to traffic through the vNIC.  
   c) Click OK. |

**What to Do Next**

Include the QoS policy in a vNIC template.
Deleting a QoS Policy

If you delete a QoS policy that is in use or disable a system class that is used in a QoS policy, any vNIC which uses that QoS policy will be assigned to the Best Effort Priority system class. In a system that implements multi-tenancy, Cisco UCS Manager will first attempt to find a matching QoS policy in the organization hierarchy.

Procedure

Step 1 In the Navigation pane, click the LAN tab.
Step 2 In 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 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 In 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 Flow Control Policies node and select Create Flow Control Policy.
Step 5 In the Create Flow Control Policy wizard, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>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.</td>
</tr>
<tr>
<td>Priority field</td>
<td>This can be:</td>
</tr>
</tbody>
</table>
### Deleting a Flow Control Policy

#### What to Do Next

Associate the flow control policy with an uplink Ethernet port or port channel.

#### Deleting a Flow Control Policy

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the <strong>Navigation</strong> pane, click the <strong>LAN</strong> tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the <strong>LAN</strong> tab, expand <strong>LAN ➤ Policies ➤ Organization_Name</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Expand the <strong>Flow Control Policies</strong> node.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Right-click the policy you want to delete and select <strong>Delete</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>If Cisco UCS Manager displays a confirmation dialog box, click <strong>Yes</strong>.</td>
</tr>
</tbody>
</table>

---

**Step 6**  Click **OK**.

---

**Name**

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>auto</strong>—Cisco UCS and the network negotiate whether PPP is used on this fabric interconnect</td>
</tr>
<tr>
<td>• <strong>on</strong>—PPP is enabled on this fabric interconnect</td>
</tr>
</tbody>
</table>

**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. |
Configuring Network-Related Policies

• Configuring vNIC Templates, page 141
• Configuring Ethernet Adapter Policies, page 144

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  In 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 on the vNIC Templates node and choose Create vNIC Template.

**Step 5** In the Create vNIC Template dialog box:

a) In the general section, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>The name of the vNIC template.</td>
</tr>
<tr>
<td>Description field</td>
<td>A user-defined description of the template.</td>
</tr>
<tr>
<td>Fabric ID field</td>
<td>The associated fabric interconnect. 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.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Target list box</th>
<th>A list of the possible targets for vNICs created from this template. This can be:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Adapter—vNICs apply to all adapters.</td>
</tr>
<tr>
<td></td>
<td>• VM—vNICs apply to all virtual machines.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Template Type field</th>
<th>This can be:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Initial Template—vNICs created from this template are not updated if the template changes.</td>
</tr>
<tr>
<td></td>
<td>• Updating Template—vNICs created from this template are updated if the template changes.</td>
</tr>
</tbody>
</table>

b) In the VLANs section, use the table to select the VLAN to assign to vNICs created from this template. The table contains the following columns:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select column</td>
<td>Check the box in this column to associate the VLAN with the vNIC template.</td>
</tr>
<tr>
<td>Name column</td>
<td>The name of the VLAN.</td>
</tr>
<tr>
<td>Native VLAN column</td>
<td>To designate one of the VLANs as the native VLAN, click the radio button in this column.</td>
</tr>
<tr>
<td>Create VLAN link</td>
<td>Click this link if you want to create a new VLAN.</td>
</tr>
</tbody>
</table>
c) In the Policies area, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Pool drop-down list</td>
<td>The MAC address pool that vNICs created from this vNIC template should use.</td>
</tr>
<tr>
<td>QoS Policy drop-down list</td>
<td>The quality of service policy that vNICs created from this vNIC template should use.</td>
</tr>
<tr>
<td>Pin Group drop-down list</td>
<td>The LAN pin group that vNICs created from this vNIC template should use.</td>
</tr>
<tr>
<td>Stats Threshold Policy drop-down list</td>
<td>The statistics collection policy that vNICs created from this vNIC template should use.</td>
</tr>
</tbody>
</table>

**Step 6** Click **OK**.

**What to Do Next**
Include the vNIC template in a service profile.

### Deleting a vNIC Template

**Procedure**

1. **Step 1** In the **Navigation** pane, click the **LAN** tab.
2. **Step 2** In the **LAN** tab, expand **LAN ➤ Policies ➤ Organization_Name**.
3. **Step 3** Expand the **vNIC Templates** node.
4. **Step 4** Right-click on the policy you want to delete and choose **Delete**.
5. **Step 5** If Cisco UCS Manager 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** In 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** In 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 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

Operating systems are sensitive to the settings in these policies. The configuration and selection of the policy is driven by the type of operating system.

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 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 policy. If the system does not include multi-tenancy, expand the root node.
Step 4 Right-click on Adapter Policies and choose Create Ethernet Adapter Policy.
Step 5 Enter a name and description for the policy in the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>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.</td>
</tr>
<tr>
<td>Description field</td>
<td>A description of the policy. We recommend including information about where and when the policy should be used.</td>
</tr>
</tbody>
</table>

Step 6 (Optional) In the Queues area, adjust the following values for the transmit, receive, and completion queues:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Count field</td>
<td>The number of queue resources to allocate. For transmit and receive queues, enter an integer between 1 and 256. For completion queues, enter an integer between 1 and 521. In general, the number of completion queues equals the number of transmit queues plus the number of receive queues.</td>
</tr>
<tr>
<td>Ring size field</td>
<td>The number of descriptors in each queue.</td>
</tr>
</tbody>
</table>
Step 7  (Optional) In the **Interrupt Handling** area, adjust the following values:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coalescing Time</td>
<td>The time to wait between interrupts or the idle period that must be</td>
</tr>
<tr>
<td></td>
<td>encountered before an interrupt is sent. Enter a value between 1 and 65535.</td>
</tr>
<tr>
<td></td>
<td>To turn off coalescing, enter 0 (zero) in this field.</td>
</tr>
<tr>
<td>Coalescing Type</td>
<td>This can be:</td>
</tr>
<tr>
<td></td>
<td>• min—The system waits for the time specified in the Coalescing Time field</td>
</tr>
<tr>
<td></td>
<td>before sending another interrupt event.</td>
</tr>
<tr>
<td></td>
<td>• idle—The system does not send an interrupt until there is a period of</td>
</tr>
<tr>
<td></td>
<td>no activity lasting as least as long as the time specified in the Coalescing</td>
</tr>
<tr>
<td></td>
<td>Time field.</td>
</tr>
<tr>
<td>Count</td>
<td>The number of interrupt resources to allocate.</td>
</tr>
<tr>
<td></td>
<td>Enter an integer between 1 and 514. In general, you should allocate one</td>
</tr>
<tr>
<td></td>
<td>interrupt resource for each completion queue.</td>
</tr>
</tbody>
</table>

Step 8  (Optional) In the **Performance Enhancement** area, adjust the following values:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive Checksum Offload</td>
<td>This can be:</td>
</tr>
<tr>
<td></td>
<td>• disabled—The CPU validates all packet checksums.</td>
</tr>
<tr>
<td></td>
<td>• enabled—The CPU sends all packet checksums to the hardware for validation.</td>
</tr>
<tr>
<td></td>
<td>This option may reduce CPU overhead.</td>
</tr>
<tr>
<td>Transmit Checksum Offload</td>
<td>This can be:</td>
</tr>
<tr>
<td></td>
<td>• disabled—The CPU calculates all packet checksums.</td>
</tr>
<tr>
<td></td>
<td>• enabled—The CPU sends all packets to the hardware so that the checksum</td>
</tr>
<tr>
<td></td>
<td>can be calculated. This option may reduce CPU overhead.</td>
</tr>
<tr>
<td>TCP Segment Offload</td>
<td>This can be:</td>
</tr>
<tr>
<td></td>
<td>• disabled—The CPU segments large TCP packets.</td>
</tr>
<tr>
<td></td>
<td>• enabled—The CPU sends large TCP packets to the hardware to be segmented.</td>
</tr>
<tr>
<td></td>
<td>This option may reduce CPU overhead and increase throughput rate.</td>
</tr>
</tbody>
</table>
Step 9  In the **RSS Hash** area, adjust the following values for the appropriate protocols:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Receive Side Scaling</strong></td>
<td>Receive-side Scaling (RSS) enables the efficient distribution of network receive processing across multiple CPUs in multiprocessor systems. This can be:</td>
</tr>
<tr>
<td></td>
<td>• <strong>disabled</strong>—The system does not use RSS.</td>
</tr>
<tr>
<td></td>
<td>• <strong>enabled</strong>—The system uses RSS.</td>
</tr>
<tr>
<td><strong>IP</strong> field</td>
<td>Whether IP is enabled for IPv4.</td>
</tr>
<tr>
<td><strong>TCP</strong> field</td>
<td>Whether TCP is enabled for IPv4.</td>
</tr>
</tbody>
</table>

**Note**  The setting of this field applies to all enabled protocols.

Step 10 In the **Failover** area, adjust the value for the following field:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Failback Timeout</strong> field</td>
<td>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.</td>
</tr>
</tbody>
</table>

Step 11  Click **OK**.
Deleting an Ethernet Adapter Policy

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the LAN tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the LAN tab, expand LAN ➤ Policies ➤ Organization_Name.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Expand the Adapter Policies node.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Right-click the Ethernet adapter policy that you want to delete and choose Delete.</td>
</tr>
<tr>
<td>Step 5</td>
<td>If Cisco UCS Manager displays a confirmation dialog box, click Yes.</td>
</tr>
</tbody>
</table>
PART IV

Storage Configuration

- Configuring Named VSANs, page 151
- Configuring SAN Pin Groups, page 155
- Configuring WWN Pools, page 157
- Configuring Storage-Related Policies, page 161
Configuring Named VSANs

This chapter includes:

- Named VSANs, page 151
- Creating a Named VSAN, page 151
- Deleting a Named VSAN, page 152

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

1. In the Navigation pane, click the SAN tab.
2. In the SAN tab, click the SAN node.
3. In the Work pane, click the VSANs tab.
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.
5. In the Create VSAN dialog box, complete the following fields:
<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
</table>
| **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 ID field for each fabric. |
| **VSAN ID** field | The unique identifier assigned to the network.  
The ID can be between 1 and 4093. |
| **FCoE VLAN ID** 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 includes a named VSAN with the same VSAN ID as the one you delete, the VSAN will not be 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:

<table>
<thead>
<tr>
<th>Subtab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>All</strong></td>
<td>Displays all VSANs in the Cisco UCS instance.</td>
</tr>
<tr>
<td><strong>Dual Mode</strong></td>
<td>Displays the VSANs that are accessible to both fabric interconnects.</td>
</tr>
<tr>
<td><strong>Switch A</strong></td>
<td>Displays the VSANs that are accessible to only fabric interconnect A.</td>
</tr>
<tr>
<td><strong>Switch B</strong></td>
<td>Displays the VSANs that are accessible to only fabric interconnect B.</td>
</tr>
</tbody>
</table>

**Step 5**  
In the table, click the VSAN you want to delete. You can use the Shift or Ctrl keys to select multiple entries.

**Step 6**  
Right-click the highlighted VSAN or VSANs and select **Delete**.

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

**Step 8**  
Click **OK**.
Configuring SAN Pin Groups

This chapter includes:

- SAN Pin Groups, page 155
- Creating a SAN Pin Group, page 155
- Deleting a SAN Pin Group, page 156

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 displays a confirmation dialog box, click Yes.
CHAPTER 20

Configuring WWN Pools

This chapter includes:

- WWN Pools, page 157
- Creating a WWNN Pool, page 158
- Deleting a WWNN Pool, page 159
- Creating a WWPN Pool, page 159
- Deleting a WWPN Pool, page 160

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:

- 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 which contains only WW node names. If you include a pool of WWNNs in a service profile, the associated server will be assigned a WWNN from that pool.
WWPN Pools

A WWPN pool is a WWN pool which 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 will be assigned a WWPN from that pool.

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 WWN Pool wizard:
   a) Enter a unique name and description for the WWN Pool.
   b) Click Next.
Step 6 In the Add WWN Blocks page of the Create WWN Pool wizard:
   a) Click Add.
   b) In the Create WWN Block page, enter the first WWN in the pool and the number of WWNs to include in the pool.
   c) Click Finish Stage.
   d) Do one of the following:
      • Repeat steps a through c to add another block to the pool
      • Click Next to move to the next page.
Step 7 In the Add Individual WWN page of the Create WWN Pool wizard:
   a) Click Add.
   b) In the World Wide Name field, enter the WWN initiator.
   c) In the Name field, enter a unique name for the WWN initiator.
   d) In the Description field, enter a description of the WWN initiator.
   e) Click Add to expand the Boot Target area.
   f) In the Boot Target WWN field, enter the WWN associated with the initiator.
   g) In the Boot Target LUN field, enter the unique identifier for the LUN associated with the initiator.
   h) Click OK.
Step 8 Click Finish.
What to Do Next
Include the WWN pool in a vHBA template.

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 displays a confirmation dialog box, click Yes.

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.
   b) Click Next.
Step 6 In the Add WWN Blocks page of the Create WWN Pool wizard:
   a) Click Add.
   b) In the Create WWN Block page, enter the first WWN in the pool and the number of WWNs to include in the pool.
   c) Click Finish Stage.
   d) Do one of the following:
      • Repeat steps a through c to add another block to the pool
Deleting a WWPN Pool

What to Do Next
Include the WWN pool in a vHBA template.

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 displays a confirmation dialog box, click Yes.
Configuring Storage-Related Policies

- Configuring vHBA SAN Connectivity Policies, page 161
- Configuring Fibre Channel Adapter Policies, page 164

Configuring vHBA SAN Connectivity Policies

vHBA Template

This policy defines how a vHBA on a server connects to the SAN. This policy 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**  
In 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 on the **vHBA Templates** node and choose **Create vHBA Template**.

**Step 5** In the **Create vHBA Template** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong> field</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>A user-defined description of the template.</td>
</tr>
<tr>
<td><strong>Fabric ID</strong> field</td>
<td>The name of the fabric interconnect that vHBAs created with this template are associated with.</td>
</tr>
<tr>
<td><strong>Template Type</strong></td>
<td>This can be:</td>
</tr>
<tr>
<td>field</td>
<td>- <strong>Initial Template</strong>—vHBAs created from this template are not updated if the template changes</td>
</tr>
<tr>
<td></td>
<td>- <strong>Updating Template</strong>—vHBAs created from this template are updated if the template changes</td>
</tr>
<tr>
<td><strong>WWN Pool</strong> drop-down list</td>
<td>The WWN pool that a vHBA created from this template uses to derive its WWN address.</td>
</tr>
<tr>
<td><strong>Pin Group</strong> drop-down list</td>
<td>The LAN pin group that is associated with vHBAs created from this template.</td>
</tr>
<tr>
<td><strong>Stats Threshold Policy</strong> drop-down list</td>
<td>The statistics collection policy that is associated with vHBAs created from this template.</td>
</tr>
</tbody>
</table>

**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  In the SAN tab, expand SAN ➤ Policies ➤ Organization_Name.
Step 3  Expand the vHBA Templates node.
Step 4  Right click on the vHBA template that you want to delete and choose Delete.
Step 5  If Cisco UCS Manager 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  In 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  In 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 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

Operating systems are sensitive to the settings in these policies. The configuration and selection of the policy is driven by the type of operating system.

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 SAN tab.

Step 2 In 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 on Fibre Channel Policies and choose Create Fibre Channel Adapter Policy.

Step 5 Enter a name and description for the policy in the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>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.</td>
</tr>
<tr>
<td>Description field</td>
<td>A description of the policy. We recommend including information about where and when the policy should be used.</td>
</tr>
</tbody>
</table>

Step 6 (Optional) In the Queues area, adjust the following values for the transmit, receive, and SCSI IO queues:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Count field</td>
<td>The number of SCSI IO queue resources the system should allocate. Enter an integer between 1 and 8.</td>
</tr>
<tr>
<td>Note</td>
<td>You can only have one transmit queue and one receive queue.</td>
</tr>
<tr>
<td>Ring size field</td>
<td>The number of descriptors in each queue. For transmit and receive queues, enter an integer between 64 and 128. For completion queues, enter an integer between 64 and 512.</td>
</tr>
</tbody>
</table>

Step 7 (Optional) In the FLogi/PLogi area, adjust the following values:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flogi Area</td>
<td>The number of times that the system tries to log into the fabric after the first failure. Enter an integer between 0 and 255. To specify that the system continue to try indefinitely, enter -1 in this field.</td>
</tr>
<tr>
<td>Retries field</td>
<td>The number of milliseconds that the system waits before it tries to log in again. Enter an integer between 1000 and 255000.</td>
</tr>
</tbody>
</table>
### Configuring Fibre Channel Adapter Policies

#### Creating a Fibre Channel Adapter Policy

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plogi Area</td>
<td>The number of times that the system tries to log into a port after the first failure. Enter an integer between 0 and 255.</td>
</tr>
<tr>
<td><strong>Retries</strong></td>
<td>The number of milliseconds that the system waits before it tries to log in again. Enter an integer between 1000 and 255000.</td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
<td>The number of milliseconds that the system waits before it tries to log in again. Enter an integer between 1000 and 255000.</td>
</tr>
</tbody>
</table>

#### Step 8
(Optional) In the **Error Handling** area, adjust the following values:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Error Detect Timeout</strong></td>
<td>The number of milliseconds to wait before the system assumes that there has been an error. Enter an integer between 1,000 and 100,000. The default is 2,000.</td>
</tr>
<tr>
<td><strong>Port Down Timeout</strong></td>
<td>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 240,000. The default is 10,000.</td>
</tr>
<tr>
<td><strong>Port Down IO Retry</strong></td>
<td>The number of times an IO request to a port is returned because the port is busy before the system decides the port is unavailable. Enter an integer between 0 and 255. The default is 8.</td>
</tr>
<tr>
<td><strong>Link Down Timeout</strong></td>
<td>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 240,000. The default is 30,000.</td>
</tr>
<tr>
<td><strong>Resource Allocation Timeout</strong></td>
<td>The number of milliseconds to wait before the system assumes that a resource cannot be properly allocated. Enter an integer between 5,000 and 100,000. The default is 10,000.</td>
</tr>
<tr>
<td><strong>FCP Error Recovery</strong></td>
<td>Whether the system uses FCP Sequence Level Error Recovery protocol (FC-TAPE). This can be:</td>
</tr>
<tr>
<td></td>
<td>• disabled</td>
</tr>
<tr>
<td></td>
<td>• enabled</td>
</tr>
</tbody>
</table>

#### Step 9
(Optional) In the **FC Port Behavior** area, adjust the following values:
### Configuring Fibre Channel Adapter Policies

#### IO Throttle Count field
The number of IO operations that can be pending in the vHBA at any given time.
Enter an integer between 256 and 4,096. The default is 512.

#### Max LUNs Per Target field
The maximum number of LUNs that the driver supports. This is usually an operating system platform limitation.
Enter an integer between 1 and 1,024. The default is 256.

#### 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 2,112. The default is 2,112.

**Step 10**  Click **OK**.

---

### Deleting a Fibre Channel Adapter Policy

#### Procedure

1. In the **Navigation** pane, click the **SAN** tab.
2. In the **SAN** tab, expand **SAN ➤ Policies ➤ Organization_Name**.
3. Expand the **Fibre Channel Policies** node.
4. Right-click on the policy you want to delete and choose **Delete**.
5. If Cisco UCS Manager displays a confirmation dialog box, click **Yes**.
Deleting a Fibre Channel Adapter Policy
PART V

Server Configuration

• Configuring Server-Related Pools, page 171
• Configuring Server-Related Policies, page 177
• Configuring Service Profiles, page 199
• Installing an OS on a Server, page 237
Configuring Server-Related Pools

- Configuring Server Pools, page 171
- Configuring UUID Suffix Pools, page 172
- Configuring the Management IP Pool, page 174

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 64GB 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 In 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:
### 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.

---

### Deleting a Server Pool

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Servers tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Servers tab, expand Servers ➤ Pools ➤ Organization_Name.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Expand the Server Pools node.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Right-click the pool you want to delete and select Delete.</td>
</tr>
<tr>
<td>Step 5</td>
<td>If Cisco UCS Manager displays a confirmation dialog box, click Yes.</td>
</tr>
</tbody>
</table>

---

### Configuring 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Servers tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Servers tab, expand Servers ➤ Pools.</td>
</tr>
<tr>
<td>Step 3</td>
<td>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.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Right click UUID Suffix Pools and select Create UUID Suffix Pool.</td>
</tr>
</tbody>
</table>
| Step 5 | In the Define Name and Description page of the Create UUID Suffix Pool wizard, fill in the following fields:  
| | **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  
| | The prefix for any UUID blocks created for this UUID pool, 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.  
| Step 7 | Do one of the following:  
| | • Repeat Steps a through c to add another block to the pool.  
| | • 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 In 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 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 server controller (BMC) in a server.

Cisco UCS Manager uses the IP addresses in a management IP pool for external access through serial over LAN and 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 on 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From field</td>
<td>The first IP address in the block.</td>
</tr>
<tr>
<td>Size field</td>
<td>The number of IP addresses in the pool.</td>
</tr>
<tr>
<td>Subnet Mask field</td>
<td>The subnet mask associated with the IP addresses in the block.</td>
</tr>
<tr>
<td>Default Gateway field</td>
<td>The default gateway associated with the IP addresses in the block.</td>
</tr>
</tbody>
</table>

Step 5 Click OK.
Deleting an IP Address Block from the Management IP Pool

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Admin tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Admin tab, expand All ➤ Communication Services ➤ Management IP Pool (ext-mgmt).</td>
</tr>
<tr>
<td>Step 3</td>
<td>Right-click on the IP address block that you want to delete and select Delete.</td>
</tr>
<tr>
<td>Step 4</td>
<td>If Cisco UCS Manager displays a confirmation dialog box, click Yes.</td>
</tr>
</tbody>
</table>
Configuring Server-Related Policies

- Configuring Boot Policies, page 177
- Configuring Chassis Discovery Policies, page 181
- Configuring IPMI Profiles, page 181
- Configuring Local Disk Configuration Policies, page 183
- Configuring Scrub Policies, page 185
- Configuring Serial over LAN Policies, page 187
- Configuring Server Autoconfiguration Policies, page 188
- Configuring Server Discovery Policies, page 190
- Configuring Server Inheritance Policies, page 191
- Configuring Server Pool Policies, page 192
- Configuring Server Pool Policy Qualifications, page 194

Configuring Boot Policies

Boot Policy

This 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.
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:

<table>
<thead>
<tr>
<th>Boot type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAN boot</td>
<td>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.</td>
</tr>
<tr>
<td>LAN boot</td>
<td>Boots from a centralized provisioning server. It is frequently used to install operating systems on a server from that server.</td>
</tr>
<tr>
<td>Local disk boot</td>
<td>If the server has a local drive, boots from that drive.</td>
</tr>
<tr>
<td>Virtual media boot</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

Procedure

1. In the Navigation pane, click the Servers tab.
2. In the Servers tab, expand Servers ➤ Policies.
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.
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.
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.
7. To add a local disk, virtual CD-ROM, or virtual floppy to the boot order:
   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.
8. To add a LAN boot to the boot order:
   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 associated vNIC in the vNIC field then click OK.
   d) Add another device to the Boot Order table or click OK to finish.
9. To add a SAN boot to the boot order:
   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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vHBA field</td>
<td>Enter the name of the vHBA you want to use for the SAN boot.</td>
</tr>
<tr>
<td>Type field</td>
<td>This can be:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot Target LUN field</td>
<td>The LUN that corresponds to the location of the boot image.</td>
</tr>
<tr>
<td>Boot Target WWN field</td>
<td>The WWN that corresponds to the location of the boot image.</td>
</tr>
<tr>
<td>Type field</td>
<td>This can be:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>

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 In 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 displays a confirmation dialog box, click Yes.
Configuring Chassis Discovery Policies

Chassis Discovery Policy

This discovery policy determines how the system reacts when you add a new chassis. If you create a chassis discovery policy, the system does the following:

- Automatically configures the chassis for the number of links between the chassis and the fabric interconnect specified in the policy.
- Specifies the power policy to be used by the chassis.

Configuring a Chassis Discovery Policy

Procedure

Step 1  In the Navigation pane, click the Equipment tab.
Step 2  On the Equipment node, select the Global Policies tab in the Work pane.
Step 3  From the Action drop-down list, select the number of links to be used by the chassis.
Step 4  In the Redundancy field of the Power Policy area, select one of the following options:
  - non-redundant
  - n+1
  - grid

Step 5  Click Save Changes.

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

- 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 In 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>The username to associate with this IPMI profile.</td>
</tr>
<tr>
<td>Password field</td>
<td>The password associated with this username.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The password a second time for confirmation purposes.</td>
</tr>
<tr>
<td>Role field</td>
<td>This can be:</td>
</tr>
<tr>
<td></td>
<td>• admin</td>
</tr>
<tr>
<td></td>
<td>• Read Only</td>
</tr>
</tbody>
</table>

   b) Click OK.
Step 8 Do one of the following:
   • Repeat Steps 6 and 7 to add another user.
   • 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 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 the RAID mode and the way the drives are partitioned.

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**: In 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.
- **Step 5**: In the Create Local Disk Configuration wizard, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>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.</td>
</tr>
</tbody>
</table>
### 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>In the Navigation pane, click the Servers tab.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>In the Servers tab, expand Servers ➤ Service Profiles.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Expand the organization that includes the service service profile with the local disk configuration policy you want to change.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use a Disk Policy</td>
<td>Select an existing local disk configuration policy from the list below this option. Cisco UCS Manager assigns this policy to the service profile.</td>
</tr>
<tr>
<td>Create a Local Disk Policy</td>
<td>Enables you to create a local disk configuration policy that can only be accessed by the selected service profile.</td>
</tr>
<tr>
<td>No Disk Policy</td>
<td>Does not use a local disk configuration policy for the selected service profile.</td>
</tr>
</tbody>
</table>

**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** In 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 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** In 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>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.</td>
</tr>
<tr>
<td>Description field</td>
<td>A description of the policy. We recommend including information about where and when the policy should be used.</td>
</tr>
<tr>
<td>Disk Scrub field</td>
<td>If this field is set to <em>yes</em>, 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 <em>no</em>, the contents of the disks are preserved.</td>
</tr>
<tr>
<td>BIOS Settings Scrub field</td>
<td>If this field is set to <em>yes</em>, when a service profile containing this scrub policy is associated with a server, the BIOS settings on that server are reset to the defaults. If this field is set to <em>no</em>, the BIOS settings are preserved.</td>
</tr>
</tbody>
</table>

**Step 6** Click *OK*.

Deleting a Scrub Policy

**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 *Scrub Policies* node.

**Step 4** Right-click the policy you want to delete and select *Delete*.

**Step 5** If Cisco UCS Manager 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
In 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>The name of the policy.</td>
</tr>
<tr>
<td></td>
<td>This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special</td>
</tr>
<tr>
<td></td>
<td>characters, and you cannot change this name after the object has been saved.</td>
</tr>
<tr>
<td>Description field</td>
<td>A description of the policy. We recommend including information about where and when the policy</td>
</tr>
<tr>
<td></td>
<td>should be used.</td>
</tr>
<tr>
<td>Admin State field</td>
<td>This can be:</td>
</tr>
<tr>
<td></td>
<td>• enabled</td>
</tr>
<tr>
<td></td>
<td>• disabled</td>
</tr>
<tr>
<td>Speed drop-down list</td>
<td>This can be:</td>
</tr>
<tr>
<td></td>
<td>• 115200</td>
</tr>
<tr>
<td></td>
<td>• 19200</td>
</tr>
<tr>
<td></td>
<td>• 38400</td>
</tr>
<tr>
<td></td>
<td>• 57600</td>
</tr>
</tbody>
</table>
Deleting a Serial over LAN Policy

**Procedure**

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

**Step 2** In the Servers tab, expand Servers ➤ Policies ➤\textit{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 displays a confirmation dialog box, click Yes.

Configuring Server Autoconfiguration Policies

**Server Autoconfiguration Policy**

This policy determines whether one or more of the following is automatically applied to a new server:

- A server pool policy qualification that qualifies the server for one or more server pools
- An organization
- A service profile template that associates the server with a service profile created from that template

**Prerequisites**

**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
- If a system implements multi-tenancy, organizations
Configuring Server Autoconfiguration Policies

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 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>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.</td>
</tr>
<tr>
<td>Description field</td>
<td>A description of the policy. We recommend including information about where and when the policy should be used.</td>
</tr>
<tr>
<td>Qualification drop-down list</td>
<td>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.</td>
</tr>
<tr>
<td>Org drop-down list</td>
<td>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.</td>
</tr>
<tr>
<td>Service Profile Template Name drop-down list</td>
<td>The service profile template associated with this policy.</td>
</tr>
</tbody>
</table>

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 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.

With this policy, an inventory of the server is conducted, then server pool policy qualifications are run to determine whether the new server qualifies for one or more server pools.

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
  • diag—Reserved for diagnostic use

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Navigation pane, click the Equipment tab.</td>
</tr>
<tr>
<td>2</td>
<td>Click the Equipment node.</td>
</tr>
<tr>
<td>3</td>
<td>In the Work pane, click the Policies tab.</td>
</tr>
<tr>
<td>4</td>
<td>Click the Server Discovery Policies subtab.</td>
</tr>
<tr>
<td>5</td>
<td>Right-click the server discover policy that you want to delete and choose Delete.</td>
</tr>
<tr>
<td>6</td>
<td>If Cisco UCS Manager displays a confirmation dialog box, click Yes.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Navigation pane, click the Equipment tab.</td>
</tr>
<tr>
<td>2</td>
<td>Click the Equipment node.</td>
</tr>
<tr>
<td>3</td>
<td>In the Work pane, click the Policies tab.</td>
</tr>
<tr>
<td>4</td>
<td>Click the Server Inheritance Policies subtab.</td>
</tr>
<tr>
<td>5</td>
<td>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.</td>
</tr>
<tr>
<td>6</td>
<td>In the Create Server Inheritance Policy dialog box, complete the following fields:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the policy.</td>
</tr>
</tbody>
</table>
### 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

• A minimum of one server pool
• Server pool policy qualifications, if you choose to have servers automatically added to pools

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Servers tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Servers tab, expand Servers ➤ Policies.</td>
</tr>
<tr>
<td>Step 3</td>
<td>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.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Right-click Server Pool Policies and select Create Server Pool Policy.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Create Server Pool Policy dialog box, complete the following fields:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>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.</td>
</tr>
<tr>
<td>Target Pool drop-down list</td>
<td>If you want to associate this policy with a server pool, select that pool from the drop-down list.</td>
</tr>
<tr>
<td>Description field</td>
<td>A description of the policy. We recommend including information about where and when the policy should be used.</td>
</tr>
<tr>
<td>Qualification drop-down list</td>
<td>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.</td>
</tr>
</tbody>
</table>

| Step 6 | Click OK.                                                                 |

Deleting a Server Pool Policy

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 Server Pool Policies node.
Step 4 Right-click the policy you want to delete and select Delete.
Step 5 If Cisco UCS Manager 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 In 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:

a) Click Create Adapter Qualifications.

b) In the Create Adapter Qualifications dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong> drop-down list</td>
<td>Choose the adapter type from the drop-down list. This can be:</td>
</tr>
<tr>
<td></td>
<td>• fcoe—Fibre Channel over Ethernet</td>
</tr>
<tr>
<td></td>
<td>• non-virtualized-eth-if</td>
</tr>
<tr>
<td></td>
<td>• non-virtualized-fc-if</td>
</tr>
<tr>
<td></td>
<td>• path-encap-consolidated</td>
</tr>
<tr>
<td></td>
<td>• path-encap-virtual</td>
</tr>
<tr>
<td></td>
<td>• protected-eth-if</td>
</tr>
<tr>
<td></td>
<td>• protected-fc-if</td>
</tr>
<tr>
<td></td>
<td>• protected-fcoe</td>
</tr>
<tr>
<td></td>
<td>• virtualized-eth-if</td>
</tr>
<tr>
<td></td>
<td>• virtualized-fc-if</td>
</tr>
<tr>
<td></td>
<td>• virtualized-scsi-if</td>
</tr>
<tr>
<td><strong>Maximum Capacity</strong></td>
<td>Enter the maximum capacity for the selected type.</td>
</tr>
</tbody>
</table>

c) Click OK.

**Step 7** (Optional) To use this policy to qualify servers according to their physical location:

a) Click Create Chassis and Server Qualifications.

b) In the Create Chassis and Server Qualifications dialog box, click Add.

c) In the first page of the Create Server Qualifications wizard, enter the range of server slot numbers where the server should be located in the From field and the To field, then click Finish Stage.

**Example:**
For example, if you want to include all servers in slots 3 through 5 in all chassis in the policy, enter 3 in the From field and 5 in the To field. However, if you want to include all servers in slots 3 and 5, enter 3 in the From field and 3 To field to create an entry for slot 3. You will need to create another server qualification entry for slot 5.

d) In the second page of the Create Server Qualifications wizard, enter the range of chassis numbers where the server should be located in the From field and the To field, then click Finish.

**Example:**
For example, if you want to include all servers in chassis 1 through 4 in the policy, enter 1 in the From field and 4 in the To field. However, if you want to include all servers in chassis 1 and 4, enter 1 in the From field and 1 To field to create an entry for chassis 1. You will need to create another server qualification entry for chassis 4.

**Step 8** (Optional) To use this policy to qualify servers according to their memory configuration:

a) Click **Create Memory Qualifications**.

b) In the **Create Memory Qualifications** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clock field</td>
<td>The minimum clock speed required, in megahertz.</td>
</tr>
<tr>
<td>Latency field</td>
<td>The maximum latency allowed, in nanoseconds.</td>
</tr>
<tr>
<td>Min Cap field</td>
<td>The minimum CPU capacity required, in megabytes.</td>
</tr>
<tr>
<td>Max Cap field</td>
<td>The maximum CPU capacity allowed, in megabytes.</td>
</tr>
<tr>
<td>Width field</td>
<td>The minimum width of the data bus.</td>
</tr>
<tr>
<td>Units field</td>
<td>The unit of measure to associate with the value in the Width field.</td>
</tr>
</tbody>
</table>

c) Click OK.

**Step 9** (Optional) To use this policy to qualify servers according to their CPU/Cores configuration:

a) Click **Create CPU/Cores Qualifications**.

b) In the **Create CPU/Cores Qualifications** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor Architecture drop-down list</td>
<td>The CPU architecture that this policy applies to.</td>
</tr>
<tr>
<td>Min Number of Cores field</td>
<td>The minimum number of CPU cores required.</td>
</tr>
<tr>
<td>Max Number of Cores field</td>
<td>The maximum number of CPU cores allowed.</td>
</tr>
<tr>
<td>Min Number of Threads field</td>
<td>The minimum number of CPU threads required.</td>
</tr>
<tr>
<td>Max Number of Threads field</td>
<td>The maximum number of CPU threads allowed.</td>
</tr>
<tr>
<td>CPU Speed field</td>
<td>The minimum CPU speed required.</td>
</tr>
<tr>
<td>CPU Stepping field</td>
<td>The minimum CPU version required.</td>
</tr>
</tbody>
</table>

c) Click OK.

**Step 10** (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:
### Configuring Server Pool Policy Qualifications

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Blocks</td>
<td>The minimum number of blocks required.</td>
</tr>
<tr>
<td>Block Size</td>
<td>The minimum block size required, in bytes.</td>
</tr>
<tr>
<td>Min Cap</td>
<td>The minimum storage capacity required, in megabytes.</td>
</tr>
<tr>
<td>Max Cap</td>
<td>The maximum storage capacity allowed, in megabytes.</td>
</tr>
<tr>
<td>Per Disk Cap</td>
<td>The minimum storage capacity per disk required, in gigabytes.</td>
</tr>
<tr>
<td>Units</td>
<td>The number of units.</td>
</tr>
</tbody>
</table>

c) Click OK.

#### Step 11
Verify the qualifications in the table and correct if necessary.

#### Step 12
Click OK.

### Deleting Server Pool Policy Qualifications

#### Procedure

1. In the Navigation pane, click the Servers tab.
2. In the Servers tab, expand Servers ➤ Policies ➤ Organization_Name.
3. Expand the Server Pool Policy Qualifications node.
4. Right-click the policy qualifications you want to delete and select Delete.
5. If Cisco UCS Manager 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

1. In the Navigation pane, click the Servers tab.
2. In the Servers tab, expand Servers ➤ Policies ➤ Organization_Name.
3. Expand the Server Pool Policy Qualifications node.
4. Choose the policy you want to modify.
5. In the Work pane, choose the Qualifications tab.
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 Service Profiles

This chapter includes:

- Service Profiles that Override Server Identity, page 199
- Service Profiles that Inherit Server Identity, page 200
- Service Profile Templates, page 200
- Creating Service Profiles, page 201
- Working with Service Profile Templates, page 217
- Managing Service Profiles, page 232

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 associated 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:

- 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 type of service profile is the simplest to use and create. This profile 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 automatically applies the identity and configuration information that is present at the time of association, such as:

- 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 have been subsequently changed before this profile is associated with the server.

Service Profile Templates

Service profile templates enable you to create a large number of similar service profiles. 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 of 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 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  In 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 201
  • Page 2: Configuring the Storage Options, page 203
  • Page 3: Configuring the Networking Options, page 207
  • Page 4: Setting the Server Boot Order, page 209
  • Page 5: Specifying the Server Assignment, page 211
  • Page 6: Adding Operational Policies, page 213

Page 1: Identifying the Service Profile

This task describes how to set the identity of a service profile on the Identify Service Profile page of the Create Service Profile (expert) wizard.

Before You Begin

This task directly follows the steps in Creating a Service Profile with the Expert Wizard, page 201.

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:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select (pool default used by default)</td>
<td>Assigns a UUID from the default UUID Suffix pool. Continue with Step 4.</td>
</tr>
<tr>
<td>Hardware Default</td>
<td>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.</td>
</tr>
<tr>
<td>XXXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX</td>
<td>Uses the UUID that you manually assign. Continue with Step 3.</td>
</tr>
<tr>
<td>Pools Pool_Name</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Step 3** *(Optional)* If you selected the XXXXXXXXX-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** In the **Description** field, 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 203.
Page 2: Configuring the Storage Options

This task describes how to configure the storage options for a service profile on the Storage page of the Create Service Profile (expert) wizard.

Before You Begin

This task directly follows Page 1: Identifying the Service Profile, page 201.

Procedure

Step 1

From the Local Storage drop-down list, choose one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Local Storage Policy to Use</td>
<td>Assigns the default local disk storage policy to this service profile.</td>
</tr>
<tr>
<td></td>
<td>Continue with Step 4.</td>
</tr>
<tr>
<td>Create a Specific Storage Policy</td>
<td>Enables you to create a local disk policy that can only be accessed by this</td>
</tr>
<tr>
<td></td>
<td>service profile.</td>
</tr>
<tr>
<td></td>
<td>Continue with Step 2.</td>
</tr>
<tr>
<td>Storage Policies Policy_Name</td>
<td>Select an existing local disk policy from the list at the bottom of the</td>
</tr>
<tr>
<td></td>
<td>drop-down list. Cisco UCS Manager assigns this policy to the service</td>
</tr>
<tr>
<td></td>
<td>profile.</td>
</tr>
<tr>
<td></td>
<td>If you do not want use any of the existing policies, but instead want to</td>
</tr>
<tr>
<td></td>
<td>create a new policy that all service profiles can access, continue with Step</td>
</tr>
<tr>
<td></td>
<td>3. Otherwise, continue with Step 4.</td>
</tr>
</tbody>
</table>

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 work-station 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.
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 new policy that will be available to all service profiles, do the following:

a) Click 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 183.

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;not set&gt;</td>
<td>Does not include a scrub policy in the service profile.</td>
</tr>
</tbody>
</table>

**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 new policy that all service profiles can access, continue with Step 5. Otherwise, continue with Step 6.

c) Click OK.

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

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

a) Click Create Scrub Policy.

b) In the Create Scrub Policy dialog box, complete the fields.

   For more information, see Creating a Scrub Policy, page 186.

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple</td>
<td>Allows you to create a maximum of two vHBAs for this service profile. Continue with Step 7.</td>
</tr>
</tbody>
</table>

**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 FibreChannel SAN in the service profile. Continue with Step 9.

**Step 7** (Optional) If you chose the simple SAN storage option, do the following:
a) From the **Node Identity** drop-down list:

- 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 **20:XX:XX:XX:XX:XX:XX:XX** to specify a WWN, and then enter the WWN in the **World Wide Node Name** field.
- Choose a WWN pool name from the list to have a WWN automatically 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:

- 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.

c) In the **vHBA 1 (Fabric B)** area:

- 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.

d) Continue with Step 9.

**Step 8** (Optional) If you chose the expert SAN storage option, do the following:

a) From the **Node Identity** drop-down list:

- 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 **20:XX:XX:XX:XX:XX:XX:XX** to specify a WWN, and then enter the WWN in the **World Wide Node Name** field.
- Choose a WWN pool name from the list to have a WWN automatically 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>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.</td>
</tr>
<tr>
<td>Use SAN Connectivity Template check box</td>
<td>Check this check box if you want to use a vHBA template.</td>
</tr>
</tbody>
</table>
Click this link if you want to create a vHBA template.

**World Wide Name Assignment**

- Use the default WWN pool, leave this field set to **Select (pool default used by default)**.
- Use the WWN assigned to the server by the manufacturer, select **Hardware Default**.
- A specific WWN, select `20:XX:XX:XX:XX:XX:XX:XX` and enter the WWN in the **WWN** field. To verify that this WWPN is available, click the corresponding link.
- A WWN 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 WWN addresses in the pool.

**d) In the VSAN area, complete the following fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric ID field</td>
<td>The associated fabric interconnect.</td>
</tr>
<tr>
<td>Select VSAN drop-down list box</td>
<td>The VSAN that this vHBA is associated with.</td>
</tr>
<tr>
<td>Create VSAN link</td>
<td>Click this link if you want to create a VSAN.</td>
</tr>
<tr>
<td>Pin Group drop-down list box</td>
<td>The pin group that this vHBA is associated with.</td>
</tr>
<tr>
<td>Create SAN Pin Group link</td>
<td>Click this link if you want to create a pin group.</td>
</tr>
</tbody>
</table>

**Operational Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stats Threshold Policy drop-down list box</td>
<td>The threshold policy that this vHBA is associated with.</td>
</tr>
</tbody>
</table>

**e) In the Adapter Performance Profile area, complete the following fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adapter Policy drop-down list box</td>
<td>The Fibre Channel adapter policy that this vHBA is associated with.</td>
</tr>
<tr>
<td>Create Fibre Channel Adapter Policy link</td>
<td>Click this link if you want to create a Fibre Channel adapter policy.</td>
</tr>
</tbody>
</table>
What to Do Next

Complete Page 3: Configuring the Networking Options, page 207.

Page 3: Configuring the Networking Options

This task describes how to configure the networking options, including LAN connectivity, on the Networking page of the Create Service Profile (expert) wizard.

Before You Begin

This task directly follows Page 2: Configuring the Storage Options, page 203.

Procedure

Step 1

In the How would you like to configure LAN connectivity? field, click one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple</td>
<td>Allows you to create a maximum of two vNICs, in dual fabric mode, for this service profile. Continue with Step 2.</td>
</tr>
<tr>
<td>Expert</td>
<td>Allows you to create an unlimited number of vNICs for this service profile. Continue with Step 3.</td>
</tr>
<tr>
<td>No vHBAs</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

b) In the vNIC 1 (Fabric B) 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.
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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>Enter a name for this vNIC.</td>
</tr>
<tr>
<td>Use LAN Connectivity Template check box</td>
<td>Enable this check box if you want to use a template.</td>
</tr>
<tr>
<td>Create vNIC Template link</td>
<td>Click this link if you want to create a vNIC template.</td>
</tr>
<tr>
<td>MAC Address Assignment drop-down list</td>
<td>If you want to:</td>
</tr>
<tr>
<td></td>
<td>• Use the default MAC address pool, leave this field set to Select (pool default used by default).</td>
</tr>
<tr>
<td></td>
<td>• Use the MAC address assigned to the server by the manufacturer, select Hardware Default.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>

In the Fabric Interconnect area, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric ID field</td>
<td>The associated fabric interconnect.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td>VLAN Trunking field</td>
<td>If you want to use VLAN trunking, click Yes. Otherwise, select No.</td>
</tr>
<tr>
<td>Select Native VLAN drop-down list box</td>
<td>The VLAN that this vNIC is associated with.</td>
</tr>
<tr>
<td>Create VLAN link</td>
<td>Click this link if you want to create a VLAN.</td>
</tr>
</tbody>
</table>
The statistics collection policy that this vNIC is associated with.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Native VLAN check box</td>
<td>Check this box if this vNIC is associated with the native VLAN.</td>
</tr>
<tr>
<td>Pin Group drop-down list box</td>
<td>Choose the LAN pin group you want associated with this vNIC.</td>
</tr>
<tr>
<td>Create LAN Pin Group link</td>
<td>Click this link if you want to create a LAN pin group.</td>
</tr>
</tbody>
</table>

**Operational Parameters Section**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stats Threshold Policy drop-down list box</td>
<td>The statistics collection policy that this vNIC is associated with.</td>
</tr>
</tbody>
</table>

**d)** In the **Adapter Performance Profile** area, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adapter Policy drop-down list box</td>
<td>The Ethernet adapter policy that this vNIC is associated with.</td>
</tr>
<tr>
<td>Create Ethernet Adapter Policy link</td>
<td>Click this link if you want to create an Ethernet adapter policy.</td>
</tr>
<tr>
<td>QoS drop-down list box</td>
<td>The quality of service policy that this vNIC is associated with.</td>
</tr>
<tr>
<td>Create QoS Policy link</td>
<td>Click this link if you want to create a quality of service policy.</td>
</tr>
</tbody>
</table>

**e)** Click **OK**.

**Step 4**
Click **Next**.

---

**What to Do Next**


---

**Page 4: Setting the Server Boot Order**

This task describes how to set the server boot order options on the **Server Boot Order** page of the Create Service Profile (expert) wizard.

**Before You Begin**

This task directly follows Page 3: Configuring the Networking Options, page 207.

**Procedure**

**Step 1**
From the **Boot Policy** drop-down list, choose one of the following:
### Option

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select Boot Policy to use</strong></td>
</tr>
<tr>
<td><strong>Create a Specific Boot Policy</strong></td>
</tr>
<tr>
<td><strong>Storage Policies Policy_Name</strong></td>
</tr>
</tbody>
</table>

#### Step 2
If you chose to create a new 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
To add a local disk, virtual CD-ROM, or virtual floppy to the boot order:
- 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 5
To add a LAN boot to the boot order:
- 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 associated vNIC in the vNIC field then click OK.
- d) Add another device to the Boot Order table or click OK to finish.

#### Step 6
To add a SAN boot to the boot order:
- 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vhBA field</td>
<td>Enter the name of the vhBA you want to use for the SAN boot.</td>
</tr>
<tr>
<td>Type field</td>
<td>This can be:</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot Target LUN field</td>
<td>The LUN that corresponds to the location of the boot image.</td>
</tr>
<tr>
<td>Boot Target WWN field</td>
<td>The WWN that corresponds to the location of the boot image.</td>
</tr>
<tr>
<td>Type field</td>
<td>This can be:</td>
</tr>
<tr>
<td></td>
<td>• <strong>primary</strong>—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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>secondary</strong>—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.</td>
</tr>
</tbody>
</table>

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

**Step 7** Click Next.

---

**What to Do Next**

Complete [Page 5: Specifying the Server Assignment, page 211](#)

---

**Page 5: Specifying the Server Assignment**

This task 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.

**Before You Begin**

This task directly follows [Page 4: Setting the Server Boot Order, page 209](#).
Procedure

Step 1  From the Server Assignment drop-down list, choose one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign Later</td>
<td>Allows you to assign a server after you have created and configured the service profile. Continue with Step 6.</td>
</tr>
<tr>
<td>Pre-provision a slot</td>
<td>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.</td>
</tr>
<tr>
<td>Select existing Server</td>
<td>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.</td>
</tr>
<tr>
<td>Select from a Pool</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.
   b) Complete the following fields:
### Page 6: Adding Operational Policies

This task 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.

#### Before You Begin

This task directly follows Page 5: Specifying the Server Assignment, page 211.

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>What to Do</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Step 1</strong> 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.</td>
</tr>
</tbody>
</table>
| 2    | **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 a new 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 182.  
  c) If you chose to create a new IPMI profile, select that profile from the IPMI Profile drop-down list. |
| 3    | **Step 3** To add a Serial over LAN policy to the service profile:  
  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 new 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 new 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 new 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:
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 new 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**
In 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary vNIC Section</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Primary vNIC check box</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Name field</strong></td>
<td>The name of the vNIC.</td>
</tr>
<tr>
<td><strong>Fabric field</strong></td>
<td>The fabric interconnect that this vNIC is associated with.</td>
</tr>
<tr>
<td><strong>Network drop-down list</strong></td>
<td>The LAN that this vNIC is associated with.</td>
</tr>
</tbody>
</table>
### Secondary vNIC Section

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secondary vNIC check box</td>
<td>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.</td>
</tr>
<tr>
<td>Name field</td>
<td>The name of the vNIC.</td>
</tr>
<tr>
<td>Fabric field</td>
<td>The fabric interconnect that this vNIC is associated with.</td>
</tr>
<tr>
<td>Network drop-down list</td>
<td>The LAN that this vNIC is associated with.</td>
</tr>
</tbody>
</table>

### Step 7

In the vHBAs area of the Create Service Profile dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary vHBA Section</td>
<td></td>
</tr>
<tr>
<td>Primary vHBA check box</td>
<td>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.</td>
</tr>
<tr>
<td>Name field</td>
<td>The name of the vHBA.</td>
</tr>
<tr>
<td>Fabric field</td>
<td>The fabric interconnect that this vHBA is associated with.</td>
</tr>
<tr>
<td>Secondary vHBA Section</td>
<td></td>
</tr>
<tr>
<td>Secondary vHBA check box</td>
<td>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.</td>
</tr>
<tr>
<td>Name field</td>
<td>The name of the vHBA.</td>
</tr>
<tr>
<td>Fabric field</td>
<td>The fabric interconnect that this vHBA is associated with.</td>
</tr>
</tbody>
</table>

### Step 8

In the Boot Order area of the Create Service Profile dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Boot Device Section</td>
<td></td>
</tr>
<tr>
<td>Primary Boot Device check box</td>
<td>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.</td>
</tr>
<tr>
<td>Type field</td>
<td>This can be:</td>
</tr>
<tr>
<td></td>
<td>• local-disk—The server boots from its local disk.</td>
</tr>
</tbody>
</table>
### Creating Service Profiles

#### Creating a Service Profile that Inherits Server Identity

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>• san</td>
<td>- The server boots from an image stored in a SAN. If you select this option, Cisco UCS Manager GUI displays the SAN area.</td>
</tr>
<tr>
<td>• lan</td>
<td>- 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.</td>
</tr>
<tr>
<td>• virtual CD-ROM</td>
<td>- The server boots from a virtual CD-ROM.</td>
</tr>
<tr>
<td>• virtual Floppy</td>
<td>- The server boots from a virtual floppy.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SAN area</th>
<th>If Type is set to san, this area contains the following field:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• vHBA</td>
<td>- The vHBA used to access the SAN boot image</td>
</tr>
<tr>
<td>• LUN</td>
<td>- The LUN that corresponds to the location of the boot image</td>
</tr>
<tr>
<td>• WWN</td>
<td>- The WWN that corresponds to the location of the boot image</td>
</tr>
</tbody>
</table>

| 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. |

<table>
<thead>
<tr>
<th>Secondary Boot Device Section</th>
<th>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.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Primary Boot Device check box</th>
<th>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.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Type field</th>
<th>This can be:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• local-disk</td>
<td>- The server boots from its local disk.</td>
</tr>
<tr>
<td>• san</td>
<td>- The server boots from an image stored in a SAN. If you select this option, Cisco UCS Manager GUI displays the SAN area.</td>
</tr>
<tr>
<td>• lan</td>
<td>- 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.</td>
</tr>
<tr>
<td>• virtual CD-ROM</td>
<td>- The server boots from a virtual CD-ROM.</td>
</tr>
<tr>
<td>• virtual Floppy</td>
<td>- The server boots from a virtual floppy.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SAN area</th>
<th>If Type is set to san, this area contains the following field:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• vHBA</td>
<td>- The vHBA used to access the SAN boot image</td>
</tr>
<tr>
<td>• LUN</td>
<td>- The LUN that corresponds to the location of the boot image</td>
</tr>
</tbody>
</table>
Creating a Default Service Profile for a Server

You cannot move a default service profile to another server.

Procedure

Step 1 In the Navigation pane, click the Equipment tab.
Step 2 In the Equipment tab, expand Equipment ➤ Chassis ➤ Chassis Number ➤ Servers.
Step 3 Choose the server for which you want to create a default service profile.
Step 4 In the Work pane, click the General tab.
Step 5 In the Actions area, click Create Default Service Profile.
Step 6 In the Create Default Service Profile dialog box:
   a) Enter a unique name and description for the service profile.
   b) 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 In 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 218
- Page 2: Specifying the Template Storage Options, page 219
- Page 3: Specifying the Template Networking Options, page 223
- Page 4: Specifying the Template Server Boot Order Options, page 226
- Page 5: Specifying the Template Server Assignment Options, page 228
- Page 6: Specifying Template Policy Options, page 229

---

**Page 1: Identifying the Service Profile Template**

This task 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.

**Before You Begin**

This task directly follows the steps in **Creating a Service Profile Template**, page 217.

**Procedure**

**Step 1** In the **Name** field, enter a unique name that you can use to identify 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.

**Step 2** From the **UUID Assignment** drop-down list, choose one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select (pool default used by default)</td>
<td>Assigns a UUID from the default UUID Suffix pool.</td>
</tr>
<tr>
<td>Hardware Default</td>
<td>Uses the UUID assigned to the server by the manufacturer.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
### Page 2: Specifying the Template Storage Options

This task describes how to configure the storage options for a service profile template on the Storage page of the Create Service Profile Template wizard.

#### Before You Begin
This task directly follows Page 1: Identifying the Service Profile Template, page 218.

#### Procedure

**Step 1**
From the Local Storage drop-down list, choose one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Local Storage Policy to Use</td>
<td>Assigns the default local disk storage policy to service profile created from this template. Continue with Step 4.</td>
</tr>
<tr>
<td>Create a Specific Storage Policy</td>
<td>Enables you to create a local disk policy that can only be accessed by service profile created from this template. Continue with Step 2.</td>
</tr>
<tr>
<td>Storage Policies Policy_Name</td>
<td>Select an existing local disk policy from the list at the bottom of the drop-down list. Cisco UCS Manager assigns this policy to 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 templates can access, continue with Step 3. Otherwise, continue with Step 4.</td>
</tr>
</tbody>
</table>

**Step 2** (Optional) If you chose Create a Specific Storage Policy, do the following:

In the Description field, enter a description of this service profile template. The description can contain up to 256 characters.

Click Next.

What to Do Next
Complete the steps in Page 2: Specifying the Template Storage Options, page 219.
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 work-station 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 new policy that will be available to all service profiles 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 183).

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;not set&gt;</td>
<td>Does not include a scrub policy in service profile created from this template.</td>
</tr>
<tr>
<td><strong>Policy_Name</strong></td>
<td>Assigns an existing scrub policy to service profile created from this template.</td>
</tr>
</tbody>
</table>

If you do not want use any of the existing policies, but instead want to create a new policy that all service profiles templates can access, continue with Step 5. Otherwise, continue with Step 6.

**Step 5** (Optional) To create a new policy that will be available to all service profiles 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 186).

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:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple</td>
<td>Allows you to create a maximum of two vHBAs for service profile created from this template. Continue with Step 7.</td>
</tr>
<tr>
<td>Expert</td>
<td>Allows you to create an unlimited number of vHBAs for service profile created from this template. Continue with Step 8.</td>
</tr>
<tr>
<td>No vHBAs</td>
<td>Does not include any vHBAs for connections to a Fibre Channel SAN in service profile created from this template. Continue with Step 9.</td>
</tr>
</tbody>
</table>

**Step 7** (Optional) If you chose the simple SAN storage option, do the following:

a) From the **WWNN Assignment** drop-down list:
   - 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 **20:XX:XX:XX:XX:XX:XX:XX** or **5X:XX:XX:XX:XX:XX:XX:XX** to specify a WWN, and then enter the WWN in the **World Wide Node Name** field. You can specify a WWN 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.
   - Choose a WWN pool name from the list to have a WWN automatically 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:
   - 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.

c) In the **vHBA 1 (Fabric B)** area:
   - 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.

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 **Select (pool default used by default)** to use the default WVN pool.
   - Choose **Derived from vHBA** to use a WWN derived from the first vHBA you specify.
• Choose 20:XX:XX:XX:XX:XX:XX:XX or 5X:XX:XX:XX:XX:XX:XX:XX to specify a WWNN, and then enter the WWNN 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.

• Choose a WWN pool name from the list to have a WWN automatically 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>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.</td>
</tr>
<tr>
<td>Use SAN Connectivity Template check box</td>
<td>Check this check box if you want to use a vHBA template.</td>
</tr>
<tr>
<td>Create vHBA Template link</td>
<td>Click this link if you want to create a vHBA template.</td>
</tr>
</tbody>
</table>
| World Wide Name Assignment drop-down list | If you want to:  
• Use the default WWN pool, leave this field set to Select (pool default used by default).  
• Use the WWN assigned to the server by the manufacturer, select Hardware Default.  
• A specific WWN, select 20:XX:XX:XX:XX:XX:XX:XX and enter the WWN in the WWN field. To verify that this WWPN is available, click the corresponding link.  
• A WWN 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 WWN addresses in the pool. |

d) In the VSAN area, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric ID field</td>
<td>The associated fabric interconnect.</td>
</tr>
<tr>
<td>Select VSAN drop-down list box</td>
<td>The VSAN that this vHBA is associated with.</td>
</tr>
<tr>
<td>Create VSAN link</td>
<td>Click this link if you want to create a VSAN.</td>
</tr>
<tr>
<td>Pin Group drop-down list box</td>
<td>The pin group that this vHBA is associated with.</td>
</tr>
</tbody>
</table>
Name | Description
---|---
Create SAN Pin Group link | Click this link if you want to create a pin group.

**Operational Parameters Section**

Stats Threshold Policy drop-down list box | The threshold policy that this vHBA is associated with.

e) In the **Adapter Performance Profile** area, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Adapter Policy drop-down list box | The Fibre Channel adapter policy that this vHBA is associated with.
| Create Fibre Channel Adapter Policy link | Click this link if you want to create a Fibre Channel adapter policy.

f) Click **OK**.

**Step 9**

Click **Next**.

**What to Do Next**

Complete Page 3: Specifying the Template Networking Options, page 223.

**Page 3: Specifying the Template Networking Options**

This task describes how to configure the networking options, including LAN connectivity, on the **Networking** page of the **Create Service Profile Template** wizard.

**Before You Begin**

This task directly follows Page 2: Specifying the Template Storage Options, page 219.

**Procedure**

**Step 1**

In the **How would you like to configure LAN connectivity?** field, click one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple</td>
<td>Allows you to create a maximum of two vNICs, in dual fabric mode, for service profile created from this template. Continue with Step 2.</td>
</tr>
<tr>
<td>Expert</td>
<td>Allows you to create an unlimited number of vNICs for service profile created from this template. Continue with Step 3.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>No vHBAs</td>
<td>Does not include any vNICs for connections to a LAN in service profile created from this template. Any server associated with these service profile will not be able to communicate with a LAN unless you modify the individual service profile later. Continue with Step 4.</td>
</tr>
</tbody>
</table>

**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.

b) In the vNIC 1 (Fabric B) 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.

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>Enter a name for this vNIC.</td>
</tr>
<tr>
<td>Use LAN Connectivity Template</td>
<td>Enable this check box if you want to use a template.</td>
</tr>
<tr>
<td>Create vNIC Template link</td>
<td>Click this link if you want to create a vNIC template.</td>
</tr>
</tbody>
</table>
| 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fabric ID field</strong></td>
<td>The associated fabric interconnect.</td>
</tr>
<tr>
<td></td>
<td>If you want this vNIC to be able to access the second fabric interconnect if</td>
</tr>
<tr>
<td></td>
<td>the default one is unavailable, check the <strong>Enable Failover</strong> check box.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Do not select <strong>Enable Failover</strong> if you plan to associate this vNIC</td>
</tr>
<tr>
<td></td>
<td>configuration with a server that has a Cisco UCS 82598KR-CI 10-Gigabit</td>
</tr>
<tr>
<td></td>
<td>Ethernet Adapter. If you do so, Cisco UCS Manager generates a configuration</td>
</tr>
<tr>
<td></td>
<td>fault when you associate the service profile with the server.</td>
</tr>
<tr>
<td><strong>VLAN Trunking field</strong></td>
<td>If you want to use VLAN trunking, click <strong>Yes</strong>. Otherwise, select <strong>No</strong>.</td>
</tr>
<tr>
<td><strong>Select Native VLAN</strong></td>
<td>The VLAN that this vNIC is associated with.</td>
</tr>
<tr>
<td><strong>Create VLAN</strong></td>
<td>Click this link if you want to create a VLAN.</td>
</tr>
<tr>
<td><strong>Native VLAN check box</strong></td>
<td>Check this box if this vNIC is associated with the native VLAN.</td>
</tr>
<tr>
<td><strong>Pin Group</strong></td>
<td>Choose the LAN pin group you want associated with this vNIC.</td>
</tr>
<tr>
<td><strong>Create LAN Pin Group</strong></td>
<td>Click this link if you want to create a LAN pin group.</td>
</tr>
<tr>
<td><strong>Operational Parameters</strong></td>
<td><strong>Stats Threshold Policy</strong> drop-down list box</td>
</tr>
<tr>
<td></td>
<td>The statistics collection policy that this vNIC is associated with.</td>
</tr>
</tbody>
</table>

d) In the **Adapter Performance Profile** area, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Adapter Policy</strong></td>
<td>The Ethernet adapter policy that this vNIC is associated with.</td>
</tr>
<tr>
<td><strong>Create Ethernet Adapter Policy</strong></td>
<td>Click this link if you want to create an Ethernet adapter policy.</td>
</tr>
<tr>
<td><strong>QoS</strong></td>
<td>The quality of service policy that this vNIC is associated with.</td>
</tr>
<tr>
<td><strong>Create QoS Policy</strong></td>
<td>Click this link if you want to create a quality of service policy.</td>
</tr>
</tbody>
</table>

e) Click **OK**.

**Step 4**  Click **Next**.
What to Do Next
Complete Page 4: Specifying the Template Server Boot Order Options, page 226.

Page 4: Specifying the Template Server Boot Order Options
This task describes how to set the server boot order options on the Server Boot Order page of the Create Service Profile Template wizard.

Before You Begin
This task directly follows Page 3: Specifying the Template Networking Options, page 223.

Procedure

Step 1
From the Boot Policy drop-down list, choose one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Boot Policy to use</td>
<td>Assigns the default boot policy to service profile created from this template.</td>
</tr>
<tr>
<td></td>
<td>Continue with Step 7.</td>
</tr>
<tr>
<td>Create a Specific Boot Policy</td>
<td>Enables you to create a local boot policy that can only be accessed by service</td>
</tr>
<tr>
<td></td>
<td>profile created from this template.</td>
</tr>
<tr>
<td></td>
<td>Continue with Step 3.</td>
</tr>
<tr>
<td>Storage Policies Policy_Name</td>
<td>Assigns an existing local disk policy to service profile created from this</td>
</tr>
<tr>
<td></td>
<td>template. If you choose this option, Cisco UCS Manager displays the details</td>
</tr>
<tr>
<td></td>
<td>of the policy.</td>
</tr>
<tr>
<td></td>
<td>If you do not want use any of the existing policies, but instead want to</td>
</tr>
<tr>
<td></td>
<td>create a new policy that all service profiles templates can access, continue</td>
</tr>
<tr>
<td></td>
<td>with Step 2. Otherwise, continue with Step 7.</td>
</tr>
</tbody>
</table>

Step 2
If you chose to create a new 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 To add a local disk, virtual CD-ROM, or virtual floppy to the boot order:
   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 5**
To add a LAN boot to the boot order:

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 associated vNIC in the **vNIC** field then click **OK**.

d) Add another device to the **Boot Order** table or click **OK** to finish.

**Step 6**
To add a SAN boot to the boot order:

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**:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>vHBA field</strong></td>
<td>Enter the name of the vHBA you want to use for the SAN boot.</td>
</tr>
<tr>
<td><strong>Type field</strong></td>
<td>This can be:</td>
</tr>
<tr>
<td></td>
<td>• <strong>primary</strong>—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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>secondary</strong>—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.</td>
</tr>
</tbody>
</table>

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**:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boot Target LUN field</strong></td>
<td>The LUN that corresponds to the location of the boot image.</td>
</tr>
<tr>
<td><strong>Boot Target WWN field</strong></td>
<td>The WWN that corresponds to the location of the boot image.</td>
</tr>
<tr>
<td><strong>Type field</strong></td>
<td>This can be:</td>
</tr>
<tr>
<td></td>
<td>• <strong>primary</strong>—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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>secondary</strong>—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.</td>
</tr>
</tbody>
</table>
e) Add another boot device to the Boot Order table or click OK to finish.

**Step 7**

Click Next.

---

**What to Do Next**

Complete Page 5: Specifying the Template Server Assignment Options, page 228.

---

**Page 5: Specifying the Template Server Assignment Options**

This task 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.

**Before You Begin**

This task directly follows Page 4: Specifying the Template Server Boot Order Options, page 226.

**Procedure**

**Step 1**

From the Server Assignment drop-down list, choose one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign Later</td>
<td>Allows you to assign a server after you have created and configured the service profile template. Continue with Step 2.</td>
</tr>
<tr>
<td>Select from a Pool</td>
<td>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 created from this template. Continue with Step 2.</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Firmware</td>
<td>To associate a host firmware package with this service profile, choose its name from the drop-down list.</td>
</tr>
</tbody>
</table>
Step 4  Click Next.

What to Do Next

Page 6: Specifying Template Policy Options
This task 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.

Before You Begin
This task directly follows Page 5: Specifying the Template Server Assignment Options, page 228.

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:
   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 a new IPMI profile that is available to all service profiles templates. For more information about how to create an IPMI profile, see Creating an IPMI Profile, page 182.
   c) If you chose to create a new IPMI profile, select that profile from the IPMI Profile drop-down list.

Step 3  To add a Serial over LAN policy to service profile created from this template:
   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 new 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.
   c) To create a new 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.
Creating Service Profiles from a Service Profile Template

Procedure

Step 1 In the Navigation pane, click the Servers tab.
Step 2 In 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 you want to create the profiles from and select Create Service Profiles From Template.
Step 5 In the Create Service Profiles From Template dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Naming Prefix</td>
<td>The prefix to use for the template name. When the system creates the service profiles, 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.</td>
</tr>
<tr>
<td>Number</td>
<td>The number of service profiles to create.</td>
</tr>
</tbody>
</table>

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 In 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select (pool default used by default)</td>
<td>Assigns a UUID from the default UUID Suffix pool.</td>
</tr>
<tr>
<td>Hardware Default</td>
<td>Uses the UUID assigned to the server by the manufacturer.</td>
</tr>
<tr>
<td></td>
<td>If you choose this option, the UUID remains unassigned until the service profile</td>
</tr>
<tr>
<td></td>
<td>is associated with a server. At that point, the UUID is set to the UUID value</td>
</tr>
<tr>
<td></td>
<td>assigned to the server by the manufacturer. If the service profile is later moved</td>
</tr>
<tr>
<td></td>
<td>to a different server, the UUID is changed to match the new server.</td>
</tr>
<tr>
<td>Pools Pool_Name</td>
<td>Assigns a UUID from the UUID Suffix pool that you select from the list at the</td>
</tr>
<tr>
<td></td>
<td>bottom of the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>Each pool name is followed by two numbers in parentheses that show the</td>
</tr>
<tr>
<td></td>
<td>number of UUIDs still available in the pool and the total number of UUIDs in</td>
</tr>
<tr>
<td></td>
<td>the pool.</td>
</tr>
</tbody>
</table>

Step 8 Click OK.
Managing Service Profiles

Cloning a Service Profile

**Procedure**

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

**Step 2** In 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 with which a service profile is associated.

**Procedure**

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

**Step 2** In 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Pool</td>
<td>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.</td>
</tr>
<tr>
<td>Server</td>
<td>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.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Custom Server</td>
<td>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 6.</td>
</tr>
</tbody>
</table>

**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 OS on the server. If the OS does not shutdown within a reasonable length of time, Cisco UCS Manager will force the server to shutdown.

**Procedure**

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

**Step 2**  In 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**  In 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 4.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Default</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXXXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX</td>
<td>Uses the UUID that you manually assign. Continue with Step 3.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pools Pool_Name</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Step 8** (Optional) If you selected the XXXXXXXXXX-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.
Deleting a Service Profile

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Servers tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Servers tab, expand Servers ➤ Service Profiles ➤ Organization_Name.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Right-click the service profile you want to delete and select Delete.</td>
</tr>
<tr>
<td>Step 4</td>
<td>If Cisco UCS Manager displays a confirmation dialog box, click Yes.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click OK.</td>
</tr>
</tbody>
</table>

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 | In 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 In 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 displays a confirmation dialog box, click Yes.
Installing an OS on a Server

This chapter includes:

- OS Installation Methods, page 237
- Installation Targets, page 238
- Installing an OS Using a PXE Installation Server, page 239
- Installing an OS Using the KVM Dongle, page 239
- Installing an OS Using the KVM Console, page 240

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 a 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 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, then 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, then 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:

a) For a service profile with a boot policy, set the boot order for the boot policy to boot from the LAN first.
   For more information, see Creating a Boot Policy, page 179

b) 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 254
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 179.
   • 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 254
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 In 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 checkbox 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 checkbox 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 179.
- 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 254

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

System Management

- Managing Time Zones, page 245
- Managing the Chassis, page 247
- Managing the Servers, page 253
- Managing the IO Modules, page 265
- Configuring Call Home, page 269
- Backing Up and Restoring the Configuration, page 285
- Configuring Settings for Faults and Events, page 295
- Recovering a Lost Password, page 299
- Configuring Statistics-Related Policies, page 303
Managing Time Zones

This chapter includes:

- Time Zones, page 245
- Setting the Time Zone, page 245
- Adding an NTP Server, page 246
- Deleting an NTP Server, page 246

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 displays a confirmation dialog box, click Yes.
- **Step 7** Click Save Changes.
Managing the Chassis

This chapter includes:

- Chassis Management in Cisco UCS Manager GUI, page 247
- Acknowledging a Chassis, page 247
- Removing a Chassis, page 248
- Recommissioning a Chassis, page 248
- Toggling the Locator LED, page 249
- Monitoring a Chassis, page 249
- View the POST Results for a Chassis, page 251

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

1. In the Navigation pane, click the Equipment tab.
2. In the Equipment tab, expand Equipment ➤ Chassis.
3. Choose the chassis that you want to acknowledge.
4. In the Work pane, click the General tab.
5. In the Actions area, click Acknowledge Chassis.
6. If Cisco UCS Manager displays a the 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Equipment tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Equipment tab, expand Equipment ➤ Chassis.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose the chassis that you want to remove.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Work pane, click the General tab.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Actions area, click Remove Chassis.</td>
</tr>
<tr>
<td>Step 6</td>
<td>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.</td>
</tr>
</tbody>
</table>

Recommissioning a Chassis

This procedure returns the chassis to the configuration and applies the chassis discovery policy to the chassis.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Equipment tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Equipment tab, expand the Equipment node.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click on the Chassis node.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Work pane, click the Decommissioned tab.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Right-click the chassis you want to enable and choose Recommission.</td>
</tr>
<tr>
<td>Step 6</td>
<td>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.</td>
</tr>
</tbody>
</table>
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  In 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  In 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 individual components in a chassis, expand those nodes.
Procedure

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

**Step 2** In 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong> tab</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Servers</strong> tab</td>
<td>Displays the status and selected properties of all servers in the chassis.</td>
</tr>
<tr>
<td><strong>Service Profiles</strong> tab</td>
<td>Displays the status of the service profiles associated with servers in the chassis.</td>
</tr>
<tr>
<td><strong>IO Modules</strong> tab</td>
<td>Displays the status and selected properties of all IO modules in the chassis.</td>
</tr>
<tr>
<td><strong>Fans</strong> tab</td>
<td>Displays the status of all fan modules in the chassis.</td>
</tr>
<tr>
<td><strong>PSUs</strong></td>
<td>Displays the status of all power supply units in the chassis.</td>
</tr>
<tr>
<td><strong>Hybrid Display</strong> tab</td>
<td>Displays detailed information about the connections between the chassis and the fabric interconnects. The display has an icon for the following:</td>
</tr>
<tr>
<td></td>
<td>• Each fabric interconnect in the system</td>
</tr>
<tr>
<td></td>
<td>• The I/O module (IOM) in the selected chassis, which is shown as an independent unit to make the connection paths easier to see</td>
</tr>
<tr>
<td></td>
<td>• The selected chassis showing the servers and PSUs</td>
</tr>
<tr>
<td><strong>Slots</strong> tab</td>
<td>Displays the status of all slots in the chassis.</td>
</tr>
<tr>
<td><strong>Installed Firmware</strong> tab</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Faults</strong> tab</td>
<td>Provides details of faults generated by the chassis.</td>
</tr>
<tr>
<td><strong>Events</strong> tab</td>
<td>Provides details of events generated by the chassis.</td>
</tr>
<tr>
<td><strong>FSM</strong> tab</td>
<td>Provides details about and the status of FSM tasks related to the chassis. You can use this information to diagnose errors with those tasks.</td>
</tr>
<tr>
<td><strong>Statistics</strong> tab</td>
<td>Provides statistics about the chassis and its components. You can view these statistics in tabular or chart format.</td>
</tr>
</tbody>
</table>
View 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the <strong>Navigation</strong> pane, click the <strong>Equipment</strong> tab.</td>
</tr>
<tr>
<td>2</td>
<td>In the <strong>Equipment</strong> tab, expand <strong>Equipment ➤ Chassis</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Choose the chassis for which you want to view the POST results.</td>
</tr>
<tr>
<td>4</td>
<td>In the <strong>Work</strong> pane, click the <strong>General</strong> tab.</td>
</tr>
<tr>
<td>5</td>
<td>In the <strong>Actions</strong> area, click <strong>View POST Results</strong>. The <strong>POST Results</strong> dialog box lists the POST results for each server in the chassis and its adapters.</td>
</tr>
<tr>
<td>6</td>
<td>(Optional) Click the link in the <strong>Affected Object</strong> column to view the properties of that adapter</td>
</tr>
<tr>
<td>7</td>
<td>Click <strong>OK</strong> to close the <strong>POST Results</strong> dialog box.</td>
</tr>
</tbody>
</table>
Turning off the Locator LED for a Chassis

View the POST Results for a Chassis
Managing the Servers

This chapter includes:

• Server Management in Cisco UCS Manager GUI, page 253
• Booting Servers, page 254
• Shutting Down Servers, page 255
• Resetting a Server, page 255
• Reacknowledging a Server, page 256
• Removing a Server from a Chassis, page 257
• Decommissioning a Server, page 257
• Reaknowledging a Server Slot in a Chassis, page 258
• Removing a Non-Existent Server from the Configuration Database, page 258
• Toggling the Locator LED, page 259
• Starting the KVM Console, page 260
• Resetting the CMOS for a Server, page 261
• Resetting the BMC for a Server, page 261
• Monitoring a Server, page 262
• Viewing the POST Results for a Server, page 263

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**

1. In the **Navigation** pane, click the **Equipment** tab.
2. In the **Equipment** tab, expand **Equipment ➤ Chassis ➤ Chassis Number ➤ Servers**.
3. Choose the server that you want to boot.
4. In the **Work** pane, click the **General** tab.
5. In the **Actions** area, click **Boot Server**.
6. If Cisco UCS Manager 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**

1. In the **Navigation** pane, click the **Servers** tab.
2. In the **Servers** tab, expand **Servers ➤ Service Profiles**.
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.
4. Choose the service profile that requires the associated server to be booted.
5. In the **Work** pane, click the **General** tab.
6. In the **Actions** area, click **Boot Server**.
7. If Cisco UCS Manager displays a confirmation dialog box, click **Yes**.
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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Equipment tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Equipment tab, expand Equipment ➤ Chassis ➤ Chassis Number ➤ Servers.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose the server that you want to shut down.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Work pane, click the General tab.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Actions area, click Shut Down.</td>
</tr>
<tr>
<td>Step 6</td>
<td>If Cisco UCS Manager displays a confirmation dialog box, click Yes.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Servers tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Servers tab, expand Servers ➤ Service Profiles.</td>
</tr>
<tr>
<td>Step 3</td>
<td>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.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Choose the service profile that requires the associated server to be shut down.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Work pane, click the General tab.</td>
</tr>
<tr>
<td>Step 6</td>
<td>In the Actions area, click Shut Down.</td>
</tr>
<tr>
<td>Step 7</td>
<td>If Cisco UCS Manager displays a confirmation dialog box, click Yes.</td>
</tr>
</tbody>
</table>

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**
In 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 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
components 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**
In 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

Perform the following procedure when you remove a server from a chassis. Do not physically remove the server first.

Procedure

Step 1  In the Navigation pane, click the Equipment tab.
Step 2  In 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 do not want to physically remove the server hardware, you must re-acknowledge the slot to have Cisco UCS Manager rediscover the server.
For more information, see Reaknowledging a Server Slot in a Chassis, page 258

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  In 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 do not want to physically remove the server hardware, you must re-acknowledge the slot to have Cisco UCS Manager rediscover the server.

For more information, see Reaknowledging a Server Slot in a Chassis, page 258

Reaknowledging 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Equipment tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Equipment tab, expand Equipment ➤ Chassis ➤ Chassis Number ➤ Servers.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose the server whose slot you want to reacknowledge.</td>
</tr>
<tr>
<td>Step 4</td>
<td>If Cisco UCS Manager displays a Resolve Slot Issue dialog box, do one of the following:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The here link in the Situation area</td>
<td>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.</td>
</tr>
<tr>
<td>OK</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 257.
**Procedure**

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

**Step 2** In 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** In 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** In 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 In 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 In 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.
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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Equipment tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Equipment tab, expand Equipment ➤ Chassis ➤ Chassis Number ➤ Servers.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose the server for which you want to reset the CMOS.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Work pane, click the General tab.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Actions area, click Recover Server.</td>
</tr>
<tr>
<td>Step 6</td>
<td>In the Recover Server dialog box, do the following:</td>
</tr>
<tr>
<td></td>
<td>a) Click Reset CMOS.</td>
</tr>
<tr>
<td></td>
<td>b) Click OK.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Equipment tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Equipment tab, expand Equipment ➤ Chassis ➤ Chassis Number ➤ Servers.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose the server for which you want to reset the BMC.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Work pane, click the General tab.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Actions area, click Recover Server.</td>
</tr>
<tr>
<td>Step 6</td>
<td>In the Recover Server dialog box, do the following:</td>
</tr>
<tr>
<td></td>
<td>a) Click Reset iBMC (Server Controller).</td>
</tr>
<tr>
<td></td>
<td>b) Click OK.</td>
</tr>
</tbody>
</table>
## Monitoring a Server

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>In the Navigation pane, click the Equipment tab.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>In the Equipment tab, expand <strong>Equipment ➤ Chassis ➤ Chassis Number ➤ Servers.</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Click the server that you want to monitor.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>In the Work pane, click one of the following tabs to view the status of the server:</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>General tab</td>
<td>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.</td>
</tr>
<tr>
<td>Inventory tab</td>
<td>The sub-tabs display the properties and status of the components of the server.</td>
</tr>
<tr>
<td>Installed Firmware tab</td>
<td>Displays the current 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.</td>
</tr>
<tr>
<td>Faults tab</td>
<td>Provides details of faults generated by the server.</td>
</tr>
<tr>
<td>Events tab</td>
<td>Provides details of events generated by the server.</td>
</tr>
<tr>
<td>FSM tab</td>
<td>Provides details about and the status of FSM tasks related to the server. You can use this information to diagnose errors with those tasks.</td>
</tr>
<tr>
<td>Statistics tab</td>
<td>Provides statistics about the server and its components. You can view these statistics in tabular or chart format.</td>
</tr>
<tr>
<td>Temperatures tab</td>
<td>Provides temperature statistics for the components of the server. You can view these statistics in tabular or chart format.</td>
</tr>
<tr>
<td>Power tab</td>
<td>Provides power statistics for the components of the server. You can view these statistics in tabular or chart format.</td>
</tr>
</tbody>
</table>

**Step 5**

In the Navigation pane, expand **Server_ID ➤ Interface Cards ➤ Interface_Card_ID.**

**Step 6**

In the Work pane, you can view the status of one or more of the following components of the interface card:

- Interface card
- DCE interfaces
- HBAs
- NICs

**Tip**

If you expand these nodes, you can view the status of the components of that element. For example, if you expand a NIC node, you can view the properties and status of 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**  In 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.
Starting the KVM Console from a Service Profile

Viewing the POST Results for a Server
Managing the IO Modules

This chapter includes:

- I/O Module Management in Cisco UCS Manager GUI, page 265
- Resetting an I/O Module, page 265
- Monitoring an I/O Module, page 266
- Viewing the POST Results for an I/O Module, page 266

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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Equipment tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Equipment tab, expand Equipment ➤ Chassis ➤ Chassis Number ➤ IO Modules.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose the I/O module that you want to reset.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Work pane, click the General tab.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Actions area, click Reset IO Module.</td>
</tr>
<tr>
<td>Step 6</td>
<td>If Cisco UCS Manager displays a confirmation dialog box, click Yes.</td>
</tr>
</tbody>
</table>
Monitoring an I/O Module

Procedure

Step 1  In the Navigation pane, click the Equipment tab.
Step 2  In 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General tab</td>
<td>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.</td>
</tr>
<tr>
<td>Fabric Ports tab</td>
<td>Displays the status and selected properties of all fabric ports in the I/O module.</td>
</tr>
<tr>
<td>Backplane Ports tab</td>
<td>Displays the status and selected properties of all backplane ports in the I/O module.</td>
</tr>
<tr>
<td>Faults tab</td>
<td>Provides details of faults generated by the I/O module.</td>
</tr>
<tr>
<td>Events tab</td>
<td>Provides details of events generated by the I/O module.</td>
</tr>
<tr>
<td>FSM tab</td>
<td>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.</td>
</tr>
<tr>
<td>Statistics tab</td>
<td>Provides statistics about the I/O module and its components. You can view these statistics in tabular or chart format.</td>
</tr>
</tbody>
</table>

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  In 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.
Configuring Call Home

This chapter includes:

- Call Home, page 269
- Call Home Considerations, page 270
- Cisco Smart Call Home, page 270
- Configuring Call Home, page 271
- Disabling Call Home, page 273
- Enabling Call Home, page 273
- Configuring System Inventory Messages, page 274
- Sending System Inventory Messages, page 274
- Configuring Call Home Profiles, page 275
- Configuring Call Home Policies, page 277
- Configuring Call Home for Smart Call Home, page 279

Call Home

Call Home provides an e-mail-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 automatically generate a case with the Technical Assistance Center.

Call Home provides email-based and web-based notification of critical system events. A versatile range of message formats are available for optimal compatibility with pager services or XML-based automated parsing applications. Common uses of this feature may include direct paging of a network support engineer, notification of a Network Operations Center, XML delivery to a support website, and utilization of Cisco Smart Call Home services for direct case generation with the Cisco Systems Technical Assistance Center (TAC).

The Call Home feature can deliver alert messages containing information about configuration, diagnostics, environmental conditions, inventory, and syslog 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 automatically 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 that is suitable for pagers or printed reports.

Call Home Considerations

How you configure Call Home depends on how you intend to use the feature. Some information to consider before you configure Call Home includes:

- 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.
- If Cisco Smart Call Home is used, an active service contract must cover the device being configured.

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:

- 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

**Tip**

By default, email alerts are sent for all critical system events. However, you can optionally configure Call Home policies to enable or disable sending email alerts for other critical system events.

### 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 **Urgency** 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact field</td>
<td>The main Call Home contact person.</td>
</tr>
<tr>
<td>Phone field</td>
<td>The telephone number for the main contact. Enter the number in international format, starting with a + (plus sign) and a country code.</td>
</tr>
<tr>
<td>Email field</td>
<td>The email address for the main contact.</td>
</tr>
<tr>
<td>Address field</td>
<td>The mailing address for the main contact.</td>
</tr>
</tbody>
</table>

Step 7  (Optional) In the **Ids** area, complete the following fields with the identification information that Call Home should use:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Id field</td>
<td>The unique identification number for the customer.</td>
</tr>
<tr>
<td>Contract Id field</td>
<td>The Call Home contract number for the customer.</td>
</tr>
<tr>
<td>Site Id field</td>
<td>The unique Call Home identification number for the customer site.</td>
</tr>
</tbody>
</table>

Step 8  In the **Email Addresses** area, complete the following fields with email information for Call Home alert messages:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From field</td>
<td>The email address that should appear in the From field on Call Home alert messages sent by the system.</td>
</tr>
<tr>
<td>Reply To field</td>
<td>The return email address that should appear in the From field on Call Home alert messages sent by the system.</td>
</tr>
</tbody>
</table>

Step 9  In the **SMTP Server** area, complete the following fields with information about the SMTP server where Call Home should send email messages:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host (IP Address or Hostname) field</td>
<td>The IP address or host name of the SMTP server.</td>
</tr>
<tr>
<td>Port field</td>
<td>The port number the system should use to talk to the SMTP server.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Periodically</td>
<td>If this field is set to on, Cisco UCS automatically sends the system inventory to the Call Home database. When the information is sent depends on the other fields in this area.</td>
</tr>
<tr>
<td>Send Interval</td>
<td>The number of days that should pass between automatic system inventory data collection.</td>
</tr>
<tr>
<td>Hour of Day to Send</td>
<td>The hour that the data should be sent using the 24-hour clock format.</td>
</tr>
<tr>
<td>Minute of Hour</td>
<td>The number of minutes after the hour that the data should be sent.</td>
</tr>
<tr>
<td>Time Last Sent</td>
<td>The date and time the information was last sent.</td>
</tr>
<tr>
<td>Note</td>
<td>This field is displayed after the first inventory has been sent.</td>
</tr>
<tr>
<td>Next Scheduled</td>
<td>The date and time for the upcoming data collection.</td>
</tr>
<tr>
<td>Note</td>
<td>This field is displayed after the first inventory has been sent.</td>
</tr>
</tbody>
</table>

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.
Configuring Call Home Profiles

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 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>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.</td>
</tr>
<tr>
<td>Level field</td>
<td>This can be:</td>
</tr>
<tr>
<td></td>
<td>• critical</td>
</tr>
<tr>
<td></td>
<td>• debug</td>
</tr>
<tr>
<td></td>
<td>• disaster</td>
</tr>
<tr>
<td></td>
<td>• fatal</td>
</tr>
<tr>
<td></td>
<td>• major</td>
</tr>
</tbody>
</table>
Creating a Call Home Profile

### Configuring Call Home Profiles

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Version</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>• minor</td>
<td></td>
</tr>
<tr>
<td>• normal</td>
<td></td>
</tr>
<tr>
<td>• notification</td>
<td></td>
</tr>
<tr>
<td>• warning</td>
<td></td>
</tr>
</tbody>
</table>

#### Alert Groups field

The group or groups that are alerted based on this Call Home profile. This can be one or more of the following:
- ciscoTac
- diagnostic
- environmental
- inventory
- license
- lifeCycle
- linecard
- supervisor
- syslogPort
- system
- test

#### Step 7

In the Email Configuration area, complete the following fields to configure the email alerts:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format field</td>
<td>This can be:</td>
</tr>
<tr>
<td>• xml</td>
<td></td>
</tr>
<tr>
<td>• shortTxt</td>
<td></td>
</tr>
</tbody>
</table>

| Max Message Size field | The maximum message size that is sent to the designated Call Home recipients. |

#### Step 8

In the Recipients area, complete the following fields to add one or more email recipients for the email alerts:

- On the icon bar to the right of the table, click +.
- 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.
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 on the profile you want to delete and choose Delete.

Step 6
Click Save Changes.

Configuring Call Home Policies

Configuring a Call Home Policy

Tip
By default, email alerts are sent for all critical system events. However, you can optionally configure Call Home policies to enable or disable sending email alerts for other 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 Policies dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State field</td>
<td>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.</td>
</tr>
<tr>
<td>Cause field</td>
<td>The event that triggers this policy. This can be:</td>
</tr>
</tbody>
</table>
### 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. |

### Configuring Call Home Policies

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>equipment-degraded</td>
<td></td>
</tr>
<tr>
<td>equipment-inoperable</td>
<td></td>
</tr>
<tr>
<td>fru-problem</td>
<td></td>
</tr>
<tr>
<td>identity-unestablishable</td>
<td></td>
</tr>
<tr>
<td>power-problem</td>
<td></td>
</tr>
<tr>
<td>thermal-problem</td>
<td></td>
</tr>
<tr>
<td>voltage-problem</td>
<td></td>
</tr>
</tbody>
</table>

**Note**: You cannot change the cause after you save this policy.

**Step 7**: Click OK.

**Step 8**: Repeat Steps 6 and 7 to configure a Call Home policy for each event that you want to have send a Call Home email alert.
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.

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 **Urgency** 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contact</strong></td>
<td>The main Call Home contact person.</td>
</tr>
<tr>
<td><strong>Phone</strong></td>
<td>The telephone number for the main contact. Enter the number in international format, starting with a + (plus sign) and a country code.</td>
</tr>
<tr>
<td><strong>Email</strong></td>
<td>The email address for the main contact.</td>
</tr>
<tr>
<td><strong>Address</strong></td>
<td>The mailing address for the main contact.</td>
</tr>
</tbody>
</table>

### Step 7
In the **Ids** area, complete the following fields with the Smart Call Home identification information:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Customer Id</strong></td>
<td>The unique identification number for the customer.</td>
</tr>
<tr>
<td><strong>Contract Id</strong></td>
<td>The Call Home contract number for the customer.</td>
</tr>
<tr>
<td><strong>Site Id</strong></td>
<td>The unique Call Home identification number for the customer site.</td>
</tr>
</tbody>
</table>

### Step 8
In the **Email Addresses** area, complete the following fields with the email information for Smart Call Home alert messages:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>From</strong></td>
<td>The email address that should appear in the From field on Call Home alert messages sent by the system.</td>
</tr>
</tbody>
</table>
### Configuring Call Home for Smart Call Home

#### Configuring the Default Cisco TAC-1 Profile

The default settings of the Cisco TAC-1 profile are:

- 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>In the <strong>Navigation</strong> pane, click the <strong>Admin</strong> tab.</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>In the <strong>Admin</strong> tab, expand <strong>All</strong> ➤ <strong>Communication Services</strong>.</td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>Click <strong>Call Home</strong>.</td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>In the <strong>Work</strong> pane, click the <strong>System Inventory</strong> tab.</td>
</tr>
<tr>
<td><strong>5</strong></td>
<td>In the <strong>Properties</strong> area, complete the following fields to specify how system inventory messages will be sent to Smart Call Home:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Send Periodically</strong> field</td>
<td>If this field is set to on, Cisco UCS automatically sends the system inventory to the Call Home database. When the information is sent depends on the other fields in this area.</td>
</tr>
<tr>
<td><strong>Send Interval</strong> field</td>
<td>The number of days that should pass between automatic system inventory data collection.</td>
</tr>
<tr>
<td><strong>Hour of Day to Send</strong> field</td>
<td>The hour that the data should be sent using the 24-hour clock format.</td>
</tr>
<tr>
<td><strong>Minute of Hour</strong> field</td>
<td>The number of minutes after the hour that the data should be sent.</td>
</tr>
<tr>
<td><strong>Time Last Sent</strong> field</td>
<td>The date and time the information was last sent. <strong>Note</strong> This field is displayed after the first inventory has been sent.</td>
</tr>
<tr>
<td><strong>Next Scheduled</strong> field</td>
<td>The date and time for the upcoming data collection. <strong>Note</strong> This field is displayed after the first inventory has been sent.</td>
</tr>
</tbody>
</table>

**Step 6** Click **Save Changes**.
Registering Smart Call Home

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Navigation pane, click the Admin tab.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Admin tab, expand All ➤ Communication Services.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Call Home.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Work pane, click the System Inventory tab.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Actions area, click Send System Inventory Now to start the registration process.</td>
</tr>
<tr>
<td>Step 6</td>
<td>When you receive the email response from Cisco, click the link in the email to complete registration for Smart Call Home.</td>
</tr>
</tbody>
</table>
CHAPTER 31

Backing Up and Restoring the Configuration

This chapter includes:

- Backup and Export Configuration, page 285
- Backup Types, page 285
- Import Configuration, page 286
- Import Methods, page 286
- System Restore, page 286
- Required User Role for Backup and Import Operations, page 286
- Backup Operations, page 287
- Import Operations, page 290
- Restoring the Configuration for a Fabric Interconnect, page 293

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.

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 and save and exports the configuration file until you set the admin state to enabled.

You can only maintain one backup operation for each location where you plan to save a backup file. If you rerun a backup operation without changing the filename, Cisco UCS Manager overwrites the existing file on the server.

Backup Types

You can perform one of the following types of backups through Cisco UCS Manager:
• **Full state**—Includes a snapshot of the entire system. You can use the file generated from this backup for disaster recovery if you need to recreate every configuration on a fabric interconnect or to rebuild a fabric interconnect.

• **All configuration**—Includes all system and logical configuration settings

• **System configuration**—Includes all system configuration settings such as usernames, roles, and locales.

• **Logical configuration**—Includes all logical configuration settings such as service profiles, VLANs, VSANs, pools, and policies

### Import Configuration

You can import any configuration file that was exported from Cisco UCS Manager. The file does not have 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 have 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

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Admin tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the All node.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Work pane, click the General tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Actions area, click Backup Configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Backup Configuration dialog box, click Create Backup Operation.</td>
</tr>
<tr>
<td>Step 6</td>
<td>In the Create Backup Operation dialog box, complete the following fields:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State field</td>
<td>This can be:</td>
</tr>
<tr>
<td>enabled</td>
<td>Cisco UCS runs the backup operation automatically as soon as you click OK.</td>
</tr>
<tr>
<td>disabled</td>
<td>Cisco UCS does not run the backup operation automatically when you click OK. If you select this option, you must manually run the backup from the Backup Configuration dialog box.</td>
</tr>
<tr>
<td>Type field</td>
<td>The information saved in the backup configuration file. This can be:</td>
</tr>
<tr>
<td>Full state</td>
<td>Includes a snapshot of the entire system. You can use this file for disaster recovery if you need to recreate every configuration on a switch or rebuild a switch.</td>
</tr>
<tr>
<td>All configuration</td>
<td>Includes all system and logical configuration information.</td>
</tr>
<tr>
<td>System configuration</td>
<td>Includes all system configuration settings such as user names, roles, and locales.</td>
</tr>
<tr>
<td>Logical configuration</td>
<td>Includes all logical configuration settings such as service profiles, LAN configuration settings, SAN configuration settings, pools, and policies.</td>
</tr>
<tr>
<td>Protocol field</td>
<td>The protocol to use when saving the configuration file to the remote server. This can be:</td>
</tr>
<tr>
<td>FTP</td>
<td></td>
</tr>
<tr>
<td>TFTP</td>
<td></td>
</tr>
<tr>
<td>SCP</td>
<td></td>
</tr>
</tbody>
</table>
### Running a Backup Operation

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the <strong>Navigation</strong> pane, click the <strong>Admin</strong> tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the <strong>All</strong> node.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the <strong>Work</strong> pane, click the <strong>General</strong> tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the <strong>Actions</strong> area, click <strong>Backup Configuration</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the <strong>Backup Operations</strong> table of the <strong>Backup Configuration</strong> dialog box, click the backup operation that you want to run.</td>
</tr>
</tbody>
</table>
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 user name 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 will continue to run until it is completed. To view the progress, re-open the **Backup Configuration** dialog box.

### 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 displays a confirmation dialog box, click **Yes**. |
| Step 8 | In the **Backup Configuration** dialog box, click one of the following: |

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Apply</strong></td>
<td>Deletes the selected backup operations without closing the dialog box.</td>
</tr>
<tr>
<td><strong>OK</strong></td>
<td>Deletes the selected backup operations and closes the dialog box.</td>
</tr>
</tbody>
</table>
Import Operations

Creating an Import Operation

You cannot import a full state configuration file. You must perform a system restore from a full state configuration 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State field</td>
<td>This can be:</td>
</tr>
<tr>
<td></td>
<td>• enabled—Cisco UCS runs the import operation automatically as soon as you click OK.</td>
</tr>
<tr>
<td></td>
<td>• disabled—Cisco UCS does not run the import operation automatically when you click OK. If you select this option, you must manually run the import from the Import Configuration dialog box.</td>
</tr>
<tr>
<td>Action field</td>
<td>You can select:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Replace—The system takes each object in the import configuration file and overwrites the corresponding object in the current configuration.</td>
</tr>
<tr>
<td>Protocol field</td>
<td>The protocol to use when communicating with the remote server. This can be:</td>
</tr>
<tr>
<td></td>
<td>• FTP</td>
</tr>
<tr>
<td></td>
<td>• SCP</td>
</tr>
<tr>
<td></td>
<td>• SFTP</td>
</tr>
<tr>
<td></td>
<td>• TFTP</td>
</tr>
</tbody>
</table>
### Running an Import Operation

You cannot import a full state configuration file. You must perform a system restore from a full state configuration file.

#### Procedure

1. **Step 1** In the Navigation pane, click the Admin tab.
2. **Step 2** Click the All node.
3. **Step 3** In the Work pane, click the General tab.
4. **Step 4** In the Actions area, click Import Configuration.
5. **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.
6. **Step 6** In the Properties area, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname field</td>
<td>The hostname from which the configuration file should be imported.</td>
</tr>
<tr>
<td>Remote File field</td>
<td>The name of the configuration file that is being imported.</td>
</tr>
<tr>
<td>User field</td>
<td>The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP.</td>
</tr>
<tr>
<td>Password field</td>
<td>The password for the remote server username. This field does not apply if the protocol is TFTP.</td>
</tr>
</tbody>
</table>

#### 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:
- **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 will continue to run until it is completed. To view the progress, re-open the Import Configuration dialog box.
a) In the **Admin State** field, click the **Enabled** radio button.
b) For all protocols except TFTP, enter the password for the user name 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 will continue to run until it is completed. To view the progress, re-open the **Import Configuration** dialog box.

---

### 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 displays a confirmation dialog box, click **Yes**.
**Step 8**
In the **Import Configuration** dialog box, click one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Apply</strong></td>
<td>Deletes the selected import operations without closing the dialog box.</td>
</tr>
<tr>
<td><strong>OK</strong></td>
<td>Deletes the selected import operations and closes the dialog box.</td>
</tr>
</tbody>
</table>
Restoring the Configuration for a Fabric Interconnect

Before You Begin
You must have access to a full state backup file to perform a system restore.

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 Springfield 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server IP</td>
<td>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.</td>
</tr>
<tr>
<td>Backup File Path</td>
<td>The file path where the full state backup file is located, including the folder names and file name.</td>
</tr>
<tr>
<td>User ID</td>
<td>The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP.</td>
</tr>
</tbody>
</table>
### Deleting One or More Import Operations

#### Restoring the Configuration for a Fabric Interconnect

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>The password for the remote server username. This field does not apply if the protocol is TFTP.</td>
</tr>
</tbody>
</table>

**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.

**What to Do Next**  
If the system has more than one fabric interconnect, repeat this procedure to restore the configuration for the second fabric interconnect.
Configuring Settings for Faults and Events

- Configuring Settings for the Fault Collection Policy, page 295
- Configuring Settings for the Core File Exporter, page 297

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 the length of time that each fault remains in the flapping and retention intervals.

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 enters a flapping or soaking interval that is designed to prevent flapping. 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 returns to the active state. If the condition does not reoccur during the flapping interval, the fault is cleared.
4. The cleared fault enters the retention interval. This interval ensures that the fault reaches the attention of an administrator, even if the condition that caused the fault has been alleviated, and that the fault is not deleted prematurely. The retention interval retains the cleared fault for the length of time specified in the fault collection policy.
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 In 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flapping Interval field</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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 hh:mm:ss field.                                                                                   |
| hh:mm:ss field            | The number of 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 TPTP. 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 In 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State field</td>
<td>This can be:</td>
</tr>
<tr>
<td></td>
<td>• enabled—If an error causes the server to perform a core dump, the system</td>
</tr>
<tr>
<td></td>
<td>sends the core dump file via FTP to a given location. When this option is</td>
</tr>
<tr>
<td></td>
<td>selected, Cisco UCS Manager GUI displays the other fields in this area</td>
</tr>
<tr>
<td></td>
<td>that enable you to specify the FTP export options.</td>
</tr>
<tr>
<td></td>
<td>• disabled—Core dump files are not automatically exported.</td>
</tr>
<tr>
<td>Description field</td>
<td>A user-defined description of the core file.</td>
</tr>
<tr>
<td>Port field</td>
<td>The port number to use when exporting the core dump file via TFTP.</td>
</tr>
<tr>
<td>Hostname field</td>
<td>The hostname to connect with via TFTP.</td>
</tr>
<tr>
<td>Path field</td>
<td>The path to use when storing the core dump file on the remote system.</td>
</tr>
</tbody>
</table>

Step 5 Click Save Changes.
Recovering a Lost Password

This chapter includes:

- Password Recovery for the Admin Account, page 299
- Determining the Leadership Role of a Fabric Interconnect, page 300
- Verifying the Firmware Versions on a Fabric Interconnect, page 300
- Recovering the Admin Account Password in a Standalone Configuration, page 300
- Recovering the Admin Account Password in a Cluster Configuration, page 301

Password Recovery for the Admin Account

The admin account is the system administrator or superuser account. If an administrator loses the password to this account, you can have a serious security issue. As a result, the procedure to recover the password for the admin account requires you to power cycle all fabric interconnects in a Cisco UCS instance.

When you recover the password for the admin account, you actually change the password for that account. You cannot retrieve the original password for that account.

You can reset the password for all other local accounts through Cisco UCS Manager. However, you must log into 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**

1. In the Navigation pane, click the Equipment tab.
2. In the Equipment tab, expand Equipment ➤ Fabric Interconnects.
3. Click the fabric interconnect for which you want to identify the role.
4. In the Work pane, click the General tab.
5. In the General, click the down arrows on the High Availability Details bar to expand that area.
6. View the Leadership field to determine the role of the fabric interconnect.

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**

1. In the Navigation pane, click the Equipment tab.
2. In the Equipment tab, select the Equipment Node.
3. In the Work pane, select the Firmware Management tab.
4. In the Installed Firmware tab, note the following firmware versions for each fabric interconnect:
   - Kernel version
   - System version

Recovering the Admin Account Password in a Standalone Configuration

**Before You Begin**

1. Physically connect the console port on the fabric interconnect to a computer terminal or console server.
2. Obtain the following information:
   - The firmware kernel version on the fabric interconnect
   - The firmware system version
Recovering the Admin Account Password in a Cluster Configuration

**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
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/fabric/kernel_firmware_version

Step 6 Enter config terminal mode.
   Fabric(boot)# config terminal

Step 7 Reset the admin password.
   Fabric(boot)(config)# admin-password
   password
   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/fabric/system_firmware_version

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/fabric/kernel_firmware_version
   b) Boot the system firmware version on the subordinate fabric interconnect.
      Fabric(boot)# load /installables/fabric/system_firmware_version
Configuring Statistics-Related Policies

This chapter includes:

- Statistics Collection Policy, page 303
- Statistics Threshold Policy, page 304
- Modifying a Statistics Collection Policy, page 304
- Configuring Statistics Threshold Policies, page 306

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 in the fabric Interconnect
- 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.

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 on 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection Interval field</td>
<td>The length of time the fabric interconnect should wait between data recordings. This can be:</td>
</tr>
<tr>
<td></td>
<td>• 30 Seconds</td>
</tr>
<tr>
<td></td>
<td>• 1 Minute</td>
</tr>
<tr>
<td></td>
<td>• 2 Minutes</td>
</tr>
<tr>
<td></td>
<td>• 5 Minutes</td>
</tr>
</tbody>
</table>
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 that 15 minute reporting interval. Instead of sending 15 statistics to Cisco UCS Manager GUI, it sends the only the most recent recording along with the average, minimum, and maximum values for the entire group.

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

Creating a Server and Server Component Threshold Policy

Tip
This procedure documents how to create 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 In 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>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.</td>
</tr>
<tr>
<td>Description field</td>
<td>A description of the threshold policy.</td>
</tr>
</tbody>
</table>

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 checkboxes:
   • 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 checkboxes:
   • 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 this step.

   • 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  In the Servers tab, expand Servers ➤ Policies ➤ Organization_Name.

Step 3  Expand the Threshold Policies node.

Step 4  Right-click on 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 checkboxes:
   - 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 checkboxes:
   - 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 this step.
   - 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Servers tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Servers tab, expand Servers ➤ Policies ➤ Organization_Name.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Expand the Threshold Policies node.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Right-click on the policy you want to delete and select Delete.</td>
</tr>
<tr>
<td>Step 5</td>
<td>If Cisco UCS Manager displays a confirmation dialog box, click Yes.</td>
</tr>
</tbody>
</table>

Adding a Threshold Class to the Uplink Ethernet Port Threshold Policy

Tip
You cannot create a new 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 | In the LAN tab, expand LAN ➤ LAN Cloud. |
| Step 3 | Expand the Threshold Policies node. |
| Step 4 | Right-click on 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. |
In the **Normal Value** field, enter the desired value for the property type.

In the **Alarm Triggers (Above Normal Value)** fields, check one or more of the following checkboxes:

- Critical
- Major
- Minor
- Warning
- Condition
- Info

In the **Up and Down** fields, enter the range of values that should trigger the alarm.

In the **Alarm Triggers (Below Normal Value)** fields, check one or more of the following checkboxes:

- Info
- Condition
- Warning
- Minor
- Major
- Critical

In the **Up and Down** fields, enter the range of values that should trigger the alarm.

**Step 7**

In the **Create Threshold Class** page of the **Create Threshold Policy** wizard, do one of 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 a new 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 on 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
   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 checkboxes:
      • Critical
      • Major
      • Minor
      • Warning
      • Condition
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 checkboxes:
   • 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 this step.
   • 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 new 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 In the SAN tab, expand SAN ➤ SAN Cloud.
Step 3 Expand the Threshold Policies node.
Step 4 Right-click on 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 checkboxes:
   - 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 checkboxes:
   - 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 this step.
   - 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
accounts
creating user 89
deleting local 91
user 81
acknowledging
chassis 247
servers 256
activate firmware 95
activating
adapter firmware 103
BMC firmware 104
firmware 101
IOM firmware 105
adapters
activating firmware 103
Cisco UCS 82598KR-CI 23
updating firmware 102
virtualization 23
adding
NTP servers 246
ports to a port channel 56, 120
administration 25
all configuration 285
architectural simplification 3
area, Fault Summary 29
associating servers 232
authentication
primary 69
remote 69
autoconfiguration policy
about 12, 188
creating 188
deleting 189
Automatically Reconnect 35

B
backing up (continued)
creating operations 287
deleting operation 289
running operations 288
types 285
user role 286
backup operations
creating 287
deleting 289
running 288
beacon
chassis 249
servers 259
best effort priority system class 20, 124, 136, 137
binding
service profiles 235
vHBAs 163
vNICs 143
BMC
activating firmware 104
resetting 261
updating firmware 103
boot policies
about 9, 177
creating 179
deleting 180
bootflash, available space 99
booting servers 254
bronze priority system class 20, 124, 136, 137
bundle, firmware 93
burned in values 8, 200

C
Call Home
about 269
Cisco TAC-1 profile 281
configuring 271
configuring policies 277
considerations 277
creating profiles 275
Call Home (continued)
deleting policies 279
deleting profiles 277
disabling 273
disabling policies 278
enabling 273
enabling policies 279
registering Smart Call Home 283
Smart Call Home 270
system inventory messages 274
canceling image downloads 101
catalog, images 94
changing
ports 53
properties 35
chassis
acknowledging 247
acknowledging servers 256
discovery policy 10, 181
enabling decommissioned 248
hybrid display 33
management 247
monitoring 249
POST results 251
reacknowledging slot 258
removing 248
removing server 257
turning off locator LED 249
turning on locator LED 249
chassis discovery policy
about 10, 181
configuring 181
chassis management 247, 248, 249
acknowledging 247
enabling decommissioned 248
monitoring 249
removing 248
turning off locator LED 249
turning on locator LED 249
CIM-XML, configuring 60
Cisco TAC-1 profile, configuring 281
Cisco UCS 82598KR-CI
virtualization 23
Cisco UCS CNA M71KR
virtualization 23
Cisco UCS Manager
about 25
GUI 29
cisco-av-pair 70
CiscoAvPair 70
cloning service profiles 232
cluster configuration
about 28
primary fabric interconnect 44
cluster configuration (continued)
subordinate fabric interconnect 46
CMOS resetting 261
communication services
about 59
CIM-XML 60
configuring 67
HTTP 61
HTTPS 61, 62, 63
SNMP 65, 66
Telnet 67
component, firmware 93
configuration
backing up 287, 288
import methods 286
importing 286
restoring 286, 290, 293
configuration, cluster 44, 46
configuration, standalone 42
configuring
CIM-XML 60
communication services 67
HTTP 61
HTTPS 61, 62, 63
ports 116
server ports 52
console, KVM 240, 260
Core File Exporter
about 297
configuring 297
creating
host firmware policy 106
management firmware policy 108
service profiles 230
D
database
backing up 285
restoring 286
decommissioning
chassis 248
servers 257
default
service profiles 217
deleting
port channels 57
service profiles 235
disabling
Call Home 273
communication services 67
port channels 120
disabling (continued)
  ports 54
  server ports 117
  uplink Ethernet port channels 56
  uplinkEthernet ports 118

disassociating servers 233

disaster recovery 285, 286

discovery policy
  chassis 10, 181
  server 12, 190, 191

DNS servers
  about 111
  adding 111
  deleting 112
  dongle, KVM 239
  downgrade firmware 98
  download firmware 95
  downloading
    canceling 101
    images 99

Ethernet
  enabling
    Call Home 271, 273
    Core File Exporter 297
    decommissioned chassis 248
    port channels 120
    ports 53
    server ports 117
    Smart Call Home 279
    SNMP 65
    Telnet 67
    uplink Ethernet port channels 56
    uplinkEthernet ports 118
  end-host mode 49, 116
  endpoints
    direct firmware update 95
    service profile update 97
  Ethernet adapter policies
    about 10, 144, 164
    creating 145
    deleting 148
  Ethernet switching mode
    about 48
  Ethernet switching mode (continued)
    modifying 49
  exiting 35
  exporting
    backup 287
    backup types 285
    configuration 285
    user role 286

F

fabric interconnects
  admin password recover 300, 301
  admin password recovery 299
  available space 99
  changing ports 53
  cluster 28
  determining leadership role 300
  disabling ports 54
  enabling ports 53
  enabling standalone for cluster 47
  ETH switching mode 48
  high availability 28
  initial setup
    about 41
    first 44
    management port 42
    second 46
    setup mode 42
    standalone 42
  mode 49
  monitoring 49
  restoring configuration 293
  system configuration type 42
  unconfiguring ports 54
  updating firmware 105
  updating UCS Manager 106
  verifying firmware 300

fault collection policy
  about 13, 295
  configuring 296
  Fault Summary area 29

faults
  collection policy 13, 295, 296
  Core File Exporter 297
  lifecycle 13, 295

FCoE 5

features
  opt-in 21
  stateless computing 21

Fibre Channel
  link-level flow control 5
Fibre Channel (continued)
  over Ethernet 5
  priority flow control 5
  uplink ports 51
Fibre Channel adapter policies
  about 10, 144, 164
  creating 164
  deleting 167
Fibre Channel priority system class 20, 124, 136, 137
filtering tables 32
firmware
  about 93
  activating 101
  activating adapters 103
  activating BMC 104
  activating IOM 105
  canceling image download 101
  direct update 95
  downgrades 98
  downloading images 99
  fabric interconnect 300
  host pack 11, 97, 106, 107
  image headers 94
  images 93, 94
  management 95
  management pack 11, 98
  management package 108
  obtaining images 99
  service profiles 97
  update stages 96, 98
  updates 94
  updating 101
  updating adapters 102
  updating BMC 103
  updating fabric interconnects 105
  updating IOM 104
  updating UCS Manager 106
  upgrade order 96
  verifying 109
flexibility 4
flow control
  link-level 5
  priority 5
flow control policy
  about 21, 136
  creating 139
full state 285

G

gold priority system class 20, 124, 136, 137
graceful shutdown 255

GUI
  about 29
  customizing tables 32
  Fault Summary area 29
  hybrid display 33
  logging in, HTTP 34
  logging in, HTTPS 34
  logging out 35
  Navigation pane 30
  session properties 35
  status bar 31
  toolbar 31
  Work pane 31
GUI Inactivity Timeout 35
guidelines
  oversubscription 18
  pinning 20

H

hard reset, server 255
hardware, stateless 21
headers, images 94
high availability 4, 28, 44, 46
  about 28
  initial setup 44, 46
host firmware pack
  about 11, 97
  creating 106
  updating 107
HTTP
  configuring 61
  logging in 34
HTTPS
  certificate request 62
  configuring 63
  creating key ring 61
  importing certificate 63
  logging in 34
  trusted point 62
hybrid display 33

I

I/O module
  management 265
I/O modules
  activating firmware 105
  monitoring 266
  POST results 266
  resetting 265
I/O modules (continued)
  updating firmware 104
IEEE 802.3x link-level flow control  5
images 93, 94
  bundle 93
  component 93
  contents 94
  headers 94
import operations
  creating 290
  deleting 292
  running 291
importing
  about 286
  creating operations 290
  deleting operation 292
  restore methods 286
  user role 286
inheritance, servers 12, 191
inherited values 8, 200
initial setup
  about 41
  cluster configuration 44, 46
  management port IP address 42
  setup mode 42
  standalone configuration 42
initial templates 8, 200
IOM
  activating firmware 105
  monitoring 266
  POST results 266
  updating firmware 104
IP
  pools 175
IP addresses
  management IP pool 16, 174
  management port 42
IP pools
  creating IP address block 174
  management 16, 174
IPMI profiles
  about 11, 181
  creating 182
  deleting 183
K
key ring (continued)
  trusted point 62
KVM console
  about 238
KVM Console
  installing OS 240
  starting from server 260
  starting from service profile 260
KVM dongle
  about 238
  installing OS 239
L
LAN
  MAC pools 133, 134
  named VLANs
    creating 122, 127
    deleting 123, 129
  pin groups 121, 122, 131, 132
    creating 121, 131
    deleting 122, 132
  uplinks manager 33
  VLANs 127
  vNIC policy 13, 141
LAN pin groups
  creating 121, 131
  deleting 122, 132
LAN Uplinks Manager
  about 33
  changing Ethernet switching mode 116
  configuring ports 116
  disabling server ports 117
  disabling uplinkEthernet ports 118
  enabling server ports 117
  enabling uplinkEthernet ports 118
  launching 115
  named VLANs
    creating 122
    deleting 123
  pin groups
    creating 121
    deleting 122
  port channels
    adding ports 120
    creating 119
    deleting 121
    disabling 120
    enabling 120
    removing ports 121
  system classes, configuring 124
  unconfiguring server ports 117
LAN Uplinks Manager (continued)
unconfiguring uplink Ethernet ports 118
lanes, virtual 20, 135
launching
GUI, HTTP 34
GUI, HTTPS 34
LAN Uplinks Manager 115
LDAP 69
LDAP provider
creating 70
deleting 75
LED locator
chassis 249
servers 259
lifecycle, faults 13, 295
link-level flow control 5
local disk configuration policy
about 11, 183
changing 184
creating 183
deleting 185
locales
about 85
adding organizations 88
creating 87
deleting 88
deleting organizations 88
locally authenticated users
creating 89
deleting 91
locating
chassis 249
servers 259
logging in
HTTP 34
HTTPS 34
logging out 35
logical configuration 285

M
MAC addresses
creating pools 133
deleting pools 134
pools 15, 133
MAC pools
creating 133
deleting 134
management
chassis 247
I/O modules 265
servers 253
management firmware pack
about 11, 98
updating 108
management firmware package
creating 108
management IP pools
about 16, 174
creating IP address block 174
deleting IP address block 175
management port IP address 42
merging configuration 286
messages, system inventory 274, 282
mobility 21
mode
domain-host 48, 49, 116
Ethernet switching 48
setup 42
switching 49, 116
monitoring
chassis 249
fabric interconnects 49
I/O modules 266
servers 262
user sessions 91
multi-tenancy
about 22
name resolution 78
opt-in 23
opt-out 23
organizations 77, 79, 80
creating 79, 80
deleting 80

N
name resolution 78, 111
named VLANs
about 127
creating 122, 127
deleting 123, 129
named VSANs
about 151
creating 151
deleting 152
Navigation pane 30
network
connectivity 6
creating 151
named VLANs 122, 123, 127, 129
creating 122, 127
deleting 123, 129
network *(continued)*
- named VSANs 151, 152
- deleting 152

NTP servers
- about 245
- adding 246
- deleting 246

O

obtaining image bundles 99
operating system installation
- about 237
  - KVM console 238, 240
  - KVM dongle 238, 239
- methods 237
- PXE 239
- targets 238

operations
- backup 287, 288, 289
- confirming 35
- import 290, 292

opt-in
- about 21
  - multi-tenancy 23
  - stateless computing 22

opt-out 21, 22, 23
- multi-tenancy 23
- stateless computing 22

organizations
- about 77
  - adding to locales 88
  - creating 79, 80
  - creating locales 87
  - deleting 80
  - deleting from the locales 88
  - deleting locales 88
  - locales 85
- multi-tenancy 22
- name resolution 78

OS installation
- about 237
  - KVM console 238, 240
  - KVM dongle 238, 239
- methods 237
- PXE 239
- targets 238

overriding
- server identity 201
- overriding server identity 7, 199, 201

oversubscription *(continued)*
- considerations 17
- guidelines 18
- overview 3

P

packages
- management firmware 108

packs
- host firmware 11, 97, 106, 107
- management firmware 11, 98, 108

pane
- Navigation 30
- Work 31

passwords, recovering admin 299, 300, 301

PFC 5

pin groups
- about 18
- LAN 121, 122, 131, 132
- SAN 155, 156

pinning
- about 18
- guidelines 20
- servers to server ports 19

platinum priority system class 20, 124, 136, 137

policies
- about 9
  - autoconfiguration 12, 188, 189
  - boot 9, 177, 179, 180
  - Call Home 277, 278, 279
  - chassis discovery 10, 181
  - Ethernet 10, 144, 164
  - fault collection 13, 295, 296
  - Fibre Channel adapter 10, 144, 164
  - flow control 21, 136, 139
  - host firmware 11, 97, 106, 107
  - IPMI profiles 11, 181, 182, 183
  - local disk configuration 11, 183, 184, 185
  - management firmware 11, 98, 108
  - QoS 12, 21, 136, 138, 139
  - scrub 14, 140, 185, 186
  - serial over LAN
    - about 14, 187
    - creating 187
    - deleting 188
  - server discovery 12, 190, 191
  - server inheritance
    - about 12, 191
    - creating 191
    - deleting 192
  - server pool 12, 192, 193, 194
policies (continued)
server pool qualification 13, 194
server pool qualifications 194, 197
statistics collection 14, 303, 304
threshold 14, 304, 306, 308, 310
vHBA 13, 161
vNIC 13, 141

pools
about 15
MAC 15, 133, 134
management IP 16, 174, 175
servers 15, 171, 172
UUID suffixes 16, 172, 173, 174
WWN 16, 157
WWNN 158, 159
WWPN 159, 160

port channels
adding ports 56, 120
creating 55, 119
deleting 57, 121
disabling 56, 120
enabling 56, 120
removing ports 57, 121

ports
changing 53
disabling 54, 117, 118
enabling 53, 117, 118
Ethernet server port 311
fabric interconnect 51
Fibre Channel port 313
management 42
pin groups 121, 122, 131, 132, 155, 156
pinning server traffic 19
server 51, 52, 116
unconfiguring 54, 117, 118
uplink 51
uplink Ethernet 52, 116, 310

POST
viewing for chassis 251
viewing for I/O modules 266
viewing for server 263

Power on Self-Test
viewing for chassis 251
viewing for I/O modules 266
viewing for server 263

PowerCycling servers 255

primary authentication
about 69
LDAP provider 70, 75
RADIUS provider 72, 75
remote 69
selecting 75
TACACS provider 73, 75

privileges
about 83
adding 86
removing 86

profiles 6

properties
session 35

provider
LDAP 70, 75
RADIUS 72, 75
TACACS 73, 75

PXE, installing OS 239

Q

QoS policies
about 12, 21, 136
creating 138
deleting 139

quality of service
about 20, 135
flow control policies 21, 136

policies 12, 21, 136, 138, 139

system classes 20, 124, 135, 137

R

RADIUS 69

RADIUS provider
creating 72
deleting 75

recognizing
server slots 258
servers 256

rebooting server 255

recommissioning, chassis 248

Reconnection Interval 35

recovering admin password 299, 300, 301
registration, Smart Call Home 283
remote authentication
user accounts 70
user roles 70

removing
chassis 248
ports from a port channel 57
ports from port channel 121
server from chassis 257
server from configuration 258

replacing configuration 286
resetting
BMC 261
resetting (continued)
CMOS 261
IOM 265
resetting server, hard 255
resolution, name 111
restoring
about 286
configuration 293
import operations 290
user role 286
role-based access control 81
roles
about 82
adding privileges 86
backing up 286
creating 85
deleting 86
privileges 83
removing privileges 86
root organization 79
running
backup operation 288
import operation 291

S
SAN
named VSANs
creating 151
deleting 152
pin groups 155, 156
vHBA policy 13, 161
VSANs 151
SAN pin groups
creating 155
deleting 156
scalability 4
scrub policy
about 14, 185
creating 186
deleting 140, 186
selecting primary authentication 75
serial over LAN policy
about 14, 187
creating 187
deleting 188
server autoconfiguration policy
about 12, 188
creating 188
deleting 189
server discovery policy
about 12, 190
server discovery policy (continued)
creating 190
deleting 191
server inheritance policy
about 12, 191
creating 191
deleting 192
server management 253
server pool policy
about 12, 192
creating 193
deleting 194
server pool policy qualification
about 13, 194
server pool policy qualifications
creating 194
deleting 197
deleting qualifications 197
server pools
associating service profile 232
creating 171
deleting 172
disassociating service profile 233
server ports
about 51
configuring
Equipment tab 52
LAN Uplink Manager 116
disabling 117
enabling 117
unconfiguring 117
server virtualization 4
servers
acknowledging 256
associating with service profiles 232
boot policies 9, 177, 179, 180
booting 254
changing UUID 233
cloning service profiles 232
configuration 6
creating service profile templates 217, 218
creating service profiles 201, 214
decommissioning 257
default service profiles 217
disassociating from service profiles 233
discovery policy 12, 190, 191
DNS 111, 112
hard reset 255
inheritance policy 12, 191
IPMI profiles 11, 181, 182, 183
KVM Console 260
local disk configuration 11, 183, 184, 185
locator LED
turning off 259
servers (continued)
  locator LED (continued)
    turning on 259
  management 253
  monitoring 262
  multi-tenancy 22
  pinning 19
  pool policy 12, 192, 193, 194
  pool qualifications 13, 194, 197
  pools 15, 171, 172
  POST results 263
  power cycling 255
  reacknowledging slots 258
  removing
    from chassis 257
    from database 258
  resetting
    BMC 261
    CMOS 261
  service profiles 6, 7, 199, 235
  service profiles from templates 230
  shutting down 255
  stateless 21
  statistics threshold policies 306, 308, 310
service profile template wizard
  opening 217
    page 1, identity 218
    page 2, storage 219
    page 3, networking 223
    page 4, server boot order 226
    page 5, server assignment 228
    page 6, policies 229
service profile templates
  binding service profiles 235
  changing UUID 231
  creating 217, 218, 219, 223, 226, 228, 229
    identity 218
    networking 223
    policies 229
    server assignment 228
    server boot order 226
    storage 219
  unbinding service profiles 236
service profile wizard
  opening 201
    page 1, identity 201
    page 2, storage 203
    page 3, networking 207
    page 4, server boot order 209
    page 5, server assignment 211
    page 6, policies 213
service profiles
  about 6
  associating 232
service profiles (continued)
  binding to template 235
  changing UUID 233
  cloning 232
  configuration 6
  creating default 217
  creating from template 230
  creating with inherited values 214
  creating with wizard 201, 203, 207, 209, 211, 213
    identity 201
    networking 207
    policies 213
    server assignment 211
    server boot order 209
  storage 203
  disassociating 233
  firmware updates 97
  inherited values 8, 200
  network connectivity 6
  override identity 7, 199
  servers
    booting 254
    KVM Console 260
    shutting down 255
  templates 8, 200
  unbinding from template 236
session properties 36
  sessions, users 91
  setting
    session properties 35
    switching mode 49, 116
setting up
  primary fabric interconnect 44
  subordinate fabric interconnect 46
setup mode 42
shutdown, graceful 255
shutting down servers 255
silver priority system class 20, 124, 136, 137
Smart Call Home
  about 270
  Cisco TAC-1 profile 281
  configuring 279
  considerations 270
  registering 283
  system inventory messages 282
SNMP
  enabling 65
  SNMPv3 users 66
  trap hosts 65
  SNMPv3 users, configuring 66
  software 93
  SSH, configuring 36
  stages, firmware updates 96, 98
  standalone configuration 42
Index

unified fabric (continued)
  Fibre Channel 5
unsupported tasks 28
updating
  firmware 94, 96, 98
  firmware order 96
  firmware, direct 95
  firmware, service profiles 97
  host firmware policy 107
  management firmware policy 108
updating firmware 101, 102, 103, 104, 105, 106
updating templates 8, 200
upgrading firmware
  activating 101
  adapters 102
  BMC 103
  downloading images 99
  fabric interconnects 105
  IOM 104
  obtaining images 99
  UCS Manager 106
  updating 101
uplink Ethernet ports
  configuring
    Equipment tab 52
    LAN Uplink Manager 116
  disabling 118
  enabling 118
  unconfiguring 118
uplink port channels
  adding ports 56, 120
  creating 55, 119
  deleting 57, 121
  disabling 56, 120
  enabling 56, 120
  removing ports 57, 121
uplink ports
  about 51
  Ethernet 52
  flow control policies 21, 136
  pin groups 121, 122, 131, 132, 155, 156
    creating 121, 131
    deleting 122, 132
uplinks, Manager for LAN 33
user accounts
  about 81
  creating 89
  deleting 91
user roles
  about 82
  adding privileges 86
  creating 85
  deleting 86
  privileges 83
user roles (continued)
  removing privileges 86
users
  access control 81
  accounts 81
  adding privileges 86
  authentication 69
  creating accounts 89
  creating roles 85
  deleting local accounts 91
  deleting roles 86
  locales
    about 85
    adding organizations 88
    creating 87
    deleting 88
    deleting organizations 88
  monitoring sessions 91
  privileges 83
  recovering admin password 299, 300, 301
  remote authentication 70
  removing privileges 86
  roles 82
  SNMPv3 66
UUID
  changing 233
  changing in service profile template 231
UUID suffix pools
  about 16, 172
  creating 173
  deleting 174
V
  verifying firmware 109
vHBA SAN Connectivity policies
  about 13, 161
  binding vHBAs 163
  creating 161
  deleting 163
  unbinding vHBAs 164
vHBA templates
  about 13, 161
  binding vHBAs 163
  creating 161
  deleting 163
  unbinding vHBAs 164
vHBAs
  binding to vHBA template 163
  unbinding from vHBA template 164
VIF status 262
virtual lanes 20, 135
virtualization
  about 23
  Cisco UCS 82598KR-CI 23
  Cisco UCS CNA M71KR 23

VLANs
  named
    about 127
    creating 122, 127
    deleting 123, 129

VMware 23
vNIC
  policy 13, 141
vNIC LAN Connectivity policies
  about 13, 141
  binding vNICs 143
  creating 141
  deleting 143
  unbinding vNICs 144

vNIC templates
  about 13, 141
  binding vNICs 143
  creating 141
  deleting 143
  unbinding vNICs 144

vNICs
  binding to vNIC template 143
  unbinding from vNIC template 144

VSANs
  creating 151
  deleting 152
  named 151

W
  Work pane 31

WWN
  creating WWNN pools 158
  creating WWPN pools 159
  deleting WWNN pools 159
  deleting WWPN pools 160

WWN pools
  about 16, 157
  creating WWNN 158
  creating WWPN 159
  deleting WWNN 159
  deleting WWPN 160

WWNN 16, 157, 158, 159

WWPN 16, 158, 159, 160