Cisco UCS Director UCS Central Management Guide, Release 6.6

First Published: 2018-04-27

Last Modified: 2018-10-10

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: https://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. (1721R)

© 2018 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 9

Preface

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`.
System output	Terminal sessions and information that the system displays appear in `this font`.

Text Type	Indication
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 . RSS feeds are a free service.

CHAPTER 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 6.6

Feature	Description	Where Documented
Support for VSAN Cluster configuration through Cisco UCS Central	This release of Cisco UCS Director introduces support for VSAN cluster configuration on servers managed via Cisco UCS Central accounts. You can use the workflow to configure servers managed through UCS Central account, install ESXi on a SD on these servers, add them to the vCenter, and create a VSAN cluster with these hosts.	Adding a Cisco UCS Central Account

CHAPTER 2

Overview

This chapter contains the following sections:

Cisco UCS Central Management through Cisco UCS Director

Cisco UCS Director uses orchestration to automate some of the steps required to configure the Cisco UCS domains registered with Cisco UCS Central and to provide a statistical analysis of the data.

When you add a Cisco UCS Central account, Cisco UCS Director performs an inventory collection on the Cisco UCS Central configuration. During inventory collection, Cisco UCS Director discovers and imports the existing configuration, including the following:

- Domain groups
- Domain group policies
- Registration policies
- Each registered Cisco UCS domain and the Cisco UCS Manager inventory for that Cisco UCS domain, including the following:
  - Fabric interconnects
  - Chassis
  - Servers

After you add a Cisco UCS Central account and its inventory collection is complete, you can use Cisco UCS Director to register more Cisco UCS Manager accounts with that Cisco UCS Central account, if desired.

Cisco UCS Director provides you with complete visibility into Cisco UCS Central and the registered Cisco UCS domains. In addition, you can use Cisco UCS Director to manage and configure those Cisco UCS domains.

Cisco UCS Central 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 Cisco UCS domains registered with Cisco UCS Central.

Configuration and Administration

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

- Global and local service profiles
- Global and local policies

Monitoring and Reporting

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

- Service profile association
- vNICs
- vHBAs
- Cisco UCS hardware, including fabric interconnects, chassis, and servers

You can also manually acknowledge any pending activities. See Viewing the Cisco UCS Central Pending Activities Report and User Acknowledgement, on page 75.

Cisco UCS Central 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 registered with Cisco UCS Central, such as the following:

- Creation of some policies
- Firmware upgrades
- User management

Read-Only Policies

You cannot create all policies in a Cisco UCS Central account. Cisco UCS Director provides a read-only view of those policies in the details of the organization that includes them. Create these read-only policies in a Cisco UCS Manager account that includes the organization.

The read-only policies include the following:

- Dynamic vNIC connection policies

- Ethernet and Fibre Channel adapter policies
- IPMI access profiles
- Local disk configuration policies
- Maintenance policies
- Network control policies
- Power control policies
- QoS policies
- Scrub policies
- Serial over LAN policies
- Server pool policies
- Server pool policy qualifications
- Threshold policies
- vNIC/vHBA placement policies

Cisco UCS Central Orchestration Tasks

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

For more information about orchestration and examples of workflows in Cisco UCS Director, see the Cisco UCS Director Orchestration Guide.

Location of Orchestration Tasks

A complete list of the Cisco UCS Central orchestration tasks is available in the Workflow Designer, in the UCS Central Tasks section of the Task Library, and in the **Cisco UCS Central Tasks** folder. The Task Library includes a description of the orchestration tasks, and 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 Central orchestration tasks include the following:

- Group assignment
- Domain groups
- Cisco UCS Manager registration

- VLANs
- Global service profiles
- Global service profile templates
- Time zones

CHAPTER 3

Configuring Cisco UCS Central Accounts

This chapter contains the following sections:

Multi-Domain Managers

A multi-domain manager is an application that can manage more than one domain. For example, Cisco UCS Central is a multi-domain manager that manages one or more registered Cisco UCS domains.

Server Management

Server Management

When you add a Cisco UCS Central account, 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.

If you choose this option, all servers are added in the Managed state.

Selected Servers

Only selected servers are managed by Cisco UCS Director. 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.

Note In order to be able to use the servers, it would be required to manually move them to Managed state.

When you move the servers from Managed to Unmanaged state, initially, the servers are moved to a Transition state. After keeping them in that state for around 6 hours, Cisco UCS Director moves them to Unmanaged state. During this time, the servers are removed from the Servers report.

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

You can monitor the servers and view the details in the Viewing the Discovered Servers Report for Cisco UCS Central Domain chapter.

Selecting a Server for Management

Before you begin

You can choose which servers you want Cisco UCS Director to manage in a Cisco UCS Central Account. For this task, make sure that you choose the **Selected Servers** option under server management, while adding a Cisco UCS Central account.

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 Expand the **UCS Central Accounts**, and click the Cisco UCS Central account that you want to work on.

Step 4 On the **UCS Central Accounts** screen, click **All UCS Domains**.

Step 5 Click a Cisco UCS domain that you want to work on and from the **More Actions** drop-down list, choose **View Details**.

Step 6 Click **Discovered Servers**.

You can see all servers in the Cisco UCS domain discovered by Cisco UCS Manager.

Step 7 Click **Manage Servers**.

Step 8 On the **Manage Servers** screen, check the boxes for those servers that you want to have managed.

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

Step 9 Click **Submit**.

Unmanaging a Server

If you have configured the server management option as **Selected Servers** while adding a Cisco UCS Central account, you can edit server state through Cisco UCS Director.

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 Expand the **UCS Central Accounts**, and click the Cisco UCS Central account that you want to work on.

Step 4 On the **UCS Central Accounts** screen, click **All UCS Domains**.

Step 5 Click a Cisco UCS domain that you want to work on and from the **More Actions** drop-down list, choose **View Details**.

Step 6 Click **Discovered Servers**.

You can see all servers in the Cisco UCS domain discovered by Cisco UCS Manager.

Step 7 Click **Unmanage Servers**.

Step 8 On the **Unmanage Servers** screen, uncheck the boxes for those servers that you no longer want to have managed.

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 6 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.

Step 9 Click **Submit**.

Cisco UCS Central Accounts

Each Cisco UCS Central account represents a single Cisco UCS Central, plus all the Cisco UCS domains registered with that Cisco UCS Central.

When you create a Cisco UCS Central account all Cisco UCS domains that are registered with that Cisco UCS Central, and their related Cisco UCS Manager accounts, are imported into Cisco UCS Director. 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.

Note Cisco UCS Central is a multi-domain manager; you do not create the Cisco UCS Central account in a pod.

Adding a Cisco UCS Central Account

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

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

Step 3 On the **Multi-Domain Managers** page, click **Add Account**.

Step 4 On the Add Account screen, from the **Account Type** drop-down list, choose UCS Central.

Step 5 Click **Submit**.

Step 6 On the **Multi-Domain Manager Account** screen, enter the information for the following fields:

Name	Description
Account Name field	A unique name that you assign to this account.
Description field	(Optional) A description of this account.
Account Type drop-down list	Is pre-populated with **UCS Central** by default. If not, choose **UCS Central**.

Name	Description
Server Managements drop-down list	Choose the servers that you want to manage in this account. It can be one of the following: • **All Servers**—This is a default option. It allows you to add all the servers. If you choose this option, all servers are added in Managed state. • **Selected Servers**—Only selected servers are managed by Cisco UCS Director. You can view them in the Discovered Servers report. Viewing the Discovered Servers Report for Cisco UCS Central Domain, on page 77 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.
Pod drop-down list	Choose the pod that you want to manage in this account. A single VSAN pod supports either a Cisco UCS Manager account or a Cisco UCS Central account.
Server Address field	The IP address of Cisco UCS Central.
Use Credential Policy check box	Check the box if you want to use a policy to provide the credentials. A **Credential Policy** drop-down list comes up. Choose a policy defined in UCS Central. Or add a new one. As a result, the User ID, Password, Transport Type, and Port fields become unavailable.
User ID field	The username that this account uses to access Cisco UCS Central. This username must be a valid account in Cisco UCS Central. **Note** When creating a UCS Central account integrated with LDAP, the username must be in the following format: **ucs-<*Domain Name*>\*username*** For example: ucs-vxendomain.com\jdoe123
Password field	The password associated with the username.
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**
Port field	The port used to access Cisco UCS Central.
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.

Step 7 Click **Submit**.

Cisco UCS Director tests the connection to Cisco UCS Central. If that test is successful, it adds the Cisco UCS Central account and discovers all infrastructure elements and registered Cisco UCS domains in 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 **Infrastructure System Parameters** 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.

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 Central Account

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Assigning a Cisco UCS Domain to a Pod

After you assign a Cisco UCS domain to a pod, Cisco UCS Director displays it as a Cisco UCS Manager account, and you can configure, monitor, and obtain reports on that account.

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 Choose an Account, and click the **All UCS Domains** tab. Then click the row for the domain that you want to assign to a pod.

Step 5 From the **More Actions** drop-down list, choose **Assign to Pod**.

Step 6 On the **Assign to Pod** screen, complete the following fields:

Name	Description
Pod drop-down list	Choose the pod to which this account belongs.
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. It is enabled or disabled anyone with administrator 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 by Cisco UCS Director. 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 by Cisco UCS Director. 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. For more information, see the Cisco UCS Director Management Guide for Cisco UCS Manager for the appropriate release.
Account Name field	A unique name that you assign to this account.
Description field	(Optional) A description of this account.
User ID field	The username that this account uses to access Cisco UCS Manager. This username must be a valid account in Cisco UCS Manager.
Password field	The password associated with the username.
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**
Port field	The port used to access Cisco UCS Manager.
Contact Email field	The email address that you can use to contact the administrator or other person responsible for this account.

Name	Description
Location field	The location of this account.
Service Provider field	(Optional) The name of the service provider associated with this account, if any.

Step 7 Click **Submit**.

Unassigning a Cisco UCS Domain from a Pod

When you unassign a Cisco UCS domain from a pod, Cisco UCS Director does not delete the related Cisco UCS Manager account. If you want to delete the account, use **Administration** > **Physical Accounts**.

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Account** page, choose an Account, and click the **All UCS Domains** tab. Then click the row for the domain that you want to unassign from a pod.

Step 5 From the **More Actions** drop-down list, choose **Unassign from Pod**.

Step 6 On the **UCSM Account** screen, 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

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organization**.

Step 6 Click **Add**.

Step 7 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.

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

Time Zones

Cisco UCS requires a domain-specific time zone setting and an NTP server to ensure the correct time displays in Cisco UCS Central. 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

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Time Zones**.

Step 6 Click **Add**.

Step 7 On the **Add Time Zone** screen, do the following:

a) From the **NTP Server Name** drop-down list, enter the IP address or hostname of the NTP server for this time zone.

b) Click the **Domain Group**, check the boxes for the domains that you want to add to the domain group.

c) From the **Time Zone** drop-down list, select a Time Zone for your account.

d) Click **Submit**.

CHAPTER 4

Configuring Domain Groups

This chapter contains the following sections:

Domain Groups

Cisco UCS Central creates a hierarchy of Cisco UCS domain groups for managing multiple Cisco UCS domains. You will have the following categories of domain groups in Cisco UCS Central:

- **Domain Group** — A group that contains multiple Cisco UCS domains. You can group similar Cisco UCS domains under one domain group for simpler management.
- **Ungrouped Domains** — When a new Cisco UCS domain is registered in Cisco UCS Central, it is added to the ungrouped domains. You can assign the ungrouped domain to any domain group.

If you have created a domain group policy, and a new registered Cisco UCS domain meets the qualifiers defined in the policy, it will automatically be placed under the domain group specified in the policy. If not, it will be placed in the ungrouped domains category. You can assign this ungrouped domain to a domain group.

Each Cisco UCS domain can only be assigned to one domain group. You can assign or reassign membership of the Cisco UCS domains at any time. When you assign a Cisco UCS domain to a domain group, the Cisco UCS domain will automatically inherit all management policies specified for the domain group.

Before adding a Cisco UCS domain to a domain group, make sure to change the policy resolution controls to local in the Cisco UCS domain. This will avoid accidentally overwriting service profiles and maintenance policies specific to that Cisco UCS domain. Even when you have enabled auto discovery for the Cisco UCS domains, enabling local policy resolution will protect the Cisco UCS domain from accidentally overwriting policies.

Important

- Make sure to create a separate domain groups for all modular server domains. Also make sure the modular server domain groups are not hierarchical.
- You must create separate infrastructure firmware policy for modular domains in Cisco UCS Central. The infrastructure firmware policies must be unique to modular servers. This will prevent any firmware policy resolution issues with other domain groups.

Creating a Domain Group

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Domain Groups**.

Step 6 Click **Add**.

Step 7 On the **Domain Group** screen, do the following:

a) In the **Name** field, enter a unique name for the domain group.
b) (Optional) In the **Description** field, enter a description for the domain group.
c) Click the **Parent Domain Group**, and check the boxes for the domains that you want to add to the domain group.
d) Click **Submit**.

Adding a Cisco UCS Domain to a Domain Group

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Ungrouped UCS Domains**. Then click the row for the domain that you want to add to a domain group.

Step 6 Click **Change Group Membership**.

Step 7 On the **Select Domain Group** screen, do the following:

a) Check the check box for the domain group to which you want to add the domain.
b) Click **Submit**.

Changing Domain Group Membership for a Cisco UCS Domain

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Ungrouped UCS Domains**. Then click the row for the domain for which you want to change the domain group.

Step 6 Click **Change Group Membership**.

Step 7 On the **Select Domain Group** screen, do the following:

a) Uncheck the check box for the domain group from which you want to remove the domain.
b) Check the check box for the domain group to which you want to add the domain.
c) Click **Submit**.

Removing a Cisco UCS Domain from a Domain Group

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **All UCS Domains**. Then click the row in the table for the domain that you want to remove from a domain group.

Step 6 Click **Delete**.

Step 7 On the **Delete Domain Group** screen, click **Submit**.

Creating a Domain Group Qualification Policy

Contains the domain group policy qualifications for the domain group policies.

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Domain Group Policy Qualifications**.

Step 6 Click **Add**.

Step 7 On the **Create Domain Group Policy Qualifications** screen, enter a unique name and description for the qualification policy. Click **Next**.

Step 8 On the **Domain Group Policy Qualification - Addresses** screen, do the following:

a) Click +. This displays the **Add Entry to** dialog box.
b) On the **Add Entry to** screen, enter the minimum and maximum IP addresses and click **Submit**.
c) After you have added all desired address qualifications, click **Next**.

If you do not want to include an address qualification in the registration policy, you can click **Next**.

Step 9 On the **Domain Group Policy Qualification - Sites** screen, do the following:

a) Click +. This displays the **Add Entry to Sites**.
b) On the **Add Entry to Sites** screen, enter the **Site Name** and **Regex** and click **Submit**.
c) After you have added all desired site qualifications, click **Next**.

If you do not want to include a site qualification in the registration policy, you can click **Next**.

Step 10 On the **Domain Group Policy Qualification - Owners** screen, do the following:

a) Click +. This displays the **Add Entry to Owners**dialog box.
b) On the **Add Entry to Owners** screen box, enter the **Owner Name** and **Regex** and click **Submit**.
c) After you have added all desired owner qualifications, click **Next**.

If you do not want to include an owner qualification in the registration policy, you can click **Next**.

Step 11 Click **Submit**.

Creating a Domain Group Policy

Before you begin

Create at least one registration policy with domain group policy qualifications that you can include in this policy.

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Domain Group Policies**.

Step 6 Click Add (+).

Step 7 On the **Add Domain Group Policy** screen, do the following:

a) In the **Name** field, enter a unique name for the domain group.
b) (Optional) In the **Description** field, enter a description for the domain group.
c) Click the **Domain Group**, and check the boxes for the domains that you want to add to the domain group policy.
d) Click the **Domain Group Policy Qualification**, and check the boxes for qualifications that you want to add to the domain group policy.

Step 8 Click **Submit**.

CHAPTER 5

Configuring Network Connections

This chapter contains the following sections:

Global VLANs

You can define global VLANs in the domain group root, or a domain group below the root. Global VLANs can only be common or global. You cannot assign them to a specific fabric interconnect.

Resolution of global VLANs takes place prior to the deployment of global service profiles. If a global service profile references a global VLAN, and that VLAN does not exist, deployment of the global service profile fails due to insufficient resources. All global VLANs created in a Cisco UCS Central account must be resolved before deploying the global service profile.

All global VLANs configured in a Cisco UCS Central account are common to the domains in which they are created. However, organization permissions must first be assigned before the Cisco UCS domains that are part of the organizations can consume the resources. By default, no organization permissions are assigned when you create a global VLAN. Once organization permissions have been granted to a VLAN, it becomes visible to those organizations. It is also available to be referenced in service profiles that are part of those organizations.

A global VLAN is visible to a Cisco UCS Manager account only if you deploy a global service profile that references the VLANs. Once a VLAN that is deployed with a global service profile becomes available in a Cisco UCS Manager account, you can include it in a local service profile and policy. You cannot turn a global VLAN into a local VLAN.

A global VLAN is not deleted when you delete a global service profile that references it. Delete the global VLAN from the Cisco UCS Central account.

Creating a Global VLAN

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Common VLANs**.

Step 6 Click **Add**.

Step 7 On the **Add VLAN** screen, do the following:

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

The VLAN name is case-sensitive.

b) In the **VLAN ID** field, enter a unique identifier to be assigned to the network.

A VLAN ID can:

- Be between 1 and 3967
- Be between 4048 and 4093
- Overlap with other VLAN IDs already defined in other domain groups
- The VLAN IDs you specify must also be supported on the switch that you are using.

c) From the **Fabric ID** drop-down list, choose the the Fabric ID.

d) In the **Domain Group** field, check the check box for the domain group in which you want to create the global VLAN.

e) Click **Submit**.

Publishing a Global VLAN

Global VLANs can be published to the associated domains, and those VLANs are then available at domain level. For a VLAN associated to a domain group (x), it can be published to any of the domains linked with the same domain group (x).

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Common VLANs**.

Step 6 From the list of VLANs, select the VLAN to be published.

Step 7 From the **More Actions** drop-down list, choose **Publish to USC Domain**.

Step 8 On the **Publish VLAN to USC Domain** screen, click the **Select** button.

Step 9 From the Select list, click the check box of the desired domain and click the **Select** button.

Step 10 In the **Publish VLAN to USC Domain**, click the **Submit** button.

Modifying Organization Permissions for a Global VLAN

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click the **Common VLANs**.

Step 6 Click the row for the global VLAN for which you want to modify organization permissions.

Step 7 From the **More Actions** drop-down list, choose **Modify Org Permissions**.

Step 8 On the **Organization List** screen, check the check boxes for the organizations in which you want to include the global VLAN.

Step 9 Click **Submit**.

IP Pools

IP pools are a collection of IP addresses. You can use IP pools in Cisco UCS Central in one of the following ways:

- For external management of Cisco UCS Manager servers.
- For iSCSI boot initiators.
- For both external management and iSCSI boot initiators in Cisco UCS Manager

Creating an IP Pool

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the IP pool and then click **View Details**.

Step 7 Click **IP Pools**.

Step 8 Click **Add**.

Step 9 On the **IP Pool** screen, enter a name and description for the IP pool.

Step 10 Expand the **IPv4 Block** field, enter the following:

Name	Description
From field	The first IP address in the block.
Size field	The number of IP addresses in the block.
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 is to access.
Secondary DNS	The secondary DNS server that this block of IP addresses is to access.
Scope	Whether the IP addresses in the block can be assigned to one or more Cisco UCS domains registered with Cisco UCS Central. This can be one of the following: **public** -The IP addresses in the block can be assigned to only one registered Cisco UCS domain. **private** -The IP addresses in the block can be assigned to multiple registered Cisco UCS domains.
ID Range Qualification Policy	Optional

Step 11 Expand the **IPv6 Block** field, enter the following:

Name	Description
From field	The first IP address in the block.
Size field	The number of IP addresses in the block.
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 is to access.
Secondary DNS	The secondary DNS server that this block of IP addresses is to access.

Name	Description
Scope	Whether the IP addresses in the block can be assigned to one or more Cisco UCS domains registered with Cisco UCS Central. This can be one of the following: **public** -The IP addresses in the block can be assigned to only one registered Cisco UCS domain. **private** -The IP addresses in the block can be assigned to multiple registered Cisco UCS domains.
ID Range Qualification Policy	Optional

Step 12 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

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the pool and then click **View Details**.

Step 7 Click **MAC Pools**.

Step 8 Click **Add**.

Step 9 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.
ID Range Qualification Policy drop-down list	Choose the ID Range Qualification Policy.

Step 10 Click **Submit**.

Adding an Address Block to a MAC Pool

Step 1 Choose **Physical** > **Compute**.
Step 2 On the **Compute** page, expand **Multi-Domain Managers**.
Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.
Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.
Step 5 Click **Organizations**.
Step 6 Click the organization in which you want to modify the pool and then click **View Details**.
Step 7 Click **MAC Pools**.
Step 8 Click the pool to which you want to add a block of addresses and then click **Create a Block of MAC Addresses**.
Step 9 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.
IP Range Qualification Policy drop-down list	Choose the IP Range Qualification Policy.

Step 10 Click **Submit**.

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 exist:

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

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organization**.

Step 6 Click the organization in which you want to create the policy and then click **View Details**.

Step 7 Click **vNIC Templates**.

Step 8 Click **Add**.

Step 9 On the **Add vNIC Template** screen, enter a unique name and description for the policy.

Step 10 From the **Fabric ID** drop-down list, choose the fabric interconnect that you want to associate with vNICs created from this template.

Step 11 Check the **Enable Failover** check box if you want vNICs created from this template to be able to access the other fabric interconnect if the chosen one is unavailable.

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 that has an adapter which does not support fabric failover, such as the Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter. If you do so, a configuration fault is generated when you associate the service profile with the server.

Step 12 Check one or both of the following **Target** check boxes to determine whether or not a VM-FEX port profile is automatically created with the appropriate settings for the vNIC template:

- **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.

Step 13 From the **Template Type** drop-down list, choose 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 14 Expand the **VLANs**, do the following to select the VLAN to be assigned to vNICs created from this template:

a) Click +. This displays the **Add Entry to VLANs**dialog box.
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 15 To associate policies with vNICs created from this template, complete the following fields:

Name	Description
MTU field	The MTU, or packet size, that vNICs created from this vNIC template must 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.
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.

Step 16 Click **Submit**.

What to do next

Include the vNIC template in a vNIC policy.

Creating a vNIC Policy

Before you begin

Make sure that at least one of the following exists in the Cisco UCS Central account and organization to which this policy applies:

- vNIC template
- Ethernet adapter policy

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

Step 2 Click **vNIC**.

Step 3 Click **Add**.

Step 4 On the **Create UCS Central vNIC Policy** screen, do the following:

a) In the **vNIC Name** field, enter a unique name for the policy.
b) From the **Account Name** drop-down list, choose a Cisco UCS Central account to which this policy applies.
c) From the **Organization** drop-down list, choose the organization to which this policy applies.

The **Use LAN Connectivity** checkbox, is selected by default.

d) From the **vNIC Template** drop-down list, choose a vNIC template.
e) From the **Adapter Policy** drop-down list, choose an adapter policy.
f) Click **Submit.**

What to do next

Include the vNIC policy 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

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organization**.

Step 6 Click the organization in which you want to create the policy and then click **View Details**.

Step 7 Click **LAN Connectivity Policies**.

Step 8 Click **Add**.

Step 9 On the **LAN Connectivity Policy** screen, enter a name and description for the policy.

Step 10 Expand **vNICs**, 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. 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 Template, on page 29.

d) Click **Submit**.

Repeat this step if you want to add more vNICs to the LAN Connectivity policy.

Step 11 After you have created all vNICs required for the policy, 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

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

Step 2 Click **Network Policy**.

Step 3 Click **Add**.

Step 4 On the **Create UCS Central Network Policy** screen, enter a name and description for the policy.

Step 5 Complete the following fields to specify the Cisco UCS Central connections for the policy:

- **UCS Central Account Name** drop-down list—Choose the Cisco UCS Central account to which you want to add this policy.
- **UCS Central Organization Name** drop-down list—Choose the Cisco UCS Central organization to which you want to add this policy.

Step 6 If this policy is to be assigned to service profiles for servers that support dynamic vNICs, choose a dynamic vNIC connection policy from the **Dynamic vNIC Connection Policy** drop-down list.

Step 7 From the **LAN Connectivity Type** drop-down list, choose one of the following connectivity types:

Option	Description
Expert	Allows you to create up to 10 vNICs that the server can use to access the LAN. Continue with Step 8.
Simple	Allows you to create a maximum of two vNICs that the server can use to access the LAN. Continue with Step 9.
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. Continue with Step 11.
Hardware Inherited	Uses the vNICs assigned to the Ethernet adapter profile associated with the server. Continue with Step 11.
Use LAN Connectivity Policy	Uses a LAN connectivity policy to determine the LAN connectivity for the server. Continue with Step 10.

Step 8 If you chose the expert LAN option, do the following:

a) In the **Add vNIC** field, specify 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 policy.
c) Continue with Step 11.

Step 9 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) Continue with Step 11.

Step 10 If you chose the LAN connectivity policy option, choose the policy that you want to associate with the server from the **LAN Connectivity Policy** drop-down list.

Step 11 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:

Global VSANs

You can define global VSANs in the domain group root, or a domain group below the root. Global VSANs are fabric-interconnect specific and can be created for either Fabric A or Fabric B. A global VSAN cannot be a common VSAN.

Resolution of global VSANs takes place prior to the deployment of global service profiles. If a global service profile references a global VSAN, and that VSAN does not exist, deployment of the global service profile fails due to insufficient resources. All global VSANs created in a Cisco UCS Central account must be resolved before deploying the global service profile.

A global VSAN is not deleted when you delete a global service profile that references it. Delete the global VSAN from the Cisco UCS Central account.

A global VSAN is visible to a Cisco UCS Manager account only if you deploy a global service profile that references the VSANs. Once a VSAN that is deployed with a global service profile becomes available in a Cisco UCS Manager account, you can include it in a local service profile and policy. You cannot turn a global VSAN into a local VSAN.

Creating a Global VSAN

You can create a global VSAN with IDs from 1 to 4093, except for those in the following reserved ranges:

- If you plan to use FC switch mode in a Cisco UCS domain, do not configure VSANs with an ID in the range from 3040 to 4078.

- If you plan to use FC end-host mode in a Cisco UCS domain, do not configure VSANs with an ID in the range from 3840 to 4079.

Note 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 for a VLAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE VLAN ID.

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **VSANs**.

Step 6 Click **Add**.

Step 7 On the **Add VSAN** screen, do the following:

a) In the **VSAN Name** field, enter a unique name for the VSAN. The VSAN name is case-sensitive.
b) In the **VSAN ID** field, enter a unique identifier to be assigned to the network.
c) In the **Domain Group** field, check the check box for the domain group in which you want to create the global VSAN.
d) From the **Fabric ID** drop-down list, choose the fabric interconnect where you want to create the global VSAN.
e) In the **FCOE VLAN** field, enter the ID for the VLAN to be used for transporting the VSAN and its Fibre Channel packets.
f) Click **Submit**.

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

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the pool and then click **View Details**.

Step 7 Click **WWNN Pools**.

Step 8 Click **Add**.

Step 9 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.
ID Range Qualification Policy drop-down list	Choose the ID Range Qualification Policy.

Step 10 Click **Submit**.

WWXN Pools

A WWXN pool is a WWN pool that contains both WW node names and WW port names.

Creating a WWXN Pool

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the pool and then click **View Details**.

Step 7 Click **WWXN Pools**.

Step 8 Click **Add**.

Step 9 On the **Add WWXN 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 WWXN address in the block.
Size field	The number of WWXN addresses in the block.
ID Range Qualification Policy drop-down list	Choose the ID Range Qualification Policy.

Step 10 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

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

Step 2 In the left pane, expand **Multi-Domain Managers**.

Step 3 In the left pane, expand **UCS Central Accounts** and then click the Cisco UCS Central account.

Step 4 In the right pane, click the **Organizations** tab.

Step 5 Click the organization in which you want to create the pool and then click **View Details**.

Step 6 Click the **WWPN Pools** tab.

Step 7 Click **Add**.

Step 8 In the **Add WWPN Pool** dialog box, 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.
ID Range Qualification Policy drop-down list	Choose the ID Range Qualification Policy.

Step 9 Click **Submit**.

Adding a WWN Block

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to modify the pool and then click **View Details**.

Step 7 Click one of the following tabs:

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

Step 8 Click the pool to which you want to add a WWN block.

Step 9 Click **Create WWN Block**.

Step 10 On the **Create WWN Block** screen, complete the following fields:

Name	Description
Description field	Type a description.
From field	The first WWNN, WWPN, or WWXN address in the block.
Size field	The number of WWNN, WWPN, or WWXN addresses in the block.
ID Range Qualification Policy drop-down list	Choose the ID Range Qualification Policy.

Step 11 Click **Submit**.

IQN Pools

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 pools created in Cisco UCS Central can be shared between Cisco UCS domains. 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

Creating an IQN Pool

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the pool and then click **View Details**.

Step 7 Click **IQN Pools**.

Step 8 Click **Add**.

Step 9 On the **IQN Pool** screen, enter a name, description, and prefix for the IQN pool.

Step 10 In the **IQNPool Block**, enter Suffix, From, Size, and ID Range Qualification Policy information.

Step 11 Click **Submit**.

vHBA Template

This template is a policy that defines how a vHBA (virtual Host Bus Adapter) on a server connects to the SAN. It is also referred to as a vHBA SAN connectivity template.

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

Creating a vHBA Template

Before you begin

One or more of the following resources must already exist:

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

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the policy and then click **View Details**.

Step 7 Click **vHBA Templates**.

Step 8 Click **Add**.

Step 9 On the **Add vHBA Template** screen, enter a unique name and description for the policy.

Step 10 From the **Fabric ID** drop-down list, choose the fabric interconnect that you want to associate with vHBAs created from this template.

Step 11 From the **VSAN** drop-down list, choose the VSAN that you want to associate with vHBAs created from this template.

Step 12 From the **Template Type** drop-down list, choose 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.

Step 13 In the **Max Data Field Size** field, enter 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.

Step 14 To associate policies with vNICs created from this template, complete the following fields:

Name	Description
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 15 Click **Submit**.

What to do next

Include the vHBA template in a vHBA policy.

Creating a vHBA Policy

Before you begin

Make sure that at least one of the following exists in the Cisco UCS Central account and organization to which this policy applies:

- vHBA template
- Fibre Channel adapter policy

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

Step 2 Click **vHBA**.

Step 3 Click **Add**.

Step 4 On the **Create UCS Central vHBA Policy** screen, do the following:

a) In the **vHBA Name** field, enter a unique name for the policy.
b) From the **Account Name** drop-down list, choose a Cisco UCS Central account to which this policy applies.
c) From the **Organization** drop-down list, choose the organization to which this policy applies.
d) From the **vHBA Template** drop-down list, choose a vHBA template.
e) From the **Adapter Policy** drop-down list, choose an adapter policy.

f) Click **Submit.**

What to do next

Include the vHBA policy in a storage policy.

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

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the policy and then click **View Details**.

Step 7 Click **SAN Connectivity Policies**.

Step 8 Click **Add**.

Step 9 On the **SAN Connectivity Policy** screen, enter a name and description for the policy.

Step 10 From the **WWNN Pool** drop-down list, choose the WWNN pool that you want to associate with this policy.

Step 11 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 Template, on page 40.

d) Click **Submit**.

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

Step 12 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

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

Step 2 Click **Storage Policy**.

Step 3 Click **Add**.

Step 4 On the **Create UCS Central Storage Policy** screen, enter a name and description for the policy.

Step 5 Complete the following fields to specify the Cisco UCS Central connections for the policy:

- **UCS Account Name** drop-down list—Choose the Cisco UCS Central account to which you want to add this policy.
- **UCS Organization Name** drop-down list—Choose the Cisco UCS Central organization to which you want to add this policy.

Step 6 From the **Local Disk Configuration Policy** drop-down list, choose the local disk configuration policy that you want to include in this storage policy.

Step 7 From the **SAN Connectivity Type** drop-down list, choose one of the following connectivity types:

Option	Description
Expert	Allows you to create up to 10 vHBAs that the server can use to access SAN storage. Continue with Step 8.
Simple	Allows you to create a maximum of two vHBAs that the server can use to access SAN storage. Continue with Step 9.
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 SAN. Continue with Step 11.
Hardware Inherited	Uses the vHBAs assigned to the Fibre Channel adapter profile associated with the server. Continue with Step 11.
Use SAN Connectivity Policy	Uses a SAN connectivity policy to determine the SAN connectivity for the server.

Option	Description
	Continue with Step 10.

Step 8 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 enough of WWNNs to assign a WWNN to each server that is associated with a 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) Continue with Step 11.

Step 9 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 enough of WWNNs to assign a WWNN to each server that is associated with a 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 is to 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 is to be associated.

d) Continue with Step 11.

Step 10 If you chose the SAN connectivity policy option, choose the policy that you want to associate with the server from the **SAN Connectivity Policy** drop-down list.

Step 11 Click **Submit**.

What to do next

Include the storage policy in a service profile.

ID Range Qualification Policy

ID range qualification policies allow you to create policies and assign them to qualified domain groups and domain IP addresses. The ID range qualification policy is then visible to those domain groups and domain IP addresses. You can also create ID range qualification policies without assigning qualified domain groups or IP addresses. If you do not set qualifiers, the policy is available to all domain groups. ID resolution occurs hierarchically in the organization structure in the same manner as other global policies.

The ID Range Qualification Policy can be associated to:

- MAC Pool

- WWNN Pool
- WWPN Pool
- WWXN Pool
- IP Pools
- IQN Pools.

After you create an ID range qualification policy, you can apply it to a block in a new pool or an existing pool.

Creating an ID Range Qualification Policy

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **ID Range Qualification Policies**.

Step 6 Click **Add**.

Step 7 On the **Create a ID Range Qualification Specification** screen, enter a name and description for the policy.

Step 8 In the **Domain Group** table, click the check box for the appropriate Domain Group or groups.

Step 9 Expand the **IPv4 Addresses** field, to select or add addresses.

Step 10 Expand the **IPv6 Addresses** field, to select or add addresses.

Step 11 Click **Submit**.

CHAPTER 7

Configuring Global Service Profiles

This chapter contains the following sections:

Global Service Profiles

Global service profiles centralize the logical configuration deployed across the data center. This centralization enables the maintenance of all service profiles in the registered Cisco UCS domains from one central location, Cisco UCS Central. When you use a global service profile, you can do the following across all Cisco UCS domains that are registered with the same Cisco UCS Central:

- Select a compute element for the service profile from any of the Cisco UCS domains.
- Migrate the service profile from one domain to another.
- Select servers from the available global server pools from any of the Cisco UCS domains.
- Associate global resources such as ID pools and policies.

For more information about global service profiles, including guidelines for implementing them, see the Cisco UCS Central configuration guides.

Global Service Profile Templates

Global service profile templates enable you to 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. Service profile templates in Cisco UCS Central are similar to the service profile templates in Cisco UCS Manager.

Creating a Global Service Profile

Before you begin

At a minimum, the following pools and policies that are required for service profiles must exist in the Cisco UCS Central account:

- UUID pool
- Storage policy
- PXE Network policy
- Blade 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 Central account.

The other policies that you can include in a global service profile are optional. However, we recommend that you review the **Add Service Profile** dialog box. Ensure that you have created all of the policies that you want to include in the global service profile before you begin.

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Global Service Profiles**.

Step 6 Click **Add**.

Step 7 On the **Create Service Profile** screen, enter a name and description for the service profile.

Step 8 From the following drop-down lists, choose the pools and policies that you want to include in this service profile:

- **Organization**—Required. Choose the organization to which the global service profile belongs.

  Note If the organization does not appear on the drop-down list, you can use the **+** button to add an addition organization to the drop-down.

- **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**—Required. Include this policy if you must have the server connected to the LAN.
- **PXE Boot Policy**—Optional. Include this policy if you want to have the server 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**—Required. Include this policy to determine the server boot.

- **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.

Step 9 **Server Power State** drop-down list—Required. 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 10 Click **Submit**.

Creating a Global 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 Central 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, import it from the Cisco UCS Central 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. Ensure that you have created all of the policies that you want to include in the template before you begin.

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Global Service Profile Templates**.

Step 6 Click **Add**.

Step 7 On the **Create Service Profile Template** screen, enter a name and description for the service profile template.

Step 8 From the **Organization** drop-down list, choose the organization to which the global service profile template belongs.

Step 9 From the **TemplateType** 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 10 From the following drop-down lists, choose the pools and policies that you want to include in this 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.
- **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 Policy**—Optional. Include this policy to specify the management IP address for the server.
- **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 11 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 12 Click **Submit**.

CHAPTER 8

Configuring Cisco UCS Server Pools and Policies

This chapter contains the following sections:

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

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the pool and then click **View Details**.

Step 7 Click **UUID Pools**.

Step 8 Click **Add**.

Step 9 On the **Add UUID Pool** screen, complete the following fields:

Name	Description
Name field	A unique name for the pool.

Name	Description
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.
ID Range Qualification Policy drop-down list	Choose the ID Range Qualification Policy.

Step 10 Click **Submit**.

Adding an Address Block to a UUID Pool

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to modify the pool and then click **View Details**.

Step 7 Click **UUID Pools**.

Step 8 Click the pool to which you want to add a block of addresses and then click **Add UUID Addresses Block**.

Step 9 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.
ID Range Qualification Policy drop-down list	Choose the ID Range Qualification Policy

Step 10 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

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the pool and then click **View Details**.

Step 7 Click **Server Pools**.

Step 8 Click **Add**.

Step 9 On the **Add Server Pool** screen, add a name and description for the pool.

Step 10 (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 11 Click **Add**.

Server Pool Qualification Policy

The Server Pool Qualification policy qualifies servers based on the servers available in the system. You can use this policy to qualify servers according to

- Server-related criteria such as model or type, product family, or chassis location
- Domain-related criteria such as domain group or domain name
- Processor-related criteria such as CPU cores, type, and configuration
- Storage configuration and capacity

- Memory type and configuration
- Other criteria such as adapter type, owner, site, or IP address

Based on the criteria added in the Server Pool Qualification policy, the servers qualified can then be used in the create server pool operation.

Creating a Server Pool Qualification Policy

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the policy and then click **View Details**.

Step 7 Click **Server Pool Qualification Policy**.

Step 8 Click **Add**.

Step 9 On the **Create Server Pool Qualification Policy** screen, type a name for the policy, an optional description, and an optional Server Model/PID. Click **Next**.

Step 10 In the **Domain** screen, click the plus (+) sign to optionally add the domain qualifier.
The **Add Entry to Domain Qualifier** screen appears. You can qualify servers based on the following criteria:

- Owner - The owner of the servers.
- Site - The site that the servers belong to.
- IP Address Range - The IP address range of the servers.
- Blade Servers - The chassis IDs and slot IDs of the servers.
- Rack Servers - The rack IDs of the servers.
- Domain Group - The domain groups that the servers belong to.
- Domain Name - The domains that the servers belong to.
- Product Family - The product family of the servers.

Step 11 In the **Add Entry to Domain Qualifier** screen, type a name for the qualifier in the **Name** box. Check the criteria you want to add. Then click the plus (+) sign to add the criteria. After adding the domain qualification option, click **Next**.

Step 12 In the **Hardware - Processors** screen, check the **Processor** box to optionally add processor-related criteria. Then click **Next**.

Step 13 In the **Hardware - Memory** screen, check the **Memory** box to optionally add memory-related criteria. Then click **Next**.

Step 14 In the **Hardware - Storage** screen, check the **Storage** box to optionally add storage-related criteria. Then click **Next**.

Step 15 In the **Hardware - Adapter** screen, check the **Adapter** box to optionally add the adapter type, number of adapters, and Model/PID.

Step 16 After adding all the criteria, click **Submit**.

Editing or Deleting a Server Pool Qualification Policy

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to modify or delete a server qualification policy and then click **View Details**.

Step 7 Click **Server Pool Qualification Policy**.

Step 8 To delete a server pool qualification policy, choose the policy and click **Delete**. A confirmation message appears. Click **Delete** again.

Step 9 To modify an existing server pool qualification policy, choose the policy and click **Edit**.
The **Edit Server Pool Qualification Policy** dialog box appears. It contains the following screens:

- Create Server Pool Policy Qualification Name
- Domain
- Hardware - Processors
- Hardware - Memory
- Hardware - Storage
- Hardware - Adapter

Step 10 After modifying existing qualification options or adding new options, click **Submit**.

Boot Policy

The Cisco UCS Manager enables you to create a boot policy for blade servers and rack 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. Specify only a primary name. Specifying a secondary name results in a configuration error.
- Specific JBOD disk number for booting from JBOD disks.
- Any LUN for backward compatibility; however, we do not recommend this. Other devices must not have bootable images to ensure a successful boot.

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. It helps 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 boots 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

Note

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.

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the policy and then click **View Details**.

Step 7 Click **Boot Policies**.

Step 8 Click **Add**.

Step 9 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.
Organization drop-down list	Is selected by default and not available to change.
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.

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 this check box is 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 10 In the **vHBAs** area, check **Add SAN Boot** and complete the following fields:

Name	Description
Add Primary SAN Boot check box	If checked, primary SAN boot is added to the boot order.
Primary vHBA field	Enter the name of the vHBA that you want to use as the first address defined for the SAN boot location. This field is dispalyed only when the **Add Primary SAN Boot** check box is checked.
Add SAN Boot Target for Primary vHBA check box	If checked, SAN boot is added for primary vHBA. This field is dispalyed only when the **Add Primary SAN Boot** check box is checked.
Add Secondary SAN Boot check box	If checked, secondary SAN boot is added to the boot order.
Secondary vHBA field	Enter the name of the vHBA that you want to use as the second address defined for the SAN boot location. This field is dispalyed only when the **Add Secondary SAN Boot** check box is checked.
Add SAN Boot Target for Secondary vHBA check box	If checked, SAN boot is added for secondary vHBA. This field is dispalyed only when the **Add Secondary SAN Boot** check box is checked.

Name	Description
Primary Boot Target LUN field	The LUN that corresponds to the location of the boot image. This field is dispalyed for Primary vHBA or Secondary vHBA only when the **Add SAN Boot Target for Primary vHBA** or **Add SAN Boot Target for Secondary vHBA** check box is checked.
Primary Boot Target WWPN field	The WWPN that corresponds to the location of the boot image. This field is dispalyed for Primary vHBA or Secondary vHBA only when the **Add SAN Boot Target for Primary vHBA** or **Add SAN Boot Target for Secondary vHBA** check box is checked.
Secondary Boot Target LUN field	The LUN that corresponds to the location of the boot image. This field is dispalyed for Primary vHBA or Secondary vHBA only when the **Add SAN Boot Target for Primary vHBA** or **Add SAN Boot Target for Secondary vHBA** check box is checked.
Secondary Boot Target WWPN field	The WWPN that corresponds to the location of the boot image. This field is dispalyed for Primary vHBA or Secondary vHBA only when the **Add SAN Boot Target for Primary vHBA** or **Add SAN Boot Target for Secondary vHBA** check box is checked.

Step 11 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

The order in which boot devices are invoked within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the policy and then click **View Details**.

Step 7 Click **Boot Policies**.

Step 8 Click **Add**.

Step 9 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.
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. If it is not selected, the vNICs/vHBAs/iSCSI are selected if they exist, otherwise the vNIC/vHBA/iSCSI with the lowest PCIe bus scan order is used.
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 10 In the **vNICs** area, check **Add LAN Boot** and enter the additional parameters, including the following:

Name	Description
Primary vNIC field	Enter the name of the vNIC that you want to use as the first address defined for the LAN boot location. This option is displayed when you check the **Add LAN Boot** check box.
Add Secondary vNIC check box	Adds secondary vNIC to the boot order.
Secondary vNIC field	Enter the name of the vNIC that you want to use as the second address defined for the LAN boot location. This option is displayed when you check the **Add Secondary vNIC** check box.

Step 11 Click **Submit**.

Local Device 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
- Local JBOD
- Local LUN
- SD Card
- Internal USB
- External USB
- Embedded Local LUN
- Embedded Local Disk

Creating a Local Device 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.

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the policy and then click **View Details**.

Step 7 Click **Boot Policies**.

Step 8 Click **Add**.

Step 9 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.
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 10 In the **Local Devices** area, choose from the following options:

Name	Description
Add Local Disk check box	Adds local disk to the boot policy. If you choose this option, add local LUN, add local JBOD, add SD card, add internal USB, add external USB, add embedded local LUN, and add embedded local disk options are not available. If you select the **Add Local Disk** check box, then you cannot select any of the secondary devices. If you select any of these local devices, then you cannot select the parent option of adding a local disk.

Name	Description
Add Local LUN check box	Adds any local LUN to the boot order. If you choose this option, add local disk option is not available.
Add Primary Local LUN check box	Adds primary local LUN to the boot order. This option is displayed when you check the **Add Local LUN** check box.
Primary Local LUN Name field	Enter the name of the local LUN that you want to use as primary. This option is displayed when you check the **Add Primary Local LUN** check box.
Add Secondary Local LUN check box	Adds secondary local LUN to the boot order. This option is displayed when you check the **Add Local LUN** check box.
Secondary Local LUN Name field	Enter the name of the local LUN that you want to use as secondary. This option is displayed when you check the **Add Secondary Local LUN** check box.
Add Local JBOD check box	Adds local JBOD to the boot order.
Primary JBOD Disk Slot Number field	Enter the slot number of the JBOD disk that you want to use as primary. This option is displayed when you check the **Add Local JBOD** check box.
Add SD Card check box	Adds SD Card to the boot order. If you choose this option, Add Local Disk, and Add Local LUN options are not available.
Add Internal USB check box	Adds Internal USB to the boot order. If you choose this option, Add Local Disk, and Add Local LUN options are not available.
Add External USB check box	Adds External USB to the boot order. If you choose this option, Add Local Disk, and Add Local LUN options are not available.
Add Embedded Local LUN check box	Adds Embedded Local LUN to the boot order.
Add Embedded Local Disk check box	Adds Embedded Local disk to the boot order.

Name	Description
Primary Embedded Local Disk Slot Number field	Enter the slot number of the embedded local disk that you want to use as primary. This option is displayed when you check the **Add Embedded Local Disk** check box.
Secondary Embedded Local Disk Slot Number field	Enter the slot number of the embedded local disk that you want to use as primary. This option is displayed when you check the **Add Embedded Local Disk** check box.
Add CD/DVD ROM Boot check box	Adds CD/DVD ROM to the boot policy. If you choose this option, Add Local CD/DVD, and Add Remote CD/DVD options are not available.
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. If you choose this option, Add Local Floppy Disk, and Add Remote Floppy Disk options are not available.
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.
Add Remote Virtual Drive check box	Adds remote virtual drive to the boot policy.

Step 11 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.

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the policy and then click **View Details**.

Step 7 Click **Boot Policies**.

Step 8 Click **Add**.

Step 9 In 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) if they exist, otherwise vNICs, vHBAs, or iSCSI vNICs with the lowest PCIe bus scan order is used.

Step 10 In the **CIMC Mounted vMedia** 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 11 Click **Submit**.

Creating a vMedia Policy and vMounts

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.

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

Step 2 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 3 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 4 Click **Organizations**.

Step 5 Choose the organization that you want to update and click **View Details**.

Step 6 Click **vMedia Policy**.

Step 7 Click **Add**.

Step 8 On the **Add vMedia Policy** screen, enter a name and description for the policy.

Step 9 From the **Retry on Mount Failure** drop-down list, choose one of the following to determine whether the vMedia will continue to mount even after a mount failure occurs:

- **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 10 Expand **vMedia Mount Points**, and check the vMedia Mount you want to use.

You can create a new vMedia mount point entry using the following steps:

a) Click **Add**.

b) On the **Add Entry to vMedia Mount Points** screen, complete the required fields, including the following:

1. **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.

2. **Mount Name**—Enter a unique name for the vMedia mount.

3. **Description**—Enter a description of the vMedia mount. You can enter up to 510 characters.

4. **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 protocol type, enter the additional parameters for that protocol type.

   - If you chose **HTTPS** protocol, enter the **User Name** and **Password** to log in to the remote server.
   - If you chose **HTTP** 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.

5. **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.

6. **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.

7. **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 11 Click **Submit**.

Creating a iSCSI Boot Policy

iSCSI boot enables a server to boot its operating system from an iSCSI target machine located remotely over a network.

Cisco UCS Manager uses the iSCSI vNIC and iSCSI boot information created for the service profile in the association process to program the adapter, located on the server. After the adapter is programmed, the server reboots with the latest service profile values. After a power-on self-test (POST), the adapter attempts to initialize using these service profile values. If the adapter can use the values and log in to its specified target, the adapter initializes and it posts an iSCSI Boot Firmware Table (iBFT) to the host memory and a valid bootable LUN to the system BIOS. The iBFT that is posted to the host memory contains the initiator and target configuration that is programmed on the primary iSCSI VNIC.

For multipath configurations, a single iSCSI Qualified Name (IQN) is configured on both the boot vNICs. If there are different IQNs configured on the boot vNICs on a host, the host will boot with the IQN that is configured on the boot vNIC with the lower PCI order.

Before you begin

- Verify that the storage array is licensed for iSCSI boot and the array side LUN masking must be properly configured.
- Determine two IP addresses, one for each iSCSI initiator. The IP addresses must be on the same subnet as the storage array. The IP addresses are assigned statically or dynamically using the Dynamic Host Configuration Protocol (DHCP).
- Verify that the operating system (OS) is iSCSI Boot Firmware Table (iBFT) compatible.

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the policy and then click **View Details**.

Step 7 Click **Boot Policies**.

Step 8 Click **Add**.

Step 9 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.
Organization drop-down list	Is selected by default and not available to change.
Reboot on Order Change check box	If checked, reboots all servers that use this boot policy after you change the boot order. If not 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 10 In the **iSCSI vNICs** area, check **Add iSCSI Boot** and enter the additional parameters, including the following:

Name	Description
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. This option is displayed when you check the **Add iSCSI Boot** check box.
Add Secondary iSCSI vNIC check box	Adds secondary iSCSI vNIC to the boot order.
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. This option is displayed when you check the **Add Secondary iSCSI vNIC** check box.

Step 11 Click **Submit**.

CHAPTER 9

Monitoring and Reporting

This chapter contains the following sections:

About Monitoring and Reporting

Cisco UCS Director displays all managed Cisco UCS components in each Cisco UCS domain registered with a Cisco UCS Central 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 Central 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 UCS Fabric Interconnect Inventory, UCS Chassis Inventory, UCS Server Inventory, and Associated vs Unassociated Servers.

  You can add some or all of these reports to your Cisco UCS Director dashboard for quick access.

  To view these reports, go to Viewing the Hardware Inventory for a Cisco UCS Domain, on page 74

- **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 monitor each registered Cisco UCS domain and the Cisco UCS Manager components for that Cisco UCS domain, including the following:

- UCS Domains
- Organizations
- Global Service Profiles
- Local Service Profiles
- VSANS
- VLANs
- Discovered Servers
- Pending Activities
- ID Range Qualification Policy
- FEX, Server, and Chassis

Viewing the Hardware Inventory for a Cisco UCS Domain

You can view the various hardware components in a Cisco UCS domain, including Fabric Interconnect Inventory, Chassis Inventory, Server Inventory, and Server Association.

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 From the **More Actions** drop-down list, choose **More Reports**.

Cisco UCS Director provides a drop-down list to select a summary report.

Viewing the Cisco UCS Central Pending Activities Report and User Acknowledgement

When changes are made to a Global 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 the server affected information.

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 On the **UCS Central Accounts** 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.

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 vMounts, on page 67.

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 Expand the **UCS Central Accounts**, and click the Cisco UCS Central account for which you want to view the report.

Step 4 Click **Organizations**.

Step 5 Choose the row with the organization for which you want to view the vMedia policy and click **View Details**.

Step 6 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.

Viewing the Cisco UCS Fabric Interconnect Report

This report shows you the number of Cisco UCS fabric interconnects in a Cisco UCS Central account and how many of them are operable.

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 Click the **UCS Central Account**.

Step 4 On the **UCS Central Accounts** screen, click **All UCS Domains**.

Step 5 Choose a Cisco UCS domain that you want to monitor.

Step 6 From the **More Actions** drop-down list, choose **View Details**.

Step 7 On the **UCS Central Domain** screen, click **Fabric Interconnects**.

Viewing the Cisco UCS Chassis Report

This report shows you the number of Cisco UCS chassis in a Cisco UCS Central account and how many of them are powered on.

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 Click the **UCS Central Account**.

Step 4 On the **UCS Central Accounts** screen, click **All UCS Domains**.

Step 5 Choose a Cisco UCS domain for which you want to view the Chassis details.

Step 6 From the **More Actions** drop-down list, choose **View Details**.

Step 7 On the **UCS Central Domain** screen, click **Chassis**.

Viewing the ID Usage Report

This report covers the ID usage utilization inventory and the tabular representation related to each domain associated to a Cisco UCS Central account.

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 Expand **UCS Central Accounts**, and click the Cisco UCS Central account.

Step 4 On the **UCS Central Accounts** page, click **All UCS Domains**.

Step 5 Click the row with the Cisco UCS domain for which you want to view the ID usage details.

Step 6 From the **More Actions** drop-down list, choose **View Details**.

Step 7 On the **UCS Central Domain** page, click **IDUsage**.

The ID usage report is displayed.

Step 8 To drill down the report, double-click a domain name (DN).

Viewing the Discovered Servers Report for Cisco UCS Central Domain

This report provides a list of all the available servers in a Cisco UCS Central Domain that are in Managed or Unmanaged state, including server type, model, serial number, power state, operation state, acknowledged or decommissioned state, service profile, availability, and transition state.

This tab also allows you to change the state of the server from managed to unmanaged and conversely. See Unmanaging a Server, on page 8.

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 Expand the **UCS Central Accounts**, click the Cisco UCS Central account.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 On the **UCS Central Accounts** screen, click **All UCS Domains**.

Step 6 Choose a Cisco UCS domain that you want to monitor.

Step 7 From the **More Actions** drop-down list, choose **View Details**.

Step 8 On the **UCS Central Domain** screen, click **Discovered Servers**.

Note The **Discovered Servers** report can also be found on **Ungrouped UCS Domains** page.

Viewing the Servers Report for Cisco UCS Central Domain

This report shows you the number of Cisco UCS servers in a Cisco UCS Central account, including server type, power state, total memory, operation state, model, serial IP address, service profile name, and availability.

Note Only managed servers are available in the Servers report.

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 Click the **UCS Central Account**.

Step 4 On the **UCS Central Accounts** screen, click **All UCS Domains**.

Step 5 Choose a Cisco UCS domain for which you want to view the server details.

Step 6 From the **More Actions** drop-down list, choose **View Details**.

Step 7 On the **UCS Central Domain** screen, click **Servers**.

Viewing the FEX Report for Cisco UCS Central Domain

This report shows you the details for fabric extenders in a Cisco UCS Central account, including ID, model, account name, serial, vendor, switch ID, and operation state.

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

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 Click **UCS Central Account**.

Step 4 On the **UCS Central Accounts** screen, click **All UCS Domains**.

Step 5 Choose a Cisco UCS domain for which you want to view the details.

Step 6 From the **More Actions** drop-down list, choose **View Details**.

Step 7 On the **UCS Central Domain** screen, click **FEX**.