System Management

This chapter includes the following sections:

- Managing DNS Policies, page 1
- Managing Power Policies, page 3
- Managing Time Zones, page 5
- SNMP Policies, page 8
- About High Availability in Cisco UCS Central, page 20
- Logs and Faults, page 22

Managing DNS Policies

Cisco UCS Central supports global DNS policies defining the DNS server and domain name. Registered Cisco UCS domains choosing to define DNS management globally within that domain's policy resolution control will defer DNS management to its registration with Cisco UCS Central.

Configuring a DNS Policy

Before You Begin

Before configuring a DNS policy in a domain group under the Domain Group root, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 Under the **Domain Groups root** node, click **Operational Policies**.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **DNS**.
Step 6 In the **Actions** area, click **Create** and complete all applicable fields.
Step 7 Click **Save**.

Deleting a DNS Policy

Deleting a DNS policy will remove all DNS server settings within that policy.

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 Under the **Domain Groups root** node, click **Operational Policies**.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **DNS**.
Step 6 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.
Step 7 Click **Save**.

Configuring a DNS Server for a DNS Policy

Before You Begin

Configure a DNS policy.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, click **Operational Policies**.

Step 4 In the **Work** pane, click **DNS**.

Step 5 In the **Actions** area, click **Add DNS Server** and complete all fields.

a) In the **Add DNS Server** dialog box, complete all fields.

b) Click **OK**.

Step 6 Click **Save**.

Deleting a DNS Server from a DNS Policy

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, click **Operational Policies**.

Step 4 In the **Work** pane, click **DNS**.

Step 5 In the **Actions** area, select the DNS server to delete and click **Delete**.
You can also right-click the DNS server to access that option.

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

Step 7 Click **Save**.

Managing Power Policies

Cisco UCS Central supports global equipment policies defining the global power allocation policy (based on policy driven chassis group cap or manual blade level cap methods), power policy (based on grid, n+1 or non-redundant methods). Registered Cisco UCS domains choosing to define power management and power supply units globally within that client's policy resolution control will defer power management and power supply units to its registration with Cisco UCS Central.

Configuring a Global Power Allocation Equipment Policy

Before You Begin

Before configuring a global power allocation equipment policy under a domain group, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 Under the **Domain Groups root** node, click **Operational Policies**.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **Equipment**.
Step 6 In the **Work** pane, click the **Global Power Allocation Policy** tab.
Step 7 In the **Actions** area, click **Create** and complete all applicable fields.
Step 8 Click **Save**.

Deleting a Global Power Allocation Equipment Policy

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 Under the **Domain Groups root** node, click **Operational Policies**.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **Equipment**.
Step 6 In the **Work** pane, click the **Global Power Allocation Policy** tab.
Step 7 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.
Step 8 Click **Save**.

Configuring a Power Equipment Policy

Before You Begin

Before configuring a power equipment policy under a domain group, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 Under the **Domain Groups root** node, click **Operational Policies**.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **Equipment**.
Step 6 In the **Work** pane, click the **Power Policy** tab.
Step 7 In the **Actions** area, click **Create** and complete all applicable fields.
Step 8 Click **Save**.

Deleting a Power Equipment Policy

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 Under the **Domain Groups root** node, click **Operational Policies**.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **Equipment**.
Step 6 In the **Work** pane, click the **Power Policy** tab.
Step 7 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.
Step 8 Click **Save**.

Managing Time Zones

Cisco UCS Central supports global date and time policies based on international time zones and defined NTP server. Registered Cisco UCS Manager clients choosing to define date and time globally within that client's policy resolution control will defer the configuration for date and time to its registration with Cisco UCS Central.

Configuring a Date and Time Policy

Before You Begin

Before configuring a date and time policy under a domain group, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 Under the **Domain Groups root** node, click **Operational Policies**.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **DateTime**.
Step 6 In the **Actions** area, click **Create** and complete all applicable fields.
Step 7 Click **Save**.

Deleting a Date and Time Policy

A date and time policy is deleted from a domain group under the domain group root. Date and time policies under the domain groups root cannot be deleted.

Deleting a date and time policy will remove all NTP server settings within that policy.

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 Expand the node for a domain group containing the policy to delete.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **DateTime**.
Step 6 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.
Step 7 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.
Step 8 Click **Save**.

Configuring an NTP Server for a Date and Time Policy

Before You Begin

To configure an NTP server for a domain group under the domain group root, a date and time policy must first have been created.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, click **Operational Policies**.

Step 4 In the **Work** pane, click **DateTime**.

Step 5 In the **Actions** area, click **Add NTP Server** and complete all fields and click **OK**.

Step 6 Click **Save**.

Configuring Properties for an NTP Server

An existing NTP server's properties may be updated before saving an NTP server instance. To change the name of an NTP server that is saved, it must be deleted and recreated.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **DateTime**.

Step 6 In the **Actions** area, select the NTP server to configure, click **Properties** and complete all fields.
You can also right-click the NTP server to access that option. The **Properties (NTP Provider)** dialog accessed by clicking **Properties** in the in the **Actions** area cannot be edited if the NTP server has been saved. To change the server name of an NTP server that was saved, delete and recreate the NTP server.

a) In the **Properties (NTP Provider)** dialog box, complete all fields.

Name	Description
NTP Server field	The IP address or hostname of the NTP server you want to use. **Note** If you use a hostname rather than an IPv4 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.

b) Click **OK**.

Step 7 Click **Save**.

Deleting an NTP Server from a Date and Time Policy

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, click **Operational Policies**.

Step 4 In the **Work** pane, click **DateTime**.

Step 5 In the **Actions** area, select the NTP server to delete and click **Delete**.
You can also right-click the NTP server to access that option. An NTP server that is deleted will inherit its settings from its domain group's parent until it is reconfigured.

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

SNMP Policies

Cisco UCS Central supports global SNMP policies enabling or disabling, defining SNMP traps and SNMP users (with regular and privacy passwords, authentication types of md5 or sha, and encryption types DES and AES-128). Registered Cisco UCS domains choosing to define SNMP policies globally within that client's policy resolution control will defer all SNMP policies to its registration with Cisco UCS Central.

The SNMP Agent functionality provides the ability to remotely monitor the Cisco UCS Central. You can also change the Cisco UCS Central host IP, and then restart the SNMP agent on the new IP. SNMP is run on both the active and standby Cisco UCS Central servers and the configuration is persisted on both. Cisco UCS Central offers read-only access to only the operating system managed information base (MIB).Through the Cisco UCS Central CLI you can configure the community strings for SNMP v1, v2c, and create and delete the SNMPv3 users.

SNMP Functional Overview

The SNMP framework consists of three parts:

- An SNMP manager—The system used to control and monitor the activities of network devices using SNMP.
- An SNMP agent—The software component within Cisco UCS Central, the managed device, that maintains the data for Cisco UCS Central and reports the data, as needed, to the SNMP manager. Cisco UCS Central includes the agent and a collection of MIBs. To enable the SNMP agent and create the relationship between the manager and agent, enable and configure SNMP in Cisco UCS Central.
- A managed information base (MIB)—The collection of managed objects on the SNMP agent. Cisco UCS Central supports only the OS MIBs.

Cisco UCS Central supports SNMPv1, SNMPv2c and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security. The following RFCs define the SNMP:

- RFC 3410 (http://tools.ietf.org/html/rfc3410)
- RFC 3411 (http://tools.ietf.org/html/rfc3411)
- RFC 3412 (http://tools.ietf.org/html/rfc3412)
- RFC 3413 (http://tools.ietf.org/html/rfc3413)
- RFC 3414 (http://tools.ietf.org/html/rfc3414)
- RFC 3415 (http://tools.ietf.org/html/rfc3415)
- RFC 3416 (http://tools.ietf.org/html/rfc3416)
- RFC 3417 (http://tools.ietf.org/html/rfc3417)
- RFC 3418 (http://tools.ietf.org/html/rfc3418)
- RFC 3584 (http://tools.ietf.org/html/rfc3584)

SNMP Support in Cisco UCS Central

Support for MIBs

Cisco UCS Central supports read-only access to OS MIBs. No set operations are available for the MIBs. The following MIBs are supported by Cisco UCS Central:

- SNMP MIB-2 System
- HOST-RESOURCES-MIB
  - hrSystem
  - hrStorage
  - hrDevice
  - hrSWRun

    - hrSWRunPerf
- UCD-SNMP-MIB
    - Memory
    - dskTable
    - systemStats
    - fileTable
- SNMP MIB-2 Interfaces
    - ifTable
- IP-MIB
- SNMP-FRAMEWORK-MIB
    - snmpEngine
- IF-MIB
- DISMAN-EVENT-MIB
- SNMP MIB-2 snmp

Note Cisco UCS Central does not provide support for IPV6 andCisco UCS Central MIBs.

Authentication Protocols for SNMPv3 Users

Cisco UCS Central supports the following authentication protocols for SNMPv3 users:

- HMAC-MD5-96 (MD5)
- HMAC-SHA-96 (SHA)

AES Privacy Protocol for SNMPv3 Users

Cisco UCS Central uses Advanced Encryption Standard (AES) as one of the privacy protocols for SNMPv3 message encryption and conforms with RFC 3826. If AES is disabled but privacy password is set, then DES is used for encryption.

If you enable AES-128 configuration and include a privacy password for an SNMPv3 user, Cisco UCS Central uses the privacy password to generate a 128-bit AES key. The AES privacy password can have a minimum of eight characters. If the passphrases are specified in clear text, you can specify a maximum of 64 characters.

SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. These notifications do not require that requests be sent from the SNMP manager. Notifications can indicate improper user

authentication, restarts, the closing of a connection, loss of connection to a neighbor router, or other significant events.

Cisco UCS Central generates SNMP notifications as traps. Traps are less reliable because the SNMP manager does not send any acknowledgment when it receives a trap, and Cisco UCS Central cannot determine if the trap was received.

SNMP Security Features

SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. SNMPv3 authorizes management operations only by configured users and encrypts SNMP messages. The SNMPv3 User-Based Security Model (USM) refers to SNMP message-level security and offers the following services:

- Message integrity—Ensures that messages have not been altered or destroyed in an unauthorized manner and that data sequences have not been altered to an extent greater than can occur non-maliciously.
- Message origin authentication—Ensures that the claimed identity of the user on whose behalf received data was originated is confirmed.
- Message confidentiality and encryption—Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

SNMP Security Levels and Privileges

SNMPv1, SNMPv2c, and SNMPv3 each represent a different security model. The security model combines with the selected security level to determine the security mechanism applied when the SNMP message is processed.

The security level determines the privileges required to view the message associated with an SNMP trap. The privilege level determines whether the message needs to be protected from disclosure or authenticated. The supported security level depends upon which security model is implemented. SNMP security levels support one or more of the following privileges:

- noAuthNoPriv—No authentication or encryption
- authNoPriv—Authentication but no encryption
- authPriv—Authentication and encryption

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

SNMP Security Models and Levels

The following table describes the combinations of SNMP security models and levels supported in Cisco UCS Central.

Table 1: SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	HMAC-MD5 or HMAC-SHA	No	Provides authentication based on the Hash-Based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm or the HMAC Secure Hash Algorithm (SHA).
v3	authPriv	HMAC-MD5 or HMAC-SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.

Configuring an SNMP Policy

Before You Begin

Before configuring a SNMP policy under a domain group, ensure that a SNMP policy is first created. Policies under the Domain Groups root which were already created by the system and are ready to configure.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the Navigation pane, expand **Domain Groups** > **Domain Group root**, or the **Domain Group** name where you want to create the policy.

Step 3 Under the **Domain Groups root** node, click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **SNMP**.

Step 6 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

a) In the **Actions** area, click **Enabled** to choose the **Admin State**.
If **Enabled**, Cisco UCS Central uses SNMP to monitor the Cisco UCS Central system. Cisco UCS uses SNMP in all Cisco UCS domains included in the domain group if the groups themselves are not configured with SNMP.

The default state is **Disabled** with no fields displayed. Leaving the default state disables the SNMP policy

b) Enter the community or the username in the **Community/Username** field.
You can use the default SNMP v1 or v2c community name or SNMP v3 username Cisco UCS includes on any trap messages it sends to the SNMP host. Enter an alphanumeric string between 1 and 32 characters. Do not use @ (at sign), \ (backslash), " (double quote), ? (question mark) or an empty space. The default is public.

c) Enter the system contact person information in the **System Contact** field.
The **System Contact** person is responsible for the SNMP implementation. Enter a string of up to 255 characters, such as an email address or a name and telephone number.

d) Enter the system location in the **System Location** field.
The **System Location** defines the location of the host on which the SNMP agent (server) runs. Enter an alphanumeric string up to 510 characters.

Step 7 Click **Save**.

What to Do Next

Create SNMP traps and SNMP users.

Creating an SNMP Trap

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 In the **Navigation** pane, click **Operational Policies**.

Step 4 In the **Work** pane, click **SNMP**.

Step 5 In the **SNMP Traps** area, click **Create SNMP Trap** and complete all applicable fields in the **Create SNMP Trap** dialog box.

a) Enter the SNMP host IP in the **IP Address** field.
Cisco UCS sends the trap to the defined IP address.

b) Enter the community or the username in the **Community/Username** field.
You can use the default SNMP v1 or v2c community name or SNMP v3 username Cisco UCS includes on any trap messages it sends to the SNMP host. Enter an alphanumeric string between 1 and 32 characters. Do not use @ (at sign), \ (backslash), " (double quote), ? (question mark) or an empty space. The default is public.

c) Enter the port number in the **Port** field.
Cisco UCS uses the defined port to communicate with the SNMP host for the trap. Enter an integer between 1 and 65535. The default port is 162.

d) Click **v1**, **v2c**, or **v3** to choose the SNMP **Version**.

e) Click **trap** to choose the SNMP trap**Type**.

f) Click **auth**, **no auth**, or **priv** to define the **v3Privilege**.

g) Click **OK**.

Step 6 Click **Save**.

Creating an SNMP User

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 In the **Navigation** pane, click **Operational Policies**.

Step 4 In the **Work** pane, click **SNMP**.

Step 5 In the **SNMP Users** area, click **Create SNMP User** and complete all applicable fields in the **Create SNMP User** dialog.

a) Enter the SNMP username in the **Name** field.
Enter up to 32 letters or numbers. The name must begin with a letter and you can also specify _ (underscore), . (period), @ (at sign), and - (hyphen).

Note You cannot create an SNMP username that is identical to locally authenticated username.

b) Click **md5** or **sha** to chose the authorization type.
c) Check the **AES-128** checkbox.
If checked, this user uses AES-128 encryption.
d) Enter the user password in the **Password** field.
e) Re-enter the user password in the **Confirm Password** field.
f) Enter the privacy password for this user in the **Privacy Password** field.
g) Re-enter the privacy password for this user in the **Confirm Privacy Password** field.
h) Click **OK**.

Step 6 Click **Save**.

Deleting an SNMP Policy

A SNMP policy is deleted from a domain group under the domain group root. SNMP policies under the domain groups root cannot be deleted.

Deleting an SNMP policy will remove all SNMP trap and SNMP User settings within that policy.

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 Under the **Domain Groups root** node, click **Operational Policies**.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **SNMP**.
Step 6 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.
Step 7 Click **Save**.

Deleting an SNMP Trap

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 In the **Navigation** pane, click **Operational Policies**.
Step 4 In the **Work** pane, click **SNMP**.
Step 5 In the **SNMP Traps** area, select the SNMP trap to delete and click **Delete**.
You can also right-click the SNMP trap to access that option.

Step 6 Click **Save**.

Deleting an SNMP User

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 In the **Navigation** pane, click **Operational Policies**.
Step 4 In the **Work** pane, click **SNMP**.
Step 5 In the **SNMP Users** area, select the SNMP user to delete and click **Delete**.
You can also right-click the SNMP user to access that option.
Step 6 Click **Save**.

Configuring a Global Fault Policy

Before You Begin

Before configuring a global fault debug policy under a domain group, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 Under the **Domain Groups root** node, click **Operational Policies**.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **Debug**.
Step 6 In the **Work** pane, click the **Global Fault Policy** tab.
Step 7 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.
Step 8 Click **Save**.

Core File Exporter

Cisco UCS uses the Core File Exporter to export core files as soon as they occur to a specified location on the network through TFTP. This functionality allows you to export the tar file with the contents of the core file.

Configuring a TFTP Core Export Policy

Before You Begin

Before configuring a TFTP core export debug policy under a domain group, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Debug**.

Step 6 In the **Work** pane, click the **TFTP Core Export Policy** tab.

Step 7 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

Step 8 Click **Save**.

Configuring a Syslog Console Policy

Before You Begin

Before configuring a syslog console debug policy under a domain group, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 Under the **Domain Groups root** node, click **Operational Policies**.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **Debug**.
Step 6 In the **Work** pane, click the **Syslog Policy** tab.
Step 7 In the **Work** pane, click the **Console** tab.
Step 8 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.
Step 9 Click **Save**.

Configuring a Syslog Monitor Policy

Before You Begin

Before configuring a syslog monitor debug policy under a domain group, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 Under the **Domain Groups root** node, click **Operational Policies**.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **Debug**.
Step 6 In the **Work** pane, click the **Syslog Policy** tab.
Step 7 In the **Work** pane, click the **Monitor** tab.
Step 8 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.
Step 9 Click **Save**.

Configuring a Syslog Remote Destination Policy

Before You Begin

Before configuring a syslog remote destination debug policy under a domain group, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Debug**.

Step 6 In the **Work** pane, click the **Syslog Policy** tab.

Step 7 In the **Work** pane, click the **Remote Destination** tab.

Step 8 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

Step 9 Click **Save**.

Configuring a Syslog Source Policy

Before You Begin

Before configuring a syslog source debug policy under a domain group, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Debug**.

Step 6 In the **Work** pane, click the **Syslog Policy** tab.

Step 7 In the **Work** pane, click the **Source** tab.

Step 8 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

Step 9 Click **Save**.

Configuring a Syslog LogFile Policy

Before You Begin

Before configuring a syslog logfile debug policy under a domain group, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Debug**.

Step 6 In the **Work** pane, click the **Syslog Policy** tab.

Step 7 In the **Work** pane, click the **LogFile** tab.

Step 8 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

Step 9 Click **Save**.

About High Availability in Cisco UCS Central

Cisco UCS Central provides high availability in a cluster setup when you deploy Cisco UCS Central in two virtual nodes. High availability provides stability and redundancy directly to your Cisco UCS Central and indirectly to your Cisco UCS Domains management. The high availability in Cisco UCS Central provides you the following:

- Simplified large scale Cisco UCS deployments with an increased number of servers, chassis, fabric interconnects, and data centers.
- UCS Central VM redundancy in a Hypervisor independent environment.
- A shared storage device to house database and image repositories.
- Built-in failure detection (DME, VM, host, or network failures) and automatic failover to ensure continuous operation.

High Availability Architecture

You will deploy Cisco UCS Central in two VMs on separate hosts to enable high availability. High availability -

- Requires at least one Cisco UCS Manager be registered with Cisco UCS Central for a cluster to support high availability
- Uses the same subnet for individual VMs and VIP addresses
- Allows you to configure a mirrored, multi-path shared storage disk on each VM that is accessible from both hosts
- Uses UCS Manager to store quorum data and determine primary node.
- Exchanges information such as heartbeat and election protocols in the same way as Cisco UCS Manager. This results in a simpler design, more code reusability, and easy to define failover conditions

Cautions and Guidelines for Using High Availability

The following are the guidelines to setup Cisco UCS Central in high availability:

- Make sure both VMs in the cluster should never be on the same server. Otherwise, a single host failure would end up bringing down the cluster.
- Each node in the cluster must have the following:
  - A primary NIC connected to the production network that is used for communicating with Cisco UCS Manager, and for heartbeat communications, with the peer node in the cluster.
  - A host bus adapter connected to the Storage Area Network (SAN), that is used to access the storage target.
- **Separate network path for management and storage network**: Make sure the management network used communications between the two Cisco UCS Central nodes are not on the same network as the network that the nodes use to access the shared disk array. The primary heartbeat mechanism relies on exchanging datagrams across the management network. The secondary heartbeat mechanism uses quorum data on Cisco UCS Manager. When you use separate network paths for management and shared disk access, that provides redundant paths between the two nodes making it easier to distinguish node failures from link failures.

Note High availability is supported only in IPv4 addressing without the DHCP. You must configure the node IPs and cluster VIPs statically during the installation. These IP addresses are allocated from the production network over which the UCS Central cluster communicates with UCSMs.

- Both VMs must be configured on IP addresses that belongs to the same subnet.
- Make sure the cluster node infrastructure does not have a single point of failure. You can connect the cluster nodes my multiple, distinct networks. You can also construct the network with redundant switches and routers or similar hardware that removes single points of failure.

- For high availability Cisco UCS Central supports the most commonly used bus types, such as SAS , Fiber Channel (FC), and iSCSI. SCSI compatibility with Persistent Reservations (PRs) is recommended. LUN masking or zoning should be used to isolate the storage volumes accessed by the cluster from other hosts on the network.

Logs and Faults

You can monitor and acknowledge the faults in registered Cisco UCS domains and Cisco UCS Central from the Cisco UCS Central GUI.

- **Cisco UCS Central Faults**: Cisco UCS Central collects and displays all the Cisco UCS Central system faults in the **Logs and Faults** tabs. You can monitor and acknowledge the faults from here. The fault details are categorized and displayed under the following tabs:
  - **mgmt-controller —** Management controller
  - **policy-mgr —** Policy manager
  - **resource-mgr —** Resource manager
  - **identifier-mgr —** Identifier manager
  - **operation-mgr —** Operation manager
  - **service-reg —** Service registry

    You can view and terminate active user sessions for local and remote users, view core files located at specified locations on the server, internal services for providers, controllers and service registries, and a categorized list of registered domains.

- **UCS Domain Faults**: Cisco UCS Central collects and displays the faults from registered Cisco UCS domains in the **Equipment** > **UCS Fault Summary** tab, in **UCS Faults** panel. The faults are displayed by type and severity level. You can click on the fault type to expand and view the exact Cisco UCS domains where the faults have occurred. When you select a specific Cisco UCS domain under the fault type, the **Work** pane displays details of the fault type. You can also launch Cisco UCS Manager GUI for the selected domain from here.

Note With Cisco UCS Central, release 1.2, a top level summary panel displays an overview of **UCS Central Fault Summary**, **UCS Domains Fault Summary** and **Pending Activities** on the Cisco UCS Central GUI.

Click one of the following three options to launch associated page on Cisco UCS Central GUI:

- **UCS Central Fault Summary**: Takes you to Logs and Faults > Faults, and displays faults in Cisco UCS Central.
- **UCS Domains Fault Summary**: Takes you to Domains > UCS Fault Summary panel and displays faults in registered Cisco UCS domains.
- **Pending Activities**: Takes you to Servers > Pending Activities.