System Management

System Policies

You can configure the system policies for all of Cisco UCS Central, or at the domain group level. To configure system policies at the domain group, see Domain Group System Policies, on page 10.

UCS Central system policies include the following:

- **Faults**—Determines when faults are cleared, the flapping interval, and the retention interval.

  Flapping Interval

  Length of time between Cisco UCS Central raising the fault and clearing the condition.

  Retention Interval

  Length of time Cisco UCS Central retains a fault in the system.

- **Syslog**—Determines the type of log files that you want to collect, and where you want to view or store them.

- **Core Dump**—Uses the Core File Exporter to export core files as they occur.

Configuring UCS Central System Policies

From the **UCS Central System Policies Manage** dialog box, you can configure the properties and settings for faults, syslog, and core dump export.

Procedure

Step 1 Click the **System Configuration** icon and choose **System Policies**.

Step 2 In the **UCS Central System Policies** dialog box, click the icon for the section that you want to configure.

- **Fault**—Perform the same tasks as the **UCS Central Fault Policy Manage** dialog box. For more information, see Managing a UCS Central Fault Policy, on page 4.
- **Syslog**—Perform the same tasks as the **UCS Central Syslog Manage** dialog box. For more information, see Managing UCS Central Syslog, on page 5.
- **Core Dump Export**—Perform the same tasks as the **UCS Central Core Dump Export Manage** dialog box. For more information, see Managing UCS Central Core Dump Export, on page 6.

Step 3 Complete the fields as required for each section.

Step 4 Click **Save**.

Related Topics

Managing a UCS Central Fault Policy, on page 4
Managing UCS Central Syslog, on page 5
Managing UCS Central Core Dump Export, on page 6

Managing Equipment Policies

Procedure

Step 1 Click the **Domain Group Navigation** icon and choose a domain group.

Step 2 Click the **Configuration** icon and choose **System Policies**.

Step 3 In **Equipment**, click **Basic** and complete the following fields:

a) In **Rack Management Action**, select how server management is configured when a new rack server is discovered:

- **Auto Acknowledged**—Cisco UCS automatically configures server management by domain based on the available server connections.
- **User Acknowledged**—Cisco UCS does not automatically configure server management. It waits until acknowledged by the user.

b) In **MAC Address Table Aging Time**, select the length of time an idle MAC address remains in the MAC address table before it is removed:

- **Mode Default**—System uses the default value. For end-host mode, the default is 14,500 seconds. For switching mode, the default is 300 seconds.

- **Never**—Cisco UCS never removes MAC addresses from the table.
- **Other**—Enter a custom value in the dd:hh:mm:ss field.

c) In **VLAN Port Count Optimization**, select whether Cisco UCS can logically group VLANs to optimize the use of ports and reduce the CPU load on the FI.

d) In **Firmware Auto Server Sync State**, select the firmware synchronization policy for recently discovered blade servers or rack servers:

- **User Acknowledged**—Cisco UCS does not synchronize firmware until the administrator acknowledges the upgrade.
- **No Actions**—Cisco UCS does not perform any firmware upgrade on the server.

e) In **Info Action**, select whether the information policy displays the uplink switches that are connected to the Cisco UCS domain.

Step 4 Click **Discovery** and complete the fields to specify how you want the system to behave when you add a new chassis or FEX:

a) In **Chassis/FEX Link Action**, select the minimum threshold for the number of links between the chassis or FEX and the fabric interconnect.

b) In **Chassis/FEX Link Grouping Preference**, select whether the links from the system IO controllers, IOMs, or FEXes to the fabric interconnects are grouped in a port channel.

c) In the **Multicast Hardware Hash**, click **Enable** to specify if Cisco UCS can use all of the links from the IOMs or FEXes to the fabric interconnects for multicast traffic.

d) In the **Backplane Speed Preference**, choose the speed that you want to use.

Step 5 Click **Power** and complete the following fields:

a) In **Power Redundancy**, select the power redundancy policy that you want to use:

- **N+1**—The total number of power supplies, plus one additional power supply for redundancy, equally share the power load for the chassis. If any additional power supplies are installed, Cisco UCS sets them to a "turned-off" state.
- **Grid**—Two power sources are turned on, or the chassis requires greater than N+1 redundancy. If one source fails, the surviving power supplies continue to provide power to the chassis.
- **Non-Redundant**—All installed power supplies are turned on and the load is evenly balanced. Only power small configurations (requiring less than 2500W) by a single power supply.

b) In **Power Allocation**, select the power allocation management mode used in the Cisco UCS domain:

- **Policy Driven Chassis Group Cap**—Configures power allocation at the chassis level through power control policies included in the associated service profiles.
- **Manual Blade Level Cap**—Configures power allocation on each individual blade server in all chassis.

c) In **ID Soaking Interval**, specify the number of seconds Cisco UCS Central waits before reassigning a pool entity that Cisco UCS released. Enter an integer between 0 and 86400.

Step 6 Click **Save**.

Managing Rack Discovery Policies

Procedure

Step 1 Click the **Domain Group Navigation** icon and choose a domain group.

Step 2 Click the **Configuration** icon and choose **System Policies**.

Step 3 In **Rack Discovery**, click **Enabled**.

Step 4 In **Basic**, for **Discovery Policy Action**, select how you want the system to behave when you add a new rack server.

- **Immediate**—Cisco UCS domain attempts to discover new servers automatically.
- **User Acknowledged**—Cisco UCS domain waits until the user tells it to search for new servers.

Step 5 Click **Policies** and select the scrub policy that you want to run on a newly discovered server.

The server must meet the criteria in the selected server pool policy qualification.

Step 6 Click **Save**.

Managing a UCS Central Fault Policy

Procedure

Step 1 In the **Actions** bar, type **Manage UCS Central Fault Policy** and press Enter.

Step 2 In the **UCS Central Fault Policy** dialog box, click **Fault** and complete the following fields:

Note The **Initial Severity** and **Action on Acknowledgment** fields are read-only. You cannot modify them.

1. Enter a time in seconds in the **Flapping Interval (Seconds)** field.

   Flapping occurs when Cisco UCS Central raises and clears a fault several times in rapid succession. To prevent this, Cisco UCS Central does not allow a fault to change its state until the user-defined amount of time has elapsed since the last state change.

   If the condition reoccurs during the flapping interval, the fault returns to the active state. If the condition does not reoccur during the flapping interval, the fault clears. The behavior depends on the setting in the **Action on Clear** field.

2. In **Soaking Interval**, choose None, or select a custom soaking interval.
3. In **Clear Interval**, select whether Cisco UCS Central should automatically mark faults as cleared based on their age.

   If you choose **None**, Cisco UCS Central does not automatically clear faults. If you choose **Custom Interval**, Cisco UCS Central automatically clears fault messages after the length of time you specify in the associated interval field.

4. In **Action on Clear**, select the actionCisco UCS Central must take when a fault is cleared.

If you choose **Retain Cleared Faults**, then Cisco UCS Central retains the cleared faults for the length of time specified in the **Retention Interval**. If you choose **Delete Cleared Faults**, then Cisco UCS Central clears the faults immediately.

5. If you set **Action on Clear** to **Retain Cleared Faults**, then in **Retention Interval**, specify the length of time Cisco UCS Central retains a fault that is marked as cleared.

   If you choose **Forever**, Cisco UCS Central retains all cleared fault messages forever. If you choose **Custom Interval**, Cisco UCS Central retains cleared fault messages for the length of time you specify in the associated interval field.

Step 3 Click **Save**.

Related Topics

Configuring UCS Central System Policies, on page 2
Managing UCS Central Syslog, on page 5
Managing UCS Central Core Dump Export, on page 6

Managing UCS Central Syslog

Procedure

Step 1 In the **Actions** bar, type **Manage UCS Central Syslog** and press Enter.

Step 2 In the **UCS Central Syslog** dialog box, click **Syslog Sources** and choose **Enabled** for each source for which you want to collect log files:

- **Faults**
- **Audits**
- **Events**

Step 3 In **Local Destination**, specify where Cisco UCS Central can add and display the syslog messages:

- **Console**—Displays syslog messages on the console and adds them to the log. Choose the logging level for the messages you want to display.
- **Monitor**—Displays syslog messages on the monitor and adds them to the log. Choose the logging level for the messages you want to display.
- **Log File**—Saves syslog messages to the log file. Choose the logging level, a filename, and the maximum file size.

Logging Level—Select the lowest message level that you want the system to store. The system stores that logging level and above:

- **Alert**
- **Critical (UCSM Critical)**
- **Error (UCSM Major)**
- **Emergency**

- **Warning (UCSM Minor)**
- **Notification (UCSM Warning)**
- **Information**
- **Debug**

Step 4 In **Remote Destination**, specify whether to store the syslog messages in a primary, secondary, or tertiary server.

Specify the following information for each remote destination:

- **Logging Level**—Select the lowest message level that you want the system to store. The system stores that level and above in the remote file:
  - **Alert**
  - **Critical (UCSM Critical)**
  - **Error (UCSM Major)**
  - **Emergency**
  - **Warning (UCSM Minor)**
  - **Notification (UCSM Warning)**
  - **Information**
  - **Debug**
- **Facility**—The facility associated with the remote destination.
- **Host Name/IPAddress**—The hostname, or IP address, on which the remote log file resides. If you are using a hostname rather than a IPv4 or IPv6 address, configure the DNS server in Cisco UCS Central.

Step 5 Click **Save**.

Related Topics

Configuring UCS Central System Policies, on page 2
Managing a UCS Central Fault Policy, on page 4
Managing UCS Central Core Dump Export, on page 6

Managing UCS Central Core Dump Export

Cisco UCS uses the Core File Exporter to export core files, through TFTP, to a specified location on the network. This exports the core file in tar format.

Procedure

Step 1 In the **Actions** bar, type **Manage UCS Central Core Dump Export** and press Enter.

Step 2 In the **UCS Central Core Dump Export** dialog box, click **Enable** to export core files.

Step 3 (Optional) Enter a description for the remote server used to store the core file.

Step 4 The **Frequency**, **Maximum No. of Files**, **Remote Copy**, and **Protocol** fields are set by default.

Step 5 (Optional) In **Absolute Remote Path**, enter the path to use when exporting the core file to the remote server.

Step 6 In **Remote Server Host Name/IP Address**, enter a hostname or IP address to connect with through TFTP

Step 7 (Optional) In **TFTP Port**, enter the port number to use when exporting the core file through TFTP. The default port number is 69.

Step 8 Click **Save**.

Related Topics

Configuring UCS Central System Policies, on page 2
Managing a UCS Central Fault Policy, on page 4
Managing UCS Central Syslog, on page 5

Configuring System Event Logs

Procedure

Step 1 In **Description**, type a description for the System Events.

Step 2 In **SEL Backup**, select if you want to **Enable** or **Disable** the backup.

Step 3 In **SEL Backup Format**, select **ASCII** or **Binary** as the format for the backup file.

Step 4 In **SEL Backup Frequency**, select one of the following options to set the time to wait between automatic backups:

- **Hourly**
- **Every 2 Hours**
- **Every 4 Hours**
- **Every 8 Hours**
- **Daily**
- **Weekly**
- **Monthly**

Step 5 In **Protocol**, select one of the following options as the protocol to communicate with the remote server.

- **FTP**
- **SFTP**
- **TFTP**
- **SCP**

Step 6 In **Absolute Remote Path ***, enter the absolute path to the file on the remote server.

If you use SCP, the absolute path is always required. If you use any other protocol, you may not need to specify a remote path, if the file resides in the default download folder. For details about how your file server is configured, contact your system administrator.

Step 7 In **Remote Server Host Name/IP Address**, type the hostname or IP address of the server where the backup configuration resides. If you use a hostname and not an IP address, you must configure a DNS server.

Step 8 In **User Name**, type the username used to log in to the remote server. This field does not apply if you select TFTP protocol.

Step 9 In **Password**, type the password used to log in to the remote server. This field does not apply if you select TFTP protocol.

Step 10 In **SEL Backup on Log Full**, select the option to create SEL backup when the log reaches the maximum size allowed.

Step 11 In **SEL Backup on Service Profile Association**, select the option to create SEL backup when the association between a server and the service profile changes.

Step 12 In **SEL Backup on Manual Log Clear**, select the option to create SEL backup when you manually clear the system log.

Step 13 In **SEL Backup on Backup Clear Interval**, select the option to create SEL backup when the time interval specified in the **SEL Backup Frequency** drop-down is reached.

Step 14 In **Clear Log on Backup**, select the option to clear all system event logs after the backup.

System Profile

The system profile allows you to configure the system information such as the interfaces, date and time, DNS, remote access, trusted points, and certificate information for all of Cisco UCS Central.

To configure the domain group system profile, see Domain Group System Profile, on page 11.

Managing the UCS Central System Profile

Procedure

Step 1 Click the **System Configuration** icon and choose **System Profile**.

Step 2 In the **UCS Central** section, you can view the Cisco UCS Central system name, mode, and virtual IPv4 and IPv6 addresses.

These values are populated when you first configure Cisco UCS Central. You cannot modify the system name and mode.

Step 3 In **Interfaces**, review or change the following management nodes:

- **Primary Node (IPv4)**
- **Primary Node (IPv6)**
- **Secondary Node (IPv4)**
- **Secondary Node (IPv6)**

Step 4 In **Date & Time**, choose the time zone and add an NTP server.

Step 5 In **DNS**, type the Cisco UCS Central domain name and add a DNS server.

Step 6 In **Remote Access**, choose a Key Ring.

Step 7 In **Trusted Points**, click **Add** to add a new trusted point and certificate chain.

Step 8 In **Certificates**, you can view the existing, or create a new key ring and certificate request.

Step 9 Click **Save**.

Related Topics

Managing the UCS Central NTP Servers, on page 9
Managing the UCS Central Management Node, on page 9
Managing the UCS Central DNS Servers, on page 10

Managing the UCS Central Management Node

Procedure

Step 1 In the Actions bar, type **Manage UCS Central Management Node** and press **Enter**.

This launches the **UCS Central Management Node Manage** dialog box.

Step 2 In **Management Node**, click the name of the node that you want to configure.

Step 3 Enter values for the **IP Address**, **Subnet Mask**, and **Default Gateway**.

Step 4 Click **Save**.

Related Topics

Managing the UCS Central System Profile, on page 8
Managing the UCS Central NTP Servers, on page 9
Managing the UCS Central DNS Servers, on page 10

Managing the UCS Central NTP Servers

Procedure

Step 1 In the Actions bar, type **Manage UCS Central NTP Servers** and press **Enter**.

This launches the **UCS Central NTP Servers Manage** dialog box.

Step 2 In **Time Zone**, select the time zone for the domain.

Step 3 In **NTP Servers**, click **Add** to add a new NTP server, or **Delete** to remove an existing one.

Step 4 Click **Save**.

Related Topics

Managing the UCS Central System Profile, on page 8
Managing the UCS Central Management Node, on page 9
Managing the UCS Central DNS Servers, on page 10

Managing the UCS Central DNS Servers

Procedure

Step 1 In the Actions bar, type **Manage UCS Central DNS Servers** and press **Enter**.

This launches the **UCS Central DNS Servers Manage** dialog box.

Step 2 In **UCS Central Domain Name**, type the name of the Cisco UCS Central domain.

Step 3 In **DNS Servers**, click **Add** to add a new DNS server, or **Delete** to remove an existing one.

Step 4 Click **Save**.

Related Topics

Managing the UCS Central System Profile, on page 8
Managing the UCS Central NTP Servers, on page 9
Managing the UCS Central Management Node, on page 9

Domain Group System Policies

You can configure the system policies at the domain group level, or for all of Cisco UCS Central. To configure system policies for UCS Central, see System Policies, on page 1.

Domain group system policies include the following:

- **Equipment**—Sets policies for the equipment in your domain group, including discovery and power policies.
- **Rack Discovery**—Determines what action is taken when a rack-mount server is discovered, and assign a scrub policy.
- **Faults**—Determines when faults are cleared, the flapping interval, and the retention interval.

  Flapping Interval

  Length of time between Cisco UCS Central raising the fault and clearing the condition.

  Retention Interval

  Length of time Cisco UCS Central retains a fault in the system.
- **Syslog**—Determines the type of log files that you want to collect, and where you want to view them or store.
- **Core Dump**—Uses the Core File Exporter to export core files as they occur.
- **Interfaces**—Sets criteria for monitoring your domain group interfaces.
- **System Events**—Sets the criteria for domain group system event logs.

Managing Domain Group System Policies

Note If you are setting the system policies for a subdomain, enable each policy before you can set it.

Procedure

Step 1 Click the **Domain Group Navigation** icon and choose a domain group.

Step 2 Click the **Settings** icon.

Step 3 Click **Launch** for System Policies.

Step 4 In **Equipment**, complete the necessary fields.

For more information, see Managing Equipment Policies, on page 2.

Step 5 In **Rack Discovery**, complete the necessary fields.

For more information, see Managing Rack Discovery Policies, on page 4.

Step 6 In **Fault**, complete the necessary fields.

For more information, see Managing a UCS Central Fault Policy, on page 4.

Step 7 In **Syslog**, complete the necessary fields.

For more information, see Managing UCS Central Syslog, on page 5.

Step 8 In **Core Dump**, complete the necessary fields.

For more information, see Managing UCS Central Core Dump Export, on page 6.

Step 9 In **Interfaces**, choose whether to enable **Interface Monitoring Policy**.

Step 10 If you select **Enabled**, complete the interface monitoring information as required.

Step 11 In **System Events**, complete the necessary fields to determine how the system event logs are collected.

For more information, see Configuring System Event Logs, on page 7.

Step 12 Click **Save**.

Domain Group System Profile

The domain group system profile allows you to configure the date and time, DNS settings, remote access, and trusted points for each domain group.

Managing the Domain Group System Profile

Procedure

Step 1 Click the **Domain Group Navigation** icon and choose root.

Step 2 Click the **Settings** icon.

Step 3 Click **Launch** for System Policies.

Step 4 In **Date & Time**, choose the time zone and add an NTP server.

Step 5 In **DNS**, type the UCS Central domain name and add a DNS server.

Step 6 In **Remote Access**, type the HTTPS, HTTPS port, and change the default values for web and shell sessions, if needed.

Note The SSH fields are read-only.

Step 7 In **Trusted Points**, click **Add** to create a trusted point and add a certificate chain.

Step 8 Click **Save**.

Schedules

Use schedules to determine when certain activities will occur. After you create a schedule in Cisco UCS Central, you can use that schedule in:

- Backup operations
- Configuration export
- Maintenance policies

Note Simple schedules, whether recurring or a one time occurrence, do not have the option to require user acknowledgment. If you want to require user acknowledgment, you must choose an advanced schedule.

Creating or Editing a Schedule

Note Simple schedules, whether recurring or single occurrence, do not require user acknowledgment. If you want to require user acknowledgment, choose an advanced schedule.

Procedure

Step 1 In the **Actions** bar, type **Create Schedule** and press Enter.

Step 2 In **Basic**, enter a **Name** and optional **Description**.

Step 3 Select **Recurring**, **One Time**, or **Advanced** for the schedule.

If **Advanced**, select to enable or disable user acknowledgment.

Step 4 Click **Schedules**.

Step 5 Click **Add** to add a schedule.

a) For **Recurring** schedules, select the start date, frequency, time, and other properties.
b) For **One Time** schedules, select the start date, time, and other properties.
c) For **Advanced** schedules, enter a name for the schedule, choose whether to use a one time or recurring schedule, and select values for the other properties.

Step 6 Click **Create**.

Server Maintenance Policy

When you change a service profile that is associated with servers in the registered domains, the change may require a server reboot. The maintenance policy determines how Cisco UCS Central reacts to the reboot request.

You can create a maintenance policy, and specify the reboot requirements, to make sure the server does not automatically reboot when changes to the service profiles occur. You can specify one of the following options for a maintenance policy:

- **On Save**: When you change a service profile, Cisco UCS Central applies the changes immediately.
- **User Acknowledgment**: Applies the changes after an admin acknowledges the changes.
- **Schedule**: Applies the changes based on the day and time you specify in the schedule.

When you create the maintenance policy, if you specify a schedule, the schedule deploys the changes in the first available maintenance window.

Note A maintenance policy only prevents an immediate server reboot when a configuration change is made to an associated service profile. However, a maintenance policy does not prevent the following actions from taking place right away:

- Deleting an associated service profile from the system
- Disassociating a server profile from a server
- Directly installing a firmware upgrade without using a service policy
- Resetting the server

Creating or Editing a Maintenance Policy

To watch a video on creating a server maintenance policy and associating it with a service profile, see Video: Creating a Global Maintenance Policy and Associating the Policy with a Service Profile.

Procedure

Step 1 In the **Actions** bar, type **Create Maintenance Policy** and press Enter.

Step 2 In the **Maintenance Policy Create** dialog box, choose **Server**.

Step 3 Choose the **Organization** where you want to create the policy, and enter the **Name** and optional **Description**.

The name is case sensitive.

Step 4 For a server maintenance policy, complete the following:

a) Select the Hard Shutdown OS Option :

- If you choose **Enabled**, Cisco UCS Manager waits for the **Hard Shutdown Timer** value specified in Cisco UCS Central before it triggers a shutdown and reboot.

  Note The **Hard Shutdown Timer** specifies time in seconds (150, 300, or 600) that Cisco UCS Manager waits before it triggers a shutdown and reboot. This timer value is specified in the global maintenance policy.

- If you choose **Disabled**, Cisco UCS Manager never performs a server shutdown.

b) Select when to apply the changes that require a reboot:

- **User Acknowledgment**—User must acknowledge configuration changes and confirm reboots.
- **Schedule**—Cisco UCS Central applies configuration changes depending on the schedule that you select. To add a new schedule to the list of values, see Creating or Editing a Schedule, on page 12.
- **On Save**—Cisco UCS Central applies configuration changes immediately on save and causes a reboot.

c) Enable **Apply on Next Reboot**, if you want Cisco UCS Central to apply the changes on the next reboot and ignore the selection in the **Apply Changes On** field.

Step 5 Click **Evaluate** to view the impact of the policy.

Step 6 Click **Create**.

Key Rings

Cisco UCS Central allows creation of key rings as a third-party certificate for stronger authentication. HTTPS uses components of the Public Key Infrastructure (PKI) to establish secure communications between two devices.

Each PKI device holds a pair of asymmetric Rivest-Shamir-Adleman (RSA) encryption keys, one kept private and one made public, stored in an internal key ring. You can decrypt a message encrypted with either key

with the other key. To send an encrypted message, the sender encrypts the message with the receiver's public key, and the receiver decrypts the message using its own private key. A sender can also prove its ownership of a public key by encrypting (also called 'signing') a known message with its own private key. If a receiver can successfully decrypt the message using the public key in question, the sender's possession of the corresponding private key is proven. Encryption keys can vary in length, with typical lengths from 2048 to 4096 bits. In general, a longer key is more secure than a shorter key. Cisco UCS Central provides a default key ring with an initial 2048-bit key pair, and allows for you to create extra key rings.

Note After you regenerate the default key ring, logging in to Cisco UCS Central can take a few minutes.

Manually regenerate the default key ring certificate if the cluster name changes or the certificate expires.

Note When you create a key ring and certificate request, Cisco UCS Central generates the certificate request with required key usages set. The key usages on a certificate signed from a CA server must include **SSL Client Authentication**, and **SSL Server Authentication**. If you use Microsoft Windows Enterprise Certification Authority Server as an internal CA, use the **Computer** template to generate the certificate. It must contain both of the key usages sets. If this template is not available in your setup, use an appropriate template which has both **SSL Client Authentication**, and **SSL Server Authentication** key usages set.

Creating a Key Ring

Procedure

Step 1 Click the **System Configuration** icon and choose **System Profile**.

Step 2 Click **Certificates**.

Step 3 Click **Add** to add a Key Ring.

Step 4 In the Basic tab, leave the Modulus at its default value, or change if necessary.

Step 5 Enter a Trusted Point.

Step 6 Paste in the certificate chain from your generated key ring.

Step 7 Click **Certificate Request**.

Step 8 Fill in the fields with valid information for your organization.

Step 9 Click **Save**.

Note After you create a valid keyring, you must deploy it to Cisco UCS Central. To deploy the keyring, navigate to **System Profile** > **Remote Access** > **Keyring**. Select the keyring you have created based on the instructions above, and click **Save**.

Creating a Trusted Point

Cisco UCS Central allows you to create a trusted point. The trusted point contains the certificate of the root certificate authority (CA) and a subordinate CA in a bundled format.

Note The root CA must contain a primary and self-signed certificate.

Procedure

Step 1 Click the **System Configuration** icon and choose **System Profile**.

Step 2 Click**Trusted Points**.

Step 3 Click **Add** to add a trusted point.

Step 4 Paste in the certificate chain from your generated key ring.

Step 5 Click **Save**.

Fault and Log Monitoring

Cisco UCS Central allows you to view fault logs, audit logs, sessions, and other events.

Note If the screen or widget that you are viewing is not current, click **Refresh** to see the latest data.

System Faults

Cisco UCS Central collects and displays all of the Cisco UCS Central system faults on the **Fault Logs** page. To view these system fault logs, click the **System Alerts** icon and choose **System Faults**. The **Faults Logs** page displays information on the type and severity level of the fault. It also allows you to monitor and acknowledge the system faults, and filter the faults that are displayed.

The faults table includes the following information for each fault:

- **Code**—ID associated with the fault
- **Timestamp**—Date and time at which the fault occurred
- **Type**—Origin of the fault
- **Cause**—Cause of the fault
- **Affected Object**—Component affected by this fault
- **Fault Details**—Details of the fault.
- **Severity**—Severity of the fault

- **Action**—Action required by the fault

To manage the information collected, see Configuring UCS Central System Policies, on page 2.

Domain Faults

Cisco UCS Central collects and displays faults from registered Cisco UCS domains in the **Domain Faults** page. It also displays Inventory faults. Cisco UCS Central categorizes and displays domain faults as follows:

- **Fault Level**—The fault level that triggers the profile:
  - **Critical**—Critical problems exist with one or more components. Research and fix these issues immediately.
  - **Major**—Serious problems exist with one or more components. Research and fix these issues immediately.
  - **Minor**—Problems exist with one or more components that may adversely affect the system performance. Research and fix these issues as soon as possible before they become major or critical issues.
  - **Warning**—Potential problems exist with one or more components that may adversely affect the system performance if they are allowed to continue. Research and fix these issues as soon as possible before they become major or critical issues.
  - **Cleared**—Condition that caused the fault is resolved, and the fault is cleared.
  - **Info**—Notification or informational message.
  - **Condition**—Informational message about a condition.
- **Filter**—Filter the data in the table.
- **Code**—Unique identifier associated with the fault.
- **Timestamp**—Day and time at which the fault occurred.
- **Type**—Information on where the fault originated.
- **Cause**—Brief description of what caused the fault.
- **Affected Object**—The name and location of the component that this issue affects, and the domain name where it is found.
- **Fault Details**—More information about the log message.
- **Severity**—Displays an icon denoting the fault severity. The icon key displays below the table.
- **Action**—Whether user acknowledgment is required.

Event Logs

Cisco UCS Central collects and displays the events that occurred in the system, such as when a user logs in or when the system encounters an error. When such events occur, the system records the event and displays

it in the **Event Logs**. To view these event logs, click the **System Alerts** icon and choose **Events**. The event logs record the following information:

- **ID**—Unique identifier associated with the event that caused the fault
- **Timestamp**—Date and time at which the event occurred
- **Trig. By**—Type of user associated with the event
- **Affected Object**—The component affected by the event
- **Event Details**—Details of the event.

Audit Logs

You can view a comprehensive list of configuration changes in Cisco UCS Central in the **Audit Logs**. When you perform configuration changes involving creating, editing or deleting tasks in the Cisco UCS Central GUI or the Cisco UCS Central CLI, Cisco UCS Central generates an audit log. In addition to the information related to configuration, the audit logs record information on the following:

- Resources that were accessed.
- Date and time at which the event occurred.
- Unique identifier associated with the log message.
- The user who triggered an action to generate the audit log. This can be an internal session or an external user who made a modification using the Cisco UCS Central GUI or the Cisco UCS Central CLI.
- The source that triggered the action.
- The component that is affected.

Core Dumps

If an error occurs that causes the system to crash, then a core dump file is created. This core dump file includes information on the state of the system before the error occurred, and the time at which the system crashed. To view the core dump files, click the **System Alerts** icon and choose **Core Dumps**. In the **Core Dumps** log table you can view the following information:

- **Timestamp**—Creation date.
- **Name**—Full name of the core dump file.
- **Description**—Type of core dump file.

Active Sessions

You can view active sessions for remote and local users in Cisco UCS Central and choose to terminate those sessions from the server. To view the active sessions, click the **System Alerts** icon and choose **Active Sessions**. In the log table you can view the following information:

- **ID**—Type of terminal from which the user logged in.

- **Timestamp**—Date and time at which the user logged in.
- **User**—User name.
- **Type**—Type of terminal from which the user logged in.
- **Host**—IP address from which the user logged in.
- **Status**—If session is currently active.
- **Actions**—Click **Terminate** to end the selected session.

Internal Services

Internal service logs provide information on various providers and the version of the Cisco UCS Central associated with the provider. To view the internal services, click the **System Alerts** icon and choose **Internal Services**.

In the **Services** section, you can view the following information:

- **Name**—Type of the provider.
- **Last Poll**—Day and time on which Cisco UCS Central last polled the provider.
- **IP Address**—IP address associated with the provider.
- **Version**—Version of Cisco UCS Central associated with the provider.
- **Status**—Operational state of the provider.

In the **Lost Domains** section, you can view the following information:

- **Domain**—Domain name.
- **Last Poll**—Day and time on which Cisco UCS Central last polled the provider.
- **Lost Visibility**—Time when Cisco UCS Central lost visibility to the provider.

Enabling Tomcat Logging

Use a terminal emulator to access the CLI.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **scope monitoring**	Enters monitoring mode.
Step 2	UCSC /monitoring # **scope sysdebug**	Enters sysdebug mode.
Step 3	UCSC /monitoring/sysdebug # **scope mgmt-logging**	Enters management logging mode.
Step 4	UCSC /monitoring/sysdebug/mgmt-logging # **set module tomcat_config** [**crit** | **debug0** |	Sets the logging level.

	Command or Action	Purpose
	debug1 | **debug2** | **debug3** | **debug4** | **info** | **major** | **minor** | **warn**]	
Step 5	UCSC /monitoring/sysdebug/mgmt-logging # **commit-buffer**	Commits the change.

Example

The following example shows how to set tomcat logging to level debug 4.

```
UCSC # scope monitoring
UCSC /monitoring # scope sysdebug
UCSC /monitoring/sysdebug # scope mgmt-logging
UCSC /monitoring/sysdebug/mgmt-logging # set module tomcat_config debug4
UCSC /monitoring/sysdebug/mgmt-logging # commit-buffer
```

Prevention of Deleting Critical Objects from Cisco UCS Central

Beginning release 2.0, Cisco UCS Central prevents you from deleting critical objects from the Cisco UCS Central GUI and the command line. When you attempt to delete any of these items from Cisco UCS Central, an error message with the potential impact displays. The table below lists the items and the procedure to follow before you attempt to delete them:

Objects in Cisco UCS Central	Required action before deleting the object from Cisco UCS Central
A service profile associated with a server	Un-associate it from the server
An organization with associated service profiles	Un-associate all service profiles in that organization, and all of its sub-organizations
A service profile template with any associated service profiles bound to it	Either unbind all associated service profiles, or un-associate all of them
A domain group with registered Cisco UCS domains, functional VLANs	• You must not have any registered domains in the domain group, or any of its sub-domain groups • You must not have any VLANs referenced by any associated service profile in it, or any of its sub-domain groups

API Communication Reports

Cisco UCS Central enables you to generate reports on active API communication between the GUI and back-end from the Cisco UCS Central GUI. You can collect these communications for use in third-party automation. You can start and stop collecting this report at any time during an active communication.

- After you stop logging the session, the report is available for you as text file from the GUI. If you want to use the file later, make sure to save the file in your local desktop.

- If you log out or your sessions expires while recording is in progress, the text file is not generated.

Generating API Communication Reports

Procedure

Step 1 On the menu bar, click the **System Tools** icon and choose **Start Logging Session**.
The system starts logging the active API communication between Cisco UCS Central GUI and the back-end.

Step 2 On the menu bar, click the **System Tools** icon and choose **Stop Logging Session**.
The API report text file saves to your system.

Tech Support Files

When you encounter an issue that requires troubleshooting or a request for assistance to the Cisco Technical Assistance Center (Cisco TAC), collect as much information as possible about Cisco UCS Central or the affected Cisco UCS domain. Cisco UCS Central outputs this information into a tech support file that you can send to Cisco TAC.

You can create a tech support file for all of Cisco UCS Central, or for the following components of a Cisco UCS domain:

- **Entire Domain**—Contains technical support data for the entire Cisco UCS domain.
- **FEX**—Contains technical support data for the given FEX.
- **Domain Management Services**—Contains technical support data for the Cisco UCS Central management services, excluding Fabric Interconnects.
- **Rack Server**—Contains technical support data for the given rack server and adapter.
- **Chassis**—Contains technical support data for the I/O module or the CIMCs on the blade servers in a given chassis only.
- **Server Memory**—Contains server memory technical support data for the given rack-mount servers and blade servers.

Before contacting Cisco TAC, see the following:

1. Generating a Tech Support File, on page 21
2. Downloading a Tech Support File, on page 22

Generating a Tech Support File

You can generate a tech support file for Cisco UCS Central or for a supported component of a Cisco UCS domain.

Procedure

Step 1 Click the **System Tools** icon and choose **Tech Support**.

Step 2 Under **Domains**, select **UCS Central** or the domain for which you want to generate tech support files.

Step 3 Click the **Generate Tech Support** icon.

Step 4 If you selected **UCS Central**, do the following:

a) Choose whether to include system data in the report.

b) Click **Yes** to generate the file.
The list page displays the tech support file collection status while the collection is in progress. When the process completes, it displays the collected time, file name and availability status.

Step 5 If you selected a domain, do the following:

a) Choose the type of data for which you want to generate tech support.

b) Choose whether or not to exclude CLI commands.

c) Click **Generate File**.
The list page displays the tech support file collection status while the collection is in progress. When the process completes, it displays the collected time, file name and availability status.

Downloading a Tech Support File

Procedure

Step 1 Click the **System Tools** icon and choose **Tech Support**.

Step 2 Under **Domains**, select **UCS Central** or the domain for which you want to view tech support files.
The right pane displays the list of available tech support files for the selected system.

Step 3 Choose the file that you want to download.

Step 4 Click **Download**.