Cisco UCS Director Management Guide for Cisco UCS Manager, Release 6.5

First Published: 2017-07-11

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

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

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Preface xiii

Audience xiii

Conventions xiii

Related Documentation xv

Documentation Feedback xv

Obtaining Documentation and Submitting a Service Request xv

CHAPTER 1

New and Changed Information for this Release 1

New and Changed Information for This Release 1

CHAPTER 2

Overview 3

Cisco UCS Management through Cisco UCS Director 3

Management of Cisco UCS Mini 3

Cisco UCS Management Tasks You Can Perform in Cisco UCS Director 4

Cisco UCS Management Tasks You Cannot Perform in Cisco UCS Director 4

Cisco UCS Manager Orchestration Tasks 5

CHAPTER 3

Configuring Cisco UCS Manager Accounts 7

Pods 7

Adding a Pod 8

Cisco UCS Manager Accounts 9

Adding a Cisco UCS Manager Account 9

Testing the Connection to a Physical Account 11

Verifying the Discovery of a Cisco UCS Manager Account 12

Viewing the Topology and Connectivity of Devices in a Cisco UCS Domain 13

Exporting the Configuration of a Cisco UCS Manager Account 13

Importing the Configuration of a Cisco UCS Manager Account 14

Selective Server Management 15
Guidelines and Limitations for Selective Server Management 15
Selecting a Server for Management 16
Unmanaging a Server 16
Registration of a Cisco UCS Manager Account with Cisco UCS Central 17
Prerequisites for Cisco UCS Central 17
Registering a Cisco UCS Manager Account with Cisco UCS Central 17
Unregistering a Cisco UCS Manager Account from Cisco UCS Central 18
Making a Policy, Service Profile, or Service Profile Template Global 18
Making a Policy, Service Profile, or Service Profile Template Local 19
Organizations 20
Organizations in a Multitenancy Environment 20
Creating an Organization 20
Locales 21
Creating a Locale 21
Time Zones 22
Adding a Time Zone 22
Cloning a Policy 22
Deleting a Pool, Policy, or Other Object 23

CHAPTER 4 **Configuring Fabric Interconnects and Ports** 25
Configuring the Fabric Interconnect Switching Mode 25
Ethernet Switching Mode 25
Changing the Ethernet Switching Mode 26
Fibre Channel Switching Mode 26
Changing Fibre Channel Switching Mode 27
Configuring Ports 28
Ports on the Cisco UCS 6100 Series Fabric Interconnect 28
Port on the Cisco UCS 6200 Series Fabric Interconnect 29
Port Modes 29
Port Types 29
Configuring the Port Mode for Fixed Module Ports 30
Configuring the Port Mode for Expansion Module Ports 30
Enabling a Port 31
Disabling a Port 31

Configuring Ethernet Ports 32
Configuring a Server Port 32
Configuring an Uplink Port 32
Configuring an FCoE Uplink Port 33
Configuring an FCoE Storage Port 33
Configuring an Appliance Port 34
Unconfiguring an Ethernet Port 36
Configuring Fibre Channel Ports 36
Configuring a Fibre Channel Storage Port 36
Configuring a Fibre Channel Uplink Port 37
Associating a Fibre Channel Port with a VSAN 37
Configuring Cisco UCS Mini Ports 37
Cisco UCS Mini Scalability Ports 37
Configuring a Scalability Port as a Server Port 38
Configuring a Scalability Port as an Uplink Port 38
Configuring a Scalability Port as an Uplink FCoE Port 39
Configuring a Scalability Port as a Storage FCoE Port 39
Configuring a Scalability Port as an Appliance Port 40
Configuring a Fibre Channel Port as an FCoE Uplink Port 40
Configuring a Fibre Channel Port as an FCoE Storage Port 41
Configuring Port Channels 41
LAN Port Channel 41
Creating a LAN Port Channel 42
SAN Port Channel 42
Creating a SAN Port Channel 43
Appliance Port Channel 43
Creating an Appliance Port Channel 44
FCoE Port Channel 45
Creating an FCoE Port Channel 45
Enabling a Port Channel 46
Disabling a Port Channel 46

CHAPTER 5 **Configuring Network Connections** 47
VLANs 47
Creating a VLAN 48

VLAN Port Count Optimization 50
Enabling VLAN Port Count Optimization 50
Viewing VLAN Optimization Sets 50
Disabling VLAN Port Count Optimization 51
VLAN Permissions 51
Enabling VLAN Permissions 52
Modifying Permissions on a VLAN 52
Disabling VLAN Permissions 52
VLAN Groups 53
Creating a VLAN Group 53
Modifying the VLAN Permissions for a VLAN Group 54
MAC Pools 54
Creating a MAC Pool 55
Adding a Block of Addresses to a MAC Pool 55
Configuring Quality of Service 56
Quality of Service 56
System Classes 57
Quality of Service Policy 58
Flow Control Policy 58
Changing QoS System Classes 58
Enabling a QoS System Class 60
Disabling a QoS System Class 61
Creating a QoS Policy 61
Creating a Flow Control Policy 64
vNICs 65
vNIC Template 65
Creating a vNIC Template 65
Creating a vNIC 69
LAN Connectivity Policy 69
Creating a LAN Connectivity Policy 70
Network Control Policy 70
Creating a Network Control Policy 71
Network Policy 73
Creating a Network Policy 74

CHAPTER 6 Configuring Storage Connections 77

VSANs 77

Creating a VSAN 78

WWN Pools 79

WWNN Pools 79

Creating a WWNN Pool 80

Adding an Initiator to a WWNN Pool 80

WWPN Pools 81

Creating a WWPN Pool 81

Adding an Initiator to a WWPN Pool 82

Adding a WWN Block 82

vHBAs 83

vHBA Template 83

Creating a vHBA Template 83

Creating a vHBA 85

Fibre Channel Adapter Policy 85

Creating a Fibre Channel Adapter Policy 86

SAN Connectivity Policy 90

Creating a SAN Connectivity Policy 91

Storage Policy 91

Creating a Storage Policy 92

Fibre Channel Zoning 93

Support for Fibre Channel Zoning in Cisco UCS 93

Storage Connection Policy 94

Configuring Fibre Channel Zoning in Cisco UCS 94

Configuring a VSAN for Fibre Channel Zoning 96

Creating a Storage Connection Policy 96

Viewing Fibre Channel Zones 97

CHAPTER 7 Configuring Cisco UCS Server Pools and Policies 99

Global Equipment Policies 99

Chassis/FEX Discovery Policy 99

Configuring the Chassis/FEX Discovery Policy 100

Rack Server Discovery Policy 100

Configuring the Rack Server Discovery Policy 101
Rack Management Connection Policy 101
Configuring the Rack Management Connection Policy 101
UUID Pools 102
Creating a UUID Pool 102
Adding an Address Block to a UUID Pool 103
Server Pools 103
Creating a Server Pool 104
Assigning a Server Pool to a Cisco UCS Director Group 104
Unassigning a Server Pool from a Cisco UCS Director Group 105
Management IP Pool 105
Adding an IP Address Block to the Management IP Pool 105
Boot Policy 106
UEFI Boot Mode 107
UEFI Secure Boot 108
UEFI Boot Parameters 108
SAN Boot 109
Creating a SAN Boot Policy 109
LAN Boot 111
Creating a LAN Boot Policy 112
Local Disk Boot 114
Creating a Local Disk Boot Policy 114
Virtual Media Boot 115
Creating a Virtual Media Boot Policy 116
Creating a vMedia Policy and vMount 117
iSCSI Boot 119
Prerequisites for iSCSI Boot 119
Configuring iSCSI Boot 120
Creating an IQN Pool 121
Adding a Block of Addresses to the iSCSI IP Pool 122
Creating an iSCSI Authentication Profile 123
Creating an iSCSI Adapter Policy 124
Example: Creating an iSCSI Boot Workflow 125
Adding a Task: Create Service Profile 126
Adding a Task: Add vNIC to Service Profile 129

Adding a Task: Add iSCSI vNIC to Service Profile 130
Adding a Task: Create Service Profile iSCSI Boot Policy 131
Adding a Task: Associate Service Profile 133
Adding a Task: Create Flexible Volume 135
Adding a Task: Create LUN 136
Adding a Task: Create Initiator Group 138
Adding a Task: Add an Initiator to Initiator Group 139
Adding a Task: Map LUN to Initiator Group 140
Adding a Task: Set Up PXE Boot 141
Adding a Task: Power On UCS Server 143
Adding a Task: Monitor PXE Boot 143
Adding a Task: Power Off UCS Server 144
Adding a Task: Modify Service Profile Boot Policy to Boot from iSCSI 145
Changing the Boot Order in a Boot Policy 147
Local Disk Configuration Policy 147
Guidelines for all Local Disk Configuration Policies 148
Guidelines for Local Disk Configuration Policies Configured for RAID 149
Creating a Local Disk Configuration Policy 150
Maintenance Policy 152
Creating a Maintenance Policy 153
Server Pool Policy Qualification Overview 154
Creating Server Pool Policy Qualifications 155
Server Pool Policy Overview 158
Creating a Server Pool Policy 159
vNIC/vHBA Placement Policies 159
vCon to Adapter Placement 160
vCon to Adapter Placement for N20-B6620-2 and N20-B6625-2 Blade Servers 161
vCon to Adapter Placement for All Other Supported Servers 161
vNIC/vHBA to vCon Assignment 162
Creating a vNIC/vHBA Placement Policy 164
Placement Policy 165
Creating a Placement Policy 166

CHAPTER 8 **Configuring Service Profiles** 169
Service Profiles 169

Service Profile Templates 170
Creating a Service Profile 170
Creating a Service Profile Template 172
Managing Service Profiles 174
Creating a Template from a Service Profile 174
Renaming a Service Profile 175
Cloning a Service Profile 176
Associating a Service Profile with a Server 176
Associating a Service Profile with a Server Pool 177
Disassociating a Service Profile from a Server 177
Assigning a Service Profile to a Cisco UCS Director Group 178
Unassigning a Service Profile from a Cisco UCS Director Group 178
Requesting Inventory Collection for a Service Profile 179
Managing Service Profile Templates 179
Creating a Service Profile from a Template 179
Cloning a Service Profile Template 180
Associating a Service Profile Template with a Server Pool 180
Disassociating a Service Profile Template from a Server Pool 181

CHAPTER 9 **Managing Cisco UCS Servers** 183
Server Management 183
Powering On a Server 184
Powering Off a Server 184
Launching the KVM Console for a Server 184
Accessing a Server Directly using the KVM Console 185
Requesting Inventory Collection for a Server 185
Issuing a Diagnostic Interrupt for a Server 186
Resetting a Server 186
Reacknowledging a Server 186
Decommissioning a Server 187

CHAPTER 10 **Monitoring and Reporting** 189
About Monitoring and Reporting 189
Monitoring a Fabric Interconnect and its Components 191
Monitoring a Chassis and its Components 192

Monitoring a Server and its Components 193
Monitoring a FEX and its Components 194
Viewing the Cisco UCS Manager Pending Activities Report and User Acknowledgement 195
TPM Monitoring 195
Inventory Reports 196
Viewing Storage Profile Management Reports 196
Viewing the Cisco UCS Chassis Inventory Report 196
Viewing the Disk Group Policy Inventory Reports 196
Viewing the Cisco UCS Fabric Interconnect Inventory Report 197
Viewing the Cisco UCS Servers Inventory Report 197
Viewing the Cisco UCS Server Association Report 198
Viewing the vMedia Policy Inventory Report 198
Exporting an Inventory Report 198
Cisco UCS Events 199
Viewing Cisco UCS Events for a Cisco UCS Manager Account 199
Cisco UCS Faults 200
Viewing Cisco UCS Faults for a Pod 200
Viewing Cisco UCS Faults for a Cisco UCS Manager Account 201
Fault Suppression 201
Adding a Fault Suppression Task for a Chassis 202
Adding a Fault Suppression Task for a FEX 203
Adding a Fault Suppression Task for an I/O Module 204
Adding a Fault Suppression Task for a Server 206
Viewing Fault Suppression Tasks 207

Preface

- Audience, page xiii
- Conventions, page xiii
- Related Documentation, page xv
- Documentation Feedback, page xv
- Obtaining Documentation and Submitting a Service Request, page xv

Audience

This guide is intended primarily for data center administrators who use Cisco UCS Director and who have responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security
- Virtualization and virtual machines

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
Document titles	Document titles appear in *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.

Text Type	Indication
System output	Terminal sessions and information that the system displays appear in `this font`.
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

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

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Related Documentation

Cisco UCS Director Documentation Roadmap

For a complete list of Cisco UCS Director documentation, see the *Cisco UCS Director Documentation Roadmap* available at the following URL: http://www.cisco.com/en/US/docs/unified_computing/ucs/ucs-director/doc-roadmap/b_UCSDirectorDocRoadmap.html.

Cisco UCS Documentation Roadmaps

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/c-series-doc.

Note The *Cisco UCS B-Series Servers Documentation Roadmap* includes links to documentation for Cisco UCS Manager and Cisco UCS Central. The *Cisco UCS C-Series Servers Documentation Roadmap* includes links to documentation for Cisco Integrated Management Controller.

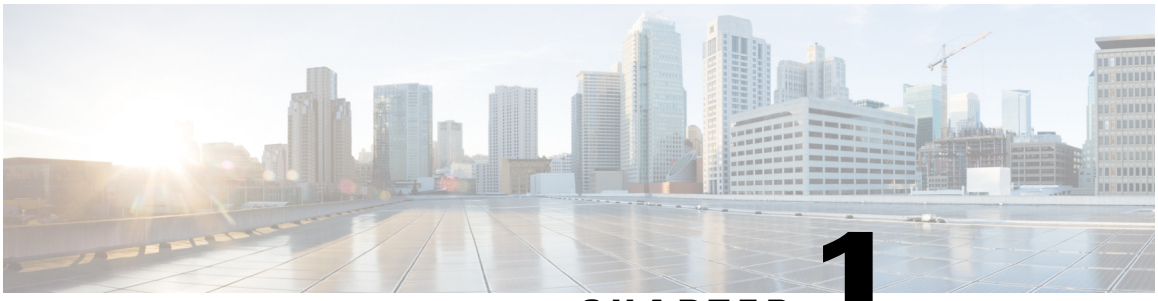
Documentation Feedback

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.



CHAPTER 1

New and Changed Information for this Release

This chapter contains the following sections:

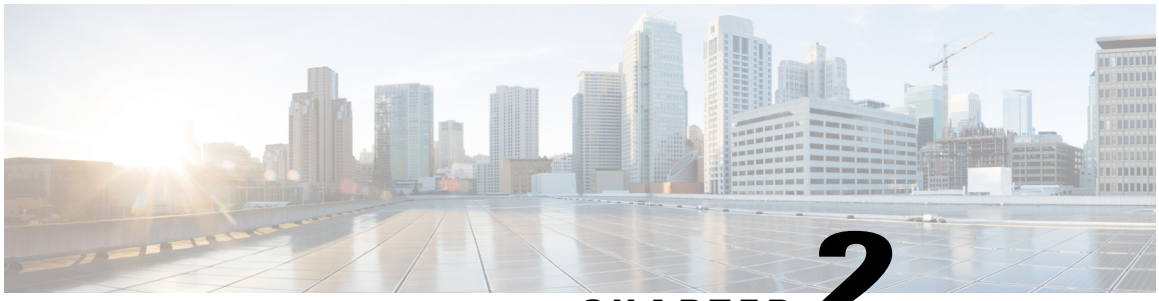
- New and Changed Information for This Release, page 1

New and Changed Information for This Release

The following table provides an overview of the significant changes to this guide for this current release. The table does not provide an exhaustive list of all changes made to this guide or of all new features in this release.

Table 1: New Features and Changed Behavior in Cisco UCS Director, Release 6.5

Feature	Description	Where Documented
Support for more than one Cisco UCS Manager in non-Generic Pods	In addition to the generic pods, more than one Cisco UCS Manager account can be added for other pods, such as FlexPod, Vblock, or VSPEX.	Cisco UCS Manager Accounts, on page 9
Pending Activities Report	This report shows you the Pending Activities that are waiting for user acknowledgement, including service profile, and server information.	Viewing the Cisco UCS Manager Pending Activities Report and User Acknowledgement, on page 195



CHAPTER 2

Overview

This chapter contains the following sections:

- Cisco UCS Management through Cisco UCS Director, page 3
- Cisco UCS Management Tasks You Can Perform in Cisco UCS Director, page 4
- Cisco UCS Management Tasks You Cannot Perform in Cisco UCS Director, page 4
- Cisco UCS Manager Orchestration Tasks, page 5

Cisco UCS Management through Cisco UCS Director

Cisco UCS Director is not a replacement for Cisco UCS Manager. Rather, Cisco UCS Director uses orchestration to automate some of the steps required to configure a Cisco UCS domain. In this way, Cisco UCS Director provides a statistical analysis of the data and a converged view of each pod.

After you add a Cisco UCS domain to Cisco UCS Director as a Cisco UCS Manager account, Cisco UCS Director provides you with complete visibility into the Cisco UCS domain. In addition, you can use Cisco UCS Director to manage and configure that Cisco UCS domain.

Note The features that you can use to manage a Cisco UCS Manager account depend on the Cisco UCS Manager release. Be sure to refer to the Cisco UCS Manager Release Notes for supported features prior to managing the account from Cisco UCS Director.

Management of Cisco UCS Mini

If the Cisco UCS domain in a Cisco UCS Manager account includes Cisco UCS Mini, you can use Cisco UCS Director to manage, configure, orchestrate, monitor, and report on Cisco UCS Mini.

For more information about Cisco UCS Mini, see the Cisco UCS Manager User Guides for Cisco UCS Mini and the Cisco UCS 5108 Server Chassis Installation Guide.

Cisco UCS Management Tasks You Can Perform in Cisco UCS Director

You can use Cisco UCS Director to perform management, monitoring, and reporting tasks for physical and virtual devices within a Cisco UCS domain.

Configuration and Administration

You can create and configure Cisco UCS hardware and software components in Cisco UCS Director, such as:

- Fabric interconnects, including ports
- Chassis, blade servers, and rack-mount servers, including autodiscovery
- I/O modules and fabric extenders (FEXes)
- Network connections
- Storage connections
- Pools
- Policies
- Service profiles

Monitoring and Reporting

You can also use Cisco UCS Director to monitor and report on your Cisco UCS domains and their components, including:

- Power consumption
- Temperature
- Server availability
- Service profile association

Cisco UCS Management Tasks You Cannot Perform in Cisco UCS Director

You cannot use Cisco UCS Director to perform certain system management tasks within a Cisco UCS domain, such as the following:

- Firmware upgrades
- User management
- Virtual machine management

Cisco UCS Manager Orchestration Tasks

Cisco UCS Director includes orchestration features that allow you to automate the configuration and management of tasks performed by Cisco UCS Manager in one or more workflows. The same workflow can include Cisco UCS Manager, network, and storage tasks.

For more information about orchestration in Cisco UCS Director, see the Cisco UCS Director Orchestration Guide.

Location of Orchestration Tasks

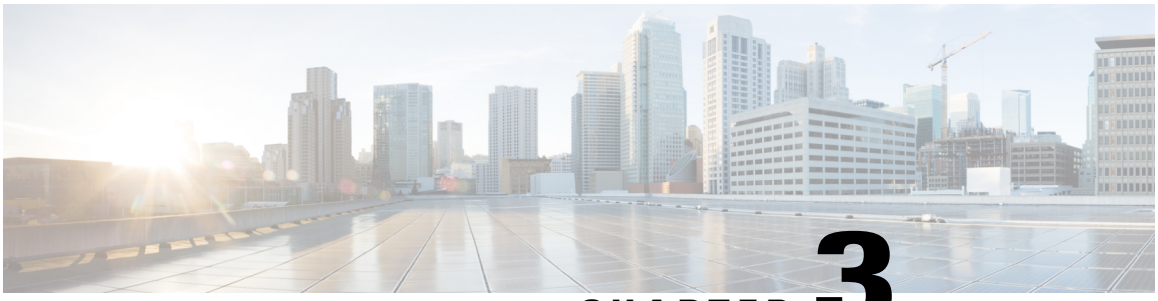
A complete list of the Cisco UCS Manager orchestration tasks is available in Workflow Designer, in the Task Library, and the **Cisco UCS Tasks** folder. The Task Library, which includes a description of the orchestration tasks, can be accessed from the following locations in Cisco UCS Director:

- **Orchestration** > **Workflows**
- `http://IP_address/app/cloudmgr/onlinedocs/cloupiaTaskLib.html` where *IP_address* is the IP address of Cisco UCS Director.

Types of Orchestration Tasks

The Cisco UCS Manager orchestration tasks include tasks to configure and manage the following:

- Servers
- Server boot
- Pools
- Policies
- VLANs
- VSANs
- vNICs
- Service profiles
- Service profile templates
- Organizations



CHAPTER 3

Configuring Cisco UCS Manager Accounts

This chapter contains the following sections:

- Pods, page 7
- Cisco UCS Manager Accounts, page 9
- Selective Server Management, page 15
- Registration of a Cisco UCS Manager Account with Cisco UCS Central, page 17
- Organizations, page 20
- Locales, page 21
- Time Zones, page 22
- Cloning a Policy, page 22
- Deleting a Pool, Policy, or Other Object, page 23

Pods

A pod is a logical grouping of physical and virtual components, including one or more physical or virtual accounts, such as a Cisco UCS Manager account for computing, a network account, or a cloud account. Each pod is a module of network, compute, storage, and application components that work together to deliver services for your data center and users. The pod is a repeatable pattern, and its components maximize the modularity, scalability, and manageability of data centers.

When you create a pod, consider what you want it to represent. For example, you can create a pod to represent the following:

- A single converged infrastructure stack, such as FlexPod, Vblock, or VSPEX
- A grouping of resources assigned to a specific customer or tenant
- The resources within a specific range of IP addresses

For systems that include Cisco UCS Central, we recommend that you create a pod for each Cisco UCS domain or domain group.

If needed, you can group pods into sites. However, a pod can only belong to one site.

You can view details of the pods and their components on the **Converged** tab in Cisco UCS Director. For information about how to create pods, see the Cisco UCS Director Administration Guide.

Adding a Pod

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Pods**.

Step 3 Click **Add**.

Step 4 On the **Add Pod** screen, complete the following fields:

Name	Description
Name field	A descriptive name for the pod.
Type drop-down list	Choose the type of pod that you want to add. This can be one of the following: • **Flexpod** • **VersaStack** • **Generic** • **ExpressPod Medium** • **VSPEX** • **ExpressPod Small** • **Vblock** • **HyperFlex** • **Virtual SAN Pod** The nongeneric pod types accommodate only specific physical and virtual components. A generic pod does not require a specific pod license. You can add any type of physical or virtual component to a generic pod. For more information about bundled pod licenses (FlexPod, Vblock, and VSPEX), which include the necessary individual device licenses to run a pod, see the Cisco UCS Director Installation and Upgrade Guides. **Note** Only VersaStack and Generic pods are supported in the IBM accounts in Cisco UCS Director.
Site drop-down list	Choose the site where you want to add the pod. If your environment does not include sites, you can omit this step.
Description field	(Optional) A description of the pod.

Name	Description
Address field	The physical location of the pod. For example, this field could include the city or other internal identification used for the pod.
Hide Pod check box	Check to hide the pod if you do not want it to show in the Converged Check View. You can continue to add or delete accounts from the pod. For example, you can use this check box to ensure that a pod that does not have any physical or virtual elements is not displayed in the Converged View.

Step 5 Click **Add**.

What to Do Next

Add one or more accounts to the pod.

Cisco UCS Manager Accounts

Each Cisco UCS Manager account represents a single Cisco UCS domain that you want to have managed by Cisco UCS Director.

For an environment that does not include Cisco UCS Central, you create Cisco UCS Manager accounts in a pod. You can have more than one Cisco UCS Manager account for a pod.

For an environment that includes Cisco UCS Central, you must create a Cisco UCS Central account under multi-domain managers. All Cisco UCS domains that are registered with that Cisco UCS Central, and their related Cisco UCS Manager accounts are brought into Cisco UCS Director when the Cisco UCS Central account is created. You can assign one or more of those Cisco UCS Manager accounts from the Cisco UCS Central account to a pod if needed. You can also register a Cisco UCS Manager account with a Cisco UCS Central account.

Adding a Cisco UCS Manager Account

Before You Begin

Add the pod to which this Cisco UCS Manager account belongs.

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 Click **Physical Accounts**.

Step 3 Click **Add**.

Step 4 On **Add Account** screen, do the following:

a) From the **Pod** drop-down list, choose the pod to which this account belongs.
b) From the **Category Type** drop-down list, choose **Computing**.
c) From the **Account Type** drop-down list, choose **UCSM**.
d) Click **Submit**.

Step 5 On the **Add Account** screen, complete the following fields:

Name	Description
Authentication Type drop-down list	Choose the type of authentication to be used for this account. This can be one of the following: • **Locally Authenticated—**A locally authenticated user account is authenticated directly through the fabric interconnect and can be enabled or disabled by anyone with admin or AAA privileges. • **Remotely Authenticated—**A remotely authenticated user account is any user account that is authenticated through LDAP, RADIUS, or TACACS+.
Server Management drop-down list	Choose how you want to have the servers in this account managed. This can be one of the following: • **All Servers—**All servers are managed. This option is the default. If you choose this option, all servers are added in the Managed state. • **Selected Servers—**Only selected servers are managed. You can add and remove servers from the managed server list as needed. If you choose this option, all servers are added in the Unmanaged state.
Account Name field	A unique name that you assign to this account.
Server Address field	The IP address of Cisco UCS Manager. For a cluster configuration, this is the virtual IP address.
Use Credential Policy check box	Check this check box if you want to use a credential policy for this account rather than enter the information manually.
Credential Policy drop-down list	If you checked the **Use Credential Policy** check box, choose the credential policy that you want to use from this drop-down list. This field is only displayed if you choose to use a credential policy.
User ID field	The username that this account will use to access Cisco UCS Manager. This username must be a valid account in Cisco UCS Manager. This field is not displayed if you choose to use a credential policy.

Name	Description
Password field	The password associated with the username. This field is not displayed if you choose to use a credential policy.
UCS Authentication Domain field	The authentication domain for the remotely authenticated account. This field is not displayed if you are using a locally authenticated account or if you choose to use a credential policy.
Transport Type drop-down list	Choose the transport type that you want to use for this account. This can be one of the following: • **http** • **https** This field is not displayed if you choose to use a credential policy.
Port field	The port used to access Cisco UCS Manager. This field is not displayed if you choose to use a credential policy.
Description field	(Optional) A description of this account.
Contact Email field	The email address that you can use to contact the administrator or other person responsible for this account.
Location field	The location of this account.
Service Provider field	(Optional) The name of the service provider associated with this account, if any.

Step 6 Click **Add**.

Cisco UCS Director tests the connection to Cisco UCS Manager. If that test is successful, it adds the Cisco UCS Manager account and discovers all infrastructure elements in Cisco UCS Manager that are associated with that account, including chassis, servers, fabric interconnects, service profiles, and pools. This discovery process and inventory collection cycle takes approximately five minutes to complete.

The polling interval configured on the **Administration** > **System** > **System Tasks** tab specifies the frequency of inventory collection.

Testing the Connection to a Physical Account

You can test the connection at any time after you add an account to a pod.

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.

Step 3 On the **Multi-Domain Managers** screen, click the row of the account for which you want to test the connection.

Step 4 Click **Test Connection**.

Step 5 When the connection test has completed, click **Close**.

What to Do Next

If the connection fails, verify the configuration of the account, including the username and password. If the username and password are correct, determine whether there is a network connectivity problem.

Verifying the Discovery of a Cisco UCS Manager Account

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, choose the pod.

Step 3 On **Compute** page, choose the pod that includes the Cisco UCS Manager account that you want to verify.

Note The left column tree structure lists nodes for **Sites**, **Unassigned Pods**, and **Multi-Domain Managers**. When a Sites node is expanded, all the pods for that site node are displayed. When you expand an **Unassigned Pods** node, all the pods that are not assigned to any site are displayed. When you expand the Multi-Domain Managers list, all multi-domain manager account types that you added to Cisco UCS Director are displayed.

Step 4 Click **Compute Accounts**.

Step 5 Choose the row of the account that you want to verify.

Step 6 Click **View Details**.

Cisco UCS Director displays a set of tabs that contain information about the components of that account that it has discovered.

Viewing the Topology and Connectivity of Devices in a Cisco UCS Domain

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account for which you want to view the topology.

Step 3 Click **Compute Accounts**.

Step 4 Click the row of the account.

Step 5 Click **View Connectivity**.
The **Topology View - UCS Device Connectivity** dialog box is displayed with a view of the topology and connectivity of the devices in the Cisco UCS Domain.

Step 6 If desired, you can modify the following view options:

- **View Mode** drop-down list—Adjusts the spacing and positioning of the devices. The mode determines which options are available for you to customize the topology view. You can choose between the following view modes:
  - **Hierarchical**
  - **Concentric**
  - **Circular**
  - **Force Directed**
- **Show Link Labels** check box—Shows or hides labels on the links between devices. These labels might not display on some view modes.
- **Allow Item Spacing** check box—Increases the distance between devices for the Hierarchical view mode.
- **Distance** control—Adjusts the distance between devices for the Concentric view mode.
- **Radius** control—Changes the radius of the circle and therefore adjusts the distance between devices for the Circular view mode.
- **Rigidity** control—Adjusts the rigidity for the Force Directed view.
- **Force Distance** control—Adjusts the distance between devices for the Force Directed view.

Step 7 Click **Close** to return to the **Compute Accounts** tab.

Exporting the Configuration of a Cisco UCS Manager Account

Cisco UCS Director exports a file named `Ucs-`*`Timestamp`*`-configuration.zip` to the location configured for downloads in your browser.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account for which you want to export the configuration.

Step 3 Click **Compute Accounts**.

Step 4 Click the row of the account.

Step 5 From the **More Actions** drop-down menu, choose **Export Configuration**.

Step 6 On the **Export UCS Configuration** screen, click **Submit**.

Step 7 When the configuration export is complete, click **Close**.

Importing the Configuration of a Cisco UCS Manager Account

You can import a configuration that has been exported from a Cisco UCS Manager account in Cisco UCS Director or from Cisco UCS Manager.

Note When you import a configuration into a Cisco UCS Manager account, you overwrite any existing configuration in that account.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account for which you want to export the configuration.

Step 3 Click **Compute Accounts**.

Step 4 Click the row of the account.

Step 5 Click **Import Configuration**.

Step 6 On the **Upload Configuration** screen, do the following:

a) Click **Select a File** and navigate to the configuration file that you want to import.

b) When the file upload is complete, click **Ok**.

c) Click **Next**.

Step 7 On the **Select Configuration** screen, check one of the following check boxes:

Option	Description
Import All Configuration	Imports all configuration settings in the file.

Option	Description
Customize Import	Imports only the configuration settings that you choose.

Step 8 Click **Submit**.

Step 9 When the configuration import is complete, click **Close**.

Selective Server Management

When you add a Cisco UCS Manager account to a pod, you can choose how you want Cisco UCS Director to manage the servers for that account. You can choose one of the following:

All Servers

All servers are managed by Cisco UCS Director. This option is the default.

Selected Servers

Only selected servers are managed by Cisco UCS Director. You can add and remove servers from the managed server list as needed.

Note Server license usage includes servers in Managed, Transition, and Decommissioned states. It does not include unmanaged servers.

Guidelines and Limitations for Selective Server Management

When you configure selective server management be aware of the following guidelines and limitations.

Changes to the Server Management Option

If you change the server management setting for an existing Cisco UCS Manager account from **All Servers** to **Selected Servers**, Cisco UCS Director moves all servers to the Unmanaged state. Initially, the servers are moved to a Transition state and removed from the servers report. Unless you select one or more servers and manually move them to the Managed state, all servers remain in that Transition state for 48 hours before Cisco UCS Director completes the move to the Unmanaged state. While a server is in Transition state, it is counted in your license usage.

If you change the server management setting for an existing Cisco UCS Manager account from **Selected Servers** to **All Servers**, Cisco UCS Director moves all servers to the Managed state.

Server Pools

Cisco UCS Director displays only the managed servers in a server pool, but the size of the pool includes all servers. For example, if a server pool contains two servers and only one server is managed by Cisco UCS

Director, all server pool reports and actions on that pool display only one (managed) server. However, the pool size is displayed as two.

Service Profiles

Cisco UCS Director does not display service profiles that are associated with unmanaged servers. Service profiles are displayed only when the server is managed by Cisco UCS Director.

If you use Cisco UCS Manager to associate a service profile with a server pool that has servers that are not managed by Cisco UCS Director, you cannot perform any further tasks on that service profile or server in Cisco UCS Director. To manage that server or service profile, you must add a Manage Server task to the appropriate orchestration workflows.

Selecting a Server for Management

Before You Begin

Configure the selective server management setting for the Cisco UCS Manager account as **Selected Servers** to be able to choose which servers you want Cisco UCS Director to manage.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **UCS Discovered Servers**.
This screen displays all servers in the Cisco UCS domain discovered Cisco UCS Manager.

Step 4 Click **Manage Servers**.

Step 5 On the **Manage Servers** screen, do the following:

a) Check the check boxes for those servers you want to have managed.

b) Click **Submit**.

Cisco UCS Director moves the selected servers to the Managed state.

Unmanaging a Server

If you have configured the server management option in a Cisco UCS Manager account for **Selected Servers**, you can unmanage servers that you no longer want to manage through Cisco UCS Director.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **UCS Discovered Servers**.
This screen displays all servers in the Cisco UCS domain discovered by Cisco UCS Manager.

Step 4 Click **Unmanage Servers**.

Step 5 In the **Unmanage Servers** dialog box, do the following:

a) Uncheck the check boxes for those servers you no longer want to have managed.

b) Click **Submit**.

Cisco UCS Director moves the selected servers to the Transition state and removes them from the servers report. The servers remain in that Transition state for 48 hours before Cisco UCS Director completes the move to the Unmanaged state. While a server is in Transition state, it is counted in your license usage.

Registration of a Cisco UCS Manager Account with Cisco UCS Central

When you add a Cisco UCS Central account, Cisco UCS Director can use that account to manage all registered Cisco UCS domains. You can also use Cisco UCS Director to register a Cisco UCS Manager account with a Cisco UCS Central account.

You can also choose whether you want to create and manage policies, service profiles, and service profile templates through the Cisco UCS Central account or the Cisco UCS Manager account by designating them as one of the following:

- **Local—**The policy, service profile, or service profile template is created and managed through a Cisco UCS Manager account.
- **Global—**The policy, service profile, or service profile template is created and managed through a Cisco UCS Central account.

Prerequisites for Cisco UCS Central

Before you register a Cisco UCS Manager account with a Cisco UCS Central account, do the following:

- Configure an NTP server and the correct time zone in Cisco UCS Director, Cisco UCS Manager, and Cisco UCS Central to ensure that they are in sync. If the time and date in one or more of them are out of sync, the registration with Cisco UCS Central may fail.
- Obtain the hostname or IP address of a Cisco UCS Central account in Cisco UCS Director.
- Obtain the shared secret that you configured when you deployed Cisco UCS Central.

Registering a Cisco UCS Manager Account with Cisco UCS Central

Before You Begin

- Add at least one Cisco UCS Central account.
- Complete the prerequisites for Cisco UCS Central.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Summary**.

Step 4 Click **Register with UCS Central**.

Step 5 On the **Register with UCS Central** screen, do the following:

a) In the **UCS Central Hostname/IP Address** field, enter the hostname or IP address of the Cisco UCS Central account.

Note If you use a hostname rather than an IP address, configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to local, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to global, configure a DNS server in Cisco UCS Central.

b) In the **Shared Secret** field, enter the shared secret (or password) for the Cisco UCS Central account.

c) Click **Submit**.

Unregistering a Cisco UCS Manager Account from Cisco UCS Central

When you unregister a Cisco UCS Manager account from Cisco UCS Central, the Cisco UCS Manager account no longer receives updates to global policies.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Summary**.

Step 4 Click the drop-down menu button and choose **Unregister from UCS Central**.

Step 5 In the **Unregister from UCS Central** dialog box, click **Submit**.

Making a Policy, Service Profile, or Service Profile Template Global

Configure a policy, service profile, or service profile template as global through the Cisco UCS Manager account.

Before You Begin

Register the Cisco UCS Manager account with the Cisco UCS Central account.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Navigate to where the policy is located.

- For a service profile, click **Service Profiles**.
- For a service profile template or a policy such as a vHBA template, click **Organizations**, click **View Details**, and then click the organization that includes the template or policy.

Step 4 Click the row for the policy, service profile, or service profile template that you want to make global.

Step 5 From the **More Actions** drop-down menu, choose **Use Global**.
For some service profiles or policies, click the drop-down menu button and choose **Use Global** from the menu.

Step 6 On the **Use Global** screen, click **Submit**.

Making a Policy, Service Profile, or Service Profile Template Local

Configure a policy, service profile, or service profile template as local through the Cisco UCS Manager account.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click Service profile, or Organization.

- For a service profile, click **Service Profiles**.
- For a service profile template or a policy such as a vHBA template, click the **Organizations** tab, click **View Details**, and then click the organization that includes the template or policy.

Step 4 Click the row in the table for the policy, service profile, or service profile template that you want to make local.

Step 5 From the **More Actions** drop-down menu, choose **Use Local**.
For some service profiles or policies, click the drop-down menu button and choose **Use Local** from the menu.

Step 6 In the **Use Local** dialog box, click **Submit**.

Organizations

Organizations in a Multitenancy Environment

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

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

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

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

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

The root organization is always the top level organization.

Creating an Organization

You can create a top-level organization which is the root. The policies and pools created in this root are system-wide and are available to all organizations in the system.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click **Add**.

Step 5 On the **Add Organization** screen, complete the following fields:

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

b) In the **Description** field, enter a description for the organization.

The **UCS Account Name** field is pre-populated with the name of the Cisco UCS Manager account that you are adding the Organization for.

c) From the **Parent Organization** drop-down list, choose the organization under which this organization will reside.

Step 6 Click **Submit**.

Locales

Each locale defines one or more organizations to which a user is allowed access, and access would be limited to the organizations specified in the locale. One exception to this rule is a locale without any organizations, which gives unrestricted access to system resources in all organizations.

A Cisco UCS domain can contain up to 48 locales. Any locales configured after the first 48 are accepted, but will be inactive with faults raised.

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. A locale that contains the Engineering organization has access to the resources for both the Software Engineering and Hardware Engineering organizations.

Creating a Locale

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Locales**.

Step 4 Click **Add**.

Step 5 On the **Add Locale** screen, complete the following fields:

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

b) In the **Description** field, enter a description for the Locale.
The **UCS Account Name** field is pre-populated with the name of the Cisco UCS Manager account you are working on.

c) In the **Organizations** field, select the chek box for the organizations that you want to add to the locale.

Step 6 Click **Submit**.

Time Zones

Cisco UCS requires a domain-specific time zone setting and an NTP server to ensure the correct time displays in Cisco UCS Manager. If you do not configure time zones, the time might not display correctly.

In addition, if your environment includes Cisco UCS Central, you must configure an NTP server and the correct time zone in Cisco UCS Manager and Cisco UCS Central to ensure that they are in sync. If the time and date in the Cisco UCS domain and Cisco UCS Central are out of sync, the registration might fail.

Adding a Time Zone

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Time Zone**.

Step 4 Click **Add**.

Step 5 On the **Add Time Zone** screen, do the following:

a) In the **NTP Server Name** field, enter the IP address or hostname of the NTP server for this time zone.

b) Click **Submit**.

Cloning a Policy

You can clone some policies and create a copy with the same settings as the original policy.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Navigate to where the policy is located.
For example, if you want to clone a boot policy, click **Organizations**, click the organization in which you want to clone a policy, and then click **View Details**.

Step 4 Click the tab for the type of policy that you want to clone.
For example, if you want to clone a boot policy, click **Boot Policies**.

Step 5 Choose the policy that you want to clone and from **More Actions** drop-down menu, choose **Clone**.

Step 6 Change the name of the policy and, if desired, the values of the other fields.

Step 7 Click **Submit**.

Deleting a Pool, Policy, or Other Object

The method you use to delete a pool, policy, or other object, such as a VLAN, is the same for all objects.

Note Before you delete an object, ensure that it is not used or referenced by another object in the system. For example, before you delete a network policy, ensure that a service profile does not reference that policy.

Procedure

Step 1 Choose **Physical** > **Compute**.

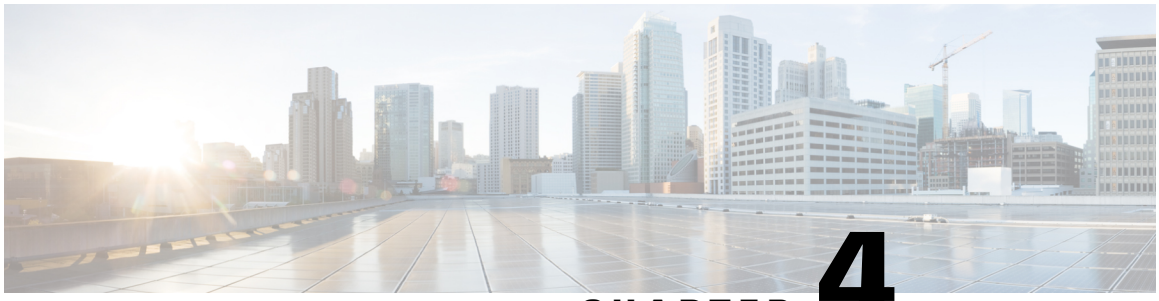
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Navigate to where the object is located.
For example, if you want to delete a VLAN, click **VLANs**.

Step 4 Choose the object that you want to delete.

Step 5 From **More Actions** drop-down menu, choose **Delete**.

Step 6 Click **Delete**.



CHAPTER 4

Configuring Fabric Interconnects and Ports

This chapter contains the following sections:

- Configuring the Fabric Interconnect Switching Mode, page 25
- Configuring Ports, page 28
- Configuring Port Channels, page 41

Configuring the Fabric Interconnect Switching Mode

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 servers (hosts) connected to it through vNICs. This behavior is achieved by pinning (either dynamically pinned or hard pinned) vNICs to uplink ports, which provides redundancy to the network, and makes the uplink ports appear as server ports to the rest of the fabric. In end-host mode, the fabric interconnect does not run the Spanning Tree Protocol (STP) but it 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 Layer 2 aggregation
- Virtual Switching System (VSS) aggregation layer

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

Switch Mode

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

- Layer 3 aggregation
- VLAN in a box

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

Changing the Ethernet Switching Mode

Note When you change the Ethernet switching mode, Cisco UCS Director issues a request to Cisco UCS Manager to restart the fabric interconnect. For a cluster configuration, Cisco UCS Director issues a request to restart both fabric interconnects sequentially. The second fabric interconnect can take several minutes to complete the change in Ethernet switching mode and become system-ready. The configuration is retained.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Fabric Interconnects**.

Step 4 Click the row for the fabric interconnect for which you want to change the switching mode.

Step 5 Click **Ethernet Mode**.

Step 6 On the **Fabric Interconnect Mode Settings** screen, enter a reason for the change in the **Reason** field and click **Change Mode**.
Cisco UCS Director issues the request to restart the fabric interconnect.

Fibre Channel Switching Mode

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

End-Host Mode

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

End-host mode is synonymous with N Port Virtualization (NPV) mode. This mode is the default Fibre Channel Switching mode.

Note When you enable end-host mode, if a vHBA is hard pinned to an uplink Fibre Channel port and this uplink port goes down, the system cannot repin the vHBA, and the vHBA remains down.

Switch Mode

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

Switch mode is not the default Fibre Channel switching mode.

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

Changing Fibre Channel Switching Mode

Note When you change the Fibre Channel switching mode, Cisco UCS Director issues a request to Cisco UCS Manager to restart the fabric interconnect. For a cluster configuration, Cisco UCS Director issues a request to restart both fabric interconnects sequentially. The second fabric interconnect can take several minutes to complete the change in Fibre Channel switching mode and become system-ready. The configuration is retained.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Fabric Interconnects**.

Step 4 Click the row for the fabric interconnect for which you want to change the switching mode.

Step 5 Click **FC Mode**.

Step 6 On the **Fabric Interconnect Mode Settings** screen, enter a reason for the change in the **Reason** field and click **Change Mode**.

Cisco UCS Director issues the request to restart the fabric interconnect.

Configuring Ports

Ports on the Cisco UCS 6100 Series Fabric Interconnect

Each Cisco UCS 6100 series fabric interconnect has a set of ports in a fixed port module that you can configure as either server ports or uplink Ethernet ports. These ports are not reserved. They cannot be used by a Cisco UCS domain 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.

Create LAN pin groups and SAN pin groups to pin traffic from servers to an uplink port.

Note Ports on the Cisco UCS 6100 series fabric interconnect are not unified. For more information on Unified Ports, see Port Modes, on page 29.

Each fabric interconnect can include the following port types:

Server Ports

Server ports handle data traffic between the fabric interconnect and the adapter cards on the servers.

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

Uplink Ethernet Ports

Uplink Ethernet ports handle Ethernet traffic between the fabric interconnect and the next layer of the network. All network-bound Ethernet traffic is pinned to one of these ports.

By default, Ethernet ports are unconfigured. However, you can configure them to function in the following ways:

- Uplink
- FCoE
- Appliance

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

Uplink Fibre Channel Ports

Uplink Fibre Channel ports handle FCoE traffic between the fabric interconnect and the next layer of the storage area network. All network-bound FCoE traffic is pinned to one of these ports.

By default, Fibre Channel ports are uplink. However, you can configure them to function as Fibre Channel storage ports. This is useful in cases where Cisco UCS requires a connection to a Direct-Attached Storage (DAS) device.

You can only configure uplink Fibre Channel ports on an expansion module. The fixed module does not include uplink Fibre Channel ports.

Port on the Cisco UCS 6200 Series Fabric Interconnect

Port Modes

For Cisco UCS 6200 series fabric interconnects, configure the port mode for the ports. The port mode determines whether a unified port on the fabric interconnect is configured to carry Ethernet or Fibre Channel traffic. The port mode is not automatically discovered by the fabric interconnect.

Changing the port mode results in the existing port configuration being deleted and replaced by a new logical port. Any objects associated with that port configuration, such as VLANs and VSANs, are removed. There is no restriction on the number of times that the port mode can be changed for a unified port.

Port Types

The port type defines the type of traffic carried over a unified port connection.

All of the port types listed are configurable on both the fixed and expansion module, including server ports, which are not configurable on the Cisco UCS 6100 series fabric interconnect expansion module, but are configurable on the Cisco UCS 6200 series fabric interconnect expansion module.

By default, unified ports changed to Ethernet port mode are set to the uplink Ethernet port type. Unified ports changed to Fibre Channel port mode are set to the Fibre Channel uplink port type. Fibre Channel ports cannot be unconfigured.

Changing the port type does not require a reboot.

When the port mode is set to Ethernet, you can configure the following port types:

- Server ports
- Ethernet uplink ports
- Ethernet port channel members
- FCoE ports
- Appliance ports
- Appliance port channel members

When the port mode is set to Fibre Channel, you can configure the following port types:

- Fibre Channel uplink ports

- Fibre Channel port channel members
- Fibre Channel storage ports
- FCoE Uplink ports

Configuring the Port Mode for Fixed Module Ports

Note The fabric interconnect will be rebooted after you configure the port mode.

You cannot configure the port mode for ports on a Cisco UCS 6100 series fabric interconnect.

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Fabric Interconnects**.
Step 4 Click the row for the fabric interconnect for which you want to set the port mode.
Step 5 Click **Configure Fixed Module Ports**.
Step 6 On the **Configure Fixed Module Ports** screen, do the following:
a) Check the check box for the ports that you want to configure.
b) Click **Submit**.

Configuring the Port Mode for Expansion Module Ports

Note The fabric interconnect will be rebooted after you configure the port mode.

You cannot configure the port mode for ports on a 6100 series fabric interconnect.

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Fabric Interconnects**.
Step 4 Click the row for the fabric interconnect for which you want to set the port mode.
Step 5 Click **Configure Expansion Module Ports**.
Step 6 On the **Configure Expansion Module Ports** screen, do the following:
a) Check the check box for the ports that you want to configure.

b) Click **Submit**.

Enabling a Port

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Fabric Interconnects**.
Step 4 Click the row for the fabric interconnect for which you want to enable a port.
Step 5 Click **View Details**.
Step 6 Click one of the following:

- **Ethernet Ports**
- **Fibre Channel Ports**

Step 7 Click the port that you want to enable.
You can Ctrl-Click to choose and enable multiple ports.
Step 8 From the **More Actions** drop-down menu, choose **Enable Port**.
Step 9 On the **Enable Port** screen, click **Submit**.

Disabling a Port

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Fabric Interconnects**.
Step 4 Click the row for the fabric interconnect for which you want to disable a port.
Step 5 Click **View Details**.
Step 6 Click one of the following:

- **Ethernet Ports**
- **Fibre Channel Ports**

Step 7 Click the port that you want to disable.
You can Ctrl-Click to choose and disable multiple ports.

Step 8 From the **More Actions** drop-down menu, choose **Disable Port**.

Step 9 On the **Disable Port** screen, click **Submit**.

Configuring Ethernet Ports

Configuring a Server Port

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Fabric Interconnects**.

Step 4 Click the row for the fabric interconnect for which you want to configure a server port.

Step 5 Click **Ethernet Ports**.

Step 6 Click the port that you want to configure as a server port.
You can Ctrl-Click to choose and configure multiple ports.

Step 7 From the **More Actions** drop-down menu, choose **Configure as Server Port**.

Step 8 On the **Configure as Server Port** screen, click **Submit**.

Configuring an Uplink Port

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Fabric Interconnects**.

Step 4 Click the row for the fabric interconnect for which you want to configure an uplink port.

Step 5 Click the **Ethernet Ports**.

Step 6 Click the port that you want to configure as an uplink port.
You can Ctrl-Click to choose and configure multiple ports.

Step 7 From the **More Actions** drop-down menu, choose **Configure as Uplink Port**.

Step 8 On the **Configure as Uplink Port** screen, click **Submit**.

Configuring an FCoE Uplink Port

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Fabric Interconnects**.
Step 4 Click the row for the fabric interconnect for which you want to configure an FCoE uplink port.
Step 5 Click **Ethernet Ports**.
Step 6 Click the port that you want to configure as an FCoE uplink port.
You can Ctrl-Click to choose and configure multiple ports.
Step 7 From the **More Actions** drop-down menu, choose **Configure as Uplink FCoE**.
Step 8 On the **Configure as FCoE Uplink Port** screen, click **Submit**.

Configuring an FCoE Storage Port

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Fabric Interconnects**.
Step 4 Click the row for the fabric interconnect for which you want to configure an FCoE storage port.
Step 5 Click **Ethernet Ports**.
Step 6 Click the port that you want to configure as an FCoE storage port.
You can Ctrl-Click to choose and configure multiple ports.
Step 7 From the **More Actions** drop-down menu, choose **Configure as Storage FCoE**.
Step 8 On the **Configure as FCoE Storage Port** screen, click **Submit**.

Configuring an Appliance Port

Procedure

Step 1 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3 In the right pane, click the **Fabric Interconnects** tab.

Step 4 Click the row in the table for the fabric interconnect for which you want to configure an appliance port.

Step 5 Click the **Ethernet Ports** tab.

Step 6 Click the port that you want to configure as an appliance port.
You can Ctrl-Click to choose and configure multiple ports.

Step 7 Click **Configure as Appliance Port**.

Step 8 In the **Configure as Appliance Port** dialog box, complete the following fields:

Name	Description
Priority drop-down list	Choose the quality of service for the port. This can be one of the following: • **Best Effort—**Do not use this priority. It is reserved for the Basic Ethernet traffic lane. • **Platinum—**Use this priority for vNIC traffic only. • **Gold—**Use this priority for vNIC traffic only. • **Bronze—**Use this priority for vNIC traffic only.
Pin Group drop-down list	Choose the LAN pin group that you want to use as the appliance pin target to the specified fabric and port, or fabric and port channel.
Network Control Policy drop-down list	Choose the network control policy associated with this port.
Flow Control Policy drop-down list	Choose the flow control policy associated with this port.

Name	Description
Admin Speed drop-down list	Choose the data transfer rate for the port so that it matches the destination to which the port is linked. This can be one of the following: • **1 Gbps** • **10 Gbps** • **20 Gbps** • **40 Gbps** **Note** The admin speed can be changed only for certain ports, and not all speeds are available on all systems. For more information, see the hardware installation guide for your fabric interconnect.
Port Mode drop-down list	Choose the port mode for the appliance port: • **Trunk—**Displays a VLANs Table that allows you to choose one or more VLANs to associate with this port. • **Access—**Displays the **Select VLAN** drop-down list that allows you to choose a single VLAN to associate with this port.

Step 9 In the **VLANs** area, do the following:

a) If you chose Trunk port mode, click **Add** in the VLANs table, complete the following fields, and then click **Submit**:

- **Name** drop-down list—Choose the VLAN that you want to associate with the appliance port.
- **Set as Native VLAN** check box—Check the check box if you want this VLAN to be the native VLAN for the port.

b) If you chose Access port mode, choose a VLAN from the **VLAN** drop-down list.

Step 10 (Optional) In the **Ethernet Target Endpoint** area, do the following if you want to add an endpoint:

a) In the **Name** field, enter a name for the target endpoint.
b) In the **MAC Address** field, enter the MAC address of the target endpoint.

Step 11 Click **Submit**.

Unconfiguring an Ethernet Port

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Fabric Interconnects**.
Step 4 Click the row for the fabric interconnect for which you want to unconfigure a port.
Step 5 Click **Ethernet Ports**.
Step 6 Click the port that you want to unconfigure
You can Ctrl-Click to choose and unconfigure multiple ports.
Step 7 From the **More Actions** drop-down menu, choose **Unconfigure**.
Step 8 On the **Unconfigure** screen, click **Submit**.

Configuring Fibre Channel Ports

Configuring a Fibre Channel Storage Port

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

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Fabric Interconnects**.
Step 4 Click the row for the fabric interconnect for which you want to configure a Fibre Channel storage port.
Step 5 Click **Fibre Channel Ports**.
Step 6 Click the port that you want to configure as a Fibre Channel storage port.
You can Ctrl-Click to choose and configure multiple ports.
Step 7 From the **More Actions** drop-down menu, choose **Configure as Storage Port**.
Step 8 On the **Configure as FC Storage Uplink Port** screen, click **Submit**.

Configuring a Fibre Channel Uplink Port

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Fabric Interconnects**.
Step 4 Click the row for the fabric interconnect for which you want to configure a Fibre Channel uplink port.
Step 5 Click the **Fibre Channel Ports** tab.
Step 6 Click the port that you want to configure as a Fibre Channel uplink port.
You can Ctrl-Click to choose and configure multiple ports.
Step 7 From the **More Actions** drop-down menu, choose **Configure as Uplink Port**.
Step 8 On the **Configure as Uplink Port** screen, click **Submit**.

Associating a Fibre Channel Port with a VSAN

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Fabric Interconnects**.
Step 4 Click the row for the fabric interconnect for which you want to associate with a VSAN.
Step 5 Click **View Details**.
Step 6 Click **Fibre Channel Ports**.
Step 7 Click the port that you want to associate with a VSAN.
You can Ctrl-Click to choose and associate multiple ports with the same VSAN.
Step 8 From the **More Actions** drop-down menu, choose **Associate VSAN**.
Step 9 On the **Associate VSAN** screen, choose a VSAN from the **VSAN** drop-down list and click **Associate**.

Configuring Cisco UCS Mini Ports

Cisco UCS Mini Scalability Ports

The Cisco UCS 6324 Fabric Interconnect contains a scalability port as well as four unified ports. The scalability port is a 40GB QSFP+ breakout port that, with proper cabling, can support four 1G or 10G SFP+ ports. A

scalability port can be used as a licensed server port for supported Cisco UCS rack servers, as an appliance port, or as an FCoE port.

Configuring a Scalability Port as a Server Port

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Fabric Interconnects**.
Step 4 Click the row for the fabric interconnect for which you want to configure a server port.
Step 5 Click **View Details**.
Step 6 Click **Scalability Ports**.
Step 7 Click the row in the table for the port that you want to configure as a server port.
You can Ctrl-Click to choose and configure multiple ports.
Step 8 From the **More Actions** drop-down menu, choose **Configure as Server Port**.
Step 9 In the **Configure as Server Port** dialog box, click **Submit**.

Configuring a Scalability Port as an Uplink Port

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Fabric Interconnects**.
Step 4 Click the row for the fabric interconnect for which you want to configure an uplink port.
Step 5 Click **View Details**.
Step 6 Click **Scalability Ports**.
Step 7 Click the row in the table for the port that you want to configure as an uplink port.
You can Ctrl-Click to choose and configure multiple ports.
Step 8 From the More Actions, drop-down meu, choose **Configure as Uplink Port**.
Step 9 On the **Configure as Uplink Port** screen, click **Submit**.

Configuring a Scalability Port as an Uplink FCoE Port

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Fabric Interconnects**.
Step 4 Click the row for the fabric interconnect for which you want to configure an uplink FCoE port.
Step 5 Click **View Details**.
Step 6 Click **Scalability Ports**.
Step 7 Click the row in the table for the port that you want to configure as an uplink FCoE port.
You can Ctrl-Click to choose and configure multiple ports.
Step 8 From **More Actions** drop-down menu, choose **Configure as Uplink FCoE Port**.
Step 9 On the **Configure as Uplink FCoE Port** screen, click **Submit**.

Configuring a Scalability Port as a Storage FCoE Port

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Fabric Interconnects**.
Step 4 Click the row for the fabric interconnect for which you want to configure a storage FCoE port.
Step 5 Click **View Details**.
Step 6 Click **Scalability Ports**.
Step 7 Click the row in the table for the port that you want to configure as a storage FCoE port.
You can Ctrl-Click to choose and configure multiple ports.
Step 8 From More Actions drop-down menu, choose **Configure as Storage FCoE Port**.
Step 9 On the **Configure as Storage FCoE Port** screen, click **Submit**.

Configuring a Scalability Port as an Appliance Port

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Fabric Interconnects**.
Step 4 Click the row for the fabric interconnect for which you want to configure an appliance port.
Step 5 Click **View Details**.
Step 6 Click **Scalability Ports**.
Step 7 Click the row in the table for the port that you want to configure as an appliance port.
You can Ctrl-Click to choose and configure multiple ports.
Step 8 From **More Actions** drop-down menu, choose **Configure as Appliance Port**.
Step 9 On the **Configure as Appliance Port** screen, click **Submit**.

Configuring a Fibre Channel Port as an FCoE Uplink Port

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Fabric Interconnects**.
Step 4 Click the row for the fabric interconnect for which you want to configure an FC uplink port.
Step 5 Click **View Details**.
Step 6 Click **Fibre Channel Ports**.
Step 7 Click the row in the table for the port that you want to configure as an FC uplink port.
You can Ctrl-Click to choose and configure multiple ports.
Step 8 From the **More Actions** drop-down menu, choose **Configure as Uplink FCoE**.
Step 9 On the **Configure as FCoE Uplink Port** screen, click **Submit**.

Configuring a Fibre Channel Port as an FCoE Storage Port

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Fabric Interconnects**.
Step 4 Click the row in the table for the fabric interconnect for which you want to configure an FC storage port.
Step 5 Click **View Details**.
Step 6 Click **Fibre Channel Ports**.
Step 7 Click the row in the table for the port that you want to configure as an FC storage port.
You can Ctrl-Click to choose and configure multiple ports.
Step 8 From the **More Actions** drop-down menu, choose **Configure as Storage FCoE**.
Step 9 On the **Configure as FCoE Storage Port** screen, click **Submit**.

Configuring Port Channels

LAN Port Channel

A LAN port channel allows you to group several physical uplink Ethernet ports (link aggregation) to create one logical Ethernet link to provide fault-tolerance and high-speed connectivity. You can add up to eight uplink Ethernet ports to a port channel.

Note Cisco UCS uses Link Aggregation Control Protocol (LACP), not Port Aggregation Protocol (PAgP), to group the uplink Ethernet ports into a port channel. If the ports on the upstream switch are not configured for LACP, the fabric interconnects treat all ports in an uplink Ethernet port channel as individual ports and forward the packets.

Creating a LAN Port Channel

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **LAN Port Channels**.

Step 4 Click **Add**.

Step 5 On the **LAN Port Channel** screen, choose **LAN Port Channel** from the **Port Channel Type** drop-down list and click **Next**.

Step 6 On the **LAN Port Channel - Details** page, do the following:

a) In the **ID** field, enter an identifier for the port channel.
This integer must be between 1 and 256. This ID cannot be changed after the port channel has been saved.

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

c) From the **Fabric ID** drop-down list, choose the fabric interconnect that you want to associate with the port channel.

d) In the **Ports** table, check the check boxes for the ports that you want to include in the port channel.

e) Click **Next**.

Step 7 On the **Summary** page, review the details of the port channel that you have created and click **Submit** to create the port channel.
If you want to change some of the details, click **Back** and return to that page.

SAN Port Channel

A SAN port channel allows you to group several physical Fibre Channel ports (link aggregation) to create one logical Fibre Channel link to provide fault-tolerance and high-speed connectivity. You can create up to four SAN port channels in each Cisco UCS domain. Each Fibre Channel port channel can include a maximum of 16 uplink Fibre Channel ports.

Creating a SAN Port Channel

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click the **SAN Port Channels**.

Step 4 Click **Add**.

Step 5 On the **SAN Port Channel** screen, choose **SAN Port Channel** from the **Port Channel Type** drop-down list and click **Next**.

Step 6 On the **SAN Port Channel - Details** page, do the following:

a) In the **ID** field, enter an identifier for the port channel.
This integer must be between 1 and 256. This ID cannot be changed after the port channel has been saved.

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

c) From the **Fabric ID** drop-down list, choose the fabric interconnect that you want to associate with the port channel.

d) From the **Admin Speed** drop-down list, choose the data transfer rate for traffic on the port channel.

e) In the **Ports** table, check the check boxes for the ports that you want to include in the port channel.

f) Click **Next**.

Step 7 On the **Summary** page, review the details of the port channel that you have created and click **Submit** to create the port channel.
If you want to change some of the details, click **Back** and return to that page.

Appliance Port Channel

An appliance port channel allows you to group several physical appliance ports to create one logical Ethernet storage link for providing fault-tolerance and high-speed connectivity. You can add up to eight appliance ports to a port channel.

Creating an Appliance Port Channel

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click the **LAN Port Channels**.

Step 4 Click **Add**.

Step 5 On the **LAN Port Channel** screen, choose **Appliance Port Channel** from the **Port Channel Type** drop-down list and click **Next**.

Step 6 On the **Appliance Port Channel - Details** page, do the following:

a) In the **ID** field, enter an identifier for the port channel.
This integer must be between 1 and 256. This ID cannot be changed after the port channel has been saved.

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

c) From the **Fabric ID** drop-down list, choose the fabric interconnect that you want to associate with the port channel.

d) From the **Priority** drop-down list, choose the QoS system class that you want to assign to this port channel.

e) From the **Protocol** drop-down list, choose one of the following protocols to assign to this port channel:

- **Static**
- **Lacp**

f) From the **Pin Group** drop-down list, choose the LAN pin group associated with this port channel.

g) From the **Network Control Policy** drop-down list, choose the network control policy associated with this port channel.

h) From the **Flow Control Policy** drop-down list, choose the flow control policy associated with this port channel.

i) From the **Port Mode** drop-down list, choose one of the following modes for the port channel:

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

j) If you choose the Trunk port mode, in the **VLANs** table, check the check boxes for the VLANs that you want to include in the port channel.

k) From the **Native VLAN** drop-down list, choose the native VLAN for this port channel.

l) If you want to add an endpoint, check the **Ethernet Target Endpoint** check box and enter the name and MAC address of the endpoint.

m) In the **Ports** table, check the check boxes for the ports that you want to include in the port channel.

n) Click **Next**.

Step 7 On the **Summary** page, review the details of the port channel that you have created and click **Submit** to create the port channel.
If you want to change some of the details, click **Back** and return to that page.

FCoE Port Channel

A Fibre Channel over Ethernet (FCoE) port channel allows you to group several physical FCoE ports to create one logical FCoE port channel. At a physical level, the FCoE port channel carries FCoE traffic over an Ethernet port channel. An FCoE port channel with a set of members is essentially an Ethernet port channel with the same members. This Ethernet port channel is used as a physical transport for FCoE traffic.

For each FCoE port channel, Cisco UCS creates a Virtual Fibre Channel (VFC) internally and binds it to an Ethernet port channel. FCoE traffic received from the hosts is sent over the VFC the same way as the FCoE traffic is sent over Fibre Channel uplinks.

Creating an FCoE Port Channel

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click the **SAN Port Channels**.

Step 4 Click **Add**.

Step 5 On the **SAN Port Channel** screen, choose **FCoE Port Channel** from the **Port Channel Type** drop-down list and click **Next**.

Step 6 On the **FCoE Port Channel - Details** page, do the following:

a) In the **ID** field, enter an identifier for the port channel.
This integer must be between 1 and 256. This ID cannot be changed after the port channel has been saved.

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

c) From the **Fabric ID** drop-down list, choose the fabric interconnect that you want to associate with the port channel.

d) From the **VSAN** drop-down list, choose the VSAN that you want to associate with the port channel.

e) In the **Ports** table, check the check boxes for the ports that you want to include in the port channel.

f) Click **Next**.

Step 7 On the **Summary** page, review the details of the port channel that you have just created and click **Submit** to create the port channel.
If you want to change some of the details, click **Back** and return to that page.

Enabling a Port Channel

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click one of the following:

- **LAN Port Channels** to enable a LAN port channel or an appliance port channel.
- **SAN Port Channels** to enable a SAN port channel or an FCoE port channel.

Step 4 Click the row for the port channel that you want to enable.

Step 5 From the **More Actions** drop-down menu, choose**Enable Port Channel**.

Step 6 On the **Enable Port Channel** screen, click **Enable**.

Disabling a Port Channel

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

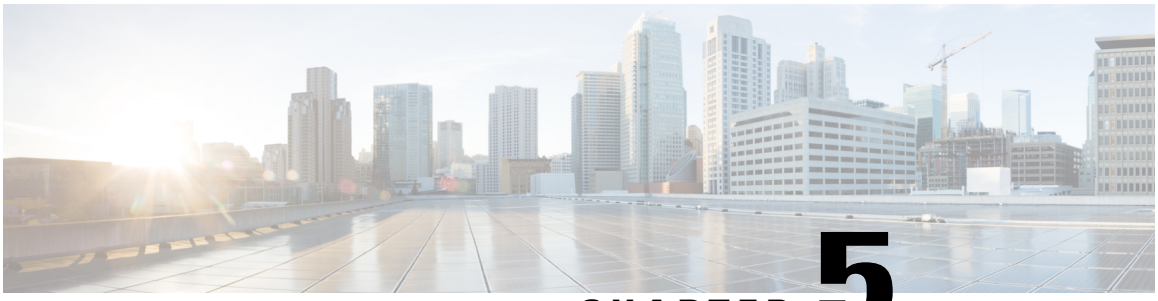
Step 3 Click one of the following:

- **LAN Port Channels** to disable a LAN port channel or an appliance port channel.
- **SAN Port Channels** to disable a SAN port channel or an FCoE port channel.

Step 4 Click the row for the port channel that you want to disable.

Step 5 From the **More Actions** drop-down menu, choose**Disable Port Channel**.

Step 6 on the **Disable Port Channel** screen, click **Disable**.



CHAPTER 5

Configuring Network Connections

This chapter contains the following sections:

- VLANs, page 47
- VLAN Port Count Optimization, page 50
- VLAN Permissions, page 51
- VLAN Groups, page 53
- MAC Pools, page 54
- Configuring Quality of Service, page 56
- vNICs, page 65
- LAN Connectivity Policy, page 69
- Network Control Policy, page 70
- Network Policy, page 73

VLANs

In Cisco UCS, a VLAN, also known as 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 must 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.

For more information about VLANs in Cisco UCS, including guidelines and recommendations, see the Cisco UCS Manager configuration guides.

Guidelines for VLAN IDs

Note You cannot create VLANs with IDs from 3968 to 4047. This range of VLAN IDs is reserved.

VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN that has an ID that overlaps with an FCoE VLAN ID.

The VLAN name is case-sensitive.

Creating a VLAN

In a Cisco UCS domain that is configured for high availability, you can create a VLAN that is accessible to both fabric interconnects or to only one fabric interconnect.

Note You cannot create VLANs with IDs from 3968 to 4047. This range of VLAN IDs is reserved.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **VLANs**.

Step 4 Click **Add**.

Step 5 On the **Add VLAN** screen, complete the following fields:

Name	Description
VLAN Name field	For a single VLAN, this is the VLAN name. The VLAN name is case-sensitive.

Name	Description
VLAN ID field	A single numeric ID for the VLAN. A VLAN ID can be one of the following: • Between 1 and 3967 • Between 4048 and 4093 • Overlap with other VLAN IDs already defined on the system You cannot create VLANs with IDs from 3968 to 4047. This range of VLAN IDs is reserved. VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN that has an ID that overlaps with an FCoE VLAN ID.
Type drop-down list	Choose the type of VLAN. This can be one of the following: • **LAN Cloud** • **Appliances**
Fabric ID drop-down list	Choose how to configure the VLAN. This can be one of the following: • **Common/Global—**The VLAN maps to the same VLAN ID in all available fabrics. • **Fabric A—**The VLAN maps to a VLAN ID that exists only in fabric A. • **Fabric B—**The VLAN maps to a VLAN ID that exists only in fabric B.
Sharing drop-down list	Choose the type of sharing for the VLAN.

Step 6 Click **Submit**.

VLAN Port Count Optimization

VLAN port count optimization allows you to map the state of multiple VLANs into a single internal state. When you enable VLAN port count optimization, Cisco UCS logically groups VLANs based on the port VLAN membership. This grouping increases the port VLAN count limit. VLAN port count optimization also compresses the VLAN state and reduces the CPU load on the fabric interconnect. This reduction in the CPU load enables you to deploy more VLANs over more vNICs. Optimizing the VLAN port count does not change any of the existing VLAN configurations on the vNICs.

VLAN port count optimization is disabled by default. You can enable or disable the option based on your needs.

Note Enabling VLAN port count optimization increases the number of available VLAN ports for use. If the port VLAN count exceeds the maximum number of VLANs in a nonoptimized state, you cannot disable VLAN port count optimization.

Note VLAN port count optimization is not supported in Cisco UCS 6100 series fabric interconnects.

Enabling VLAN Port Count Optimization

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **LAN Global Policies**.

Step 4 Check the **Enable VLAN Port Count Optimization** check box.

Step 5 Click **Save**.

Viewing VLAN Optimization Sets

VLAN port count optimization groups are automatically created by Cisco UCS, based on the VLAN IDs in the system. All the VLANs in the group share the same IGMP policy. The following VLANs are not included in a VLAN optimization set:

- FCoE VLANs
- Primary PVLANs and secondary PVLANs
- VLANs that are specified as a SPAN source
- VLANs configured as a single allowed VLAN on an interface and port profiles with a single VLAN

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **VLAN Optimization Sets**.

Disabling VLAN Port Count Optimization

Note If the port VLAN count exceeds the maximum number of VLANs in a nonoptimized state, you cannot disable VLAN port count optimization.

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **LAN Global Policies**.
Step 4 Uncheck the **Enable VLAN Port Count Optimization** check box.
Step 5 Click **Save**.

VLAN Permissions

VLAN permissions restrict access to VLANs based on specified organizations. Based on the service profile organizations that the VLANs belong to, VLAN permissions also restrict the set of VLANs that you can assign to service profile vNICs. VLAN permissions is an optional feature and is disabled by default. You can enable or disable the feature based on your requirements. If you disable the feature, all the VLANs are globally accessible to all organizations. VLAN permissions are also known as org permissions for VLANs.

If you do not enable VLAN permissions, you cannot modify the permissions for VLANs.

If you enable VLAN permissions, you can specify the organizations available for a VLAN. The VLAN is then only available to that specific organization and all its suborganizations. Users from other organizations cannot access the VLAN. You can also modify VLAN permissions at any point, based on changes in your VLAN access requirements.

Caution When you assign VLAN permissions to an organization at the root level, all suborganizations can access that VLAN. After you assign VLAN permissions at the root level, if you change the permissions for a VLAN that belong to a suborganization, that VLAN becomes unavailable to the root level organization.

Enabling VLAN Permissions

By default, VLAN permissions are disabled. If you want to restrict VLAN access by creating permissions for different organizations, enable the org permission option.

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **LAN Global Policies**.
Step 4 Check the **Enable Org Permissions** check box.
Step 5 Click **Save**.

Modifying Permissions on a VLAN

Before You Begin

Enable VLAN permissions before you assign org permissions to a VLAN.

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **VLANs**.
Step 4 Click the row for the VLAN for which you want to modify org permissions.
Step 5 Click **Modify Org Permissions**.
Step 6 On the **Organization List** screen, check the check boxes for the organizations for which you want to give permissions to the VLAN and click **Submit**.

Disabling VLAN Permissions

By default, VLAN permissions are disabled. If you had enabled the option, assigned VLAN permissions to different network groups, and no longer want to use the option, you can disable the option globally. When VLAN org permissions are disabled, the permissions that you assigned to the VLANs still exist in the system but they are not enforced. If you want to use VLAN permissions later, you can enable the feature to use the previously assigned permissions.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **LAN Global Policies**.

Step 4 Uncheck the **Enable Org Permissions** check box.

Step 5 Click **Save**.

VLAN Groups

VLAN groups allow you to group VLANs on Ethernet uplink ports by function or by VLANs that belong to a specific network. You can define VLAN membership and apply the membership to multiple Ethernet uplink ports on the fabric interconnect.

After you assign a VLAN to a VLAN group, any changes made to the VLAN group are applied to all Ethernet uplink ports that are part of that VLAN group. The VLAN group also enables you to identify VLAN overlaps between disjoint VLANs that must not be connected.

You can configure uplink Ethernet ports under a VLAN group. After you configure an uplink Ethernet port for a VLAN group, that port will only support the VLANs in that group.

Creating a VLAN Group

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **VLAN Groups**.

Step 4 Click **Add**.

Step 5 On the **Create VLAN Group** screen, do the following to add VLANs to the group:

a) In the **Name** field, enter a unique name for the VLAN group.
The VLAN group name is case-sensitive.

b) In the **VLANs** table, choose the VLANs that you want to add to the group.
If the VLANs that you want to include in the group do not exist yet, click **Add** in the table and create a new VLAN. For more information, see Creating a VLAN, on page 48.

c) After you have added all desired VLANs to the group, click **Next**.

Step 6 (Optional) On the **VLAN Group - Add Uplink Ports** page, add the ports that you want to include in the VLAN group and click **Next**.

Step 7 (Optional) On the **VLAN Group - Add Uplink Port Channels** page, add the port channels that you want to include in the VLAN group and click **Next**.

Step 8 Click **Submit**.

Modifying the VLAN Permissions for a VLAN Group

When you modify the organization access permissions for a VLAN group, the change in permissions applies to all VLANs in that VLAN group.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **VLAN Groups**.

Step 4 Click **Modify Org Permissions**.

Step 5 On the **Organization List** screen, check the check boxes for the organizations for which you want to give permissions to the VLAN group and click **Submit**.

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 multitenancy, you can use the organizational hierarchy to ensure that MAC pools can be used only by specific applications or business services. Cisco UCS uses the name resolution policy to assign MAC addresses from the pool.

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

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

Creating a MAC Pool

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the pool and then click **View Details**.

Step 5 Click **MAC Pools**.

Step 6 Click **Add**.

Step 7 On the **Add MAC Pool** screen, complete the following fields:

Name	Description
Name field	A unique name for the pool.
Description field	A description for the pool.
First MAC Address field	The first MAC address in the block.
Size field	The number of MAC addresses in the block.

Step 8 Click **Submit**.

Adding a Block of Addresses to a MAC Pool

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to modify the pool and then click **View Details**.

Step 5 Click **MAC Pools**.

Step 6 Click the pool to which you want to add a block of addresses and then click **Create a Block of MAC Addresses**.

Step 7 On the **Add MAC Pool Block** screen, complete the following fields:

Name	Description
First MAC Address field	The first MAC address in the block.
Size field	The number of MAC addresses in the block.

Step 8 Click **Submit**.

Configuring Quality of Service

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

Global QoS changes made to the QoS system class may result in brief data-plane interruptions for all traffic. Some examples of such changes are:

- Changing the MTU size for an enabled class
- Changing packet drop for an enabled class
- Changing the CoS value for an enabled class

Guidelines and Limitations for Quality of Service on Cisco UCS 6300 Series Fabric Interconnect

- Cisco UCS 6300 Series Fabric Interconnect uses a shared buffer for all system classes.
- Multicast optimization is not supported.
- When you change the QoS parameters for any class causes traffic disruption to all classes. The following table lists the changes in the QoS system class and the conditions that trigger a system reboot.

QoS System class status	Condition	FI Reboot Status
Enabled	Change between drop and no drop	Yes
No-drop	Change between enable and disable	Yes
Enable and no-drop	Change in MTU size	Yes

- The subordinate FI reboots first as a result of the change in the QoS system class. The primary FI reboots only after you acknowledge it in **Pending Activities**.

Guidelines and Limitations for Quality of Service on Cisco UCS Mini

- Cisco UCS Mini uses a shared buffer for all system classes.
- The bronze class shares the buffer with SPAN. We recommend using either SPAN or the bronze class.
- Multicast optimization is not supported.
- Changing the QoS parameters for any class causes traffic disruption to all classes.
- When mixing Ethernet and FC or FCoE traffic, the bandwidth distribution is not equal.
- Multiple streams of traffic from the same class may not be distributed equally.
- Use the same CoS values for all no-drop policies to avoid any FC or FCoE performance issues.
- Only the platinum and gold classes support no-drop policies.

System Classes

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

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

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

Table 2: System Classes

System Class	Description
Platinum Gold Silver Bronze	A configurable set of system classes that you can include in the QoS policy for a service profile. Each system class manages one lane of traffic. All properties of these system classes are available for you to assign custom settings and policies. For Cisco UCS Mini, packet drop can only be disabled on the platinum and gold classes. Only one platinum and one gold class can be configured as a no drop class at a time.
Best Effort	A system class that sets the quality of service for the lane reserved for basic Ethernet traffic. Some properties of this system class are preset and cannot be modified. For example, this class has a drop policy that allows it to drop data packets if required. You cannot disable this system class.

System Class	Description
Fibre Channel	A system class that sets the quality of service for the lane reserved for Fibre Channel over Ethernet traffic. Some properties of this system class are preset and cannot be modified. For example, this class has a no-drop policy that ensures it never drops data packets. You cannot disable this system class. **Note** FCoE traffic has a reserved QoS system class that should not be used by any other type of traffic. If any other type of traffic has a CoS value that is used by FCoE, the value is remarked to 0.

Quality of Service Policy

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

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

Flow Control Policy

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

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

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

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

Changing QoS System Classes

The type of adapter in a server limits the maximum transmission unit (MTU) supported. For example, network MTU above the maximums may cause the packet to be dropped for the following adapters:

- The Cisco UCS M71KR CNA adapter, which supports a maximum MTU of 9216.
- The Cisco UCS 82598KR-CI adapter, which supports a maximum MTU of 14000.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **QoS System Class**.

Step 4 Click the row for the QoS system class that you want to modify.

Step 5 Click **Edit**.

Step 6 On the **Modify QoS System Class** screen, change one or more of the following fields:

Name	Description
Enabled check box	If checked, the associated QoS class is configured on the fabric interconnect and can be assigned to a QoS policy. If unchecked, the class is not configured on the fabric interconnect and any QoS policies associated with this class default to Best Effort or, if a system class is configured with a CoS of 0, to the CoS 0 system class. **Note** This field is always checked for the Best Effort and Fibre Channel system classes.
CoS field	The class of service. You can enter an integer value between 0 and 6, with 0 being the lowest priority and 6 being the highest priority. We recommend that you do not set the value to 0, unless you want that system class to be the default system class for traffic if the QoS policy is deleted or the assigned system class is disabled. **Note** This field is set to 7 for internal traffic and to any for Best Effort. Both of these values are reserved and cannot be assigned to any other priority.
Packet Drop check box	If checked, packet drop is allowed for this class. If unchecked, packets cannot be dropped during transmission. **Note** This check box is always unchecked for the Fibre Channel class, which never allows dropped packets, and always checked for Best Effort, which always allows dropped packets.

Name	Description
Weight drop-down list	Choose the weight assigned to packets in the system class. This can be one of the following: • An integer between 1 and 10. If you enter an integer, the system determines the percentage of network bandwidth assigned to the priority level as described in the Weight (%) field. • **best-effort**. • **none**.
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 system class.
MTU drop-down list	Choose the MTU for the channel. This can be one of the following: • An integer between 1500 and 9216. This value corresponds to the maximum packet size. • **fc—**A predefined packet size of 2240. • **normal—**A predefined packet size of 1500. **Note** This field is always set to fc for the Fibre Channel system class.

Step 7 Click **Submit**.

Enabling a QoS System Class

The Best Effort and Fibre Channel system classes are enabled by default.

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **QoS System Class**.
Step 4 Click the row for the QoS system class that you want to enable.
Step 5 Click **Edit**.
Step 6 On the **Modify QoS System Class** screen, uncheck the **Enabled** check box and click **Submit**.

Disabling a QoS System Class

You cannot disable the Best Effort or Fibre Channel system classes.

All QoS policies that are associated with a disabled system class default to Best Effort, unless the disabled system class is configured with a Cos of 0. If the disabled system class is configured with a Cos of 0, the associated QoS policies default to the Cos 0 system class.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **QoS System Class**.

Step 4 Click the row for the QoS system class that you want to disable.

Step 5 Click **Edit**.

Step 6 On the **Modify QoS System Class** screen, uncheck the **Enabled** check box and click **Submit**.

Creating a QoS Policy

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click **QoS Policies**.

Step 6 Click **Add**.

Step 7 On the **Create QoS Policy** screen, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Description field	A description for the policy.

Name	Description
Priority drop-down list	Choose the priority assigned to this QoS policy. This can be one of the following: • **Fc—**Use this priority for QoS policies that control vHBA traffic only. • **Platinum—**Use this priority for QoS policies that control vNIC traffic only. • **Gold—**Use this priority for QoS policies that control vNIC traffic only. • **Silver—**Use this priority for QoS policies that control vNIC traffic only. • **Bronze—**Use this priority for QoS policies that control vNIC traffic only. • **Best Effort—**Do not use this priority. It is reserved for the Basic Ethernet traffic lane. If you assign this priority to a QoS policy and configure another system class as CoS 0, Cisco UCS does not default to this system class. It defaults to the priority with CoS 0 for that traffic.
Burst field	The normal burst size for servers that use this policy. This field determines how large traffic bursts can be before some traffic is considered to exceed the rate limit. The default is 10240. The minimum value is 0, and the maximum value is 65535. This setting is not applicable to all adapters.

Name	Description
Rate drop-down list	Choose the expected average rate of traffic. Traffic that falls under this rate will always conform. This can be one of the following: • **line-rate—**Equals a value of 0 and specifies no rate limiting. This is the default value. • **Specify Manually—**Enables you to specify the rate in a field. The minimum value is 0, and the maximum value is 40,000,000. The granularity for rate limiting on a Cisco UCS M81KR Virtual Interface Card adapter is 1 Mbps. These adapters treat the requested rate as a "not-to-exceed" rate. Therefore, a value of 4.5 Mbps is interpreted as 4 Mbps. Any requested rate of more than 0 and less than 1 Mbps is interpreted as 1 Mbps, which is the lowest supported hardware rate limit. Rate limiting is not applicable to all adapters. For example, this setting is not supported on the Cisco UCS VIC-1240 Virtual Interface Card.
Host Control drop-down list	Choose whether Cisco UCS controls the class of service (CoS) for a vNIC. This setting has no effect on a vHBA. This can be one of the following: • **None—**Cisco UCS uses the CoS value associated with the priority selected in the Priority drop-down list regardless of the CoS value assigned by the host. • **Full—**If the packet has a valid CoS value assigned by the host, Cisco UCS uses that value. Otherwise, Cisco UCS uses the CoS value associated with the priority selected in the **Priority** drop-down list. This setting is not applicable to all adapters.

Step 8 Click **Submit**.

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 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Flow Control Policies**.

Step 4 Click **Add**.

Step 5 On the **Create Flow Control Policy** screen, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Priority drop-down list	Choose the PPP configuration. This can be one of the following: • **Auto—**Cisco UCS and the network negotiate whether PPP is used on this fabric interconnect. • **On—**PPP is enabled on this fabric interconnect.
Receive drop-down list	Choose what happens when pause requests are received from the network. This can be one of the following: • **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.

Name	Description
Send drop-down list	Choose what happens if the incoming packet rate becomes too high. This can be one of the following: • **Off—**Traffic on the port flows normally regardless of the packet load. • **On—**Cisco UCS sends a pause request to the network if the incoming packet rate becomes too high. The pause remains in effect for a few milliseconds before traffic is reset to normal levels.

Step 6 Click **Submit**.

vNICs

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.

A VM-FEX port profile is not automatically created with the correct settings when you create a vNIC template. If you want to create a VM-FEX port profile, you must configure the target of the vNIC template as a VM.

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

Note If your server has two Emulex or QLogic NICs (Cisco UCS CNA M71KR-E or Cisco UCS CNA M71KR-Q), you must configure vNIC policies for both adapters in your service profile to get a user-defined MAC address for both NICs. If you do not configure policies for both NICs, Windows still detects both of them in the PCI bus. Because the second Ethernet interface is not part of your service profile, Windows assigns it a hardware MAC address. If you then move the service profile to a different server, Windows sees additional NICs because one NIC did not have a user-defined MAC address.

Creating a vNIC Template

Before You Begin

One or more of the following resources must already exist:

- Named VLAN

- MAC pool
- QoS policy
- LAN pin group
- Statistics threshold policy

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click **vNIC Templates**.

Step 6 Click **Add**.

Step 7 On the **Add vNIC Template** screen, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Description field	A description for the policy.
Fabric ID drop-down list	Choose the fabric interconnect that vNICs created with this template are associated with. If you want vNICs created from this template to be able to access the second fabric interconnect if the default one is unavailable, check the **Enable Failover** check box. **Note** Do not enable vNIC fabric failover under the following circumstances: • If the Cisco UCS domain is running in Ethernet Switch Mode. vNIC fabric failover is not supported in that mode. If all Ethernet uplinks on one fabric interconnect fail, the vNICs do not fail over to the other. • If you plan to associate one or more vNICs created from this template with a server adapter that does not support a fabric failover, such as the Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter. If you do so, Cisco UCS Manager generates a configuration fault when you associate the service profile with the server.

Name	Description
Target check boxes	If checked, the target that you choose determines whether a VM-FEX port profile is automatically created with the appropriate settings for the vNIC template. This can be one of the following: • **Adapter—**The vNICs apply to all adapters. No VM-FEX port profile is created if you choose this option. • **VM—**The vNICs apply to all virtual machines. A VM-FEX port profile is created if you choose this option.
Template Type drop-down list	Choose the type of template. This can be one of the following: • **Initial Template—**vNICs created from this template are not updated if the template changes. • **Updating Template—**vNICs created from this template are updated if the template changes.

Step 8 In the **VLANs** area, do the following to select the VLAN to be assigned to vNICs created from this template:

a) Click + (add).

b) In the **Add Entry to VLANs** dialog box, complete the following fields and click **Submit**:

- **Name** drop-down list—Choose the VLAN that you want to associate with the vNIC template.
- **Set as Native VLAN** check box—Check the check box if you want this VLAN to be the native VLAN for the port.

Step 9 To associate policies with vNICs created from this template, complete the following fields:

Name	Description
MTU field	The maximum transmission unit (MTU), or packet size, that vNICs created from this vNIC template should use. Enter an integer between 1500 and 9216. **Note** If the vNIC template has an associated QoS policy, the MTU specified here must be equal to or less than the MTU specified in the associated QoS system class. If this MTU value exceeds the MTU value in the QoS system class, packets might be dropped during data transmission.

Name	Description
MAC Pool drop-down list	Choose the MAC address pool that vNICs created from this vNIC template should use.
QoS Policy drop-down list	Choose the quality of service policy that vNICs created from this vNIC template should use.
Network Control Policy drop-down list	Choose the network control policy that vNICs created from this vNIC template should use.
Pin Group drop-down list	Choose the LAN pin group that vNICs created from this vNIC template should use.
Stats Threshold Policy drop-down list	Choose the statistics collection policy that vNICs created from this vNIC template should use.
VNIC Template Connection Policy drop-down list	Choose the collection policy that vNICs created from this template should use. It can be one of the following: • **Dynamic Policy** • **usNIC Policy** • **VMQ Policy** Only usNIC and VM connection policies created in Cisco UCS Manager are displayed in this drop-down list. **Note** This field is available only with Cisco UCS Manager Release 2.2.
usNIC Template Connection Policy drop-down list	(*Displays only if you choose* **usNIC Policy** *as the VNIC Template connection policy*.) Choose the usNIC collection policy that vNICs created from this vNIC template should use.
VMQ Template Connection Policy drop-down list	(*Displays only if you choose* **VMQ Policy** *as the VNIC Template connection policy.*) Choose the VM collection policy that vNICs created from this vNIC template should use.

Step 10 Click **Submit**.

What to Do Next

Include the vNIC template in a network policy.

Creating a vNIC

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **UCS Manager**.

Step 2 Click **vNIC**.

Step 3 Click **Add**.

Step 4 On the **Create vNIC** screen, complete the following fields to specify the Cisco UCS connections for the vNIC:

Name	Description
vNIC Name field	A unique name for the vNIC.
UCS Account Name drop-down list	Choose the Cisco UCS Manager account to which you want to add this vNIC.
UCS Organization Name drop-down list	Choose the Cisco UCS organization to which you want to add this vNIC.
vNIC Template drop-down list	Choose the vNIC template that you want to assign to this vNIC.
Adapter Policy drop-down list	Choose one of the following Ethernet adapter policies: • **Default** • **Windows** • **VMware** • **Linux**

Step 5 Click **Submit**.

What to Do Next

Include this vNIC in a network policy.

LAN Connectivity Policy

LAN connectivity policies determine the connections and the network communication resources between the server and the LAN on the network. These policies use pools to assign MAC addresses to servers and to identify the vNICs that the servers use to communicate with the network.

Note We do not recommend that you use static IDs in connectivity policies because these policies are included in service profiles and service profile templates and can be used to configure multiple servers.

Creating a LAN Connectivity Policy

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click **LAN Connectivity Policies**.

Step 6 Click **Add**.

Step 7 On the **LAN Connectivity Policy** screen, enter a name and description for the policy.

Step 8 In the **vNICs** table, click **Add** and do the following:

a) Enter a name for the vNIC.

b) To use a vNIC template to create the vNIC, check the **Use vNIC Template** check box and select the appropriate template and adapter policy from the drop-down lists that are displayed.

c) To create a new vNIC without a template, do not check the **Use vNIC Template** check box and complete the fields that are displayed.
For more information about these fields, see Creating a vNIC, on page 69.

d) Click **Submit**.

Repeat this step if you want to add additional vNICs to the policy.

Step 9 After you have created all vNICs required for the policy, click **Submit**.

Network Control Policy

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

- Whether the Cisco Discovery Protocol (CDP) is enabled or disabled
- How the virtual interface (VIF) behaves if no uplink port is available in end-host mode
- The action taken on the remote Ethernet interface, vEthernet interface, or vFibre Channel interface when the associated border port fails
- Whether the server can use different MAC addresses when sending packets to the fabric interconnect
- Whether MAC registration occurs on a per-VNIC basis or for all VLANs

Action on Uplink Fail

By default, the **Action on Uplink Fail** property in the network control policy is configured with a value of link-down. For adapters such as the Cisco UCS M81KR Virtual Interface Card, this default behavior directs Cisco UCS Manager to bring the vEthernet or vFibre Channel interface down if the associated border port fails. For Cisco UCS systems using a non-VM-FEX capable converged network adapter that supports both Ethernet and FCoE traffic, such as Cisco UCS CNA M72KR-Q and the Cisco UCS CNA M72KR-E, this default behavior directs Cisco UCS Manager to bring the remote Ethernet interface down if the associated border port fails. In this scenario, any vFibre Channel interfaces that are bound to the remote Ethernet interface are brought down as well.

Note If your implementation includes those types of non-VM-FEX capable converged network adapters mentioned in this section and the adapter is expected to handle both Ethernet and FCoE traffic, we recommend that you configure the **Action on Uplink Fail** property with a value of warning. This configuration might result in an Ethernet teaming driver not being able to detect a link failure when the border port goes down.

MAC Registration Mode

MAC addresses are installed only on the native VLAN by default, which maximizes the VLAN port count in most implementations.

Note If a trunking driver is being run on the host and the interface is in promiscuous mode, we recommend that you set the Mac Registration Mode to All VLANs.

Creating a Network Control Policy

MAC address-based port security for Emulex Converged Network Adapters (N20-AE0102) is not supported. When MAC address-based port security is enabled, the fabric interconnect restricts traffic to packets that contain the MAC address that it first learns, which is either the source MAC address used in the Fibre Channel over Ethernet (FCoE) Initialization Protocol packet or the MAC address in an Ethernet packet, whichever is sent first by the adapter. This configuration can result in either FCoE or Ethernet packets being dropped.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click **Network Control Policies**.

Step 6 Click **Add**.

Step 7 On the **Create Network Control Policy** screen, complete the following fields:

Name	Description
Name field	A unique name for the policy.
CDP drop-down list	Choose whether the Cisco Discovery Protocol (CDP) is enabled on servers associated with a service profile that includes this policy. This can be one of the following: • **Disabled** • **Enabled**
Action on Uplink Fail drop-down list	Choose how the virtual interface (VIF) behaves if no uplink port is available when the fabric interconnect is in end-host mode. This can be one of the following: • **Link Down—**Changes the operational state of a vNIC to down when uplink connectivity is lost on the fabric interconnect, and enables a fabric failover for vNICs. • **Warning—**Maintains server-to-server connectivity even when no uplink port is available, and disables a fabric failover when uplink connectivity is lost on the fabric interconnect. The default is **Link Down**. **Note** If your implementation includes those types of non-VM-FEX capable converged network adapters and the adapter is expected to handle both Ethernet and FCoE traffic, we recommend that you configure the Action on Uplink Fail property with a value of **Warning**. Note that this configuration might result in an Ethernet teaming driver not being able to detect a link failure when the border port goes down.

Name	Description
Forge drop-down list	Choose whether forged MAC addresses are allowed or denied when packets are sent from the server to the fabric interconnect. This can be one of the following: • **Allow—**All server packets are accepted by the fabric interconnect, regardless of the MAC address associated with the packets. • **Deny—**After the first packet has been sent to the fabric interconnect, all other packets must use the same MAC address or they will be silently rejected by the fabric interconnect. This option enables port security for the associated vNIC. If you plan to install VMware ESX on the associated server, you must configure MAC Security to allow for the network control policy applied to the default vNIC. If you do not configure MAC Security to **Allow**, the ESX installation might fail because the MAC Security permits only one MAC address while the installation process requires more than one MAC address.

Step 8 Click **Submit**.

Network Policy

The network policy is a Cisco UCS Director policy that configures the connections between a server and the LAN, including the virtual network interface cards (vNICs) used by the server. Depending upon the configuration you choose, this policy can be used to configure two or more vNICs for the server. You can choose to create the vNICs in this policy or use a LAN connectivity policy to determine the vNIC configuration.

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

Creating a Network Policy

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **UCS Manager**.

Step 2 Click **Network Policy**.

Step 3 Click **Add**.

Step 4 On the **Add Network Policy** screen, complete the following fields:

Name	Description
Policy Name field	The name of the policy.
Policy Description field	The description of the policy.
UCS Account Name drop-down list	Choose the Cisco UCS Manager account to which you want to add this policy.
UCS Organization Name drop-down list	Choose the Cisco UCS organization to which you want to add this policy.
Dynamic vNIC Connection Policy drop-down list	Choose a dynamic vNIC connection policy if the policy is being assigned to service profiles for servers that support dynamic vNICs.
LAN Connectivity Type drop-down list	Choose one of the following connectivity types: • **Expert—**Allows you to create up to 10 vNICs that the server can use to access the LAN. • **Simple—**Allows you to create a maximum of two vNICs that the server can use to access the LAN. • **No vNICs—**Does not allow you to create any vNICs. If you choose this option, any server associated with a service profile that includes this policy is not connected to the LAN. • **Hardware Inherited—**Uses the vNICs assigned to the Ethernet adapter profile associated with the server. • **Use LAN Connectivity Policy—**Uses a LAN connectivity policy to determine the LAN connectivity for the server.

Step 5 If you chose the **Expert** LAN option, do the following:

a) In the **Add vNIC** drop-down, choose the number of vNICs that you want to add to the network policy. Up to 10 vNICS can be created.

b) From the **Template For vNIC1 ... vNIC10** drop-down list, choose a vNIC template.

c) Go to Step 8.

Step 6 If you chose the **Simple** LAN option, do the following:

a) In the **vNIC0 (Fabric A)** area, complete the following fields:

- In the **vNIC0 Name** field, enter a unique name for the vNIC.
- From the **Select VLAN** drop-down list, choose the name of the VLAN with which this vNIC should be associated.

b) In the **vNIC1 (Fabric B)** area, complete the following fields:

- In the **vNIC1 Name** field, enter a unique name for the vNIC.
- From the **Select VLAN** drop-down list, choose the name of the VLAN with which this vNIC should be associated.

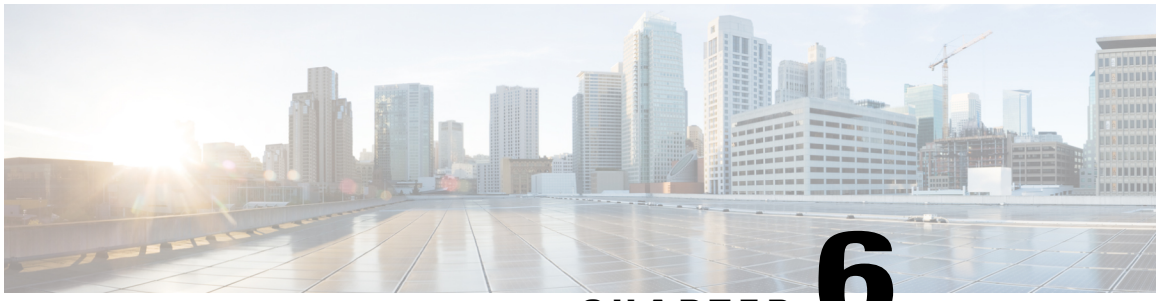
c) Go to Step 8.

Step 7 If you chose the **Use LAN Connectivity Policy** option, choose the policy that you want to associate with the server from the **LAN Connectivity Policy** drop-down list.

Step 8 Click **Submit**.

What to Do Next

Include the network policy in a service profile.



CHAPTER 6

Configuring Storage Connections

This chapter contains the following sections:

- VSANs, page 77
- WWN Pools, page 79
- vHBAs, page 83
- Fibre Channel Adapter Policy, page 85
- SAN Connectivity Policy, page 90
- Storage Policy, page 91
- Fibre Channel Zoning, page 93

VSANs

In Cisco UCS, a VSAN, also known as 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 VSAN knows that the traffic on another VSAN exists but cannot read or access that traffic.

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 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.

For more information about VSANs in Cisco UCS, including guidelines and recommendations, see the Cisco UCS Manager configuration guides.

Named VSANs in Cluster Configurations

In a cluster configuration, a VSAN can be configured to be accessible only to the Fibre Channel uplink ports on one fabric interconnect or to the Fibre Channel uplink ports on both fabric interconnects.

Named VSANs and the FCoE VLAN ID

Configure each VSAN with an FCoE VLAN ID. This property determines which VLAN is used for transporting the VSAN and its Fibre Channel packets.

For FIP-capable, converged network adapters, such as the Cisco UCS CNA M72KR-Q and the Cisco UCS CNA M72KR-E, the VSAN must be configured with a VLAN that is not the native VLAN for the FCoE VLAN ID. This configuration ensures that FCoE traffic can pass through these adapters.

In the following sample configuration, a service profile with a vNIC and vHBA mapped to fabric A is associated with a server that has FIP capable, converged network adapters:

- The vNIC is configured to use VLAN 10.
- VLAN 10 is also designated as the native VLAN for the vNIC.
- The vHBA is configured to use VSAN 2.
- Therefore, VSAN 2 cannot be configured with VLAN 10 as the FCoE VLAN ID. VSAN 2 can be mapped to any other VLAN configured on fabric A.

Creating a VSAN

Note Fibre Channel over Ethernet (FCoE) VLANs in the SAN cloud and VLANs in the LAN cloud must have different IDs. Using the same ID for an FCoE VLAN in a VSAN and a VLAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that FCoE VLAN. Ethernet traffic is dropped on any VLAN that has an ID that overlaps with an FCoE VLAN ID.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **VSANs**.

Step 4 Click **Add**.

Step 5 On the **Add VSAN** screen, complete the following fields:

Name	Description
VSAN Name field	A unique name for the VSAN.
VSAN ID field	The unique identifier assigned to the network.
Type drop-down list	Choose the type of VSAN. This can be one of the following: • **SAN Cloud** • **Storage Cloud** If you are creating a VSAN for Fibre Channel zoning, we recommend that you choose **Storage Cloud**.

Name	Description
Fabric ID drop-down list	Choose how to configure the VSAN. This can be one of the following: • **Common/Global—**The VSAN maps to the same VSAN ID in all available fabrics. • **Fabric A—**The VSAN maps to a VSAN ID that exists only in fabric A. • **Fabric B—**The VSAN maps to a VSAN ID that exists only in fabric B.
FCoE VLAN field	The unique identifier assigned to the VLAN used for Fibre Channel connections. For FCoE Initialization Protocol (FIP)-capable, converged network adapters, such as the Cisco UCS CNA M72KR-Q and the Cisco UCS CNA M72KR-E, the named VSAN must be configured with a named VLAN that is not the native VLAN for the FCoE VLAN ID. This configuration ensures that FCoE traffic can pass through these adapters.

Step 6 Click **Submit**.

What to Do Next

If you plan to use this VSAN for Fibre Channel zoning, see Configuring a VSAN for Fibre Channel Zoning, on page 96.

WWN Pools

WWNN Pools

A WWNN (World Wide Node Name) pool is a WWN (World Wide Name) pool that contains only WW (World Wide) node names. If you include a pool of WWNNs in a service profile, the associated server is assigned a WWNN from that pool. You can view the WWN blocks and initiators in a WWNN pool by double-clicking the pool in the **WWNN Pools** tab.

Creating a WWNN Pool

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the pool and then click **View Details**.

Step 5 Click **WWNN Pools**.

Step 6 Click **Add**.

Step 7 On the **Add WWNN Pool** screen, complete the following fields:

Name	Description
Name field	A unique name for the pool.
Description field	A description for the pool.
From field	The first WWNN address in the block.
Size field	The number of WWNN addresses in the block.

Step 8 Click **Submit**.

Adding an Initiator to a WWNN Pool

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to modify the pool and then click **View Details**.

Step 5 Click **WWNN Pools**.

Step 6 Click the pool to which you want to add an initiator.

Step 7 Click **Create WWNN Initiator**.

Step 8 On the **Create WWNN Initiator** screen, complete the following fields:

Name	Description
Name field	A unique name for the initiator.

Name	Description
Description field	A description for the initiator.
World Wide Name field	The WWN for the initiator.

Step 9 Click **Submit**.

WWPN Pools

A WWPN (World Wide Port Name) pool is a WWN pool that contains only WW port names. If you include a pool of WWPNs in a service profile, the port on each vHBA of the associated server is assigned a WWPN from that pool. You can view the WWN blocks and initiators in a WWPN pool by double-clicking the pool in the **WWPN Pools** tab.

Creating a WWPN Pool

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Organizations**.
Step 4 Click the organization in which you want to create the pool and then click **View Details**.
Step 5 Click **WWPN Pools**.
Step 6 Click **Add**.
Step 7 On the **Add WWPN Pool** screen, complete the following fields:

Name	Description
Name field	A unique name for the pool.
Description field	A description for the pool.
From field	The first WWPN address in the block.
Size field	The number of WWPN addresses in the block.

Step 8 Click **Submit**.

Adding an Initiator to a WWPN Pool

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Organizations**.
Step 4 Click the organization in which you want to modify the pool and then click **View Details**.
Step 5 Click **WWPN Pools**.
Step 6 Click the pool to which you want to add an initiator.
Step 7 Click **Create WWPN Initiator**.
Step 8 On the **Create WWPN Initiator** screen, complete the following fields:

Name	Description
Name field	A unique name for the initiator.
Description field	A description for the initiator.
World Wide Name field	The WWN for the initiator.

Step 9 Click **Submit**.

Adding a WWN Block

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Organizations**.
Step 4 Click the organization in which you want to modify the pool and then click **View Details**.
Step 5 Click one of the following:

- **WWNN Pools**
- **WWPN Pools**

Step 6 Click the pool to which you want to add a WWN block.
Step 7 Click **Create WWN Block**.
Step 8 On the **Create WWN Block** screen, complete the following fields:

Name	Description
From field	The first WWNN or WWPN address in the block.
Size field	The number of WWN or WWPN addresses in the block.

Step 9 Click **Submit**.

vHBAs

vHBA Template

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

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

Creating a vHBA Template

Before You Begin

One or more of the following resources must already exist:

- VSAN
- WWPN pool
- SAN pin group
- Statistics threshold policy

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Organizations**.
Step 4 Click the organization in which you want to create the policy and then click **View Details**.
Step 5 Click **vHBA Templates**.
Step 6 Click **Add**.
Step 7 On the **Add vHBA Template** screen, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Description field	A description for the policy.
Fabric ID drop-down list	Choose the fabric interconnect that vHBAs created with this template are associated with.
VSAN drop-down list	Choose the VSAN that you want to associate with vHBAs created from this template.
Template Type drop-down list	Choose the type of template that you want to use. This can be one of the following: • **Initial Template—**vHBAs created from this template are not updated if the template changes. • **Updating Template—**vHBAs created from this template are updated if the template changes.
Max Data Field Size field	The maximum size of the Fibre Channel frame payload bytes that the vHBA supports. Enter an integer between 256 and 2112. The default is 2048.
WWPN Pool drop-down list	Choose the WWPN pool that a vHBA created from this template uses to derive its WWPN address.
QoS Policy drop-down list	Choose the QoS policy that is associated with vHBAs created from this template.
Pin Group drop-down list	Choose the SAN pin group that is associated with vHBAs created from this template.
Stats Threshold Policy drop-down list	Choose the statistics threshold policy that is associated with vHBAs created from this template.

Step 8 Click **Submit**.

What to Do Next

Include the vHBA template in a storage policy.

Creating a vHBA

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **UCS Manager**.

Step 2 Click **vHBA**.

Step 3 Click **Add**.

Step 4 On the **Create vHBA** screen, complete the following fields to specify the Cisco UCS connections for the vHBA:

Name	Description
vHBA Name field	A unique name for the vHBA.
UCS Account Name drop-down list	Choose the Cisco UCS Manager account to which you want to add this vHBA.
UCS Organization Name drop-down list	Choose the Cisco UCS organization to which you want to add this vHBA.
vHBA Template drop-down list	Choose the vHBA template that you want to assign to this vHBA.
Adapter Policy drop-down list	Choose one of the following Ethernet adapter policies: • **Default** • **Windows** • **VMware** • **Linux**

Step 5 Click **Submit**.

What to Do Next

Include this vHBA in a storage policy.

Fibre Channel Adapter Policy

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

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

Creating a Fibre Channel Adapter Policy

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click **FC Adapter Policies**.

Step 6 Click **Add**.

Step 7 On the **Create Fibre Channel Adapter Policy** screen, enter a name and description for the policy.

Step 8 In the **Resources** area, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Description field	A description for the policy.
Ring Size field for transmit queues	The number of descriptors in each transmit queue. This parameter applies to Extended Link Services (ELS) and Common Transport (CT) fibre channel frames for generic services. It does not affect the performance of the adapter. Enter an integer between 64 and 128. The default is 64.
Ring Size field for receive queues	The number of descriptors in each receive queue. This parameter applies to Extended Link Services (ELS) and Common Transport (CT) fibre channel frames for generic services. It does not affect the performance of the adapter. Enter an integer between 64 and 128. The default is 64.

Name	Description
Ring Size field for SCSI I/O queues	The number of descriptors in each SCSI I/O queue. Enter an integer between 64 and 512. The default is 512. The number of descriptors can affect the performance of the adapter, so we recommend that you do not change the default value.

Step 9 In the **Options** area, complete the following fields:

Name	Description
FCP Error Recovery drop-down list	Choose whether the system uses FCP Sequence Level Error Recovery (FC-TAPE) protocol for sequence level error recovery with tape devices. This enables or disables the Read Exchange Concise (REC) and Sequence Retransmission Request (SRR) functions on the VIC firmware. This can be one of the following: • **Disabled—**This is the default. • **Enabled—**You should select this option if your system is connected to one or more tape drive libraries. **Note** This parameter applies only to a server with a Virtual Interface Card (VIC) adapter, such as the Cisco UCS M81KR Virtual Interface Card.
Flogi Retries field	The number of times that the system tries to log in to the fabric after the first failure. Enter any integer. To specify that the system is to continue to try indefinitely, enter infinite in this field. We recommend that you consult your storage array documentation for the optimal value for this parameter. **Note** This parameter applies only to a server with a VIC adapter or a converged network adapter such as the Cisco UCS M71KR-E Emulex Converged Network Adapter.

Name	Description
Flogi Timeout field	The number of milliseconds that the system waits before it tries to log in again. Enter an integer between 1000 and 255000. The default is 4,000. We recommend that you consult your storage array documentation for the optimal value for this parameter. **Note** This parameter applies only to a server with a VIC adapter or a converged network adapter.
Plogi Retries field	The number of times that the system tries to log into a port after the first failure. Enter an integer between 0 and 255. The default is 8. We recommend that you consult your storage array documentation for the optimal value for this parameter. **Note** This parameter applies only to a server with a VIC adapter.
Plogi Timeout field	The number of milliseconds that the system waits before it tries to log in again. Enter an integer between 1000 and 255000. The default is 20,000. We recommend that you consult your storage array documentation for the optimal value for this parameter. **Note** This parameter applies only to a server with a VIC adapter.
Port Down Timeout field	The number of milliseconds that a remote Fibre Channel port should be offline before informing the SCSI upper layer that the port is unavailable. This parameter is important for host multipathing drivers and it is one of the key indicators used for error processing. Enter an integer between 0 and 240000. The default is 30,000. For a server with a VIC adapter running ESX, the recommended value is 10,000. We recommend that you consult your storage array documentation for the optimal value for this parameter. **Note** This parameter applies only to a server with a VIC adapter.

Name	Description
Port Down IO Retry field	The number of times that 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. We recommend that you consult your storage array documentation for the optimal value for this parameter. **Note** This parameter applies only to a server with a VIC adapter running Windows.
Link Down Timeout field	The number of milliseconds that the uplink port should be offline before it informs the system that the uplink port is down and fabric connectivity has been lost. Enter an integer between 0 and 240000. The default is 30,000. We recommend that you consult your storage array documentation for the optimal value for this parameter. **Note** This parameter applies only to a server with a VIC adapter running Windows.
IO Throttle Count field	The maximum number of data or control I/O operations that can be pending in the vHBA at one time. If this value is exceeded, the additional I/O operations wait in the queue until the number of pending I/O operations decreases and the additional operations can be processed. **Note** This parameter is not the same as the LUN queue depth, which is controlled by Cisco UCS Manager based on the operating system installed on the server. Enter an integer between 1 and 1024. The default is 16. We recommend that you consult your storage array documentation for the optimal value for this parameter. **Note** This parameter applies only to a server with a network adapter such as the Cisco UCS M71KR-E Emulex Converged Network Adapter or the Cisco UCS M71KR-Q QLogic Converged Network Adapter. Servers with a VIC adapter ignore this parameter.

Name	Description
Max LUNs Per Target field	The maximum number of LUNs that the Fibre Channel driver will export or show. The maximum number of LUNs is usually controlled by the operating system running on the server. Enter an integer between 1 and 1024. The default value is 256. For servers running ESX or Linux, the recommended value is 1024. We recommend that you consult your operating system documentation for the optimal value for this parameter. **Note** This parameter applies only to a server with a VIC adapter or a network adapter.
Interrupt Mode drop-down list	Choose the method used to send interrupts to the operating system from the driver. This can be one of the following: • **MSI-X—**Message Signaled Interrupts (MSI) with the optional extension. We recommend that you select this option if the operating system on the server supports it. • **MSI—**MSI only. • **INTx—**PCI INTx interrupts. **Note** This parameter applies only to a server with a VIC adapter or a network adapter running an operating system other than Windows. The Windows operating system ignores this parameter.

Step 10 Click **Submit**.

SAN Connectivity Policy

SAN connectivity policies determine the connections and the network communication resources between the server and the LAN on the network. These policies use pools to assign WWNs and WWPNs to servers and to identify the vHBAs that the servers use to communicate with the network.

Note We do not recommend that you use static IDs in connectivity policies, because these policies are included in service profiles and service profile templates and can be used to configure multiple servers.

Creating a SAN Connectivity Policy

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click **SAN Connectivity Policies**.

Step 6 Click **Add**.

Step 7 On the **SAN Connectivity Policy** screen, enter a name and description for the policy.

Step 8 From the **WWNN Pool** drop-down list, choose the WWNN pool that you want to associate with this policy.

Step 9 In the **vHBAs** table, click **Add** and do the following:

a) Enter a name for the vHBA.

b) To use a vHBA template to create the vHBA, check the **Use vHBA Template** check box and choose the appropriate template from the drop-down list that is displayed.

c) To create a new vHBA without a template, do not check the **Use vHBA Template** check box and complete the fields that are displayed.
For more information about these fields, see Creating a vHBA, on page 85.

d) Click **Submit**.

Repeat this step if you want to add additional vHBAs to the policy.

Step 10 After you have created all vHBAs required for the policy, click **Submit**.

Storage Policy

The storage policy is a Cisco UCS Director policy that configures the connections between a server and SAN storage, including the World Wide Node Name (WWNN) assigned to the server and the virtual host bus adapters (vHBAs) used by the server. Depending upon the configuration you choose, this policy can be used to configure two or more vHBAs for the server. You can choose to create the vHBAs in this policy or use a SAN connectivity policy to determine the vHBA configuration.

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

Creating a Storage Policy

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **UCS Manager**.

Step 2 Click **Storage Policy**.

Step 3 Click **Add**.

Step 4 Enter a name and description for the policy.

Step 5 On the **Add Storage Policy** screen, complete the following fields to specify the Cisco UCS connections for the storage policy:

Name	Description
Policy Name field	A unique name for the storage policy.
Policy description field	The description for the storage policy.
UCS Account Name drop-down list	Choose the Cisco UCS Manager account to which you want to add this storage policy.
UCS Organization Name drop-down list	Choose the Cisco UCS organization to which you want to add this storage policy.
Local Disk Configuration Policy drop-down list	Choose the local disk configuration policy that you want to include in this storage policy.
SAN Connectivity Type drop-down list	Choose one of the following connectivity types: • **Expert—**Allows you to create up to 10 vHBAs that the server can use to access SAN storage. • **Simple—**Allows you to create a maximum of two vHBAs that the server can use to access SAN storage. • **No vHBAs—**Does not allow you to create any vHBAs. If you choose this option, any server associated with a service profile that includes this policy is not connected to the SAN. • **Hardware Inherited—**Uses the vHBAs assigned to the Fibre Channel adapter profile associated with the server. • **Use SAN Connectivity Policy—**Uses a SAN connectivity policy to determine the SAN connectivity for the server.

Step 6 If you chose the **Expert** SAN storage option, do the following:

a) From the **WWNN Pool** drop-down list, choose the WWNN pool that you want to assign to this policy. The WWNN pool must contain a sufficient number of WWNNs to assign a WWNN to each server that is associated with the service profile that uses this storage policy.

b) In the **Add vHBA** drop-down, choose the number of vHBAs (up to 10) that you want to add to the storage policy.
c) From the **Template For vHBA1 .....vHBA10** list, choose a vHBA template for each vHBA.
d) Go to Step 9.

Step 7 If you chose the **Simple** SAN storage option, do the following:

a) From the **WWNN Pool** drop-down list, choose the WWNN pool that you want to assign to this policy. The WWNN pool must contain a sufficient number of WWNNs to assign a WWNN to each server that is associated with the service profile that uses this storage policy.

b) In the **vHBA0 (Fabric A)** area, complete the following fields:

- In the **vHBA0 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 **vHBA1 (Fabric B)** area, complete the following fields:

- In the **vHBA1 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) Go to Step 9.

Step 8 If you chose the **Use SAN Connectivity Policy** option, choose the policy that you want to associate with the server from the **SAN Connectivity Policy** drop-down list.

Step 9 Click **Submit**.

What to Do Next

Include the storage policy in a service profile.

Fibre Channel Zoning

Support for Fibre Channel Zoning in Cisco UCS

Cisco UCS supports switch-based Fibre Channel zoning and Cisco UCS local Fibre Channel zoning (also known as Cisco UCS Manager-based Fibre Channel zoning). You cannot configure a combination of zoning types in the same Cisco UCS domain. You can configure a Cisco UCS domain with one of the following types of zoning:

- No zoning
- Cisco UCS local Fibre Channel zoning—This configuration combines direct attach storage with local zoning. Fibre Channel or FCoE storage is directly connected to the fabric interconnects and zoning is configured in Cisco UCS, using local zoning. Any existing Fibre Channel or FCoE uplink connections must be disabled. Cisco UCS does not currently support active Fibre Channel or FCoE uplink connections that coexist with the utilization of the Cisco UCS local zoning feature.

- Switch-based Fibre Channel zoning—This configuration combines direct attach storage with uplink zoning. The Fibre Channel or FCoE storage is directly connected to the fabric interconnects and zoning is performed externally to the Cisco UCS domain through a Cisco MDS or Nexus 5000 Series switch. This configuration does not support local zoning in the Cisco UCS domain.

Note Zoning is configured on a per-VSAN basis. You cannot enable zoning at the fabric level.

For more information about Fibre Channel zoning, including guidelines for implementing it, see the Cisco UCS Manager configuration guides.

Storage Connection Policy

The storage connection policy contains a collection of target storage ports on storage arrays that you use to configure Cisco UCS local Fibre Channel zoning. You can create this policy underneath an organization or an initiator group. This policy is known as a Fibre Channel storage connection policy in Cisco UCS Manager.

You add vHBA initiator groups to a storage connection policy through the Fibre Channel target endpoints.

The storage arrays in these zones must be directly connected to the fabric interconnects. The target storage ports on these arrays that you include in the storage connection policy can be either Fibre Channel storage ports or FCoE storage ports. You use the WWN of a port to add it to the policy and to identify the port for the Fibre Channel zone.

Note Cisco UCS does not create Fibre Channel storage by default.

Configuring Fibre Channel Zoning in Cisco UCS

Note This procedure provides a high-level overview of the steps required to configure a Cisco UCS domain for Cisco UCS local Fibre Channel zoning. Ensure that you complete all of the following steps.

Procedure

	Command or Action	Purpose
Step 1	If you have not already done so, disconnect the fabric interconnects in the Cisco UCS domain from any external Fibre Channel switches, such as an MDS.	If the Cisco UCS domain still includes zones that were managed by the external Fibre Channel switch, enter the **clear-unmanaged-fc-zone-all** command on every affected VSAN to remove those zones. You must perform this step in the Cisco UCS Manager CLI.

	Command or Action	Purpose
Step 2	Configure the Fibre Channel switching mode for both fabric interconnects in Fibre Channel switch mode.	You cannot configure Fibre Channel zoning in end-host mode. See Changing Fibre Channel Switching Mode, on page 27.
Step 3	Configure the Fibre Channel and FCoE storage ports that you require to carry traffic for the Fibre Channel zones.	See Configuring Fabric Interconnects and Ports, on page 25.
Step 4	Create one or more VSANs and enable Fibre Channel zoning on all VSANs that you require to carry traffic for the Fibre Channel zones.	For a cluster configuration, we recommend that you create the VSANs that you intend to include in a storage zone and use the common or global configuration to ensure that they are accessible to both fabric interconnects. See Creating a VSAN, on page 78 and Configuring a VSAN for Fibre Channel Zoning, on page 96.
Step 5	Create a LAN connectivity policy.	See Creating a LAN Connectivity Policy, on page 70.
Step 6	Create a network policy and add the LAN connectivity policy to it.	See Creating a Network Policy, on page 74.
Step 7	Create a SAN connectivity policy.	See Creating a SAN Connectivity Policy, on page 91.
Step 8	Create a storage policy and add the SAN connectivity policy to it.	See Creating a Storage Policy, on page 92.
Step 9	Create one or more storage connection policies and include one or more Fibre Channel target endpoints to serve as vHBA initiator groups.	See Creating a Storage Connection Policy, on page 96.
Step 10	Create a service profile and add the network policy and storage policy to it.	See Creating a Service Profile, on page 170.
Step 11	Associate the service profile with a server.	
Step 12	View and generate reports for the Fibre Channel zones through a service profile and/or organization.	(Optional) See Viewing Fibre Channel Zones, on page 97.
Step 13	If you modify the LAN and/or SAN connectivity policies, which causes the server to reboot, request inventory collection for the service profile and the server.	(Optional) See Requesting Inventory Collection for a Service Profile, on page 179 and Requesting Inventory Collection for a Server, on page 185.

Configuring a VSAN for Fibre Channel Zoning

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **VSANs**.
Step 4 Click the VSAN that you want to configure for Fibre Channel zoning.
Step 5 Click **FC Zoning Settings**.
Step 6 On the **FC Zoning Settings** screen, check the **Enable FC Zoning** check box.
Step 7 Click **Save**.

Creating a Storage Connection Policy

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Organizations**.
Step 4 Click the organization in which you want to create the policy and then click **View Details**.
Step 5 Click **Storage Connection Policies**.
Step 6 Click **Add**.
Step 7 On the **Storage Connection Policy** screen, enter a name and description for the policy.
Step 8 In the **Zoning Type** drop-down list, choose one of the following options:

- **None—**No Fibre Channel zoning.
- **Single Initiator Single Target—**Cisco UCS Director automatically creates one zone for each vHBA and storage port pair. Each zone has two members. We recommend that you configure this type of zoning unless you expect the number of zones to exceed the maximum supported.
- **Single Initiator Multiple Targets—**Cisco UCS Director automatically creates one zone for each vHBA. We recommend that you configure this type of zoning if you expect the number of zones to reach or exceed the maximum supported.

Step 9 In the **FC Target Endpoints** table, click **Add** and do the following:
a) Complete the following fields:

Name	Description
WWPN field	The WWPN (WWN) assigned to the physical target port on the Fibre Channel or FCoE storage array that the server uses to access the LUNs configured on the storage array.
Fabric ID drop-down list	Choose the fabric interconnect used for communications with the target endpoint.
VSAN drop-down list	Choose the VSAN used for communications with the target endpoint.

b) Click **Submit**.

Repeat this step until you have created all desired target endpoints.

Step 10 Click **Submit**.

Viewing Fibre Channel Zones

Before You Begin

You must have Fibre Channel Zoning configured to view any Fibre Channel zones.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click one of the following:

- **Organizations**
- **Service Profiles**

Step 4 Click the **FC Zones**.

Step 5 (Optional) To customize the columns that you see in the table and any report that you generate, do the following:

a) On the table menu bar, click the **Customize Table Columns** button.

b) In the **Customize Report Table** dialog box, check or uncheck the check boxes to determine which elements you see in the report and click **Save**.

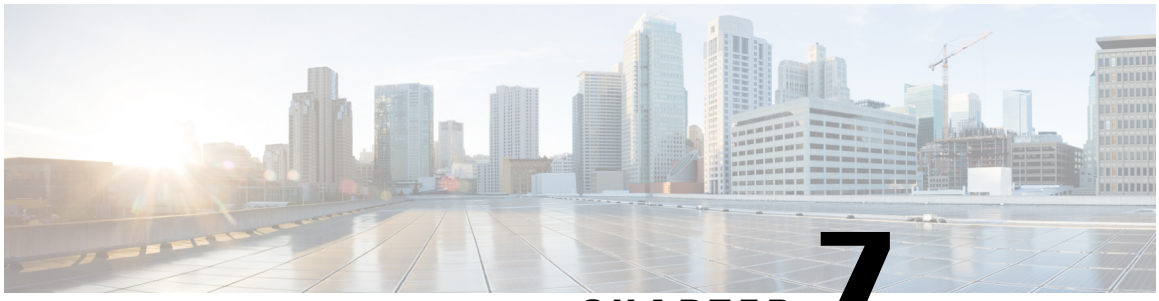
Step 6 (Optional) To export a report of what you see in the tab, do the following:

a) On the table menu bar, click **Export Report**.

b) In the **Export Report** dialog box, select a report format and click **Generate Report**.

c) When the report has generated, click **Download**.

d) If the report opens in a separate tab, use the download button from your browser to download the report.
e) In the **Export Report** dialog box, click **Close**.



CHAPTER 7

Configuring Cisco UCS Server Pools and Policies

This chapter contains the following sections:

- Global Equipment Policies, page 99
- UUID Pools, page 102
- Server Pools, page 103
- Management IP Pool, page 105
- Boot Policy, page 106
- Local Disk Configuration Policy, page 147
- Maintenance Policy, page 152
- Server Pool Policy Qualification Overview, page 154
- Server Pool Policy Overview, page 158
- vNIC/vHBA Placement Policies, page 159
- Placement Policy, page 165

Global Equipment Policies

Chassis/FEX Discovery Policy

The chassis/FEX discovery policy determines how the system reacts when you add a new chassis or FEX. Cisco UCS uses the settings in the chassis/FEX discovery policy to determine:

- the minimum threshold for the number of links between the chassis or FEX and the fabric interconnect
- whether to group links from the IOM to the fabric interconnect in a fabric port channel

For more information about chassis links, including an overview of how the chassis/FEX discovery policy works in a multichassis Cisco UCS domain, see the Cisco UCS Manager configuration guides.

Configuring the Chassis/FEX Discovery Policy

You can configure a chassis policy to specify how the system reacts when a new chassis is added.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Equipment Global Policies**.

Step 4 Check the **Chassis/FEX Discovery Policy** check box.

Step 5 From the **Action** drop-down list, choose the minimum threshold for the number of links between the chassis or Fabric Extender (FEX) and the fabric interconnect:

- **1-link**
- **2-link**
- **4-link**
- **8-link**

Step 6 From the **Link Grouping Preference** drop-down list, choose whether the links from the IOMs or FEXes to the fabric interconnects are grouped in a port channel.

Note The link grouping preference takes effect only if both sides of the links between an IOM or FEX and the fabric interconnect support fabric port channels. If one side of the links does not support fabric port channels, this preference is ignored and the links are not grouped in a port channel.

Step 7 Click **Save**.

Rack Server Discovery Policy

The rack server discovery policy determines how the system reacts when you add a new rack-mount server. Cisco UCS uses the settings in the rack server discovery policy to determine whether any data on the hard disks are scrubbed and whether server discovery occurs immediately or must wait for explicit user acknowledgment. For manual acknowledgement, see Viewing the Cisco UCS Manager Pending Activities Report and User Acknowledgement, on page 195.

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

Configuring the Rack Server Discovery Policy

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Equipment Global Policies**.

Step 4 Check the **Rack Server Discovery Policy** check box.

Step 5 From the **Action** drop-list, choose what happens when you add a new rack server:

- **Immediate—**The new server is discovered automatically.
- **User-acknowledged—**Nothing happens until you acknowledge the new server.

  To apply user acknowledgement, see Viewing the Cisco UCS Manager Pending Activities Report and User Acknowledgement, on page 195.

Step 6 From the **Scrub Policy** drop-down list, choose the scrub policy to run on a newly discovered server if that server meets the criteria in the server pool policy qualification.

Step 7 Click **Save**.

Rack Management Connection Policy

The rack management connection policy determines whether a newly added rack-mount server is automatically managed by Cisco UCS or whether it must wait for explicit user acknowledgment. We recommend that you configure this policy for auto-acknowledgment.

Configuring the Rack Management Connection Policy

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Equipment Global Policies**.

Step 4 Check the **Rack Management Connection Policy** check box.

Step 5 From the **Action** drop-down list, choose one of the following:

- **auto-acknowledged—**Acknowledgment happens automatically.
- **user-acknowledged—**Nothing happens until you acknowledge the server.

  To apply user acknowledgement, see Viewing the Cisco UCS Manager Pending Activities Report and User Acknowledgement, on page 195.

Step 6 Click **Save**.

UUID Pools

A UUID pool is a collection of SMBIOS (Systems Management Built In Operating System) UUIDs (Universally Unique Identifiers) that are available to be assigned to servers. The first number of digits that constitute the prefix of the UUID are fixed. The remaining digits, the UUID suffix, are variable. A UUID 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 pools in service profiles, you do not have to manually configure the UUID of the server associated with the service profile.

Creating a UUID Pool

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the pool and then click **View Details**.

Step 5 Click **UUID Pools**.

Step 6 Click **Add**.

Step 7 On the **Add UUID Pool** screen, complete the following fields:

Name	Description
Name field	A unique name for the pool.
Description field	A description for the pool.
Prefix drop-down list	Choose how the prefix is created. This can be one of the following: • **Derived—**The system creates the prefix. • **Other—**You specify the desired prefix. If you select this option, a text field displays where you can enter the desired prefix, in the format XXXXXXXX-XXXX-XXXX.
From field	The first UUID address in the block.
Size field	The number of UUID addresses in the block.

Step 8 Click **Submit**.

Adding an Address Block to a UUID Pool

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to modify the pool and then click **View Details**.

Step 5 Click **UUID Pools**.

Step 6 Click on the pool to which you want to add a block of addresses and then click **Add UUID Addresses Block**.

Step 7 On the **Add UUID Pool Block** screen, complete the following fields:

Name	Description
From field	The first UUID address in the block.
Size field	The number of UUID addresses in the block.

Step 8 Click **Submit**.

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

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

Creating a Server Pool

Cisco UCS Director displays only the managed servers in a server pool, but the size of the pool includes all servers. For example, if a server pool contains two servers and only one server is managed by Cisco UCS Director, all server pool reports and actions on that pool display only one (managed) server. However, the pool size is displayed as two.

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Organizations**.
Step 4 Click the organization in which you want to create the pool and then click **View Details**.
Step 5 Click **Server Pools**.
Step 6 Click **Add**.
Step 7 On the **Add Server Pool** screen, add a name and description for the pool
Step 8 (Optional) In the **Servers** field, do the following to add servers to the pool:
a) Click **Select**.
b) On the **Select Items** page, check the check boxes for the servers that you want to add to the pool
c) Click **Select**.
Step 9 Click **Add**.

Assigning a Server Pool to a Cisco UCS Director Group

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Organizations**.
Step 4 Click the organization that contains the pool you want to assign and then click **View Details**.
Step 5 Click **Server Pools**.
Step 6 Click the row in the table for the pool that you want to assign to a Cisco UCS Director group.
Step 7 Click **Assign Group**.
Step 8 On the **Select Group** screen, do the following:
a) From the **Group** drop-down list, choose the Cisco UCS Director group to which you want to assign this server pool.
b) In the **Label** field, enter a label to identify this server pool.
c) Click **Submit**.

Unassigning a Server Pool from a Cisco UCS Director Group

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Organizations**.
Step 4 Click the organization that contains the pool you want to unassign and then click **View Details**.
Step 5 Click **Server Pools**.
Step 6 On the **Server Pool** page, click the row for the pool that you want to unassign from a Cisco UCS Director group and then click **View Details**.
Step 7 Click **UCS Servers**.
Step 8 Click the row for the server that you want to unassign.
Step 9 From **More Actions** drop-down menu, choose **Unassign Group**.
Step 10 On the **Unassign Group** screen, click **Unassign**.

Management IP Pool

A management IP pool is a collection of external IP addresses. Each block of IP addresses in the management IP pool is reserved for external access that terminates in the CIMC (Cisco Integrated Management Controller) on a server.

All IP addresses in the management IP pool must be in the same subnet as the IP address of the fabric interconnect.

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

Adding an IP Address Block to the Management IP Pool

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

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Management IP Pool**.

Step 4 Click **Add**.

Step 5 On the **Create Block of IP Addresses** screen, complete the following fields:

Name	Description
From field	The first IP address in the block.
Size field	The number of IP addresses in the pool.
Subnet Mask field	The subnet mask associated with the IP addresses in the block. This must be the same subnet mask as the fabric interconnect.
Default Gateway field	The default gateway associated with the IP addresses in the block.

Step 6 Click **Submit**.

Boot Policy

The Cisco UCS Manager enables you to create a boot policy for blade servers, rack servers, and modular servers.

The Cisco UCS Manager boot policy overrides the boot order in the BIOS setup menu and determines the following:

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

For example, you can 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 can either create a named boot policy to associate with one or more service profiles, or create a boot policy for a specific service profile. A boot policy must be included 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, Cisco UCS Manager applies the default boot policy.

Note Changes to a boot policy might be propagated to all servers created with an updating service profile template that includes that boot policy. Re-association of the service profile with the server to rewrite the boot order information in the BIOS is automatically triggered.

You can also specify the following for the boot policy:

- Local LUN name. The name specified is the logical name in the storage profile, not the deployed name. For modular servers, you can specify both a primary and secondary name. For other servers, specify only a primary name. Specifying a secondary name results in a configuration error.
- Specific JBOD disk number for booting from JBOD disks. This is not supported for the Modular servers.
- Any LUN for backward compatibility; however, we do not recommend this. Other devices must not have bootable images to ensure a successful boot.

UEFI Boot Mode

Unified Extensible Firmware Interface (UEFI) is a specification that defines a software interface between an operating system and platform firmware. Cisco UCS Manager uses UEFI to replace the BIOS firmware interfaces. This allows the BIOS to run in UEFI mode while still providing legacy support.

You can choose either legacy or UEFI boot mode when you create a boot policy. Legacy boot mode is supported for all Cisco UCS servers. UEFI boot mode is supported only on M3 and higher servers, and allows you to enable UEFI secure boot mode.

UEFI PXE boot is supported with all Cisco VIC adapters on Cisco UCS rack servers integrated with Cisco UCS Manager Release 2.2(4) and later releases. Beginning with Cisco UCS Manager Release 2.2(1), UEFI PXE boot is supported on all Cisco blade servers.

The following limitations apply to the UEFI boot mode:

- UEFI boot mode is not supported with the following combinations:
  - Gen-3 Emulex and QLogic adapters on Cisco UCS blade and rack servers integrated with Cisco UCS Manager.
  - iSCSI boot for all adapters on Cisco UCS rack servers integrated with Cisco UCS Manager.
- If you want to use UEFI boot mode with two iSCSI LUNs, you must manually specify a common iSCSI initiator name in the service profile that is applied to both underlying iSCSI eNICs rather than allowing Cisco UCS Manager to select the name from an IQN suffix pool. If you do not supply a common name, Cisco UCS Manager will not be able to detect the second iSCSI LUN.
- You cannot mix UEFI and legacy boot mode on the same server.
- The server will boot correctly in UEFI mode only if the boot devices configured in the boot policy have UEFI-aware operating systems installed. If a compatible OS is not present, the boot device is not displayed on the **Actual Boot Order** tab in the **Boot Order Details** area.
- In some corner cases, the UEFI boot may not succeed because the UEFI boot manager entry was not saved correctly in the BIOS NVRAM. You can use the UEFI shell to enter the UEFI boot manager entry manually. This situation could occur in the following situations:

- If a blade server with UEFI boot mode enabled is disassociated from the service profile, and the blade is manually powered on using the **Equipment** tab or the front panel.
- If a blade server with UEFI boot mode enabled is disassociated from the service profile, and a direct VIC firmware upgrade is attempted.
- If a blade or rack server with UEFI boot mode enabled is booted off SAN LUN, and the service profile is migrated.

You can create UEFI boot parameters in Cisco UCS Manager. UEFI Boot Parameters, on page 108 provides more information.

UEFI Secure Boot

Cisco UCS Manager supports UEFI secure boot on Cisco UCS B-Series M3 and M4 Blade servers, Cisco UCS C-Series M3 and M4 Rack servers, and Cisco UCS S-Series M4 Rack servers. When UEFI secure boot is enabled, all executables, such as boot loaders and adapter drivers, are authenticated by the BIOS before they can be loaded. To be authenticated, the images must be signed by either the Cisco Certificate Authority (CA) or a Microsoft CA.

The following limitations apply to UEFI secure boot:

- UEFI boot mode must be enabled in the boot policy.
- The Cisco UCS Manager software and the BIOS firmware must be at Release 2.2 or greater.

Note UEFI boot mode is supported on Cisco UCS C-Series and S-Series rack servers beginning with Release 2.2(3a).

- User-generated encryption keys are not supported.
- UEFI secure boot can only be controlled by Cisco UCS Manager.
- If you want to downgrade to an earlier version of Cisco UCS Manager, and you have a server in secure boot mode, you must disassociate, then re-associate the server before downgrading. Otherwise, server discovery is not successful.

UEFI Boot Parameters

UEFI boot mode for servers is dependent on information that is stored on the platform hardware. The boot entry, which contains information about the UEFI OS boot loader, is stored in the BIOS flash of the server. In Cisco UCS Manager releases earlier than Release 2.2(4), when a service profile is migrated from one server to another server, the boot loader information is not available on the destination server. Hence, the BIOS cannot load the boot loader information for the server to boot in UEFI boot mode.

Cisco UCSM Release 2.2(4) introduces UEFI boot parameters to provide the BIOS with information about the location of the UEFI OS boot loader on the destination server from where the BIOS loads it. Now, the server can use the boot loader information and boot in UEFI boot mode.

SAN Boot

You can configure a boot policy to boot one or more servers from an operating system image on the SAN. The boot policy can include a primary and a secondary SAN boot. If the primary boot fails, the server attempts to boot from the secondary.

Cisco recommends using 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 same operating system image. Therefore, the new server appears as the same server to the network.

To use a SAN boot, ensure that the following is configured:

- The Cisco UCS domain must be able to communicate with the SAN storage device that hosts the operating system image.
- A boot target LUN (Logical Unit Number) on the device where the operating system image is located.

Note SAN boot is not supported on Gen-3 Emulex adapters on Cisco UCS blade and rack servers.

Creating a SAN Boot Policy

Tip We recommend that the boot order in a boot policy include either a local disk or a SAN LUN, but not both, to avoid the possibility of the server booting from the wrong storage type. If you configure a local disk and a SAN LUN for the boot order storage type and the operating system or logical volume manager (LVM) is configured incorrectly, the server might boot from the local disk rather than the SAN LUN.

For example, on a server with Red Hat Linux installed, where the LVM is configured with default LV names and the boot order is configured with a SAN LUN and a local disk, Linux reports that there are two LVs with the same name and boots from the LV with the lowest SCSI ID, which could be the local disk.

Before You Begin

If you are creating a boot policy that boots the server from a SAN LUN and you require reliable SAN boot operations, we recommend that you first remove all local disks from servers associated with a service profile that includes the boot policy.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click **Boot Policies**.

Step 6 Click **Add**.

Step 7 On the **Add Boot Policy** screen, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Description field	A description for the policy.
Reboot on Order Change check box	If checked, reboots all servers that use this boot policy after you change the boot order. If this check box is checked and if CD-ROM or Floppy is the last device in the boot order, deleting or adding the device does not directly affect the boot order and the server does not reboot.
Enforce vNIC/vHBA Name check box	If checked, a configuration error is displayed if one or more of the vNICs, vHBAs, or iSCSI vNICs listed in the Boot Order table matches the server configuration in the service profile. If not checked, the policy uses the vNICs, vHBAs, or iSCSI vNICs (as appropriate for the boot option) from the server configuration in the service profile. It does not report whether the vNICs, vHBAs, or iSCSI vNICs specified in the boot policy match the server configuration in the service profile.
Boot Mode drop-down list	The boot mode for the servers that use this boot policy. It can be one of the following: • **Legacy** • **UEFI** With this option, you can specify second-level boot devices and you can enable the secure boot option.
Boot Security check box	(*Displays only when* **UEFI** *is selected as the boot mode*.) Enables the secure boot option for the servers that use this boot policy.

Step 8 In the **Add Boot Device** area, check **Add SAN Boot** and enter the additional parameters, including the following:

- In the **Primary vHBA** field, enter the name of the vHBA that you want to use as the first address defined for the SAN boot location.
- In the **Secondary vHBA** field, enter the name of the vHBA that you want to use as the second address defined for the SAN boot location.
- If either or both of the primary and secondary vHBAs points to a bootable SAN image, check the appropriate **Add SAN Boot Target** box for that vHBA and complete the following fields:

Name	Description
Primary Boot Target LUN field	The LUN that corresponds to the location of the boot image.
Primary Boot Target WWPN field	The WWPN that corresponds to the location of the boot image.
Secondary Boot Target LUN field	The LUN that corresponds to the location of the boot image.
Secondary Boot Target WWPN field	The WWPN that corresponds to the location of the boot image.

Step 9 Check **Add iSCSI Boot**, and enter additional parameters, including the following:

- In the **Add Primary iSCSI vNIC** field, enter the name of the iSCSI vNIC that you want to use as the first address defined for the boot location.
- In the **Add Secondary iSCSI vNIC** field, enter the name of the iSCSI vNIC that you want to use as the second address defined for the boot location.

Step 10 Click **Submit**.

LAN Boot

You can configure a boot policy to boot one or more servers from a centralized provisioning server on the LAN. A LAN (or PXE) boot is frequently used to install operating systems on a server from that LAN server.

You can add more than one type of boot device to a LAN boot policy. For example, you could add a local disk or virtual media boot as a secondary boot device.

Creating a LAN Boot Policy

You can add more than one type of boot device to a boot policy. For example, you could add a local disk boot as a secondary boot device.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click **Boot Policies**.

Step 6 Click **Add**.

Step 7 On the **Add Boot Policy** screen, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Description field	A description for the policy.
Reboot on Order Change check box	If checked, reboots all servers that use this boot policy after you change the boot order. If this check box is checked and if CD-ROM or Floppy is the last device in the boot order, deleting or adding the device does not directly affect the boot order and the server does not reboot.
Enforce vNIC/vHBA Name check box	If checked, a configuration error is displayed if one or more of the vNICs, vHBAs, or iSCSI vNICs listed in the Boot Order table matches the server configuration in the service profile. If not checked, the policy uses the vNICs, vHBAs, or iSCSI vNICs (as appropriate for the boot option) from the server configuration in the service profile. It does not report whether the vNICs, vHBAs, or iSCSI vNICs specified in the boot policy match the server configuration in the service profile.
Boot Mode drop-down list	The boot mode for the servers that use this boot policy. It can be one of the following: • **Legacy** • **UEFI** With this option, you can specify second-level boot devices and you can enable the secure boot option.

Name	Description
Boot Security check box	(*Displays only when* **UEFI** *is selected as the boot mode*.) Enables the secure boot option for the servers that use this boot policy.

Step 8 On the **Add Local Device** area, choose from the following options:

Name	Description
Add Local Disk check box	Adds local disk to the boot policy.
Add Local LUN check box	Adds local LUN to the boot order.
Add SD Card check box	Adds SD Card to the boot order.
Add Internal USB check box	Adds Internal USB to the boot order.
Add External USB check box	Adds External USB to the boot order.
Add CD ROM check box	Adds CD ROM to the boot policy.
Add Local CD/DVD check box	Adds Local CD/DVD to the boot order.
Add Remote CD/DVD check box	Adds Remote CD/DVD to the boot policy.
Add Floppy Disk check box	Adds Floppy Disk to the boot policy.
Add Local Floppy Disk check box	Adds local floppy disk to the boot order.
Add Remote Floppy Disk check box	Adds remote floppy disk to the boot order.

Step 9 In the **Add Boot Device** area, check **Add LAN Boot** and enter the additional parameters, including the following: .

- In the **Primary vNIC** field, enter the name of the vNIC that you want to use as the first address defined for the LAN boot location.
- In the **Secondary vNIC** field, enter the name of the vNIC that you want to use as the second address defined for the LAN boot location.

Step 10 In the **Add Boot Device** area, check **Add iSCSI Boot**, and enter the additional parameters, including the following:

- In the **Primary iSCSI vNIC** field, enter the name of the vNIC that you want to use as the first address defined for the LAN boot location.
- In the **Secondary iSCSI vNIC** field, enter the name of the vNIC that you want to use as the second address defined for the LAN boot location.

Step 11 Click **Submit**.

Local Disk Boot

If a server has a local drive, you can configure a boot policy to boot the server from that device or from any of the following local devices:

- Local hard disk drive
- SD card
- Internal USB
- External USB

Creating a Local Disk Boot Policy

You can add more than one type of boot device to a boot policy. For example, you could add a local disk boot as a secondary boot device.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click **Boot Policies**.

Step 6 Click **Add**.

Step 7 On the **Add Boot Policy** screen, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Description field	A description for the policy.
Reboot on Order Change check box	If checked, reboots all servers that use this boot policy after you change the boot order. If checked and if CD-ROM or Floppy is the last device in the boot order, deleting or adding the device does not directly affect the boot order and the server does not reboot.

Name	Description
Enforce vNIC/vHBA Name check box	If checked, a configuration error is displayed if one or more of the vNICs, vHBAs, or iSCSI vNICs listed in the Boot Order table matches the server configuration in the service profile. If not checked, the policy uses the vNICs, vHBAs, or iSCSI vNICs (as appropriate for the boot option) from the server configuration in the service profile. It does not report whether the vNICs, vHBAs, or iSCSI vNICs specified in the boot policy match the server configuration in the service profile.
Boot Mode drop-down list	The boot mode for the servers that use this boot policy. It can be one of the following: • **Legacy** • **UEFI** With this option, you can specify second-level boot devices and you can enable the secure boot option.
Boot Security check box	Enables the secure boot option for the servers that use this boot policy. This option is visible only when UEFI is selected as the boot mode.

Step 8 In the **Add Local Device** area, check the **Add Local Disk** check box.
There are more secondary options such as adding local LUN, SD card, CD ROM, internal and external USB devices as local boot devices. If you select the **Add Local Disk** check box, then you cannot select any of these secondary devices. If you select any of these local devices, then you cannot select the parent option of adding a local disk.

Step 9 Click **Submit**.

Virtual Media Boot

You can configure a boot policy to boot one or more servers from a virtual media device that is accessible from the server. A virtual media device mimics the insertion of a physical CD/DVD disk (read-only) or floppy disk (read-write) into a server. This type of server boot is typically used to manually install operating systems on a server.

Creating a Virtual Media Boot Policy

You can add more than one type of boot device to a boot policy. For example, you could add a local disk boot as a secondary boot device.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click **Boot Policies**.

Step 6 Click **Add**.

Step 7 On the **Add Boot Policy** screen, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Description field	A description for the policy.
Reboot on Order Change check box	If checked, reboots all servers that use this boot policy after you change the boot order. If this check box is checked and if CD-ROM or Floppy is the last device in the boot order, deleting or adding the device does not directly affect the boot order and the server does not reboot.
Enforce vNIC/vHBA Name check box	If checked, a configuration error is displayed if one or more of the vNICs, vHBAs, or iSCSI vNICs listed in the Boot Order table matches the server configuration in the service profile. If not checked, the policy uses the vNICs, vHBAs, or iSCSI vNICs (as appropriate for the boot option) from the server configuration in the service profile. It does not report whether the vNICs, vHBAs, or iSCSI vNICs specified in the boot policy match the server configuration in the service profile.
Boot Mode drop-down list	The boot mode for the servers that use this boot policy. It can be one of the following: • **Legacy** • **UEFI** With this option, you can specify second-level boot devices and you can enable the secure boot option.

Name	Description
Boot Security check box	Enables the secure boot option for the servers that use this boot policy. This option is visible only when UEFI is selected as the boot mode.

Step 8 In the **Add Boot Device** area, check one or both of the following options to select the vMedia device to add to the boot policy:

- **Add CIMC Mounted CD/DVD**
- **Add CIMC Mounted HDD**

Step 9 Click **Submit**.

Creating a vMedia Policy and vMount

vMedia enables dynamic mapping of an external image file to the server's CIMC. If a vMedia file is mapped as a CDD, then the image file presents itself as a CD-ROM image. vMedia can be referenced as a device in a Boot Policy, from which a server attempts to boot.

vMedia policies are bound to Service Profiles (SPs). Any given SP can have only one vMedia policy active at any given time. However, the policy can include one or more vMedia Mount.

Note Changing the vMedia Policy for a service profile does **not** cause service profile reconfiguration, reboot, or service interruption.

Before You Begin

Make sure that you have the required minimum version of Cisco UCS Manager, the BIOS, and CIMC. See Cisco UCS Director Compatibility Matrix.

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Organizations**.
Step 4 Choose the organization that you want to update and click **View Details**.
Step 5 Click **vMedia Policy**.
Step 6 Click **Add**.
Step 7 On the **Add vMedia Policy** screen, enter a name and description for the policy.
Step 8 From the **Retry on Mount Failure** drop-down list, choose one of the following to specify a retry mode:

- **Yes—**If you choose this option, the remote server continues to try mounting the vMedia until the operation is successful or until you disable this option.
- **No—**If you choose this option, the remote server does not try to mount the vMedia again if there is a mount failure.

Step 9 Expand **vMedia Mount Points**, and click **Add** to create a new vMedia mount using the following steps:

a) Click **Add**.

b) On the **Add Entry to vMedia Mount Points** screen, complete the required fields, including the following:

- **Device Type—**Choose one of the following options: HDD, or CDD. For each vMedia Policy, you can create a maximum of two vMedia mounts, one for each device type.
- **Mount Name—**Enter a unique name for the vMedia mount.
- **Description—**Enter a description of the vMedia mount. You can enter up to 510 characters.
- **Protocol—**Choose the network access protocol to use when communicating with the mounted remote server. Supported protocols are: HTTPS, HTTP, CIFS, or NFS. After you choose the type, enter the additional parameters for that protocol type.
  - If you chose **HTTPS** as the protocol, enter the **User Name** and **Password** to log in to the remote server.
  - If you chose **HTTP** as the protocol, enter the **User Name** and **Password** to log in to the remote server.
  - If you chose **CIFS** protocol, choose an **Authentication protocol** to use when communicating with the mounted remote server. If you do not choose an authentication protocol, it is set to Default.

    (Optional): Enter a **User Name** and **Password** to log in to the remote server.
  - If you chose **NFS** protocol, no additional parameters are required.
- **Remote Server Host Name/IP Address—**Enter the hostname or IP address of the location where the backup file is going to be stored. This can be a server, storage array, local drive, or any read/write media that the fabric interconnect can access through the network.

  Note If you use a hostname, configure the Cisco UCS Domain to use a DNS server. The DNS name can be used when an inband network is configured for that server.
- **Absolute Remote Path—**Enter the full path to the remote vMedia file.

  Note If the selected protocol is CIFS, then use forward slashes in the path.
- **Generate File Name from Service Profile Name—**Choose one of the following options:
  - **None—**If you choose this option, enter a **Remote File Name** that the vMedia policy must use.
  - **Service-Profile-Name—**If you choose this option, the service profile name is used as the image name.

c) Click **Submit**.

Step 10 Click **Submit**.

iSCSI Boot

iSCSI boot enables a server with a virtual interface card (VIC adapter) to boot its operating system from an iSCSI target machine located remotely over a network. Cisco UCS Director supports iSCSI boot with the following storage:

- EMC VNX
- NetApp ONTAP
- NetApp Data Fabric Manager (DFM)
- NetApp C-Mode

When you configure iSCSI boot in Cisco UCS Director, you first configure iSCSI boot for Cisco UCS and then configure the iSCSI boot workflow for Cisco UCS Director.

For more information about iSCSI boot within Cisco UCS, including guidelines for implementing it, see the Cisco UCS Manager configuration guides.

Prerequisites for iSCSI Boot

The following prerequisites must be met before you configure iSCSI boot:

- The Cisco UCS domain, including all firmware, must be at Cisco UCS, Release 2.0(1m) or later.
- The Cisco UCS servers must have a supported VIC adapter, such as the following:
  - Cisco UCS M81KR Virtual Interface Card
  - Cisco UCS VIC-1240 Virtual Interface Card
  - Cisco UCS VIC-1280 Virtual Interface Card
- The storage array must be licensed for iSCSI boot.
- The array side LUN masking and network interface must be properly configured with access to the VLAN that the iSCSI traffic uses.
- The appropriate aggregates and volumes must be created in the storage array.
- The uplink ports from the fabric interconnects must also have access to the iSCSI traffic VLAN.
- The server operating system (OS) must be iSCSI Boot Firmware Table (iBFT) compatible.

Configuring iSCSI Boot

Note This procedure provides a high-level overview of the steps required to configure iSCSI boot. Ensure that you complete all of the following steps.

Procedure

	Command or Action	Purpose
Step 1	Create the required VLANs to carry iSCSI traffic.	See Creating a VLAN, on page 48.
Step 2	Create one or more MAC pools for the servers within the appropriate organizations.	See Creating a MAC Pool, on page 55.
Step 3	Create one or more vNIC templates within the appropriate organizations.	See Creating a vNIC Template, on page 65.
Step 4	Create a vNIC for fabric A and fabric B.	See Creating a vNIC, on page 69.
Step 5	Create a network policy that includes those vNICs.	See Creating a Network Policy, on page 74.
Step 6	Create a storage policy.	See Creating a Storage Policy, on page 92.
Step 7	Create one or more IQN pools within the appropriate organizations.	See Creating an IQN Pool, on page 121.
Step 8	Create one or more IP address blocks for the iSCSI IP Pool.	See Adding a Block of Addresses to the iSCSI IP Pool, on page 122.
Step 9	Create an initiator and target iSCSI authentication profile.	See Creating an iSCSI Authentication Profile, on page 123.
Step 10	Create one or more iSCSI adapter policies.	See Creating an iSCSI Adapter Policy, on page 124.
Step 11	Create an iSCSI boot workflow and add the required tasks to that workflow.	The following example shows the workflow to create an iSCSI boot workflow for NetApp ONTAP storage: **1** Example: Creating an iSCSI Boot Workflow, on page 125 **2** Adding a Task: Create Service Profile, on page 126 **3** Adding a Task: Add vNIC to Service Profile, on page 129 **4** Adding a Task: Add iSCSI vNIC to Service Profile, on page 130 **5** Adding a Task: Create Service Profile iSCSI Boot Policy, on page 131

	Command or Action	Purpose
		6 Adding a Task: Associate Service Profile, on page 133 **7** Adding a Task: Create Flexible Volume, on page 135 **8** Adding a Task: Create LUN, on page 136 **9** Adding a Task: Create Initiator Group, on page 138 **10** Adding a Task: Add an Initiator to Initiator Group, on page 139 **11** Adding a Task: Map LUN to Initiator Group, on page 140 **12** Adding a Task: Set Up PXE Boot, on page 141 **13** Adding a Task: Power On UCS Server, on page 143 **14** Adding a Task: Monitor PXE Boot, on page 143 **15** Adding a Task: Power Off UCS Server, on page 144 **16** Adding a Task: Modify Service Profile Boot Policy to Boot from iSCSI, on page 145 **17** Add a second Power On UCS Server task.

Creating an IQN Pool

An IQN pool is a collection of iSCSI Qualified Names (IQNs) for use as initiator identifiers by iSCSI vNICs in a Cisco UCS domain. IQN pool members are of the form *prefix*:*suffix*:*number*, where you can specify the prefix, suffix, and a block (range) of numbers. An IQN pool can contain more than one IQN block, with different number ranges and different suffixes, but sharing the same prefix.

Note Usually, the maximum IQN size (prefix + suffix + additional characters) is 223 characters. When using the Cisco UCS NIC M51KR-B adapter, limit the IQN size to 128 characters.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the pool and then click **View Details**.

Step 5 Click **IQN Pools**.

Step 6 Click **Add**.

Step 7 On the **Create IQN Pool** screen, complete the following fields to define Name and Description:

Name	Description
Name field	A unique name for the iSCSI Qualified Name (IQN) pool.
Description field	A user-defined description of the pool.
Prefix field	The prefix for any IQN blocks created for this pool.

Step 8 Click **Next**.

Step 9 On the **Add IQN Blocks** screen, do the following:

a) Click **Add**.

b) On the **Add Entry to IQN Pool Blocks** page, complete the following fields:

Name	Description
Suffix field	The suffix for this block of IQNs.
From field	The first suffix number in the block.
Size field	The number of suffixes in the block.

c) Click **Submit**.

Repeat this step until you have added all desired IQN pool blocks.

Step 10 Click **Submit**.

Adding a Block of Addresses to the iSCSI IP Pool

The iSCSI IP pool is a group of IP addresses that is reserved for iSCSI boot. This IP pool must not contain any IP addresses that have been assigned as static IP addresses for a server or service profile.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **iSCSI IP Pool**.

Step 4 Click **Add**.

Step 5 On the **Create Block of IP Addresses** screen, complete the following fields:

Name	Description
From field	The first IP address in the block.
Size field	The number of IP addresses in the pool.

Name	Description
Subnet Mask field	The subnet mask associated with the IP addresses in the block.
Default Gateway field	The default gateway associated with the IP addresses in the block.
Primary DNS field	The primary DNS server that this block of IP addresses must access.
Secondary DNS field	The secondary DNS server that this block of IP addresses must access.

Step 6 Click **Submit**.

Creating an iSCSI Authentication Profile

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Organizations**.
Step 4 Click the organization in which you want to create the policy and then click **View Details**.
Step 5 Click **iSCSI Auth Profiles**.
Step 6 Click **Add**.
Step 7 On the **iSCSI Authentication Profile** screen, complete the following fields:

Name	Description
Name field	A unique name for the iSCSI authentication profile.
User ID field	The user ID associated with this profile.
Password field	The password associated with this profile.
Confirm Password field	The password again for confirmation purposes.

Step 8 Click **Submit**.

Creating an iSCSI Adapter Policy

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click **iSCSI Adapter Policy**.

Step 6 Click **Add**.

Step 7 On the **iSCSI Adapter Policy** screen, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Connection Timeout field	The number of seconds to wait until Cisco UCS assumes that the initial sign-in has failed and the iSCSI adapter is unavailable. Enter an integer between 0 and 255. If you enter 0, Cisco UCS uses the value set in the adapter firmware (default: 15 seconds).
LUN Busy Retry Count field	The number of times to retry the connection if there is a failure during iSCSI LUN discovery. Enter an integer between 0 and 60. If you enter 0, Cisco UCS uses the value set in the adapter firmware (default: 15 seconds).
DHCP Timeout field	The number of seconds to wait before the initiator assumes that the DHCP server is unavailable. Enter an integer between 60 and 300 (default: 60 seconds).
Enable TCP Timestamp check box	Check this box if you want to use a TCP timestamp. With this setting, transmitted packets are given a time stamp of when the packet was sent so that the packet's round-trip time can be calculated, when needed. **Note** This option only applies to servers with the Cisco UCS NIC M51KR-B adapter.
HBA Mode check box	Check this box to enable HBA mode (also known as TCP offload). **Note** This option must only be enabled for servers with the Cisco UCS NIC M51KR-B adapter running the Windows operating system.
Boot to Target check box	Check this box to boot from the iSCSI target. **Note** This option only applies to servers with the Cisco UCS NIC M51KR-B adapter. It must be disabled until you have installed an operating system on the server.

Step 8 Click **Submit**.

Example: Creating an iSCSI Boot Workflow

This example shows how to create an iSCSI boot workflow for NetApp ONTAP. The steps for configuring the Cisco UCS components are the same for all types of storage.

Procedure

Step 1 Choose **Orchestration**.

Step 2 On the **Orchestration** page, click **Workflows**.

Step 3 Click **Add Workflow**.

Step 4 On the **Add Workflow** screen, complete the Workflow details.

Name	Description
Name field	A unique name for the workflow. We recommend that this name describe the purpose of the workflow.
Description field	A description for the workflow.
Workflow Context drop-down list	Choose the context in which the workflow is used. This can be one of the following: • **Any—**Allows the workflow to be used in any context. • **Selected VM—**Allows the workflow to be executed only when a VM is selected.
Save as Compound Task check box	If checked, the workflow is defined as a compound task.
Place in New Folder check box	The folder where you want to save the workflow. If you check this check box, enter a folder name in the **Folder Name** field.
Select Folder drop-down list	Choose the folder in which you want to save the workflow. This drop-down list is only visible if you do not check the **Place in New Folder** check box.

Step 5 Click **Next**.

Step 6 On the **Add User Inputs** page, do the following:

a) Click **Add**.

b) On the **Add User Inputs** screen, complete the following fields and then click **Submit**:
If you configure the workflow with the required user inputs, you can configure workflow tasks to prompt for certain values when the workflow is run.

Name	Description
Input Label field	The label assigned to the input.
Input Description field	A description for the input.
Input Type field	The type of input category.
Admin Input field	Input from the administrator based on the input type. The inputs are not required to be provided by the end user who executes the workflow. You can also prevent an end user from providing certain types.
Admin Input List field	The current administrator's list of inputs. The input order can be rearranged.
Admin Input Filter field	The administrator's input filter value used to define custom inputs based on a filter (static or dynamic). For example, you can filter on aggregate, volumes, and POD

Repeat this step if you want to add more user inputs.

Step 7 Click **Submit**.
If you created the workflow in a new folder, you might need to click **Refresh** to see that folder in the folder list.

What to Do Next

Add tasks to the empty workflow.

Adding a Task: Create Service Profile

This procedure assumes that you have created a workflow, as described in Example: Creating an iSCSI Boot Workflow, on page 125, and that you are already on the **Workflow** tab within Orchestration.

Procedure

Step 1 Choose **Orchestration**.

Step 2 On the **Orchestration** page, click **Workflows**.

Step 3 Click the row for the iSCSI workflow to which you want to add the task.

Step 4 From the **More Actions** drop-down list, choose **Workflow Designer**

Step 5 On the **Available Tasks** screen of the Workflow Designer, expand **Physical Compute Tasks** > **Cisco UCS Tasks**.

Step 6 Click the **Create UCS Service Profile** task, and then drag and drop the selected task onto the workflow designer window.

Step 7 In the **Task Information** screen, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details .

d) Click **Next**.

Step 8 In the **User Mapping Inputs** screen do the following:

a) If you want to be prompted to enter some of the configuration attributes for the service profile when the workflow is run, check one or more of the following check boxes and choose a user input:

Note To map user inputs, you must have added the user inputs with the appropriate permissions to the workflow.

- **Service Profile Name**
- **Description**
- **Organization**
- **Storage Policy**
- **Network Policy**
- **PXE Boot Policy**
- **Server Boot Policy**
- **IP Address**
- **Subnet Mask**
- **Default Gateway**
- **Server Power State**

b) Click **Next**.

Step 9 In the **Task Inputs** screen, do the following:

a) For those configuration attributes for which you did not choose to prompt for user input, complete the following fields:

- **Service Profile Name—**Required. Enter a unique name for the service profile.
- **Description—**Optional. Enter a description for the service profile.
- **Organization—**Required. Choose the organization in which you want to run the workflow and create the service profile. This option also chooses the Cisco UCS Manager account for the workflow.
- **UUID Assignment—**Required. Include this policy to specify the UUID for the server.
- **Storage Policy—**Required. Specify the storage policy that you created for iSCSI boot.
- **Network Policy—**Required. Specify the network policy
- **Placement Policy—**Optional. Include this policy if you want to specify the vNIC, vHBA, and vCon placement for the server.
- **PXE Boot Policy—**Optional. Include this policy if you want to have the server to perform a PXE boot. The secondary boot in this policy must be from a local disk or a SAN boot. If you do not include this policy, the server uses the server boot policy to determine the boot order.
- **Server Boot Policy—**Required. Include this policy to determine the server boot order.
- **BIOS Policy—**Optional. Include this policy if you want to change any of the default settings for the BIOS on the server.
- **IPMI Access Profile—**Optional. Include this policy if you want to be able to access the server through IPMI.
- **SOL Configuration Profile—**Optional. Include this policy if you want to be able to access the server through Serial over LAN.
- **Threshold Policy—**Optional. Include this policy to specify the thresholds for the server.
- **Scrub Policy—**Optional. Include this policy if you want to specify what happens to the local data and BIOS settings on a server during discovery and disassociation.
- **Host Firmware Policy—**Optional. Include this policy if you want to use a host firmware package to upgrade the server firmware.
- **Maintenance Policy—**Optional. Include this policy if you want to specify what happens when change that requires a server reboot is made to this service profile.
- **Power Control Policy—**Optional. Include this policy if the service profile is associated with a blade server and you want to specify the initial power allocation for the server.
- **Server Power State—**Required. Sets the power state that is applied to the server when it is associated with this service profile.

b) Click **Submit**.

Adding a Task: Add vNIC to Service Profile

This task adds a third vNIC to the service profile that serves as an overlay vNIC for the iSCSI vNIC.

Procedure

Step 1 Choose **Orchestration**.

Step 2 On the **Orchestration** page, click **Workflows**.

Step 3 Click the row for the iSCSI workflow to which you want to add the task.

Step 4 From the **More Actions** drop-down list, choose **Workflow Designer**

Step 5 On the **Available Tasks** screen of the Workflow Designer, expand **Physical Compute Tasks** > **Cisco UCS Tasks**.

Step 6 Click **Add vNIC to Service Profile** task, and then drag and drop the selected task onto the workflow designer window.

Step 7 In the **Task Information** screen, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details

d) Click **Next**.

Step 8 In the **User Mapping Inputs** screen, do the following:

a) If you want to be prompted to enter some of the configuration attributes for the vNIC when the workflow is run, check one or more of the following check boxes and choose a user input:

Note To map user inputs, you must have added the user inputs with the appropriate permissions to the workflow.

- **Service Profile—**Chooses an existing service profile to which you want to add the vNIC.
- **vNIC Name—**Adds an existing vNIC to the service profile.

b) Click **Next**.

Step 9 In the **Task Inputs** screen, do the following:

a) For those configuration attributes for which you did not choose to prompt for user input, complete the following fields:
Use this option if you want to create a new vNIC to add to the service profile.

- **Service Profile Name—**Required. Choose an existing service profile that is configured for iSCSI boot.
- **vNIC Name—**Required.

- **MAC Pool—**Required.
- **Fabric ID—**Required.
- **Enable Failover—**Required. Check this check box.
- **VLANs—**Required. Choose a VLAN you created to carry iSCSI traffic.
- **Set as Native VLAN—**Optional.
- **MTU—**Required. Enter a value between 1500 and 9000.
- **Pin Group—**Optional.
- **Adapter Policy—**Optional.
- **QoS Policy—**Optional.
- **Network Control Policy—**Optional.
- **Stats Threshold Policy—**Optional.

b) Click **Submit**.

Adding a Task: Add iSCSI vNIC to Service Profile

Procedure

Step 1 Choose **Orchestration**.

Step 2 On the **Orchestration** page, click **Workflows**.

Step 3 Click the row for the iSCSI workflow to which you want to add the task.

Step 4 From the **More Actions** drop-down list, choose **Workflow Designer**

Step 5 On the **Available Tasks** screen of the Workflow Designer, expand **Physical Compute Tasks** > **Cisco UCS Tasks**.

Step 6 Click **Add iSCSI vNIC to Service Profile** task, and then drag and drop the selected task onto the workflow designer window.

Step 7 On the **Task Information** screen, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details

d) Click **Next**.

Step 8 On the **User Mapping Inputs** screen, do the following:

a) If you want to be prompted to enter some of the configuration attributes for the vNIC when the workflow is run, check one or more of the following check boxes and choose a user input:

Note To map user inputs, you must have added the user inputs with the appropriate permissions to the workflow.

- **Service Profile—**Prompts for the service profile to which you want to add the vNIC.
- **iSCI vNIC Name—**Adds an existing iSCSI vNIC to the service profile.
- **Overlay vNIC Name—**Uses an existing overlay vNIC.
- **VLANs—**Uses existing VLANs.

b) Click **Next**.

Step 9 On the **Task Inputs** screen, do the following:

a) For those configuration attributes for which you did not choose to prompt for user input, complete the following fields:

- **Service Profile Name—**Required. Choose an existing service profile that is configured for iSCSI boot.
- **iSCSI vNIC Name—**Required.
- **Overlay vNIC—**Required. Choose the third vNIC that you added to the service profile.
- **iSCSI Adapter Policy—**Optional.
- **MAC Pool—**DO NOT select a MAC Pool.
- **VLANs—**Required. Choose a VLAN you created to carry iSCSI traffic.

b) Click **Submit**.

Adding a Task: Create Service Profile iSCSI Boot Policy

Procedure

Step 1 Choose **Orchestration**.

Step 2 On the **Orchestration** page, click **Workflows**.

Step 3 Click the row for the iSCSI workflow to which you want to add the task.

Step 4 From the **More Actions** drop-down list, choose **Workflow Designer**

Step 5 On the **Available Tasks** screen of the Workflow Designer, expand **Physical Compute Tasks** > **Cisco UCS Tasks**.

Step 6 Click the **Create Service Profile iSCSI Boot Policy** task, and then drag and drop the selected task onto the workflow designer window.

Step 7 On the **Task Information** screen, do the following:

a) Enter a task name and comment to identify the task.
b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:
   - Check the **Retry Execution** check box.
   - From the **Retry Count** drop-down list, choose the number of retry attempts.
   - In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.
c) Review the task details
d) Click **Next**.

Step 8 In the **User Mapping Inputs** screen, do the following:

a) If you want to be prompted to enter some of the configuration attributes for the policy when the workflow is run, check one or more of the following check boxes and choose a user input:

Note To map user inputs, you must have added the user inputs with the appropriate permissions to the workflow.

- **Service Profile—**Uses an existing service profile to create the iSCSI boot policy.
- **Primary vNIC—**Adds an existing vNIC as the primary vNIC for a LAN boot.
- **Secondary vNIC—**Adds an existing vNIC as the secondary vNIC for a LAN boot.
- **Primary iSCSI vNIC—**Adds an existing iSCSI vNIC as the primary iSCSI vNIC.
- **Select Filer—**Allows you to choose an existing Filer or vFiler where the LUN was created.
- **iSCSI Target Name—**Allows you to specify the target node name for the filer.
- **IPv4 Address—**Allows you to specify the iSCSI-enabled VLAN IP address on the filer.

b) Click **Next**.

Step 9 On the **Task Inputs** screen, do the following:

a) For those configuration attributes for which you did not choose to prompt for user input, complete the following fields:

Name	Description
Service Profile button	Choose an existing service profile that is configured for iSCSI boot.
Add LAN Boot check box	Check this check box to add a LAN boot to the policy.
Primary vNIC field	The primary vNIC that you want to use for the LAN boot. This field is only visible if you check the **Add LAN Boot** check box.
Secondary vNIC field	The secondary vNIC that you want to use for the LAN boot. This field is only visible if you check the **Add LAN Boot** check box.
Set Boot Parameters check box	Check this check box to configure the iSCSI boot parameters. The following fields are only visible if you check this check box.

Name	Description
Set iSCSI Boot Parameters area	
Authentication Profile button	Choose an iSCSI authentication profile.
Initiator Name Assignment button	Choose the IQN pool from which initiators are assigned for the iSCSI vNIC.
Initiator IP Address Policy drop-down list	Choose how the IP address is assigned to the iSCSI vNIC. By default, the IP address is assigned from the iSCSI IP pool.
Create iSCSI Static Target area	
Select Filer button	Choose the filer, such as a NetApp filer or vFiler, where the LUN associated with the target is created.
iSCSI Target Name drop-down list	Choose the target node for the filer.
Port field	The port ID for the connection to the storage array.
Authentication Profile button	Choose the associated iSCSI authentication profile.
IPv4 Address drop-down list	Choose the iSCSI-enabled VLAN IP address on the filer.
LUN ID field	The LUN identifier in the iSCSI target.

b) Click **Submit**.

Adding a Task: Associate Service Profile

This procedure assumes that you have created a workflow, as described in Example: Creating an iSCSI Boot Workflow, on page 125, and that you are already on the **Workflow** tab within Orchestration.

Procedure

Step 1 Choose **Orchestration**.

Step 2 On the **Orchestration** page, click **Workflows**.

Step 3 Click the row for the iSCSI workflow to which you want to add the task.

Step 4 From the **More Actions** drop-down list, choose **Workflow Designer**

Step 5 On the **Available Tasks** screen of the Workflow Designer, expand **Physical Compute Tasks** > **Cisco UCS Tasks**.

Step 6 Click the **Associate UCS Service Profile** task, and then drag and drop the selected task onto the workflow designer window.

Step 7 In the **Task Information** screen, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details

d) Click **Next**.

Step 8 In the **User Mapping Inputs** screen of the **Add Task (Associate UCS Service Profile)** wizard, do the following:

a) If you want to be prompted to enter some of the configuration attributes when the workflow is run, check one or more of the following check boxes and choose a user input:

Note To map user inputs, you must have added the user inputs with the appropriate permissions to the workflow.

- **Service Profile—**Chooses the service profile that you want to associate with a server.
- **Server—**Chooses the server to which you want to associate the service profile.
- **Server Pool—**Chooses the server pool that contains the type of server to which you want to associate the service profile.

b) Click **Next**.

Step 9 In the **Task Inputs** screen of the **Add Task (Associate UCS Service Profile)** wizard, do the following:

a) For those configuration attributes for which you did not choose to prompt for user input, complete the following fields:

- **Service Profile—**Required. Choose an existing service profile that is configured for iSCSI boot.
- **Server Selection Scope—**Required. Choose how you want to select the server.
- **Server—**Required if you chose a scope of **Include Servers**. Choose the server to which you want to associate the service profile.

- **Server Pool—**Required if you chose a scope of **Include Server Pools**. Choose the server pool that contains the type of server to which you want to associate the service profile.

b) Click **Submit**.

Adding a Task: Create Flexible Volume

We recommend that you create a volume of at least 12 GB for an ESXi installation.

Procedure

Step 1 Choose **Orchestration**.

Step 2 On the **Orchestration** page, click **Workflows**.

Step 3 Click the row for the iSCSI workflow to which you want to add the task.

Step 4 From the **More Actions** drop-down list, choose **Workflow Designer**

Step 5 On the **Available Tasks** screen of the Workflow Designer,expand **Physical Storage Tasks** > **NetApp Tasks** > **NetApp ONTAP Tasks**.

Step 6 Click the **Create Flexible Volume** task, and then drag and drop the selected task onto the workflow designer window.

Step 7 In the **Task Information** screen of the **Add Task (Create Flexible Volume)** wizard, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details

d) Click **Next**.

Step 8 In the **User Mapping Inputs** screen of the **Add Task (Create Flexible Volume)** wizard, do the following:

a) If you want to be prompted to enter some of the configuration attributes for the volume when the workflow is run, check one or more of the following check boxes and choose a user input:

Note To map user inputs, you must have added the user inputs with the appropriate permissions to the workflow.

- **Aggregate Name—**Chooses the aggregate where you want to create the volume.
- **Volume Name—**Assigns a name to the volume.
- **Volume Size—**Specifies the size of the volume as an integer.
- **Volume Size Units—**Specifies the unit of size, such as MB, GB, or TB.
- **Space Guarantee—**Specifies the type of space guarantee.

- **Snapshot Size—**Specifies the percentage of the volume snapshot.

b) Click **Next**.

Step 9 In the **Task Inputs** screen of the **Add Task (Create Flexible Volume)** wizard, do the following:

a) For those configuration attributes for which you did not choose to prompt for user input, complete the following fields:

- **Aggregate Name—**Choose the aggregate where you want to create the volume.
- **Volume Name—**Enter a unique name for the volume.
- **Volume Size—**Enter the size of the volume as an integer. You must
- **Volume Size Units—**Choose the unit of size.
- **Space Guarantee—**Choose the type of space guarantee.
- **Snapshot Size—**Enter the percentage of the volume snapshot.
- **Security Style NTFS—**Do not check this check box.
- **NFS Export—**Do not check this check box.

b) Click **Submit**.

Adding a Task: Create LUN

We recommend that you create a LUN of at least 10 GB for an ESXi installation.

Procedure

Step 1 Choose **Orchestration**.

Step 2 On the **Orchestration** page, click **Workflows**.

Step 3 Click the row for the iSCSI workflow to which you want to add the task.

Step 4 From the **More Actions** drop-down list, choose **Workflow Designer**

Step 5 On the **Available Tasks** screen of the Workflow Designer, expand **Physical Storage Tasks** > **NetApp Tasks** > **NetApp ONTAP Tasks**.

Step 6 Click **Create LUN** task, and then drag and drop the selected task onto the workflow designer window.

Step 7 In the **Task Information** screen, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details
d) Click **Next**.

Step 8 In the **User Mapping Inputs** screen, do the following:

a) If you want to be prompted to enter some of the configuration attributes for the volume when the workflow is run, check one or more of the following check boxes and choose a user input:

Note To map user inputs, you must have added the user inputs with the appropriate permissions to the workflow.

- **Volume Name—**Specifies the volume where you want to create the LUN.
- **LUN Name—**Specifies the name of the LUN you want to create.
- **OS Type—**Specifies the type of OS for the LUN.
- **LUN Size—**Specifies the size of the LUN as an integer.
- **LUN Size Units—**Specifies the unit of size, such as MB, GB, or TB.

b) Click **Next**.

Step 9 In the **Task Inputs** screen, do the following:

a) For those configuration attributes for which you did not choose to prompt for user input, complete the following fields:

- **Volume Name—**Select the volume where you want to create the LUN.
- **LUN Name—**Enter the name of the LUN you want to create.
- **OS Type—**Choose the type of OS for the LUN.
- **LUN Size—**Enter the size of the LUN as an integer.
- **LUN Size Units—**Choose the unit of size, such as MB, GB, or TB.
- **Reserve Space—**Check this check box if you want to reserve the space for the LUN.

b) Click **Submit**.

Adding a Task: Create Initiator Group

Procedure

Step 1 Choose **Orchestration**.

Step 2 On the **Orchestration** page, click **Workflows**.

Step 3 Click the row for the iSCSI workflow to which you want to add the task.

Step 4 From the **More Actions** drop-down list, choose **Workflow Designer**

Step 5 On the **Available Tasks** screen of the Workflow Designer,expand **Physical Storage Tasks** > **NetApp Tasks** > **NetApp ONTAP Tasks**.

Step 6 Click the **Create Initiator Group** task, and then drag and drop the selected task onto the workflow designer window.

Step 7 In the **Task Information** screen, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details

d) Click **Next**.

Step 8 In the **User Mapping Inputs** screen of the **Add Task (Create Initiator Group)** wizard, do the following:

a) If you want to be prompted to enter some of the configuration attributes for the volume when the workflow is run, check one or more of the following check boxes and choose a user input:

Note To map user inputs, you must have added the user inputs with the appropriate permissions to the workflow.

- **Filer Identity Name—**Specifies the filer where you want to create the initiator group
- **Initiator Group Name—**Specifies the name of the initiator group you want to create.
- **Group Type—**Specifies iSCSI for the type of initiator group.
- **OS Type—**Specifies the type of OS for the initiators in the group.
- **Port Set—**Specifies the port set.

b) Click **Next**.

Step 9 In the **Task Inputs** screen of the **Add Task (Create Initiator Group)** wizard, do the following:

a) For those configuration attributes for which you did not choose to prompt for user input, complete the following fields:

- **Filer Identity Name—**Choose the filer where you want to create the initiator group
- **Initiator Group Name—**Enter the name of the initiator group you want to create.

- **Group Type—**Choose iSCSI for the type of initiator group.
- **OS Type—**Choose the type of OS for the initiators in the group.
- **Port Set—**Enter the port set.

b) Click **Submit**.

Adding a Task: Add an Initiator to Initiator Group

This procedure assumes that you have created a workflow, as described in Example: Creating an iSCSI Boot Workflow, on page 125, and that you are already on the **Workflow** tab within Orchestration.

Procedure

Step 1 In the left pane, expand the folder where the workflow is located and click the row for the iSCSI workflow to which you want to add the task.

Step 2 On the icon bar, click the purple drop-down list icon and choose **Workflow Designer**.

Step 3 In the **Available Tasks** pane of the Workflow Designer, expand **Physical Storage Tasks** > **NetApp Tasks** > **NetApp ONTAP Tasks**.

Step 4 Click the **Add an Initiator to Initiator Group** task, and then drag and drop the selected task onto the workflow designer window.

Step 5 In the **Task Information** screen of the **Add Task (Add an Initiator to Initiator Group)** wizard, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details

d) Click **Next**.

Step 6 In the **User Mapping Inputs** screen of the **Add Task (Add an Initiator to Initiator Group)** wizard, do the following:

a) If you want to be prompted to enter some of the configuration attributes for the volume when the workflow is run, check one or more of the following check boxes and choose a user input:

Note To map user inputs, you must have added the user inputs with the appropriate permissions to the workflow.

- **Initiator Group Name—**Specifies the name of the initiator group to which you want to add an initiator.
- **Initiator Name—**Specifies the initiator you want to add to the group.

b) Click **Next**.

Step 7 In the **Task Inputs** screen of the **Add Task (Add an Initiator to Initiator Group)** wizard, do the following:

a) For those configuration attributes for which you did not choose to prompt for user input, complete the following fields:

- **Initiator Group Name—**Choose the initiator group to which you want to add an initiator.
- **Initiator Name—**Enter the initiator you want to add to the group. To add more than one initiator, separate the names with commas.
- **Force—**Check this check box if you want to forcibly add the initiator to the group.

b) Click **Submit**.

Adding a Task: Map LUN to Initiator Group

This procedure assumes that you have created a workflow, as described in Example: Creating an iSCSI Boot Workflow, on page 125, and that you are already on the **Workflow** tab within Orchestration.

Procedure

Step 1 In the left pane, expand the folder where the workflow is located and click the row for the iSCSI workflow to which you want to add the task.

Step 2 On the icon bar, click the purple drop-down list icon and choose **Workflow Designer**.

Step 3 In the **Available Tasks** pane of the Workflow Designer, expand **Physical Storage Tasks** > **NetApp Tasks** > **NetApp ONTAP Tasks**.

Step 4 Click the **Create Initiator Group** task, and then drag and drop the selected task onto the workflow designer window.

Step 5 In the **Task Information** screen of the **Add Task (Map LUN to Initiator Group)** wizard, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details

d) Click **Next**.

Step 6 In the **User Mapping Inputs** screen of the **Add Task (Map LUN to Initiator Group)** wizard, do the following:

a) If you want to be prompted to enter some of the configuration attributes for the volume when the workflow is run, check one or more of the following check boxes and choose a user input:

Note To map user inputs, you must have added the user inputs with the appropriate permissions to the workflow.

- **Filer Identity Name—**Specifies the filer for the initiator group.
- **Initiator Group Name—**Specifies the initiator group you want to map.
- **LUN ID—**Specifies the LUN that you want to map to the initiator group.
- **LUN Path—**Specifies the file path to the LUN.

b) Click **Next**.

Step 7 In the **Task Inputs** screen of the **Add Task (Map LUN to Initiator Group)** wizard, do the following:

a) For those configuration attributes for which you did not choose to prompt for user input, complete the following fields:

- **Filer Identity Name—**Choose the filer for the initiator group.
- **Initiator Group Name—**Choose the initiator group you want to map.
- **LUN ID—**Check this box to specify the LUN that you created earlier in the workflow.
- **LUN Path—**Choose the file path to the LUN.

b) Click **Submit**.

Adding a Task: Set Up PXE Boot

This procedure assumes that you have created a workflow, as described in Example: Creating an iSCSI Boot Workflow, on page 125, and that you are already on the **Workflow** tab within Orchestration.

Procedure

Step 1 In the left pane, expand the folder where the workflow is located and click the row for the iSCSI workflow to which you want to add the task.

Step 2 On the icon bar, click the purple drop-down list icon and choose **Workflow Designer**.

Step 3 In the **Available Tasks** pane of the Workflow Designer, expand **Network Services Tasks**.

Step 4 Click the **Setup PXE Boot** task, and then drag and drop the selected task onto the workflow designer window.

Step 5 In the **Task Information** screen of the **Add Task (Setup PXE Boot)** wizard, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details

d) Click **Next**.

Step 6 In the **User Mapping Inputs** screen of the **Add Task (Setup PXE Boot)** wizard, do the following:

a) If you want to be prompted to enter some of the configuration attributes for the volume when the workflow is run, check one or more of the following check boxes and choose a user input.

Note To map user inputs, you must have added the user inputs with the appropriate permissions to the workflow.

- **Server MAC Address—**Specifies the MAC address for the server you want to PXE boot. If you want to set up multiple servers, separate the entries with commas.
- **Server IP Address—**Specifies the IP address for the server. If you want to set up multiple servers, place a hyphen (-) between the first and last IP addresses, or separate the entries with commas.
- **Server Net Mask—**Specifies the net mask used to PXE boot.
- **Server Host Name—**Specifies the host name for the server.
- **Server Gateway—**Specifies the gateway used to PXE boot.
- **Root Password—**Specifies the root password for the server.
- **Timezone—**Specifies the time zone for the server.

b) Click **Next**.

Step 7 In the **Task Inputs** screen of the **Add Task (Setup PXE Boot)** wizard, do the following:

a) For those configuration attributes for which you did not choose to prompt for user input, complete the following fields:

- **OS Type—**Choose the OS for the server.
- **Server MAC Address—**Enter the MAC address for the server you want to PXE boot. If you want to set up multiple servers, separate the entries with commas.
- **Server IP Address—**Enter the IP address for the server. If you want to set up multiple servers, place a hyphen (-) between the first and last IP addresses, or separate the entries with commas.
- **Server Net Mask—**Enter the net mask used to PXE boot.
- **Server Host Name—**Enter the host name for the server.
- **Server Gateway—**Enter the gateway used to PXE boot.
- **Server Name Server—**Enter the name server used to PXE boot.
- **Management VLAN—**Enter the VLAN used to PXE boot.
- **Root Password—**Enter the root password for the server.
- **Timezone—**Choose the time zone for the server.

b) Click **Submit**.

Adding a Task: Power On UCS Server

This procedure assumes that you have created a workflow, as described in Example: Creating an iSCSI Boot Workflow, on page 125, and that you are already on the **Workflow** tab within Orchestration.

Procedure

Step 1 In the left pane, expand the folder where the workflow is located and click the row for the iSCSI workflow to which you want to add the task.

Step 2 On the icon bar, click the purple drop-down list icon and choose **Workflow Designer**.

Step 3 In the **Available Tasks** pane of the Workflow Designer, expand **Physical Compute Tasks** > **Cisco UCS Tasks**.

Step 4 Click the **Power On UCS Server** task, and then drag and drop the selected task onto the workflow designer window.

Step 5 In the **Task Information** screen of the **Add Task (Power On UCS Server)** wizard, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details

d) Click **Next**.

Step 6 In the **User Mapping Inputs** screen of the **Add Task (Power On UCS Server)** wizard, do the following:

a) If you want to be prompted to specify the server that you want to power on when the workflow is run, check the **Server** check box and choose a user input.

b) Click **Next**.

Step 7 In the **Task Inputs** screen of the **Add Task (Power On UCS Server)** wizard, do the following:

a) If you did not choose to prompt for user input, choose the server that you want to power on from the **Server** drop-down list.

b) Click **Submit**.

Adding a Task: Monitor PXE Boot

This procedure assumes that you have created a workflow, as described in Example: Creating an iSCSI Boot Workflow, on page 125, and that you are already on the **Workflow** tab within Orchestration.

Procedure

Step 1 In the left pane, expand the folder where the workflow is located and click the row for the iSCSI workflow to which you want to add the task.

Step 2 On the icon bar, click the purple drop-down list icon and choose **Workflow Designer**.

Step 3 In the **Available Tasks** pane of the Workflow Designer, expand **Network Services Tasks**.

Step 4 Click the **Monitor PXE Boot** task, and then drag and drop the selected task onto the workflow designer window.

Step 5 In the **Task Information** screen of the **Add Task (Monitor PXE Boot)** wizard, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details

d) Click **Next**.

Step 6 In the **User Mapping Inputs** screen of the **Add Task (Monitor PXE Boot)** wizard, do the following:

a) If you want to be prompted to enter the PXE request ID when the workflow is run, check the **PXE Request ID** check box and choose a user input.

Note To map user inputs, you must have added the user inputs with the appropriate permissions to the workflow.

b) Click **Next**.

Step 7 In the **Task Inputs** screen of the **Add Task (Monitor PXE Boot)** wizard, do the following:

a) For those configuration attributes for which you did not choose to prompt for user input, complete the following fields:

- **PXE Request ID—**Enter the PXE request ID.
- **Max Wait Time—**Choose the maximum number of hours you want to wait for the PXE boot to complete.

b) Click **Submit**.

Adding a Task: Power Off UCS Server

This procedure assumes that you have created a workflow, as described in Example: Creating an iSCSI Boot Workflow, on page 125, and that you are already on the **Workflow** tab within Orchestration.

Procedure

Step 1 In the left pane, expand the folder where the workflow is located and click the row for the iSCSI workflow to which you want to add the task.

Step 2 On the icon bar, click the purple drop-down list icon and choose **Workflow Designer**.

Step 3 In the **Available Tasks** pane of the Workflow Designer, expand **Physical Compute Tasks** > **Cisco UCS Tasks**.

Step 4 Click the **Power Off UCS Server** task, and then drag and drop the selected task onto the workflow designer window.

Step 5 In the **Task Information** screen of the **Add Task (Power Off UCS Server)** wizard, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details

d) Click **Next**.

Step 6 In the **User Mapping Inputs** screen of the **Add Task (Power Off UCS Server)** wizard, do the following:

a) If you want to be prompted to specify the server that you want to power off when the workflow is run, check the **Server** check box and choose a user input.

b) Click **Next**.

Step 7 In the **Task Inputs** screen of the **Add Task (Power Off UCS Server)** wizard, do the following:

a) If you did not choose to prompt for user input, choose the server that you want to power off from the **Server** drop-down list.

b) Click **Submit**.

Adding a Task: Modify Service Profile Boot Policy to Boot from iSCSI

This procedure assumes that you have created a workflow, as described in Example: Creating an iSCSI Boot Workflow, on page 125, and that you are already on the **Workflow** tab within Orchestration.

Procedure

Step 1 In the left pane, expand the folder where the workflow is located and click the row for the iSCSI workflow to which you want to add the task.

Step 2 On the icon bar, click the purple drop-down list icon and choose **Workflow Designer**.

Step 3 In the **Available Tasks** pane of the Workflow Designer, expand **Physical Compute Tasks** > **Cisco UCS Tasks**.

Step 4 Click the **Modify Service Profile Boot Policy to Boot from iSCSI** task, and then drag and drop the selected task onto the workflow designer window.

Step 5 In the **Task Information** screen of the **Add Task (Modify Service Profile Boot Policy to Boot from iSCSI)** wizard, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details

d) Click **Next**.

Step 6 In the **User Mapping Inputs** screen of the **Add Task (Modify Service Profile Boot Policy to Boot from iSCSI)** wizard, do the following:

a) If you want to be prompted to specify the service profile that you want to modify when the workflow is run, check the **Service Profile** check box and choose a user input.

b) Click **Next**.

Step 7 In the **Task Inputs** screen of the **Add Task (Modify Service Profile Boot Policy to Boot from iSCSI)** wizard, do the following:

a) If you did not choose to prompt for user input, click the **Service Profile** button to choose the service profile that you want to modify.

b) Click **Submit**.

Changing the Boot Order in a Boot Policy

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to modify a policy and then click **View Details**.

Step 5 Click **Boot Policies**.

Step 6 Choose the boot policy that you want to clone and click **Manage Boot Devices Order**.

Step 7 Use the following buttons to change the order of the boot devices:

- **Move Up**
- **Move Down**
- **Delete**

Step 8 When you are done, click **Back**.

Local Disk Configuration Policy

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

The local disk modes include the following:

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

  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 on the server after you apply the **No RAID** mode. This can lead to a mismatch between the RAID configuration in the policy and the actual disk configuration shown in the **Inventory** > **Storage** tab for the server.

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.

- **RAID 5 Striped Parity—**Data is striped across all disks in the array. Part of the capacity of each disk stores parity information that can be used to reconstruct data if a disk fails. RAID 5 provides good data throughput for applications with high read request rates.
- **RAID 6 Striped Dual Parity—**Data is striped across all disks in the array and two parity disks are used to provide protection against the failure of up to two physical disks. In each row of data blocks, two sets of parity data are stored.
- **RAID 10 Mirrored and Striped—**RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates.
- **RAID 50 Striped Parity and Striped —**Data is striped across multiple striped parity disk sets to provide high throughput and multiple disk failure tolerance.
- **RAID 60 Striped Dual Parity and Striped —**Data is striped across multiple striped dual parity disk sets to provide high throughput and greater disk failure tolerance.

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

Note For a Cisco UCS C-Series server integrated with Cisco UCS Manager, with an embedded on-board RAID controller, the local disk mode should always be **Any Configuration**, and the RAID must be configured directly on the controller.

Guidelines for all Local Disk Configuration Policies

Before you create a local disk configuration policy, consider the following guidelines:

No Mixed HDDs and SSDs

Do not include HDDs and SSDs in a single server or RAID configuration.

Do Not Assign a Service Profile with the Default Local Disk Configuration Policy from a B200 M1 or M2 to a B200 M3

Due to the differences in the RAID/JBOD support provided by the storage controllers of B200 M1 and M2 servers and those of the B200 M3 server, you cannot assign or re-assign a service profile that includes the default local disk configuration policy from a B200M1 or M2 server to a B200 M3 server. The default local disk configuration policy includes those with Any Configuration or JBOD configuration.

JBOD Mode Support

The B200 M3 server supports JBOD mode for local disks.

Note Only B200 M1, B200 M2, B200 M3, B250 M1, B250 M2 and B22 M3 blade servers support the JBOD mode for local disks.

Guidelines for Local Disk Configuration Policies Configured for RAID

Configure RAID Settings in Local Disk Configuration Policy for Servers with MegaRAID Storage Controllers

If a blade server or integrated rack-mount server has a MegaRAID controller, you must configure RAID settings for the drives in the Local Disk Configuration policy included in the service profile for that server. You can do this either by configuring the local disk configuration policy in the service profile using one of the defined RAID modes for that server, or you can use the **Any Configuration** mode with the LSI Utilities toolset to create the RAID volumes.

If you do not configure your RAID LUNs before installing the OS, disk discovery failures might occur during the installation and you might see error messages such as “No Device Found.”

Server May Not Boot After RAID1 Cluster Migration if Any Configuration Mode Specified in Service Profile

After RAID1 clusters are migrated, you need to associate a service profile with the server. If the local disk configuration policy in the service profile is configured with **Any Configuration** mode rather than **RAID1**, the RAID LUN remains in "inactive" state during and after association. As a result, the server cannot boot.

To avoid this issue, ensure that the service profile you associate with the server contains the identical local disk configuration policy as the original service profile before the migration and does not include the **Any Configuration** mode.

Do Not Use JBOD Mode on Servers with MegaRAID Storage Controllers

Do not configure or use JBOD mode or JBOD operations on any blade server or integrated rack-mount server with a MegaRAID storage controllers. JBOD mode and operations are not intended for nor are they fully functional on these servers.

Maximum of One RAID Volume and One RAID Controller in Integrated Rack-Mount Servers

A rack-mount server that has been integrated with Cisco UCS Manager can have a maximum of one RAID volume irrespective of how many hard drives are present on the server.

All the local hard drives in an integrated rack-mount server must be connected to only one RAID Controller. Integration with Cisco UCS Manager does not support the connection of local hard drives to multiple RAID Controllers in a single rack-mount server. We therefore recommend that you request a single RAID Controller configuration when you order rack-mount servers to be integrated with Cisco UCS Manager.

In addition, do not use third party tools to create multiple RAID LUNs on rack-mount servers. Cisco UCS Manager does not support that configuration.

Maximum of One RAID Volume and One RAID Controller in Blade Servers

A blade server can have a maximum of one RAID volume irrespective of how many drives are present in the server. All the local hard drives must be connected to only one RAID controller. For example, a B200 M3 server has an LSI controller and an Intel Patsburg controller, but only the LSI controller can be used as a RAID controller.

In addition, do not use third party tools to create multiple RAID LUNs on blade servers. Cisco UCS Manager does not support that configuration.

Number of Disks Selected in Mirrored RAID Should Not Exceed Two

If the number of disks selected in the Mirrored RAID exceed two, RAID 1 is created as a RAID 10 LUN. This issue can occur with the Cisco UCS B440 M1 and B440 M2 servers.

License Required for Certain RAID Configuration Options on Some Servers

Some Cisco UCS servers require a license for certain RAID configuration options. When Cisco UCS Manager associates a service profile containing this local disk policy with a server, Cisco UCS Manager verifies that the selected RAID option is properly licensed. If there are issues, Cisco UCS Manager displays a configuration error during the service profile association.

For RAID license information for a specific Cisco UCS server, see the *Hardware Installation Guide* for that server.

B420 M3 Server Does Not Support All Configuration Modes

The B420 M3 server does not support the following configuration modes in a local disk configuration policy:

- No RAID
- RAID 6 Striped Dual Parity

In addition, the B420 M3 does not support JBOD modes or operations.

Single-Disk RAID 0 Configurations Not Supported on Some Blade Servers

A single-disk RAID 0 configuration is not supported in the following blade servers:

- Cisco UCS B200 M1
- Cisco UCS B200 M2
- Cisco UCS B250 M1
- Cisco UCS B250 M2

Creating a Local Disk Configuration Policy

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click **Local Disk Configuration Policies**.

Step 6 Click **Add**.

Step 7 On the **Local Disk Configuration Policy** screen, do the following:

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

b) In the **Description** field, enter a description of the policy.
We recommend that you include information about where and when the policy should be used.

c) From the **Mode** drop-down list, choose one of the following local disk policy modes:

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

  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 on the server after you apply the **No RAID** mode. This can lead to a mismatch between the RAID configuration in the policy and the actual disk configuration shown in the **Inventory** > **Storage** tab for the server.

  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.
- **RAID 5 Striped Parity—**Data is striped across all disks in the array. Part of the capacity of each disk stores parity information that can be used to reconstruct data if a disk fails. RAID 5 provides good data throughput for applications with high read request rates.
- **RAID 6 Striped Dual Parity—**Data is striped across all disks in the array and two parity disks are used to provide protection against the failure of up to two physical disks. In each row of data blocks, two sets of parity data are stored.
- **RAID 10 Mirrored and Striped—**RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates.
- **RAID 50 Striped Parity and Striped —**Data is striped across multiple striped parity disk sets to provide high throughput and multiple disk failure tolerance.
- **RAID 60 Striped Dual Parity and Striped —**Data is striped across multiple striped dual parity disk sets to provide high throughput and greater disk failure tolerance.

Note Some Cisco UCS servers require a license for certain RAID configuration options. When Cisco UCS Manager associates a service profile containing this local disk policy with a server, Cisco UCS Manager verifies that the selected RAID option is properly licensed. If there are issues, Cisco UCS Manager displays a configuration error during the service profile association.

For RAID license information for a specific Cisco UCS server, see the *Hardware Installation Guide* for that server.

d) If you want the server to retain the configuration in this local disk configuration policy even if the server is disassociated from the service profile, check the **Protect Configuration** check box.

Caution Protect Configuration becomes non-functional if one or more disks in the server are defective or faulty.

This property is checked by default.

When a service profile is disassociated from a server and a new service profile associated, the setting for the Protect Configuration property in the new service profile takes precedence and overwrites the setting in the previous service profile.

Note If you disassociate the server from a service profile with this option enabled and then associate it with a new service profile that includes a local disk configuration policy with different properties, the server returns a configuration mismatch error and the association fails.

e) From the **Flex Flash State** drop-down list, choose whether you want to enable or disable the SD card module.

Note This parameter only applies to a server with an SD card module.

f) Click **Submit**.

What to Do Next

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

Maintenance Policy

A maintenance policy determines what kind of request Cisco UCS Director sends to Cisco UCS Manager for a server reboot, when changes are made to

- A service profile associated with a server,
- Or to a service profile bound to an updating template.

The maintenance policy specifies how the service profile changes are deployed. This deployment can occur in one of the following ways:

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

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

To apply user acknowledgement, see Viewing the Cisco UCS Manager Pending Activities Report and User Acknowledgement, on page 195.

Note A maintenance policy only prevents an immediate server reboot when a configuration change is made to an associated service profile. However, a maintenance policy does not prevent the following actions from taking place right away:

- Deleting an associated service profile from the system
- Disassociating a server profile from a server
- Directly installing a firmware upgrade without using a service policy
- Resetting the server

For more information about maintenance policies and deferred deployment of service profile changes, including guidelines for implementing them, see the Cisco UCS Manager configuration guides.

Creating a Maintenance Policy

Before You Begin

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click **Maintenance Policies**.

Step 6 Click **Add**.

Step 7 On the **Create Maintenance Policy** screen, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Description field	A description of the policy. We recommend that you include information about where and when the policy should be used.

Name	Description
Reboot Policy drop-down list	Choose when the reboot occurs for servers associated with a service profile that includes this maintenance policy. This can be one of the following: • **Timer Automatic—**All service profile associations and changes are deferred until the maintenance window defined by the schedule shown in the **Schedule** field. • **Immediate—**The server is rebooted automatically as soon as the service profile association is complete or service profile changes are saved by the user. • **User Ack—**The user must reboot the server manually after the service profile association is complete or changes are made. For manual acknowledgement, see Viewing the Cisco UCS Manager Pending Activities Report and User Acknowledgement, on page 195.
Schedule drop-down list	Choose the schedule that sets the time period when you want maintenance operations, such as service profile associations and changes, to occur. During the scheduled time period, the servers associated with service profiles that include this maintenance policy are rebooted and all service profile changes are completed. This field is only available if the **Reboot Policy** is set to **Timer Automatic**.The schedule specifies when maintenance operations can be applied to the server.

Step 8 Click **Submit**.

What to Do Next

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

Server Pool Policy Qualification Overview

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

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

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

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

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

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

Creating Server Pool Policy Qualifications

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click **Server Pool Policy Qualifications**.

Step 6 Click **Add**.

Step 7 On the **Create Server Pool Policy Qualifications** screen, enter a name and description for the policy and click **Next**.

Step 8 On the **Adapter Qualifications** page, do the following to add adapter qualifications to the policy or click **Next** if you do not want to add them:

a) Check the **Add Adapter Qualifications** check box.

b) From the **Type** drop-down list, choose the type of adapter that you want to include in the policy. After you save the adapter qualification, this type cannot be changed.

c) In the **Model(RegEx)** field, enter a regular expression that the adapter PID must match.

d) In the **Maximum Capacity** field, enter the maximum capacity for the selected type.
e) Click **Next**.

Step 9 On the **Chassis/Server Qualifications** page, do the following to add chassis qualifications and server qualifications to the policy, or click **Next** if you do not want to add them:

a) Check the **Add Chassis/Server Qualifications** check box.
b) From the **First Chassis ID** field, enter the first chassis ID from which server pools associated with this policy can draw.
After you save the adapter qualification, this type cannot be changed.
c) In the **Number of Chassis** field, enter the total number of chassis to include in the pool, starting with the chassis identified in the **First Chassis ID** field.
d) In the **Server Qualification Ranges** field, enter the range of server locations that you want to use.
If you want to enter more than one range, separate the ranges by commas. For example, enter 1:5,2:6.
e) Click **Next**.

Example:
For example, if you want to use chassis 5, 6, 7, and 8, enter 5 in the **First Chassis ID** field and 4 in the **Number of Chassis** field. If you want to use only chassis 3, enter 3 in the **First Chassis ID** field and 1 in the **Number of Chassis** field.

Step 10 On the **Memory Qualifications** page, do the following to add memory qualifications to the policy, or click **Next** if you do not want to add them:

a) Check the **Add Memory Qualifications** check box.
b) Complete the following fields:

Name	Description
Clock field	The minimum clock speed required, in megahertz.
Min Cap field	The minimum memory capacity required, in megabytes.
Max Cap field	The maximum memory capacity allowed, in megabytes.
Width field	The minimum width of the data bus.
Latency field	The maximum latency allowed, in nanoseconds.
Units field	The unit of measure to associate with the value in the Width field.

c) Click **Next**.

Step 11 On the **CPU/Cores Qualifications** page, do the following to add CPU qualifications and cores qualifications to the policy,or click **Next** if you do not want to add them:

a) Check the **Add CPU/Cores Qualifications** check box.
b) Complete the following fields:

Name	Description
Processor Architecture drop-down list	Choose the CPU architecture to which this policy applies.
Min Number of Cores field	The minimum number of CPU cores required. This integer can be between 1 and 65535.
Max Number of Cores field	The maximum number of CPU cores allowed. This integer can be between 1 and 65535.
Min Number of Threads field	The minimum number of CPU threads required. This integer can be between 1 and 65535 in the associated text field.
Max Number of Threads field	The maximum number of CPU threads allowed. This integer can be between 1 and 65535.
CPU Speed field	The minimum CPU speed required.
Model(RegEx) field	A regular expression that the processor PID must match.
CPU Stepping field	The minimum CPU version required.

c) Click **Next**.

Step 12 On the **Storage Qualifications** page, do the following to add storage qualifications to the policy, or click **Next** if you do not want to add them:

a) Check the **Add Storage Qualifications** check box.

b) Complete the following fields:

Name	Description
Diskless drop-down list	Choose whether the available storage must be diskless. Your choice can be one of the following: • **Unspecified—**Either storage type is acceptable. • **Yes—**The storage must be diskless. • **No—**The storage cannot be diskless. If you choose **Yes**, no additional fields are displayed.
Min Cap field	The minimum storage capacity across all disks in the server, in megabytes.

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

c) Click **Next**.

Step 13 On the **Power Group Qualifications** page, do the following to add power group qualifications to the policy, or click **Next** if you do not want to add them:

a) Check the **Add Power Group Qualifications** check box.
b) From the **Power Group** drop-down list, choose the power group that you want to include in the policy.
c) Click **Next**.

Step 14 On the **Rack Qualifications** page, do the following to add rack-mount server qualifications to the policy, or click **Next** if you do not want to add them:

a) Check the **Add Rack Qualifications** check box.
b) From the **First Slot ID** field, enter the first rack-mount server ID from which server pools associated with this policy can draw.
After you save the adapter qualification, this type cannot be changed.
c) In the **Number of Slots** field, enter the total number of rack-mount server slots to include in the pool, starting with the server slot identified in the **First Slot ID** field.
d) Click **Next**.

Step 15 On the **Server Model Qualifications** page, do the following to add rack-mount server qualifications to the policy, or click **Next** if you do not want to add them:

a) Check the **Add Server Model Qualifications** check box.
b) In the **Model(RegEx)** field, enter a regular expression that the server model PID must match.
c) Click **Next**.

Step 16 Click **Submit**.

Server Pool Policy Overview

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

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

Creating a Server Pool Policy

Before You Begin

This policy requires that at least one of the following resources exists in the system:

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

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click **Server Pool Policies**.

Step 6 Click **Add**.

Step 7 On the **Create Server Pool Policy** screen, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Description field	A description for the policy.
Target Pool drop-down list	Choose a server pool to associate with the policy.
Qualification drop-down list	Choose a server pool qualification policy to associate with the policy.

Step 8 Click **Submit**.

vNIC/vHBA Placement Policies

vNIC/vHBA placement policies are used to determine the following:

- How the virtual network interface connections (vCons) are mapped to the physical adapters on a server.
- What types of vNICs or vHBAs can be assigned to each vCon.

Each vNIC/vHBA placement policy contains four vCons that are virtual representations of the physical adapters. When a vNIC/vHBA placement policy is assigned to a service profile, and the service profile is associated with a server, the vCons in the vNIC/vHBA placement policy are assigned to the physical adapters and the vNICs and vHBAs are assigned to those vCons.

For blade or rack servers that contain one adapter, Cisco UCS assigns all vCons to that adapter. For servers that contain four adapters, Cisco UCS assigns vCon1 to Adapter1, vCon2 to Adapter2, vCon3 to Adapter3, and vCon4 to Adapter4.

For blade or rack servers that contain two or three adapters, Cisco UCS assigns the vCons based on the type of server and the selected virtual slot mapping scheme, which can be **Round Robin** or **Linear Ordered**. For details about the available mapping schemes, see vCon to Adapter Placement, on page 160.

After Cisco UCS assigns the vCons, it assigns the vNICs and vHBAs based on the **Selection Preference** for each vCon. This can be one of the following:

- **All—**All configured vNICs and vHBAs can be assigned to the vCon, whether they are explicitly assigned to it, unassigned, or dynamic. This is the default.
- **Assigned Only—**vNICs and vHBAs must be explicitly assigned to the vCon. You can assign them explicitly through the service profile or the properties of the vNIC or vHBA.
- **Exclude Dynamic—**Dynamic vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for all static vNICs and vHBAs, whether they are unassigned or explicitly assigned to it.
- **Exclude Unassigned—**Unassigned vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for dynamic vNICs and vHBAs and for static vNICs and vHBAs that are explicitly assigned to it.
- **Exclude usNIC—**Cisco usNICs cannot be assigned to the vCon. The vCon can be used for all other configured vNICs and vHBAs, whether they are explicitly assigned to it, unassigned, or dynamic.

Note An SRIOV usNIC that is explicitly assigned to a vCon set to **Exclude usNIC** will remain assigned to that vCon.

If you do not include a vNIC/vHBA placement policy in the service profile, Cisco UCS defaults to the **Round Robin** vCon mapping scheme and the **All** vNIC/vHBA selection preference, distributing the vNICs and vHBAs between the adapters based on the capabilities and relative capacities of each adapter.

vCon to Adapter Placement

Cisco UCS maps every vCon in a service profile to a physical adapter on the server. How that mapping occurs and how the vCons are assigned to a specific adapter in a server depends on the following:

- The type of server. N20-B6620-2 and N20-B6625-2 blade servers with two adapter cards use a different mapping scheme than other supported rack or blade servers.
- The number of adapters in the server.
- The setting of the virtual slot mapping scheme in the vNIC/vHBA placement policy, if applicable.

You must consider this placement when you configure the vNIC/vHBA selection preference to assign vNICs and vHBAs to vCons.

Note vCon to adapter placement is not dependent upon the PCIE slot number of the adapter. The adapter numbers used for the purpose of vCon placement are not the PCIE slot numbers of the adapters, but the ID assigned to them during server discovery.

vCon to Adapter Placement for N20-B6620-2 and N20-B6625-2 Blade Servers

In N20-B6620-2 and N20-B6625-2 blade servers, the two adapters are numbered left to right while vCons are numbered right to left. If one of these blade servers has a single adapter, Cisco UCS assigns all vCons to that adapter. If the server has two adapters, the vCon assignment depends upon the virtual slot mapping scheme:

- **Round Robin—**Cisco UCS assigns vCon2 and vCon4 to Adapter1 and vCon1 and vCon3 to Adapter2. This is the default.
- **Linear Ordered—**Cisco UCS assigns vCon3 and vCon4 to Adapter1 and vCon1 and vCon2 to Adapter2.

vCon to Adapter Placement for All Other Supported Servers

For all other servers supported by Cisco UCS in addition to the N20-B6620-2 and N20-B6625-2 blade servers, the vCon assignment depends on the number of adapters in the server and the virtual slot mapping scheme.

For blade or rack servers that contain one adapter, Cisco UCS assigns all vCons to that adapter. For servers that contain four adapters, Cisco UCS assigns vCon1 to Adapter1, vCon2 to Adapter2, vCon3 to Adapter3, and vCon4 to Adapter4.

For blade or rack servers that contain two or three adapters, Cisco UCS assigns the vCons based on the selected virtual slot mapping scheme: Round Robin or Linear Ordered.

Table 3: vCon to Adapter Placement Using the Round - Robin Mapping Scheme

Number of Adapters	vCon1 Assignment	vCon2 Assignment	vCon3 Assignment	vCon4 Assignment
1	Adapter1	Adapter1	Adapter1	Adapter1
2	Adapter1	Adapter2	Adapter1	Adapter2
3	Adapter1	Adapter2	Adapter3	Adapter2
4	Adapter1	Adapter2	Adapter3	Adapter4

Round Robin is the default mapping scheme.

Table 4: vCon to Adapter Placement Using the Linear Ordered Mapping Scheme

Number of Adapters	vCon1 Assignment	vCon2 Assignment	vCon3 Assignment	vCon4 Assignment
1	Adapter1	Adapter1	Adapter1	Adapter1

Number of Adapters	vCon1 Assignment	vCon2 Assignment	vCon3 Assignment	vCon4 Assignment
2	Adapter1	Adapter1	Adapter2	Adapter2
3	Adapter1	Adapter2	Adapter3	Adapter3
4	Adapter1	Adapter2	Adapter3	Adapter4

Note If you are using a vCon policy with two adapters in the Cisco UCS B440 M2 Blade Server, be aware of the following mapping.

- vCon 2 to adapter 1 maps first
- vCon 1 to adapter 2 maps second ZXA Q

vNIC/vHBA to vCon Assignment

Cisco UCS provides two options for assigning vNICs and vHBAs to vCons through the vNIC/vHBA placement policy: explicit assignment and implicit assignment.

Explicit Assignment of vNICs and vHBAs

With explicit assignment, you specify the vCon and, therefore, the adapter to which a vNIC or vHBA is assigned. Use this assignment option when you must determine how the vNICs and vHBAs are distributed between the adapters on a server.

To configure a vCon and the associated vNICs and vHBAs for explicit assignment, do the following:

- Set the vCon configuration to any of the available options. You can configure the vCons through a vNIC/vHBA placement policy or in the service profile associated with the server. If a vCon is configured for **All**, you can still explicitly assign a vNIC or vHBA to that vCon.
- Assign the vNICs and vHBAs to a vCon. You can make this assignment through the virtual host interface placement properties of the vNIC or vHBA or in the service profile associated with the server.

If you attempt to assign a vNIC or vHBA to a vCon that is not configured for that type of vNIC or vHBA, a message displays that advises you of the configuration error.

During service profile association, Cisco UCS validates the configured placement of the vNICs and vHBAs against the number and capabilities of the physical adapters in the server before assigning the vNICs and vHBAs according to the configuration in the policy. Load distribution is based on the explicit assignments to the vCons and adapters configured in this policy.

If the adapters do not support the assignment of one or more vNICs or vHBAs, Cisco UCS raises a fault against the service profile.

Implicit Assignment of vNICs and vHBAs

With implicit assignment, Cisco UCS determines the vCon and, therefore, the adapter to which a vNIC or vHBA is assigned according to the capability of the adapters and their relative capacity. Use this assignment option if the adapter to which a vNIC or vHBA is assigned is not important to your system configuration.

To configure a vCon for implicit assignment, do the following:

- Set the vCon configuration to **All**, **Exclude Dynamic**, or **Exclude Unassigned**. You can configure the vCons through a vNIC/vHBA placement policy or in the service profile associated with the server.
- Do not set the vCon configuration to **Assigned Only**. Implicit assignment cannot be performed with this setting.
- Do not assign any vNICs or vHBAs to a vCon.

During service profile association, Cisco UCS verifies the number and capabilities of the physical adapters in the server and assigns the vNICs and vHBAs accordingly. Load distribution is based on the capabilities of the adapters, and placement of the vNICs and vHBAs is performed according to the actual order determined by the system. For example, if one adapter can accommodate more vNICs than another, that adapter is assigned more vNICs.

If the adapters cannot support the number of vNICs and vHBAs configured for that server, Cisco UCS raises a fault against the service profile.

Implicit Assignment of vNICs in a Dual Adapter Environment

When you use implicit vNIC assignment for a dual slot server with an adapter card in each slot, Cisco UCS typically assigns the vNICs/vHBAs as follows:

- If the server has the same adapter in both slots, Cisco UCS assigns half the vNICs and half the vHBAs to each adapter.
- If the server has one non-VIC adapter and one VIC adapter, Cisco UCS assigns two vNICs and two vHBAs to the non-VIC adapter and the remaining vNICs and vHBAs to the VIC adapter.
- If the server has two different VIC adapters, Cisco UCS assigns the vNICs and vHBAs proportionally, based on the relative capabilities of the two adapters.

The following examples show how Cisco UCS would typically assign the vNICs and vHBAs with different combinations of supported adapter cards:

- If you want to configure four vNICs and the server contains two Cisco UCS M51KR-B Broadcom BCM57711 adapters (with two vNICs each), Cisco UCS assigns two vNICs to each adapter.
- If you want to configure 50 vNICs and the server contains a Cisco UCS CNA M72KR-E adapter (2 vNICs) and a Cisco UCS M81KR Virtual Interface Card adapter (128 vNICs), Cisco UCS assigns two vNICs to the Cisco UCS CNA M72KR-E adapter and 48 vNICs to the Cisco UCS M81KR Virtual Interface Card adapter.
- If you want to configure 150 vNICs and the server contains a Cisco UCS M81KR Virtual Interface Card adapter (128 vNICs) and a Cisco UCS VIC-1240 Virtual Interface Card adapter (256 vNICs), Cisco UCS assigns 50 vNICs to the Cisco UCS M81KR Virtual Interface Card adapter and 100 vNICs to the Cisco UCS VIC-1240 Virtual Interface Card adapter.

Note Exceptions to this implicit assignment occur if you configure the vNICs for fabric failover and if you configure dynamic vNICs for the server.

For a configuration that includes vNIC fabric failover where one adapter does not support vNIC failover, Cisco UCS implicitly assigns all vNICs that have fabric failover enabled to the adapter that supports them. If the configuration includes only vNICs that are configured for fabric failover, no vNICs are implicitly assigned to the adapter that does not support them. If some vNICs are configured for fabric failover and some are not, Cisco UCS assigns all failover vNICs to the adapter that supports them and a minimum of one nonfailover vNIC to the adapter that does not support them, according to the ratio above.

For a configuration that includes dynamic vNICs, the same implicit assignment would occur. Cisco UCS assigns all dynamic vNICs to the adapter that supports them. However, with a combination of dynamic vNICs and static vNICs, at least one static vNIC is assigned to the adapter that does not support dynamic vNICs.

Creating a vNIC/vHBA Placement Policy

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click **vNIC/vHBA Placement Policies**.

Step 6 Click **Add**.

Step 7 On the **Add Network Control Policy** screen, complete the following fields:

Name	Description
Name field	A unique name for the policy.

Name	Description
Virtual Slot drop-down list	Choose the virtual network interface for each virtual slot. This can be one of the following: • **All—**All configured vNICs and vHBAs can be assigned to the vCon, whether they are explicitly assigned to it, unassigned, or dynamic. This is the default. • **Assigned Only—**vNICs and vHBAs must be explicitly assigned to the vCon. You can assign them explicitly through the service profile or the properties of the vNIC or vHBA. • **Exclude Dynamic—**Dynamic vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for all static vNICs and vHBAs, whether they are unassigned or explicitly assigned to it. • **Exclude Unassigned—**Unassigned vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for dynamic vNICs and vHBAs and for static vNICs and vHBAs that are explicitly assigned to it. • **Exclude usNIC—**Cisco usNICs cannot be assigned to the vCon. The vCon can be used for all other configured vNICs and vHBAs, whether they are explicitly assigned to it, unassigned, or dynamic. **Note** An SRIOV usNIC that is explicitly assigned to a vCon set to **Exclude usNIC** will remain assigned to that vCon.

Step 8 Click **Submit**.

Placement Policy

The placement policy is a Cisco UCS Director policy that allows you to select and map vCons to vNICs and vHBAs. Depending upon the configuration you choose, you can allow the system to do the placement, choose the placement yourself, or use a vNIC/vHBA placement policy to determine the placement.

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

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

You 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 Placement Policy

Before You Begin

Before you create a placement policy, review the guidelines for vNIC/vHBA placement policies in the Cisco UCS Manager configuration guides to ensure that you understand the impact of the choices that you make.

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **UCS Manager**.

Step 2 Click **Placement Policy**.

Step 3 Click **Add**.

Step 4 In the **Add Placement Policy** screen, complete the following fields:

a) In the **Policy Name** field, enter a name for the placement policy.

b) In the **Policy Description** field, enter a description for the policy.

c) From the **UCS Account Name** drop-down list, choose the Cisco UCS Manager account to which you want to add this policy.

d) From the **UCS Organization Name** drop-down list, choose the Cisco UCS organization to which you want to add this policy.

e) From the **Storage Policy** drop-down list, choose the storage policy that you want to apply to this policy.

f) From the **Network Policy** drop-down list, choose the network policy that you want to apply to this policy.

g) From the **Select Placement Type** drop-down list, choose one of the following options:

- **Let System Perform Placement—**Cisco UCS Director determines the optimal placement for the vNICs and vHBAs. If you choose this option, continue with Step 6.
- **Manual Placement—**You choose the virtual network interface preferences for each of the vCons. If you choose this option, continue with Step 5.
- **Select Placement Policy—**The vNIC/vHBA placement policy that you choose determines the placement of the vNICs and vHBAs. If you choose this option, choose a policy from the **Select vNIC/vHBA Placement Policy** drop-down list and continue with Step 6.

Step 5 If you chose the manual placement option, do the following:

a) In the **Virtual Network Interface Selection Preference** area, choose one of the following options from the drop-down list for each of the vCons.

- **All—**All configured vNICs and vHBAs can be assigned to the vCon, whether they are explicitly assigned to it, unassigned, or dynamic. This is the default.
- **Assigned Only—**vNICs and vHBAs must be explicitly assigned to the vCon. You can assign them explicitly through the service profile or the properties of the vNIC or vHBA.

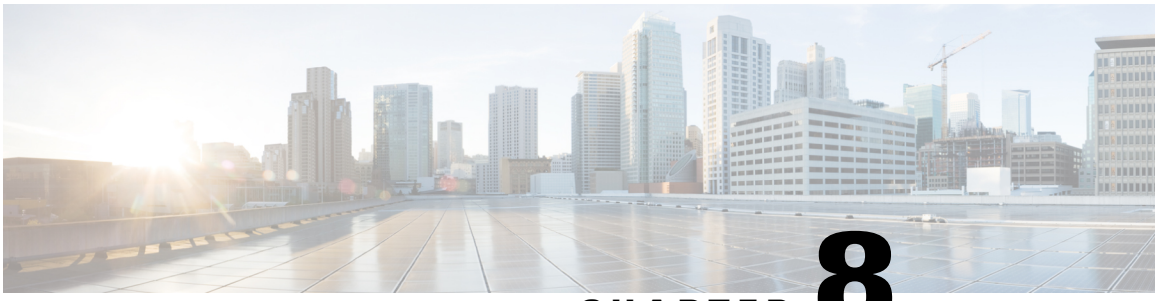
- **Exclude Dynamic—**Dynamic vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for all static vNICs and vHBAs, whether they are unassigned or explicitly assigned to it.
- **Exclude Unassigned—**Unassigned vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for dynamic vNICs and vHBAs and for static vNICs and vHBAs that are explicitly assigned to it.
- **Exclude usNIC—**Cisco usNICs cannot be assigned to the vCon. The vCon can be used for all other configured vNICs and vHBAs, whether they are explicitly assigned to it, unassigned, or dynamic.

  Note An SRIOV usNIC that is explicitly assigned to a vCon set to **Exclude usNIC** will remain assigned to that vCon.

b) Click **Next**.
c) From the **Select Virtual Interface (vNIC/vHBA)** drop-down list, choose a vNIC or vHBA.
d) Click **Add**.
e) From the **Assign to Virtual Network Interface** drop-down list, choose the vCon where you want to place the vNIC or vHBA.
f) Repeat steps 5c to 5e until you have placed all the vNICs and vHBAs.
g) Click **Next** and continue with Step 6.

Step 6 On the **Virtual Interface Order** screen do the following:
a) In the **Virtual Network Interface** table, review the order of the vHBAs and vNICs.
b) If necessary, check the check box for a vNIC or vHBA and one or more of the following to set the interface order:
   - Click the **Move UP** or **Move DOWN** buttons to move the vNIC or vHBA up or down in order.
   - Choose a number from the **Virtual Interface Order** drop-down list to set the desired order.

Step 7 After you have completed the placement configuration, click **Submit**.



CHAPTER 8

Configuring Service Profiles

This chapter contains the following sections:

- Service Profiles, page 169
- Service Profile Templates, page 170
- Creating a Service Profile, page 170
- Creating a Service Profile Template, page 172
- Managing Service Profiles, page 174
- Managing Service Profile Templates, page 179

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 hosts. The service profile maintains configuration information about the server hardware, interfaces, fabric connectivity, and server and network identity.

Every active server must be associated with a service profile.

Note You can view a service profile by clicking the **Service Profiles** tab for a Cisco UCS Manager account.

Note 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.

For more information about service profiles, including the types of service profiles and guidelines for using them, see the Cisco UCS Manager configuration guides.

Service Profile Templates

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

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

Cisco UCS supports the following types of service profile templates:

Initial template

Service profiles created from an initial template inherit all the properties of the template. However, after you create the profile, it is no longer connected to the template. If you must change one or more profiles created from this template, change each profile individually.

Updating template

Service profiles created from an updating template inherit all the properties of the template and remain connected to the template. Any changes to the template automatically update the service profiles created from the template.

Creating a Service Profile

You can also create a service profile on the **Service Profiles** tab for a Cisco UCS Manager account.

Before You Begin

At a minimum, the following pools and policies that are required for service profiles must exist in the Cisco UCS Manager account:

- UUID pool
- Storage policy
- Network policy
- Boot policy

Note You cannot create a host firmware package in Cisco UCS Director. If you want to incorporate this policy in a service profile, import it from the Cisco UCS Manager account.

The other policies that you can include in a service profile are optional. However, we recommend that you review the **Create Service Profile** dialog box and ensure that you have created all of the policies that you want to include in the service profile before you begin.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Service Profiles**.

Step 4 Click **Add**.

Step 5 On the **Add Service Profile** screen, enter a name and description for the service profile.

Step 6 From the following drop-down lists, choose the organization, pools and policies that you want to include in this service profile:

- **Organization—**Required. Organization under which to create the Service Profile.
- **UUID Assignment—**Required. Include this policy to specify the UUID for the server.
- **Storage Policy—**Required. Include this policy to specify the SAN connectivity for the server.
- **PXE Network Policy—**Optional. Include this policy if you must have the server connected to the LAN.
- **Placement Policy—**Optional. Include this policy if you want to specify the vNIC, vHBA, and vCon placement for the server.
- **PXE Boot Policy—**Optional. Include this policy if you want to have the server to perform a PXE boot. The secondary boot in this policy must be from a local disk or a SAN boot. If you do not include this policy, the server uses the blade boot policy to determine the boot order.
- **Blade Boot Policy—**Optional. Include this policy to determine the server boot order.
- **BIOS Policy—**Optional. Include this policy if you want to change any of the default settings for the BIOS on the server.
- **IPMI Access Profile—**Optional. Include this policy if you want to be able to access the server through IPMI.
- **SOL Configuration Profile—**Optional. Include this policy if you want to be able to access the server through Serial over LAN.
- **Management IP** Address**—**Optional. Include this policy to specify the outband and inband management IP address for the server.

  If you select **Outband IPv4**, then specify either a static or pooled management IP address policy. If you select a static policy, then enter the IP address, subnet mask, and default gateway details. If you select pooled, then select the outband pool names.

  If you select **Inband**, then specify either an IPv4 or IPv6 Management IP address static policy. If you select IPv4 with the static policy, then enter the IP address, subnet mask, and default gateway details. If you select IPv6 with the static policy, then enter the IP address, prefix, and default gateway details.
- **Threshold Policy—**Optional. Include this policy to specify the thresholds for the server.
- **Scrub Policy—**Optional. Include this policy if you want to specify what happens to the local data and BIOS settings on a server during discovery and disassociation.
- **Host Firmware Policy—**Optional. Include this policy if you want to use a host firmware package to upgrade the server firmware.

- **Maintenance Policy—**Optional. Include this policy if you want to specify what happens when change that requires a server reboot is made to this service profile.
- **Power Control Policy—**Optional. Include this policy if the service profile is associated with a blade server and you want to specify the initial power allocation for the server.

Step 7 From the **Server Power State** drop-down list, choose one of the following to set the power state that is 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.

Step 8 From the **vMedia Policy** drop-down list, choose a vMedia policy.

Step 9 From the **Storage Profile** select list, click the check box for a storage profile and then click **Select**.

Step 10 Click **Submit**.

Creating a Service Profile Template

Before You Begin

At a minimum, the following pools and policies that are required for service profile templates must exist in the Cisco UCS Manager account:

- UUID pool
- Storage policy
- Network policy
- Boot policy

Note You cannot create a host firmware package in Cisco UCS Director. If you want to incorporate this policy in a service profile template, you must import it from the Cisco UCS Manager account.

The other policies that you can include in a service profile template are optional. However, we recommend that you review the **Create Service Profile Template** dialog box and ensure that you have created all of the policies that you want to include in the template before you begin.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click **Service Profile Templates**.

Step 6 Click **Add**.

Step 7 On the **Create Service Profile Template** screen, enter a name and description for the template.

Step 8 From the **Type** drop-down list, choose one of the following:

- **Initial Template—**Any service profiles created from this template are not updated if the template changes.
- **Updating Template—**Any service profiles created from this template are updated if the template changes.

Step 9 From the following drop-down lists, choose the pools and policies that you want to include in this template:

- **UUID Assignment—**Required. Include this policy to specify the UUID pool used for the server.
- **Storage Policy—**Required. Include this policy to specify the SAN connectivity for the server.
- **Network Policy—**Optional. Include this policy if you need to have the server connected to the LAN.
- **Placement Policy—**Optional. Include this policy if you want to specify the vNIC, vHBA, and vCon placement for the server.
- **Blade Boot Policy—**Optional. Include this policy to determine the server boot order.
- **BIOS Policy—**Optional. Include this policy if you want to change any of the default settings for the BIOS on the server.
- **IPMI Access Profile—**Optional. Include this policy if you want to be able to access the server through IPMI.
- **SOL Configuration Profile—**Optional. Include this policy if you want to be able to access the server through Serial over LAN.
- **Management IP Address—**Optional. Include this policy to specify the outband and inband management IP address for the server.

  If you select **Outband IPv4**, then you can specify a pooled management IP address policy. If you select pooled, then you must select the outband pool names.

  If you select **Inband**, then you must specify either an IPv4 or IPv6 Management IP address policy. If you select a pooled policy, then you must select the inband pool names.
- **Threshold Policy—**Optional. Include this policy to specify the thresholds for the server.
- **Scrub Policy—**Optional. Include this policy if you want to specify what happens to the local data and BIOS settings on a server during discovery and disassociation.
- **Host Firmware Package—**Optional. Include this policy if you want to use a host firmware package to upgrade the server firmware.

- **Maintenance Policy—**Optional. Include this policy if you want to specify what happens when change that requires a server reboot is made to a service profile created from this template.
- **Power Control Policy—**Optional. Include this policy if the service profile is associated with a blade server and you want to specify the initial power allocation for the server.
- **Server Power State—**Required. Select the server power state to be applied to the server when a Service Profile is associated.
- **vMedia Policy—**Optional. Include this policy if it is bound to a service profile to allow for an external image file to be dynamically mapped to the server. A service profile can have only one vMedia Policy at a time.
- **Storage Profile—**Optional. Include the storage profile to define the number of storage disks, roles and usage of these disks, and other storage parameters. A storage profile encapsulates the storage requirements for one or more service profiles.

  You can also search for a Storage profile and or filter on a specific profile.

Step 10 Click **Submit**.

Managing Service Profiles

Creating a Template from a Service Profile

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Service Profiles**.

Step 4 Click the row for the service profile from which you want to create a service profile template.

Step 5 From **More Actions** drop-down menu, choose **Create Template**.

Step 6 On the **Create Template** screen, do the following:

a) In the **Service Profile Template Name** field, enter a unique name for the template.

b) From the **Type** drop-down list, choose one of the following:

- **Initial Template—**Any service profiles created from the template are not updated if the template changes.
- **Updating Template—**Any service profiles created from the template are updated if the template changes.

c) From the **Organization** drop-down list, choose the organization for the service profile template.

d) Click **Submit**.

Renaming a Service Profile

When you rename a service profile, the following occurs:

- Event logs and audit logs that reference the previous name for the service profile are retained under that name.
- A new audit record is created to log the rename operation.
- All records of faults against the service profile under its previous name are transferred to the new service profile name.

Note You cannot rename a service profile that has pending changes.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Service Profiles**.

Step 4 Click the row for the service profile that you want to rename.

Step 5 From **More Actions** drop-down menu, choose **Create Rename**.

Step 6 On the **Rename** screen, do the following:

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

b) If desired, check one or both of the following check boxes:

Name	Description
Affected Workflows	Allows you to choose which of the workflows that reference the service profile are updated with the new service profile name. If you do not check this check box, no workflows are updated with the new service profile name.
Affected SRs	Allows you to choose which of the SRs that reference the service profile are updated with the new service profile name. If you do not check this check box, no SRs are updated with the new service profile name.

c) Click **Submit**.

Cloning a Service Profile

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Service Profiles**.

Step 4 Click the row for the service profile that you want to clone.

Step 5 From **More Actions** drop-down menu, choose **Clone**.

Step 6 On the **Clone Service Profile** screen, do the following:

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

b) From the **Organization** drop-down list, choose an organization for the cloned service profile.

c) Click **Submit**.

Step 7 Navigate to the service profile you created and make sure that all options are correct.

Associating a Service Profile with a Server

You can also associate a service profile with a server on the **Service Profiles** tab for a Cisco UCS Manager account.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Service Profiles**.

Step 4 Click the row for the server that you want to associate with a service profile.

Step 5 From **More Actions** drop-down menu, choose **Associate**.

Step 6 On the **Associate Server Profile** screen, choose **Existing Server** to associate with.

Step 7 Expand **Existing Server**, and check the check box for the service that you want to associate with the server and click **Validate**.

Step 8 Click **Submit**.
Cisco UCS Director sends a request to Cisco UCS Manager to associate the service profile with the server.

A progress bar indicates the status of the association. You can click **Close** to close the progress indicator and move to a different page. Closing this progress indicator does not affect the association process.

Associating a Service Profile with a Server Pool

Before You Begin

Create at least one server pool that includes at least one available server.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Service Profiles**.

Step 4 Click the row for the service profile that you want to associate with a server pool.

Step 5 From **More Actions** drop-down menu, choose **Associate**.

Step 6 On the **Associate Server Profile** screen, choose **Existing Server Pool** to associate with.

Step 7 Expand **Existing Server Pool**, and check the check box for the service that you want to associate with the server and click **Validate**.

Step 8 Click **Submit**.
Cisco UCS Director sends a request to Cisco UCS Manager to associate the service profile with the server pool.

A progress bar indicates the status of the association. You can click **Close** to close the progress indicator and move to a different page. Closing this progress indicator does not affect the association process.

Disassociating a Service Profile from a Server

When you disassociate a service profile, Cisco UCS Director sends a request to Cisco UCS Manager to disassociate the service profile. Cisco UCS Manager attempts to shut down the operating system on the server. If the operating system does not shut down within a reasonable length of time, Cisco UCS Manager forces the server to shut down.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **UCS Servers**.

Step 4 Click the row for the server that you want to disassociate from its service profile.

Step 5 From **More Actions** drop-down menu, choose **Disassociate**.

Step 6 On the **Disassociate Server** screen, click **Disassociate**.
A progress bar indicates the status of the disassociation task. You can click **Close** to close the progress indicator and move to a different page. Closing this progress indicator does not affect the disassociation process.

Assigning a Service Profile to a Cisco UCS Director Group

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Service Profiles**.

Step 4 Click the row for the service profile that you want to assign to a group.

Step 5 From **More Actions** drop-down menu, choose **Assign Group**.

Step 6 On the **Select Group** screen, do the following:

a) From the **Group** drop-down list, choose the Cisco UCS Director group to which you want to assign this service profile.

b) In the **Label** field, enter a label to identify this service profile.

c) Click **Submit**.

Unassigning a Service Profile from a Cisco UCS Director Group

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Service Profiles**.

Step 4 Click the row for the service profile that you want to unassign from a Cisco UCS Director group.

Step 5 From **More Actions** drop-down menu, choose **Unassign Group**.

Step 6 On the **Unassign Group** screen, click **Unassign**.

Requesting Inventory Collection for a Service Profile

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Service Profiles**.
Step 4 Click the row for the service profile for which you want to request inventory collection.
Step 5 From **More Actions** drop-down menu, choose **Request Inventory Collection**.
Step 6 On the **Collect Inventory** screen, click **Submit**.

Managing Service Profile Templates

Creating a Service Profile from a Template

You can create up to 255 service profiles from a service profile template at one time.

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Organizations**.
Step 4 Click the organization that contains the service profile template from which you want to create a service profile and then click **View Details**.
Step 5 Click **Service Profile Templates**.
Step 6 Click the row for the service profile template from which you want to create a service profile.
Step 7 From **More Actions** drop-down menu, choose **Create Service Profile**.
Step 8 On the **Create Service Profile** screen, do the following:
a) In the **Service Profile Name Prefix** field, enter a unique prefix to be added to the name of each service profile that you create.
b) In the **Number of Service Profiles** field, enter the number of service profiles that you want to create. You can create between 1 and 255 service profiles.
c) Click **Submit**.
Step 9 To view the service profile(s) that you created, do the following:
a) Click **Back** to return to the **Organizations** tab.
b) Click the **Service Profiles** tab.
c) Click **Refresh**.

The **Template Instance** column in the **Service Profiles** table lists the template from which you created the service profile.

Cloning a Service Profile Template

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click **Service Profile Templates**.

Step 6 Click the row for the service profile template that you want to clone.

Step 7 From **More Actions** drop-down menu, choose **Clone**.

Step 8 On the **Clone Service Profile Template** screen, do the following:

a) In the **Name** field, enter a unique name for the cloned service profile template.

b) From the **Organization** drop-down list, choose an organization for the cloned service profile template.

c) Click **Submit**.

Step 9 Navigate to the service profile template you created and make sure that all options are correct.

Associating a Service Profile Template with a Server Pool

Before You Begin

Create at least one server pool that includes at least one available server.

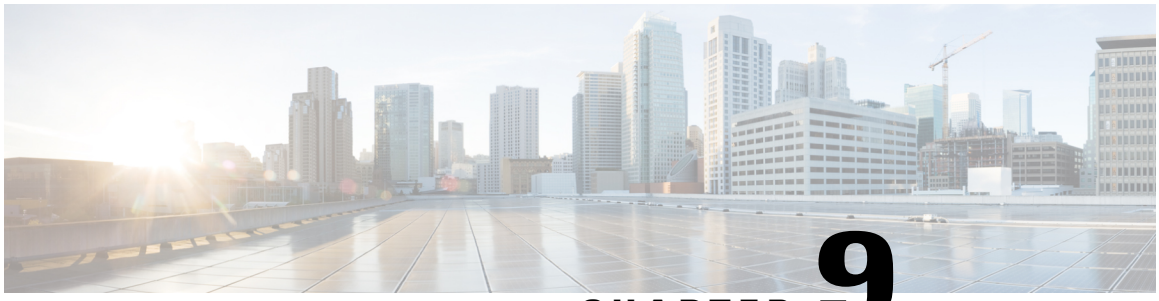
Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Organizations**.
Step 4 Click the organization that contains the service profile template you want to associate and then click **View Details**.
Step 5 Click **Service Profile Templates**.
Step 6 Click the row for the service profile template that you want to associate with a server pool.
Step 7 From **More Actions** drop-down menu, choose **Associate**.
Step 8 On the **Select Server Pool to Associate Server Profile Template** screen, expand the **Server Pool** and check one or more check boxes for the server pools that you want to associate with the service profile template..
Step 9 Expand **Server Pool Policy Qualification** and check one or more check boxes for the server pool policy qualifications.
Step 10 Click **Associate**.

Disassociating a Service Profile Template from a Server Pool

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Organizations**.
Step 4 Click the organization that contains the service profile template you want to disassociate and then click **View Details**.
Step 5 Click **Service Profile Templates**.
Step 6 Click the row for the service profile template that you want to disassociate from a server pool.
Step 7 From **More Actions** drop-down menu, choose **Disassociate**.
Step 8 On the **Disassociate Service Profile Template** screen, click **Disassociate**.



CHAPTER 9

Managing Cisco UCS Servers

This chapter contains the following sections:

- Server Management, page 183
- Powering On a Server, page 184
- Powering Off a Server, page 184
- Launching the KVM Console for a Server, page 184
- Accessing a Server Directly using the KVM Console, page 185
- Requesting Inventory Collection for a Server, page 185
- Issuing a Diagnostic Interrupt for a Server, page 186
- Resetting a Server, page 186
- Reacknowledging a Server, page 186
- Decommissioning a Server, page 187

Server Management

You can manage and monitor all blade and rack-mount servers in a Cisco UCS domain through Cisco UCS Director.

For information about how to select servers for management, see Selective Server Management, on page 15.

Powering On a Server

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **UCS Servers**.
Step 4 Click the row for the server that you want to power on.
Step 5 From the **More Actions** drop-down menu, choose **Power On**.
Step 6 Click **Submit**.

Powering Off a Server

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **UCS Servers**.
Step 4 Click the row for the server that you want to power on.
Step 5 From the **More Actions** drop-down menu, choose**Power Off**.
Step 6 Click **Submit**.

Launching the KVM Console for a Server

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **UCS Servers**.
Step 4 Click the row for the server for which you want to start the KVM console.
Step 5 From the **More Actions** drop-down menu, choose **Launch KVM Console**.
Step 6 Click **Submit**.
Cisco UCS Director downloads the `kvm.jnlp` file.
Step 7 Double-click on the `kvm.jnlp` file in your downloads folder.

The KVM Console opens in a separate window.

If you do not have the required Java Runtime Environment (JRE) installed, click **More Info** in the dialog box and follow the instructions to download and install the JRE.

Accessing a Server Directly using the KVM Console

You can access a UCS server directly using the KVM console.

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **UCS Servers**.
Step 4 Click the for the server that you want to access directly using the KVM console.
Step 5 From the **More Actions** drop-down menu, choose **KVM Direct Access**.
Step 6 Click **Submit**.
The KVM Console opens in a separate window.
Step 7 Enter the user name and password, and select a domain.
Step 8 Click **Launch KVM**.

Requesting Inventory Collection for a Server

Procedure

Step 1 On the menu bar, choose **Physical** > **Compute**.
Step 2 Expand the pod and click Cisco UCS Manager account
Step 3 Click **UCS Servers**.
Step 4 Click the row in the table for the server for which you want to request inventory collection.
Step 5 Click **Request Inventory Collection**.
Step 6 Click **Submit**.

Issuing a Diagnostic Interrupt for a Server

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **UCS Servers**.

Step 4 Click the row or the server for which you want to issue a diagnostic interrupt.

Step 5 From the **More Actions** drop-down menu, choose **Server Maintenance**.

Step 6 On the **Server Maintenance** screen, do the following:

a) From the **Server Maintenance** drop-down list, choose **Diagnostic Interrupt**.

b) Click **Yes**.

A Non Makeable Interrupt (NMI) is issued to the BIOS or operating system from the Cisco Integrated Management Controller (CIMC). This action creates a core dump or stack trace, depending on the operating system installed on the server.

Resetting a Server

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **UCS Servers**.

Step 4 Click the row for the server that you want to reset.

Step 5 From the **More Actions** drop-down menu, choose **Reset**.

Step 6 Click **Submit**.

Reacknowledging a Server

Perform the following procedure if you need to have Cisco UCS Manager rediscover the server and all endpoints in the server. For example, you can use this procedure if a server is stuck in an unexpected state, such as the discovery state.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **UCS Servers**.

Step 4 Click the row for the server that you want to re-acknowledge.

Step 5 From the **More Actions** drop-down menu, choose **Server Maintenance**.

Step 6 On the **Server Maintenance** screen, do the following:

a) From the **Server Maintenance** drop-down list, choose **Re-acknowledge**.

b) Click **Yes**.

Cisco UCS Director sends a request to have Cisco UCS Manager disconnect the server and then build the connections between the server and the fabric interconnect or fabric interconnects in the system. The acknowledgment may take several minutes to complete.

Decommissioning a Server

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **UCS Servers**.

Step 4 Click the row for the server that you want to decommission.

Step 5 From the **More Actions** drop-down menu, choose **Server Maintenance**.

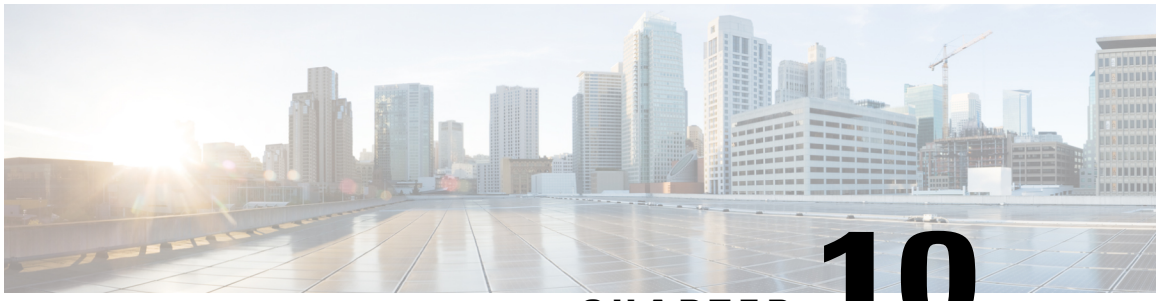
Step 6 On the **Server Maintenance** screen, do the following:

a) From the **Server Maintenance** drop-down list, choose **Decommission**.

b) In the **Reason** field, enter the reason for decommissioning the server.

c) Click **Yes**.

Cisco UCS Director shuts down the server, removes it from the Cisco UCS configuration, and adds it to the **Decommissioned Servers** tab.



CHAPTER 10

Monitoring and Reporting

This chapter contains the following sections:

- About Monitoring and Reporting, page 189
- Monitoring a Fabric Interconnect and its Components, page 191
- Monitoring a Chassis and its Components, page 192
- Monitoring a Server and its Components, page 193
- Monitoring a FEX and its Components, page 194
- Viewing the Cisco UCS Manager Pending Activities Report and User Acknowledgement, page 195
- TPM Monitoring, page 195
- Inventory Reports, page 196
- Cisco UCS Events, page 199
- Cisco UCS Faults, page 200
- Fault Suppression, page 201

About Monitoring and Reporting

Cisco UCS Director displays all managed Cisco UCS components in each Cisco UCS domain that has been added as a Cisco UCS Manager account. These components can be hardware or software.

Reports

Cisco UCS Director provides several different kinds of reports that you can use to view the status of a Cisco UCS Manager pod and its components. All of these reports can be manually refreshed for real-time data and exported to PDF, CSV, or XLS format for you to share with others.

The available reports include:

- **Summary reports** for comparison data and other information about the components of the pod. These reports display in bar, pie, and tabular charts to provide insight into how the system is performing, such as system overview, policies applied, server inventory and status, servers that are associated vs. unassociated, and so on.

You can add some or all of these reports to your Cisco UCS Director dashboard for quick access.

- **Tabular reports** for detailed information about specific components. They provide the status of the components in a pod. You can export the data from any tabular report in PDF, CSV, or XLS format. If you have scheduled inventory collection, the status is updated regularly. Otherwise, you can click **Refresh** on the tabular report to get real-time status.

  You can access tabular reports from any page after you choose the pod. Reports are available for the following components:

  - Compute reports
  - Storage reports
  - Network reports

- **More reports** include Top 5 reports and other reports for detailed information about high-performing resources. You can select the report type to display as tabular, trending, or instant. You can customize some of these reports by choosing the report widget and time duration.

Inventory Collection

When you add a pod, Cisco UCS Director discovers and collects the inventory of that pod. You can view the collected inventory and the status of the pod and its components in the summary reports and on the report pages. This status can be updated on a regular schedule through system tasks and manually by component.

Components You Can Monitor

You can view the inventory, monitor details, and view reports for each component including the following:

- Fabric interconnects
- Chassis and its components, including fan modules, power supply units (PSUs), I/O modules, servers, and decommissioned servers.
- Servers
- Organizations
- Service profiles
- VSANS
- VLANs
- Port channels
- QoS system classes
- Chassis discovery policy
- Management IP pool
- Flow control policies
- Pending Activities
- vMedia Policy
- Locales

- Faults and events

Monitoring a Fabric Interconnect and its Components

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Fabric Interconnects**.

Step 4 Click the row in the table for the fabric interconnect that you want to monitor.

Step 5 Click **View Details**.
Cisco UCS Director displays information about the current status of the selected component. Click the tabs in the window for more details about that component.

Step 6 Click on one of the following to view the status of the fabric interconnect or a specific component in the fabric interconnect:

Name	Description
License Status	Overview of the available licenses, the license usage, and any license violations.
Summary	Summary of the current status of the fabric interconnect and its components, including CPU utilization and data usage statistics.
Power Supply Units	List of the PSUs with their current status.
Fans	List of the fans in the fabric interconnect with their current status.
Ethernet Ports	List of the Ethernet ports in the fabric interconnect, including their location and current status.
Fibre Channel Ports	List of the Fibre Channel ports in the fabric interconnect, including their location, current status, and associated VSAN.
Events	List of current events for the fabric interconnect and its components, with information about each event.
Faults	List of the current faults for the fabric interconnect and its components, with information about each fault.
More Reports	Additional reports that you can generate for the fabric interconnect and its components, including data usage, CPU utilization, and memory usage reports.

Step 7 To return to the main window, click **Back**.

Monitoring a Chassis and its Components

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **UCS Chassis**.

Step 4 Click the row for the chassis that you want to monitor.

Step 5 Click **View Details**.
Cisco UCS Director displays information about the current status of the selected component. Click the tabs in the window for more details about that component.

Step 6 Click on one of the following to view the status of the chassis or a specific component in the chassis:

Name	Description
Summary	Summary of the current status of the chassis and its components.
Servers	List of the servers in the chassis with their location and current status.
Fan Modules	List of the fan modules in the chassis with their current status.
Power Supply Units	List of the PSUs in the chassis with their current status.
Events	List of the current events for the chassis and its components, with information about each event.
Suppression Tasks	List of the fault suppression tasks, if any, including the associated policy and schedule.
IO Modules	List of the I/O modules in the chassis with their location and current status.
Faults	List of the current faults for the chassis and its components, with information about each fault.
More Reports	Additional reports that you can generate for the chassis and its components, such as an input/output power trend report.

Step 7 To return to the main window, click **Back**.

Monitoring a Server and its Components

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **UCS Servers**.

Step 4 Click the row for the server that you want to monitor.

Step 5 Click **View Details**.
Cisco UCS Director displays information about the current status of the selected component. Click the tabs in the window for more details about that component.

Step 6 Click on one of the following to view the status of the server or a specific component in the server:

Name	Description
License Status	Overview of the available licenses, the license usage, and any license violations.
Summary	Summary of the current status of the server and its components, including power and temperature statistics.
Interface cards	List of the adapters in the server with their location and current status. To view the DCE interfaces, vNICs, and vHBAs on a adapter, choose the adapter and click **View Details**.
Fan Modules	List of the fan modules in the server with their current status. This tab is only available for rack-mount servers. To view the fans in a fan module, choose the fan module and click **View Details**.
Power Supply Units	List of the PSUs in the server with their current status. This tab is only available for rack-mount servers.
Events	List of the current events for the server and its components, with information about each event.
Suppression Tasks	List of the fault suppression tasks, if any, including the associated policy and schedule.
Processor Units	List of the CPUs in the server with their location and current status.
Memory Units	List of the memory units in the server with their type, location, and current status.
Storage Controllers	List of the storage controllers in the server.

Name	Description
Faults	List of the current faults for the server and its components, with information about each fault.
Service Request Details	List of the service requests for the server and its components, including the asset type and change description.
More Reports	Additional reports that you can generate for the server and its components, including voltage, power, and temperature reports.

Step 7 To return to the main window, click **Back**.

Monitoring a FEX and its Components

For a Cisco UCS domain that includes one or more rack-mount servers, you can use Cisco UCS Director to monitor each Fabric Extender (FEX) that connects the rack-mount servers to the fabric interconnects.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account

Step 3 Click **FEX**.

Step 4 Click the row for the FEX that you want to monitor.

Step 5 Click **View Details**.
Cisco UCS Director displays information about the current status of the selected component. Click the tabs in the window for more details about that component.

Step 6 Click on one of the following to view the status of the FEX or a specific component in the FEX:

Name	Description
License Status	Overview of the available licenses, the license usage, and any license violations.
Power Supply Units	List of the PSUs with their current status.
Fans	List of the fans in the FEX with their current status.
Suppression Tasks	List of the fault suppression tasks, if any, including the associated policy and schedule.
IO Modules	List of the I/O modules in the FEX with their location and current status.

Name	Description
Faults	List of the current faults for the fabric interconnect and its components, with information about each fault.

Step 7 To return to the main window, click **Back**.

Viewing the Cisco UCS Manager Pending Activities Report and User Acknowledgement

When changes are made to a service profile that is already associated with a server, you must reboot the server to complete the process. The Reboot policy determines when the disruptive changes are implemented. If the maintenance policy is not set to Immediate, all the changes made stay in pending mode until the specified maintenance window or until you acknowledge it explicitly.

This report shows you the **Pending Activities** that are waiting for user acknowledgement, including service profile name, and server affected information.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, choose a **Pod**.

Step 3 Choose a **Cisco UCS Manager Account** under the **Pod**.

Step 4 On the **UCS Manager Account** screen, click the drop-down list at the far right to choose **Pending Activities**. You can view the activities that are in pending state and require user acknowledgement.

a) Select the pending activity that you want to deploy immediately, and click **Acknowledge** to apply the changes.

b) On the **Acknowledge Pending Activity** screen, click **Acknowledge**.
Cisco UCS Manager immediately reboots the server affected by the pending activity.

After the activity has been acknowledged, it is removed from the pending activities report.

TPM Monitoring

Trusted Platform Module (TPM) is included on all Cisco UCS M3 blade and rack-mount servers. Operating systems can use TPM to enable encryption. For example, Microsoft's BitLocker Drive Encryption uses the TPM on Cisco UCS servers to store encryption keys.

Cisco UCS Manager enables monitoring of TPM, including whether TPM is present, enabled, or activated.

Inventory Reports

Viewing Storage Profile Management Reports

Reports are added to Storage Profile, Storage Profile LUN and PCH Controller definitions. Storage Profile data is collected from the Cisco UCS Manager appliance based on the version of the Cisco UCS Manager. If the version is supported, Storage Profile inventory collects the Storage profile related data and the collected data is represented as tabular reports

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Storage Profiles**.
Step 4 From the **Storage Profiles** list, choose the organization.
Step 5 Click **View Details**.
Step 6 Click on either **Local LUNs**, the **PCH Controller Definitions**, or the **Storage Profiles Usage-Service Profiles/Template** to see the respective report.

Viewing the Cisco UCS Chassis Inventory Report

This report shows you the number of chassis in a Cisco UCS Manager account and how many of them are powered on.

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **More Reports**.
Step 4 From the **Reports** drop-down list, choose **UCS Chassis Inventory**.

Viewing the Disk Group Policy Inventory Reports

Disk Group Policy data is collected from the Cisco UCS Manager appliance based on the version of the Cisco UCS Manager. If the version is supported, Disk Group Policy inventory collection is done.

The collected data is represented as tabular reports.

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Organizations**.
Step 4 From the **Organizations** list, choose the organization.
Step 5 Click **View Details**.
Step 6 Click **DiskGroup Policy**.
Step 7 From the **DiskGroup Policy** list, choose a disk.
Step 8 Click **View Details**.
Step 9 Click on either the **Virtual Drive** or the **Disk Group** to see the respective report.

Viewing the Cisco UCS Fabric Interconnect Inventory Report

This report shows you the number of fabric interconnects in a Cisco UCS Manager account and how many of them are operable.

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **More Reports**.
Step 4 From the **Reports** drop-down list, choose **UCS Fabric Interconnect Inventory**.

Viewing the Cisco UCS Servers Inventory Report

This report shows you the number of Cisco UCS servers in a Cisco UCS Manager account and how many of those servers are operable.

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **More Reports**.
Step 4 From the **Reports** drop-down list, choose **UCS Server Inventory**.

Viewing the Cisco UCS Server Association Report

This report shows you the number of associated, unassociated, and other Cisco UCS servers in a Cisco UCS Manager account.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **More Reports**.

Step 4 From the **Reports** drop-down list, choose **UCS Servers Associated vs Unassociated**.

Viewing the vMedia Policy Inventory Report

This report shows you the vMedia Policy distinguished name (DN), description, the retry option for mount failure, policy level, and owner. You can also drill down on the policy report to obtain a list of all the vMedia mounts available under the vMedia policy.

You can also create, edit, or delete a vMedia policy. See Creating a vMedia Policy and vMount, on page 117.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod with the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Choose the row with the organization for which you want to view the vMedia policy and click **View Details**.

Step 5 Click **vMedia Policy**.
vMedia policies include one or more vMedia mounts. In most cases, there is one vMedia Mount per vMedia Policy. To view the **vMedia Mount** report, select the vMedia Policy and click **View Details**. The report shows you the vMedia mounts for the policy, including distinguished name (DN), mount name, device type, protocol, authentication information, remote server information, remote path, remote filename, and user.

Exporting an Inventory Report

You can export an inventory report in PDF, CSV, or XLS format.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **More Reports**.

Step 4 From the **Reports** drop-down list, choose the report that you want to export.

Step 5 Click**Export Report**.

Step 6 On the **Export Report** screen, choose the desired report format from the **Select Report Format** drop-down list and then click **Generate Report**.

Step 7 After the report has been generated, click **Download**.

Step 8 After you have downloaded the report, click **Close**.

Cisco UCS Events

In Cisco UCS, each event represents a nonpersistent condition in the Cisco UCS domain. After Cisco UCS Manager creates and logs an event, the event does not change. For example, if you power on a server, Cisco UCS Manager creates and logs an event for the beginning and the end of that request.

You can view all events in a Cisco UCS Manager account from Cisco UCS Director. You can view Cisco UCS events for individual Cisco UCS Manager accounts or for specific components in the account, such as a server or fabric interconnect.

Viewing Cisco UCS Events for a Cisco UCS Manager Account

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Events**.

Step 4 (Optional) To view events for a component within the account, do the following:

a) Navigate to the component, such as servers or fabric interconnects.
b) Click on the row for the component for which you want to view events.
c) Click **View Details**.
d) Click **Events**.

Step 5 (Optional) To customize the columns that you see in the table and any report that you generate, do the following:

a) On the table menu bar, click the **Customize Table Columns** button.
b) In the **Customize Report Table** dialog box, check or uncheck the check boxes to determine which elements you see in the report and click **Save**.

Step 6 (Optional) To export a report of what you see in the tab, do the following:

a) On the table menu bar, click **Export Report**.
b) In the **Export Report** dialog box, select a report format and click **Generate Report**.
c) When the report has generated, click **Download**.
d) If the report opens in a separate tab, use the download button from your browser to download the report.
e) In the **Export Report** dialog box, click **Close**.

Cisco UCS Faults

Each Cisco UCS fault represents a failure in the Cisco UCS domain or an alarm threshold that has been raised. During the lifecycle of a fault, it can change from one state or severity to another.

Each fault includes information about the operational state of the affected object at the time the fault was raised. If the fault is transitional and the failure is resolved, the object transitions to a functional state.

You can view all faults in a Cisco UCS Manager account from Cisco UCS Director. You can also view Cisco UCS faults at the pod level, either for individual Cisco UCS Manager accounts or for specific components in the account.

For more information about Cisco UCS faults, see the Cisco UCS Faults and Error Messages Reference and the Cisco UCS Manager B-Series Troubleshooting Guide.

Viewing Cisco UCS Faults for a Pod

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Faults**.
Step 4 (Optional) To export a report of what you see in the tab, do the following:
a) On the table menu bar, click **Export Report**.
b) In the **Export Report** dialog box, select a report format and click **Generate Report**.
c) When the report has generated, click **Download**.
d) If the report opens in a separate tab, use the download button from your browser to download the report.
e) In the **Export Report** dialog box, click **Close**.

Viewing Cisco UCS Faults for a Cisco UCS Manager Account

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Faults**.

Step 4 (Optional) To view faults for a component or object within the account, do the following:

a) Navigate to the component or object, such as service profiles, servers, or organizations.
b) Click on the row in the table for the component or object for which you want to view faults.
c) Click **View Details**.
d) Click the **Faults**.

Step 5 (Optional) To customize the columns that you see in the table and any report that you generate, do the following:

a) On the table menu bar, click the **Customize Table Columns** button.
b) In the **Customize Report Table** dialog box, check or uncheck the check boxes to determine which elements you see in the report and click **Save**.

Step 6 (Optional) To export a report of what you see in the tab, do the following:

a) On the table menu bar, click **Export Report**.
b) In the **Export Report** dialog box, select a report format and click **Generate Report**.
c) When the report has generated, click **Download**.
d) If the report opens in a separate tab, use the download button from your browser to download the report.
e) In the **Export Report** dialog box, click **Close**.

Fault Suppression

Fault suppression allows you to suppress SNMP trap and Call Home notifications during a planned maintenance time. You can create a fault suppression task to prevent notifications from being sent whenever a transient fault is raised or cleared.

Faults remain suppressed until the time duration has expired, or the fault suppression tasks have been manually stopped by the user. After the fault suppression has ended, Cisco UCS Director sends notifications for any outstanding suppressed faults that have not been cleared.

Adding a Fault Suppression Task for a Chassis

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **UCS Chassis**.

Step 4 Click the row for the chassis for which you want to suppress faults.

Step 5 Click **Start/Stop Fault Suppression**.

Step 6 On the **Fault Suppression** screen, expand **Locally Defined Suppression Tasks** and click **Add**.

Step 7 On the **Add Entry to Locally Defined Suppression Tasks** screen, complete the following fields and click **Submit**:

Name	Description
Name field	A unique name for the fault suppression task.
Select Fixed Time Interval/Schedule drop-down list	Choose when the fault suppression task will run. This can be one of the following: • **Fixed Time Interval—**Specifies the start time and duration for the fault suppression task. Specify the day and time that the fault suppression task should start in the **Start Time** field. Click the calendar icon at the end of this field to choose the start time from a pop-up calendar. Specify the length of time that this task should run in the **Task Duration** field. To specify that this task should run until it is manually stopped, enter 00:00:00:00 in this field. • **Schedule—**Configures the start time and duration using a predefined schedule. Choose the schedule from the **Schedule** drop-down list.

Name	Description
Suppression Policy drop-down list	Choose the predefined suppression policy to be applied to this task. This can be one of the following: • **default-server-maint—**Suppresses faults for blade servers. • **default-iom-maint—**Suppresses faults for IOMs in a chassis. • **default-chassis-all-maint—**Suppresses faults for the chassis and all components installed into the chassis, including all blade servers, power supplies, fan modules, and IOMs. • **default-chassis-phys-maint—**Suppresses faults for the chassis and all fan modules and power supplies installed into the chassis.

Repeat this step to add additional fault suppression tasks.

Step 8 When you have added all fault suppression tasks, click **Submit**.

Adding a Fault Suppression Task for a FEX

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **FEX**.

- **Chassis** tab
- **FEX** tab

Step 4 Click the row in the table for the FEX for which you want to suppress faults.

Step 5 Click the row for the Chassis or FEX for which you want to suppress faults on an I/O module and click **View Details**.

Step 6 Click **Start/Stop Fault Suppression**.

Step 7 On the **Fault Suppression** screen, expand **Locally Defined Suppression Tasks** and click **Add**.

Step 8 On the **Add Entry to Locally Defined Suppression Tasks** screen, complete the following fields and click **Submit**:

Name	Description
Name field	A unique name for the fault suppression task.
Select Fixed Time Interval/Schedule drop-down list	Choose when the fault suppression task will run. This can be one of the following: • **Fixed Time Interval—**Specifies the start time and duration for the fault suppression task. Specify the day and time that the fault suppression task should start in the **Start Time** field. Click the calendar icon at the end of this field to choose the start time from a pop-up calendar. Specify the length of time that this task should run in the **Task Duration** field. To specify that this task should run until it is manually stopped, enter 00:00:00:00 in this field. • **Schedule—**Configures the start time and duration using a predefined schedule. Choose the schedule from the **Schedule** drop-down list.
Suppression Policy drop-down list	Choose the predefined suppression policy to be applied to this task. This can be one of the following: • **default-fex-phys-maint—**Suppresses faults for the FEX and all fan modules and power supplies in the FEX. • **default-fex-all-maint—**Suppresses faults for the FEX and all power supplies, fan modules, and IOMs in the FEX. • **default-iom-maint—**Suppresses faults for IOMs in the FEX.

Repeat this step to add additional fault suppression tasks.

Step 9 When you have added all fault suppression tasks, click **Submit**.

Adding a Fault Suppression Task for an I/O Module

You can suppress faults on an I/O module in a FEX or chassis.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click one of the following:

- **Chassis** tab
- **FEX** tab

Step 4 Click the row for the Chassis or FEX for which you want to suppress faults on an I/O module and click **View Details**.

Step 5 Click **IO Modules**.

Step 6 Click the row for the I/O module for which you want to suppress faults.

Step 7 Click **Start/Stop Fault Suppression**.

Step 8 On the **Fault Suppression** screen, expand **Locally Defined Suppression Tasks** and click **Add**.

Step 9 On the **Add Entry to Locally Defined Suppression Tasks** screen, complete the following fields and click **Submit**:

Name	Description
Name field	A unique name for the fault suppression task.
Select Fixed Time Interval/Schedule drop-down list	Choose when the fault suppression task will run. This can be one of the following: • **Fixed Time Interval—**Specifies the start time and duration for the fault suppression task. Specify the day and time that the fault suppression task should start in the **Start Time** field. Click the calendar icon at the end of this field to choose the start time from a pop-up calendar. Specify the length of time that this task should run in the **Task Duration** field. To specify that this task should run until it is manually stopped, enter 00:00:00:00 in this field. • **Schedule—**Configures the start time and duration using a predefined schedule. Choose the schedule from the **Schedule** drop-down list.
Suppression Policy drop-down list	Choose the predefined suppression policy to be applied to this task. This policy is **default-iom-maint**, which suppresses faults for IOMs in a chassis or FEX.

Repeat this step to add additional fault suppression tasks.

Step 10 When you have added all fault suppression tasks, click **Submit**.

Adding a Fault Suppression Task for a Server

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **UCS Servers**.

Step 4 Click the row for the server for which you want to suppress faults.

Step 5 Click **Start/Stop Fault Suppression**.

Step 6 On the **Fault Suppression** screen, expand **Locally Defined Suppression Tasks** and click **Add**.

Step 7 On the **Add Entry to Locally Defined Suppression Tasks** screen, complete the following fields and click **Submit**:

Name	Description
Name field	A unique name for the fault suppression task.
Select Fixed Time Interval/Schedule drop-down list	Choose when the fault suppression task will run. This can be one of the following: • **Fixed Time Interval—**Specifies the start time and duration for the fault suppression task. Specify the day and time that the fault suppression task should start in the **Start Time** field. Click the calendar icon at the end of this field to choose the start time from a pop-up calendar. Specify the length of time that this task should run in the **Task Duration** field. To specify that this task should run until it is manually stopped, enter 00:00:00:00 in this field. • **Schedule—**Configures the start time and duration using a predefined schedule. Choose the schedule from the **Schedule** drop-down list.
Suppression Policy drop-down list	Choose the pre-defined suppression policy to be applied to this task. This policy can be **default-server-maint**, which suppresses faults for blade and rack-mount servers.

Repeat this step to add additional fault suppression tasks.

Step 8 When you have added all fault suppression tasks, click **Submit**.

Viewing Fault Suppression Tasks

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click one of the following:

- **Chassis**
- **FEX**
- **UCS Servers**

Step 4 Click the row for the chassis, FEX, or server for which you want to view fault suppression tasks and click **View Details**.

Step 5 Click **Suppression Tasks**.