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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: 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)

© 2016–2017 Cisco Systems, Inc. All rights reserved.
CONTENTS

PREFACE

Preface ix
  Audience ix
  Conventions ix
  Related Cisco UCS Documentation xi
  Documentation Feedback xi

CHAPTER 1

New and Changed Information for This Release 1

CHAPTER 2

System Monitoring Overview 3
  System Monitoring Overview 3
  The Cisco UCS Manager Core and Fault Generation 4
  Cisco UCS Manager User Documentation 6

CHAPTER 3

Syslog 9
  Syslog 9
  Configuring the Syslog Using Cisco UCS Manager GUI 10

CHAPTER 4

System Event Log 15
  System Event Log 15
  Viewing the System Event Log for an Individual Server 16
  Viewing the System Event Log for the Servers in a Chassis 16
  Configuring the SEL Policy 16
  Copying One or More Entries in the System Event Log 19
  Printing the System Event Log 19
  Refreshing the System Event Log 19
  Manually Backing Up the System Event Log 20
<table>
<thead>
<tr>
<th>Content</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding a Threshold Class to an Existing Server and Server Component</td>
<td>59</td>
</tr>
<tr>
<td>Threshold Policy</td>
<td></td>
</tr>
<tr>
<td>Adding a Threshold Class to the Uplink Ethernet Port Threshold Policy</td>
<td>60</td>
</tr>
<tr>
<td>Adding a Threshold Class to the Ethernet Server Port, Chassis, and</td>
<td>61</td>
</tr>
<tr>
<td>Fabric Interconnect Threshold Policy</td>
<td></td>
</tr>
<tr>
<td>Adding a Threshold Class to the Fibre Channel Port Threshold Policy</td>
<td>63</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHAPTER 10</th>
<th>Call Home and Smart Call Home Configuration</th>
<th>65</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Home and Smart Call Home Configuration</td>
<td>65</td>
<td></td>
</tr>
<tr>
<td>Call Home in UCS Overview</td>
<td>65</td>
<td></td>
</tr>
<tr>
<td>Call Home Considerations and Guidelines</td>
<td>66</td>
<td></td>
</tr>
<tr>
<td>Cisco UCS Faults and Call Home Severity Levels</td>
<td>67</td>
<td></td>
</tr>
<tr>
<td>Anonymous Reporting</td>
<td>68</td>
<td></td>
</tr>
<tr>
<td>Enabling Anonymous Reporting</td>
<td>68</td>
<td></td>
</tr>
<tr>
<td>Configuring Call Home</td>
<td>69</td>
<td></td>
</tr>
<tr>
<td>Configuring Call Home Profiles</td>
<td>73</td>
<td></td>
</tr>
<tr>
<td>Configuring Call Home Policies</td>
<td>77</td>
<td></td>
</tr>
<tr>
<td>Cisco Smart Call Home</td>
<td>78</td>
<td></td>
</tr>
<tr>
<td>Configuring Smart Call Home</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Configuring the Default Cisco TAC-1 Profile</td>
<td>82</td>
<td></td>
</tr>
<tr>
<td>Configuring System Inventory Messages for Smart Call Home</td>
<td>83</td>
<td></td>
</tr>
<tr>
<td>Registering Smart Call Home</td>
<td>83</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHAPTER 11</th>
<th>Database Health Monitoring</th>
<th>85</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS Manager Database Health Monitoring</td>
<td>85</td>
<td></td>
</tr>
<tr>
<td>Changing Internal Backup Interval</td>
<td>85</td>
<td></td>
</tr>
<tr>
<td>Triggering Health Check</td>
<td>86</td>
<td></td>
</tr>
<tr>
<td>Changing Health Check Interval</td>
<td>86</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHAPTER 12</th>
<th>Hardware Monitoring</th>
<th>87</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring a Fabric Interconnect</td>
<td>87</td>
<td></td>
</tr>
<tr>
<td>Monitoring a Blade Server</td>
<td>88</td>
<td></td>
</tr>
<tr>
<td>Monitoring a Rack-Mount Server</td>
<td>90</td>
<td></td>
</tr>
<tr>
<td>Monitoring an IO Module</td>
<td>92</td>
<td></td>
</tr>
<tr>
<td>Monitoring Crypto Cards</td>
<td>93</td>
<td></td>
</tr>
</tbody>
</table>
Traffic Monitoring 115
Guidelines and Recommendations for Traffic Monitoring 117
Creating an Ethernet Traffic Monitoring Session 118
Setting the Destination for an Existing Ethernet Traffic Monitoring Session 119
Clearing the Destination for an Existing Ethernet Traffic Monitoring Session 120
Creating a Fibre Channel Traffic Monitoring Session 120
Setting the Destination for an Existing Fibre Channel Traffic Monitoring Session 121
Clearing the Destination for an Existing Fibre Channel Traffic Monitoring Session 122
Adding Traffic Sources to a Monitoring Session 122
Activating a Traffic Monitoring Session 123
Deleting a Traffic Monitoring Session 124

CHAPTER 14

NetFlow Monitoring 125
NetFlow Monitoring 125
NetFlow Monitoring Limitations 126
Enabling NetFlow Monitoring 127
Creating a Flow Record Definition 127
Viewing Flow Record Definitions 128
Defining the Exporter Profile 128
Creating a Flow Collector 129
Creating a Flow Exporter 130
Creating a Flow Monitor 131
Creating a Flow Monitor Session 132
Associating a Flow Monitor Session to a vNIC 132
Preface

• Audience, on page ix
• Conventions, on page ix
• Related Cisco UCS Documentation, on page xi
• Documentation Feedback, on page xi

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

• Server administration
• Storage administration
• Network administration
• Network security

Conventions

<table>
<thead>
<tr>
<th>Text Type</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUI elements</td>
<td>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.</td>
</tr>
<tr>
<td>TUI elements</td>
<td>In a Text-based User Interface, text the system displays appears in this font.</td>
</tr>
<tr>
<td>System output</td>
<td>Terminal sessions and information that the system displays appear in this font.</td>
</tr>
<tr>
<td>CLI commands</td>
<td>CLI command keywords appear in this font. Variables in a CLI command appear in this font.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
</tbody>
</table>
### Text Type | Indication
--- | ---
{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.

---

**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.

---

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

---

**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 Cisco UCS Documentation

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: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_roadmap.html

For a complete list of all C-Series documentation, see the Cisco UCS C-Series Servers Documentation Roadmap available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/ucs_rack_roadmap.html.

For information on supported firmware versions and supported UCS Manager versions for the rack servers that are integrated with the UCS Manager for management, refer to Release Bundle Contents for Cisco UCS Software.

Other Documentation Resources

Follow Cisco UCS Docs on Twitter to receive document update notifications.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-docfeedback@external.cisco.com. We appreciate your feedback.
CHAPTER 1

New and Changed Information for This Release
System Monitoring Overview

This guide describes how to configure and use system monitoring to manage a Cisco UCS Manager environment.

Cisco UCS Manager can detect system faults: critical, major, minor, and warnings. We recommend that:

- You monitor all faults of either critical or major severity status, as immediate action is not required for minor faults and warnings.
- You monitor faults that are not of type Finite State Machine (FSM), as FSM faults will transition over time and resolve.

This guide covers the following information:

- **System Log**
  - System logs including faults, failures, and alarm thresholds (Syslog)
  - The three types of Syslogs: Fault, Event, and Audit logs
  - The Global Fault Policy and settings that control Syslogs

- **System Event Log**
  - System hardware events for servers and chassis components and their internal components (System Event Log [SEL] logs)
  - The SEL policy that controls SEL logs

- **Simple Network Management Protocol**
  - SNMP for monitoring devices from a central network management station and the host and user settings
  - Fault suppression policies for SNMP traps, Call Home notifications, and specific devices
• Core File Exporter and logs, such as Syslog, Audit Log, and the System Event Log
• Statistics Collection and Threshold Policies for adapters, chassis, host, ports, and servers
• Call Home and Smart Call Home Cisco embedded device support
• Hardware monitoring using the Cisco UCS Manager user interface
• Traffic Monitoring sessions for analysis by a network analyzer
• Cisco Netflow Monitor for IP network traffic accounting, usage-based network billing, network planning, security, Denial of Service monitoring capabilities, and network monitoring

The Cisco UCS Manager Core and Fault Generation

The Cisco UCS Manager core is made up of three elements, which are the Data Management Engine, Application Gateway, and user accessible northbound interface. The northbound interface comprises of SNMP, Syslog, XML API, and UCSM CLI.

You can monitor the Cisco UCS Manager servers through XML API, SNMP, and Syslog. Both SNMP and Syslog are interfaces used only used for monitoring as they are read-only, so no configuration changes are allowed from these interfaces. Alternatively, the XML API is a monitoring interface that is read-write, which allows you to monitor Cisco UCS Manager, and change the configuration if needed.
The DME (Data Management Engine) is the center of the Cisco UCS Manager system, which maintains:

- The Cisco UCS XML database which houses the inventory database of all physical elements (blade and rack mount servers, chassis, modules, and fabric interconnects).
- The logical configuration data for profiles, policies, pools, vNIC, and vHBA templates.
- The various networking-related configuration details like VLANs, VSANs, port channels, network uplinks, and server downlinks.

The DME monitors:

- The current health and state of all components of all physical and logical elements in a Cisco UCS domain.
- The transition information of all Finite State Machine (FSM) tasks occurring.

Only the current information of inventory, health, and configuration data of the managed endpoints are stored in the Cisco UCS XML database resulting in near real time. By default the DME does not store a historical log of faults that have occurred on a Cisco UCS domain. As fault conditions are raised on the endpoints, the
DME creates faults in the Cisco UCS XML database. As those faults are mitigated, the DME clears and removes the faults from the Cisco UCS XML database.

**Application Gateway (AG)**

Application Gateways are software agents that communicate directly with the endpoints to relay the health and state of the endpoints to the DME. AG-managed endpoints include servers, chassis, modules, fabric extenders, fabric interconnects, and NX-OS. The AGs actively monitor the server through the IPMI and SEL logs using the Cisco Integrated Management Controller (CIMC). They provide the DME with the health, state, configuration, and potential fault conditions of a device. The AGs manage configuration changes from the current state to the desired state during FSM transitions when changes are made to the Cisco UCS XML database.

The module AG and chassis AG communicate with the Chassis Management Controller (CMC) to get information about the health, state, configuration, and fault conditions observed by the CMC. The fabric interconnect NX-OS AG communicates directly with NX-OS to get information about the health, state, configuration, statistics, and fault conditions observed by NX-OS on the fabric interconnects. All AGs provide the inventory details to the DME about the endpoints during the various discovery processes. The AGs perform the state changes necessary to configure an endpoint during FSM-triggered transitions, monitor the health and state of the endpoints, and notify the DME of any faults.

**Northbound Interfaces**

The northbound interfaces include SNMP, Syslog, CLI, and XML API. The XML API present in the Apache webserver layer sends login, logout, query, and configuration requests using HTTP or HTTPS. SNMP and Syslog are both consumers of data from the DME.

SNMP informs and traps are translated directly from the fault information stored in the Cisco UCS XML database. SNMP GET requests are sent through the same object translation engine in reverse, where the DME receives a request from the object translation engine. The data is translated from the XML database to an SNMP response.

Syslog messages use the same object translation engine as SNMP, where the source of the data (faults, events, audit logs) is translated from XML into a Cisco UCS Manager-formatted Syslog message.

---

**Cisco UCS Manager User Documentation**

Cisco UCS Manager offers you a new set of smaller, use-case based documentation described in the following table:

<table>
<thead>
<tr>
<th>Guide</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS Manager Getting Started Guide</td>
<td>Discusses Cisco UCS architecture and Day 0 operations, including Cisco UCS Manager initial configuration and configuration best practices.</td>
</tr>
<tr>
<td>Cisco UCS Manager Administration Guide</td>
<td>Discusses password management, role-based access configuration, remote authentication, communication services, CIMC session management, organizations, backup and restore, scheduling options, BIOS tokens, and deferred deployments.</td>
</tr>
<tr>
<td>Guide</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cisco UCS Manager Infrastructure Management Guide</td>
<td>Discusses physical and virtual infrastructure components used and managed by Cisco UCS Manager.</td>
</tr>
<tr>
<td>Cisco UCS Manager Firmware Management Guide</td>
<td>Discusses downloading and managing firmware, upgrading through Auto Install, upgrading through service profiles, directly upgrading at endpoints using firmware auto sync, managing the capability catalog, deployment scenarios, and troubleshooting.</td>
</tr>
<tr>
<td>Cisco UCS Manager Server Management Guide</td>
<td>Discusses the new licenses, registering Cisco UCS domain with Cisco UCS Central, power capping, server boot, server profiles, and server-related policies.</td>
</tr>
<tr>
<td>Cisco UCS Manager Storage Management Guide</td>
<td>Discusses all aspects of storage management, such as SAN and VSAN in Cisco UCS Manager.</td>
</tr>
<tr>
<td>Cisco UCS Manager Network Management Guide</td>
<td>Discusses all aspects of network management, such as LAN and VLAN connectivity in Cisco UCS Manager.</td>
</tr>
<tr>
<td>Cisco UCS Manager System Monitoring Guide</td>
<td>Discusses all aspects of system and health monitoring, including system statistics in Cisco UCS Manager.</td>
</tr>
</tbody>
</table>
Syslog

Cisco UCS Manager generates system log, or syslog messages to record the following incidents that take place in the Cisco UCS Manager system:

- Routine system operations
- Failures and errors
- Critical and emergency conditions

There are three kinds of syslog entries: Fault, Event, and Audit.

Each syslog message identifies the Cisco UCS Manager process that generated the message and provides a brief description of the operation or error that occurred. The syslog is useful both in routine troubleshooting, incident handling, and management.

Cisco UCS Manager collects and logs syslog messages internally. You can send them to external syslog servers running a syslog daemon. Logging to a central syslog server helps in aggregation of logs and alerts. Some syslog messages to monitor include, DIMM problems, equipment failures, thermal problems, voltage problems, power problems, high availability (HA) cluster problems, and link failures.

---

**Note**

The FSM faults, threshold faults, and unresolved policy events are not sent to syslog server. However, SNMP traps are generated for the threshold fault events.

Syslog messages contain an event code and fault code. To monitor syslog messages, you can define syslog message filters. These filters can parse the syslog messages based on the criteria you choose. You can use the following criteria to define a filter:

- By event or fault codes: Define a filter with a parsing rule to include only the specific codes that you intend to monitor. Messages that do not match these criteria are discarded.
• By severity level: Define a filter with a parsing rule to monitor syslog messages with specific severity levels. You can set syslog severity levels individually for OS functions, to facilitate logging and display of messages ranging from brief summaries to detailed information for debugging.

Cisco devices can send their log messages to a Unix-style syslog service. A syslog service simply accepts messages, then stores them in files or prints them according to a simple configuration file. This form of logging is the best available for Cisco devices because it can provide protected long-term storage of logs.

### Configuring the Syslog Using Cisco UCS Manager GUI

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>In the Navigation pane, click Admin.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Expand All &gt; Faults, Events, and Audit Log.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Click Syslog.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>In the Local Destinations area, complete the following fields:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Console Section</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Admin State field</strong></td>
<td>Indicate whether Cisco UCS displays Syslog messages on the console. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Enabled—Syslog messages are displayed on the console as well as added to the log.</td>
</tr>
<tr>
<td></td>
<td>• Disabled—Syslog messages are added to the log but are not displayed on the console.</td>
</tr>
<tr>
<td><strong>Level field</strong></td>
<td>If this option is enabled, select the lowest message level that you want displayed. Cisco UCS displays that level, and above, on the console. This level can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Emergencies</td>
</tr>
<tr>
<td></td>
<td>• Alerts</td>
</tr>
<tr>
<td></td>
<td>• Critical</td>
</tr>
<tr>
<td><strong>Monitor Section</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Admin State</strong></td>
<td>Indicate whether Cisco UCS displays Syslog messages on the monitor. This state can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—Syslog messages are displayed on the monitor as well as added to the log.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—Syslog messages are added to the log but not displayed on the monitor.</td>
</tr>
<tr>
<td></td>
<td>If <strong>Admin State</strong> is enabled, Cisco UCS Manager GUI displays the remaining fields in this section.</td>
</tr>
<tr>
<td><strong>Level</strong> drop-down list</td>
<td>If this option is <strong>enabled</strong>, select the lowest message level that you want displayed. The system displays that level, and above, on the monitor. This level can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Emergencies</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Alerts</strong>                                                                     \</td>
</tr>
<tr>
<td></td>
<td>• <strong>Critical</strong>                                                                   \</td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>                                                                     \</td>
</tr>
<tr>
<td></td>
<td>• <strong>Warnings</strong>                                                                   \</td>
</tr>
<tr>
<td></td>
<td>• <strong>Notifications</strong>                                                              \</td>
</tr>
<tr>
<td></td>
<td>• <strong>Information</strong>                                                                \</td>
</tr>
<tr>
<td></td>
<td>• <strong>Debugging</strong>                                                                  \</td>
</tr>
</tbody>
</table>

**File Section**

<table>
<thead>
<tr>
<th><strong>Admin State</strong> field</th>
<th>Indicates whether Cisco UCS stores messages in a system log file on the fabric interconnect. This state can be one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—Messages are saved in the log file.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—Messages are not saved.</td>
</tr>
<tr>
<td></td>
<td>If <strong>Admin State</strong> is enabled, Cisco UCS Manager GUI displays the remaining fields in this section.</td>
</tr>
</tbody>
</table>
Step 5

In the Remote Destinations area, complete the following fields to configure up to three external logs that can store messages generated by the Cisco UCS components:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Admin State</strong></td>
<td>This can be one of the following:</td>
</tr>
<tr>
<td><strong>Enabled</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Disabled</strong></td>
<td></td>
</tr>
</tbody>
</table>

If **Admin State** is enabled, Cisco UCS Manager GUI displays the remaining fields in this section.
**Syslog**

**Configuring the Syslog Using Cisco UCS Manager GUI**

In the **Local Sources** area, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Level** drop-down list | Select the lowest message level that you want the system to store. The system stores that level, and above, in the remote file. This level can be one of the following:  
  - Emergencies  
  - Alerts  
  - Critical  
  - Errors  
  - Warnings  
  - Notifications  
  - Information  
  - Debugging |
| **Hostname** field | The hostname or IP address on which the remote log file resides.  
  **Note**: If you use a hostname rather than an IPv4 or IPv6 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. |
| **Facility** drop-down list | This can be one of the following:  
  - Local0  
  - Local1  
  - Local2  
  - Local3  
  - Local4  
  - Local5  
  - Local6  
  - Local7 |
| **Faults Admin State** field | If this field is **Enabled**, Cisco UCS logs all system faults. |
| **Audits Admin State** field | If this field is **Enabled**, Cisco UCS logs all audit log events. |
### Events Admin State field

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events Admin State</td>
<td>If this field is Enabled, Cisco UCS logs all system events.</td>
</tr>
</tbody>
</table>

**Step 7** Click **Save Changes**.
System Event Log

The System Event Log (SEL) resides on the CIMC in NVRAM. The SEL is used for troubleshooting system health. It records most server-related events, such as instances of over or under voltage, temperature events, fan events, and BIOS events. The types of events supported by SEL include BIOS events, memory unit events, processor events, and motherboard events.

The SEL logs are stored in the CIMC NVRAM, through a SEL log policy. It is best practice to periodically download and clear the SEL logs. The SEL file is approximately 40KB in size, and no further events can be recorded once it is full. It must be cleared before additional events can be recorded.

You can use the SEL policy to back up the SEL to a remote server, and optionally to clear the SEL after a backup operation occurs. Backup operations can be triggered based on specific actions, or they can be set to occur at regular intervals. You can also manually back up or clear the SEL.

The backup file is automatically generated. The filename format is sel-SystemName-ChassisID-ServerID-ServerSerialNumber-Timestamp.

For example, sel-UCS-A-ch01-serv01-QCI12522939-20091121160736.
Viewing the System Event Log for an Individual Server

**Procedure**

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

**Step 2**  
Expand Equipment > Chassis > Chassis Number > Servers.

**Step 3**  
Click the server for which you want to view the system event log.

**Step 4**  
In the Work pane, click the SEL Logs tab.

Cisco UCS Manager retrieves the system event log for the server and displays the list of events.

---

Viewing the System Event Log for the Servers in a Chassis

**Procedure**

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

**Step 2**  
On the Equipment tab, expand Equipment > Chassis > Chassis_Name.

**Step 3**  
In the Work pane, click the SEL Logs tab.

Cisco UCS Manager retrieves the system event log for the server and displays the list of events.

**Step 4**  
In the Server table, click the server for which you want to view the system event log.

Cisco UCS Manager retrieves the system event log for the server and displays the list of events.

---

Configuring the SEL Policy

**Procedure**

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

**Step 2**  
Click the Equipment node.

**Step 3**  
In the Work pane, click the Policies tab.

**Step 4**  
Click the SEL Policy subtab.

**Step 5**  
(Optional) In the General area, type a description of the policy in the Description field.

The other fields in this area are read-only.

**Step 6**  
In the Backup Configuration area, complete the following fields:
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Protocol field** | The protocol to use when communicating with the remote server. This can be one of the following:  
|                 | • FTP  
|                 | • TFTP  
|                 | • SCP  
|                 | • SFTP  
|                 | • **USB A**—The USB drive inserted into fabric interconnect A.  
|                 | This option is only available for certain system configurations.  
|                 | • **USB B**—The USB drive inserted into fabric interconnect B.  
|                 | This option is only available for certain system configurations. |
| **Hostname field** | The hostname or IP address of the server on which the backup configuration resides. If you use a hostname rather than an IPv4 or IPv6 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.  
|                 | **Note** The name of the backup file is generated by Cisco UCS. The name is in the following format:  
|                 | `sel-system-name-chassis-id-`  
|                 | `servblade-id-blade-serial-`  
|                 | `timestamp` |
| **Remote Path field** | The absolute path to the file on the remote server, if required.  
|                 | 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, provided that the file resides in the default download folder. For details about how your file server is configured, contact your system administrator. |
### Configuring the SEL Policy

#### Name | Description
--- | ---
**Backup Interval** drop-down list | The time to wait between automatic backups. This can be one of the following:
- **Never**—Do not perform any automatic SEL data backups.
- **1 Hour**
- **2 Hours**
- **4 Hours**
- **8 Hours**
- **24 Hours**
- **1 Week**
- **1 Month**
**Note** | If you want the system to create automatic backups, make sure that you check the **Timer** check box in the **Action** option box.

**Format** field | The format to use for the backup file. This can be one of the following:
- **Ascii**
- **Binary**

**Clear on Backup** check box | If checked, Cisco UCS clears all system event logs after the backup is completed.

**User** field | The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or USB.

**Password** field | The password for the remote server username. This field does not apply if the protocol is TFTP or USB.

**Action** check box | For each box that is checked, the system creates an SEL backup when that event is encountered:
- **Log Full**—The log reaches the maximum size allowed.
- **On Change of Association**—The association between a server and its service profile changes.
- **On Clear**—The user manually clears a system event log.
- **Timer**—The time interval specified in the **Backup Interval** drop-down list is reached.

**Reset Configuration** button | Click this button to reset the background configuration information.

### Step 7
Click **Save Changes**.
Copying One or More Entries in the System Event Log

This task assumes that you are viewing the system event log for a server from the SEL Logs tab for a server or a chassis.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>After the Cisco UCS Manager GUI displays the system event log in the SEL Logs tab, use your mouse to highlight the entry or entries that you want to copy from the system event log.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click <strong>Copy</strong> to copy the highlighted text to the clipboard.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Paste the highlighted text into a text editor or other document.</td>
</tr>
</tbody>
</table>

Printing the System Event Log

This task assumes that you are viewing the system event log for a server from the SEL Logs tab for a server or a chassis.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>After the Cisco UCS Manager GUI displays the system event log in the SEL Logs tab, click <strong>Print</strong>.</th>
</tr>
</thead>
</table>
| Step 2 | In the **Print** dialog box, do the following:  
  a) (Optional) Modify the default printer, or any other fields or options.  
  b) Click **Print**. |

Refreshing the System Event Log

This task assumes that you are viewing the system event log for a server from the SEL Logs tab for a server or a chassis.

**Procedure**

After the Cisco UCS Manager GUI displays the system event log in the SEL Logs tab, click **Refresh**.  
Cisco UCS Manager retrieves the system event log for the server and displays the updated list of events.
Manually Backing Up the System Event Log

This task assumes that you are viewing the system event log for a server from the SEL Logs tab for a server or a chassis.

Before you begin

Configure the system event log policy. The manual backup operation uses the remote destination configured in the system event log policy.

Procedure

After Cisco UCS Manager GUI displays the system event log in the SEL Logs tab, click Backup. Cisco UCS Manager backs up the system event log to the location specified in the SEL policy.

Manually Clearing the System Event Log

This task assumes that you are viewing the system event log for a server from the SEL Logs tab for a server or a chassis.

Procedure

After Cisco UCS Manager GUI displays the system event log in the SEL Logs tab, click Clear.

Note This action triggers an automatic backup if Clear is enabled in the SEL policy Action option box.
Core File Exporter

Critical failures in the Cisco UCS components, such as a fabric interconnect or an I/O module, can cause the system to create a core dump file. Cisco UCS Manager uses the Core File Exporter to immediately export the core dump files to a specified location on the network through TFTP. This functionality allows you to export the tar file with the contents of the core dump file. The Core File Exporter provides system monitoring and automatic export of core dump files that need to be included in TAC cases.

Configuring the Core File Exporter

Procedure

1. In the Navigation pane, click Admin.
2. Expand All > Faults, Events, and Audit Log.
3. Click Settings.
4. In the Work pane, click the TFTP Core Exporter tab.
5. On the TFTP Core Exporter tab, complete the following fields:
Disabling the Core File Exporter

**Procedure**

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

**Step 2** Expand All > Faults, Events, and Audit Log.

**Step 3** Click Settings.

**Step 4** In the Work pane, click the Settings tab.

**Step 5** In the TFTP Core Exporter area, click the disabled radio button in the Admin State field.

---

**Core File Exporter**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Admin State</strong> field</td>
<td>This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—If an error causes the server to perform a core dump, Cisco UCS automatically sends the core dump file via FTP to a given location. When this option is selected, the Cisco UCS Manager GUI displays the other fields that enable you to specify the FTP export options. The Core File Exporter provides system monitoring and automatic export of core files that need to be included in TAC cases.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—Core dump files are not automatically exported.</td>
</tr>
<tr>
<td><strong>Description</strong> field</td>
<td>A user-defined description of the core file. Entry up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), &quot; (double quote), = (equal sign), &gt; (greater than), &lt; (less than), or ’ (single quote).</td>
</tr>
<tr>
<td><strong>Port</strong> field</td>
<td>The port number to use when exporting the core dump file via TFTP.</td>
</tr>
<tr>
<td><strong>Hostname</strong> field</td>
<td>The hostname or IPv4 or IPv6 address to connect with via TFTP.</td>
</tr>
<tr>
<td><strong>Path</strong> field</td>
<td>The path to use when storing the core dump file on the remote system.</td>
</tr>
</tbody>
</table>

**Note** If you use a hostname rather than an IPv4 or IPv6 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.
**Step 6**  Click **Save Changes**.
Disabling the Core File Exporter
Audit Logs

- Audit Logs, on page 25
- Viewing the Audit Logs, on page 25

Audit Logs

Audit Logs record system events that occurred, where they occurred, and which users initiated them.

Viewing the Audit Logs

You can view, export, print, or refresh the audit logs displayed on the Audit Logs page.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Navigation pane, click Admin.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Expand All &gt; Faults, Events, and Audit Log.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the work pane, click the Audit Logs tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>The Work pane displays the audit logs.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID column</td>
<td>The unique identifier associated with the message.</td>
</tr>
<tr>
<td>Affected Object</td>
<td>The component that is affected by this issue.</td>
</tr>
<tr>
<td></td>
<td>Click the object name to view the properties for this object.</td>
</tr>
<tr>
<td>Trig column</td>
<td>The user role associated with the user that triggered the event.</td>
</tr>
<tr>
<td>User column</td>
<td>The type of user.</td>
</tr>
<tr>
<td>Session ID column</td>
<td>The session ID associated with the session during which the event occurred.</td>
</tr>
<tr>
<td>Created at column</td>
<td>The day and time that the fault occurred.</td>
</tr>
</tbody>
</table>
### Table: Description of Audit Log Columns

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Indication</strong> column</td>
<td>This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Creation</strong>—A component was added to the system.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Modification</strong>—An existing component was changed.</td>
</tr>
<tr>
<td><strong>Description</strong> column</td>
<td>More information about the fault.</td>
</tr>
<tr>
<td><strong>Modified Properties</strong> column</td>
<td>The system properties that were changed by the event.</td>
</tr>
</tbody>
</table>
CHAPTER 7

Fault Collection and Suppression

• Configuring Settings for the Fault Collection Policy, on page 27
• Configuring Fault Suppression, on page 29

Configuring Settings for the Fault Collection Policy

Global Fault Policy

The global fault policy controls the lifecycle of a fault in a Cisco UCS domain, including when faults are cleared, the flapping interval (the length of time between the fault being raised and the condition being cleared), and the retention interval (the length of time a fault is retained in the system).

A fault in Cisco UCS has the following lifecycle:

1. A condition occurs in the system and Cisco UCS Manager raises a fault. This is the active state.

2. When the fault is alleviated, it enters a flapping or soaking interval that is designed to prevent flapping. Flapping occurs when a fault is raised and cleared several times in rapid succession. During the flapping interval, the fault retains its severity for the length of time specified in the global fault policy.

3. If the condition reoccurs during the flapping interval, the fault returns to the active state. If the condition does not reoccur during the flapping interval, the fault is cleared.

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

5. If the condition reoccurs during the retention interval, the fault returns to the active state. If the condition does not reoccur, the fault is deleted.

Configuring the Global Fault Policy

Procedure

Step 1 In the Navigation pane, click Admin.
Step 2  Expand All > Faults, Events, and Audit Log.
Step 3  Click Settings.
Step 4  In the Work pane, click the Global Fault Policy tab.
Step 5  In the Global Fault Policy tab, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Flapping Interval</strong> field</td>
<td>Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, Cisco UCS Manager does not allow a fault to change its state until this amount of time has elapsed since the last state change. If the condition reoccurs during the flapping interval, the fault returns to the active state. If the condition does not reoccur during the flapping interval, the fault is cleared. What happens at that point depends on the setting in the Clear Action field. Enter an integer between 5 and 3,600. The default is 10.</td>
</tr>
</tbody>
</table>
| **Initial Severity** field  | This can be one of the following:  
|                             | • Info  
|                             | • Condition  
|                             | • Warning |
| **Action on Acknowledgment** field | Acknowledged actions are always deleted when the log is cleared. This option cannot be changed. |
| **Clear Action** field      | The action Cisco UCS Manager takes when a fault is cleared. This can be one of the following:  
|                             | • Retain—Cisco UCS Manager GUI displays the **Length of time to retain cleared faults** section.  
|                             | • Delete—Cisco UCS Manager immediately deletes all fault messages as soon as they are marked as cleared. |
| **Clear Interval** field    | Indicate whether Cisco UCS Manager automatically clears faults after a certain length of time. This can be one of the following:  
|                             | • Never—Cisco UCS Manager does not automatically clear any faults.  
|                             | • other—Cisco UCS Manager GUI displays the dd:hh:mm:ss field. |
| dd:hh:mm:ss field           | The number of days, hours, minutes, and seconds that should pass before Cisco UCS Manager automatically marks that fault as cleared. What happens then depends on the setting in the Clear Action field. |

Step 6  Click Save Changes.
Fault Suppression

Fault Suppression allows you to suppress SNMP trap and Call Home notifications during a planned maintenance time. You can create a fault suppression task to prevent notifications from being sent whenever a transient fault is raised or cleared.

Faults remain suppressed until the time duration has expired, or the fault suppression tasks have been manually stopped by you. After the fault suppression has ended, Cisco UCS Manager will send notifications for any outstanding suppressed faults that have not been cleared.

You can configure fault suppression using the following methods.

Fixed Time Intervals or Schedules

You can use the following to specify the maintenance window during which you want to suppress faults:

- Fixed time intervals allow you to create a start time and a duration when fault suppression is active. Fixed time intervals cannot be reused.

- Schedules are used for one time occurrences or recurring time periods. They can be saved and reused.

Suppression Policies

These policies define which causes and types of faults you want to suppress. Only one policy can be assigned to a task. The following policies are defined by Cisco UCS Manager:

- **default-chassis-all-maint**—Suppresses faults for the chassis and all components installed into the chassis, including all servers, power supplies, fan modules, and IOMs.

  This policy applies only to chassis.

- **default-chassis-phys-maint**—Suppresses faults for the chassis, all fan modules, and power supplies installed into the chassis.

  This policy applies only to chassis.

- **default-fex-all-maint**—Suppresses faults for the FEX, all power supplies, fan modules, and IOMs in the FEX.

  This policy applies only to FEXes.

- **default-fex-phys-maint**—Suppresses faults for the FEX, all fan modules and power supplies in the FEX.

  This policy applies only to FEXes.

- **default-server-maint**—Suppresses faults for servers.

  This policy applies to chassis, organizations, and service profiles.

  **Note** When applied to a chassis, only servers are affected.
Cisco UCS Manager does not suppress SNMP MIB-2 faults generated by NX-OS network operating system designed to support high performance, high reliability server access switches used in the data center. These SNMP MIB-2 faults have no association with this fault suppression policy.

- **default-iom-maint**—Suppresses faults for IOMs in a chassis or FEX.
  
  This policy applies only to chassis, FEXes, and IOMs.

**Suppression Tasks**

You can use these tasks to connect the schedule or fixed time interval and the suppression policy to a component.

**Note**

After you create a suppression task, you can edit the fixed time interval or schedule of the task in both the Cisco UCS Manager GUI and Cisco UCS Manager CLI. However, you can only change between using a fixed time interval and using a schedule in the Cisco UCS Manager CLI.

### Viewing Suppressed Faults

**Procedure**

1. In the **Navigation** pane, click **Admin**.
2. Expand **All > Faults, Events, and Audit Log**.
3. Click **Faults**.
4. In the **Work** pane, choose the **Suppressed** icon in the **Severity** area.

   To view only the suppressed faults, uncheck the other icons in the **Severity** area.

### Configuring Fault Suppression for a Chassis

**Configuring Fault Suppression Tasks for a Chassis**

**Procedure**

1. In the **Navigation** pane, click **Equipment**.
2. Expand **Equipment > Chassis**.
3. Click the chassis for which you want to create a fault suppression task.
4. In the **Work** pane, click the **General** tab.
Step 5  
In the **Actions** area, click **Start Fault Suppression**.

**Tip**  
To configure fault suppression tasks for multiple chassis, use the **Ctrl** key to select multiple chassis in the **Navigation** pane. Right-click one of the selected chassis and choose **Start Fault Suppression**.

Step 6  
In the **Start Fault Suppression** dialog box, complete the following fields:

| Name field | The name of the fault suppression task.  
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved. |
|---|---|
| **Select Fixed Time Interval/Schedule** field | Specify when the fault suppression task will run. This can be one of the following:  
- **Fixed Time Interval**—Choose this option to specify the start time and duration for the fault suppression task.  
  Specify the day and time the fault suppression task should start in the **Start Time** field. Click the down arrow at the end of this field to select the start time from a pop-up calendar.  
  Specify the length of time this task should run in the **Task Duration** field. To specify that this task should run until it is manually stopped, enter **00:00:00:00** in this field.  
- **Schedule**—Choose this option to configure the start time and duration using a pre-defined schedule.  
  Choose the schedule from the **Schedule** drop-down list. To create a new schedule, click **Create Schedule**. |
| Policy drop-down list | Choose the suppression policy from the drop-down list:  
- **default-chassis-all-maint**—Suppresses faults for the chassis and all components installed into the chassis, including all servers, power supplies, fan modules, and IOMs.  
- **default-chassis-phys-maint**—Suppresses faults for the chassis, all fan modules, and power supplies installed into the chassis.  
- **default-server-maint**—Suppresses faults for servers.  
  **Note**  
  When applied to a chassis, only servers are affected.  
- **default-iom-maint**—Suppresses faults for IOMs in a chassis or FEX. |

Step 7  
Click **OK**.
Viewing Fault Suppression Tasks for a Chassis

**Procedure**

**Step 1** In the **Navigation** pane, click **Equipment**.
**Step 2** Expand **Equipment > Chassis**.
**Step 3** Click the chassis for which you want to view fault suppression task properties.
**Step 4** In the **Work** pane, click the **General** tab.
**Step 5** In the **Actions** area, click **Suppression Task Properties**.

In the **Suppression Tasks** dialog box, you can add new fault suppression tasks, delete existing fault suppression tasks, or modify existing fault suppression tasks.

Deleting Fault Suppression Tasks for a Chassis

This procedure deletes all fault suppression tasks for a chassis. To delete individual tasks, use the **Delete** button on the **Suppression Tasks** dialog box. See **Viewing Fault Suppression Tasks for a Chassis**, on page 32.

**Procedure**

**Step 1** In the **Navigation** pane, click **Equipment**.
**Step 2** Expand **Equipment > Chassis**.
**Step 3** Click the chassis for which you want to delete all fault suppression tasks.
**Step 4** In the **Work** pane, click the **General** tab.
**Step 5** In the **Actions** area, click **Stop Fault Suppression**.

**Tip** To delete fault suppression tasks for multiple chassis, use the **Ctrl** key to select multiple chassis in the **Navigation** pane. Right-click one of the selected chassis and choose **Stop Fault Suppression**.

**Step 6** If a confirmation dialog box displays, click **Yes**.

Configuring Fault Suppression for an I/O Module

Configuring Fault Suppression Tasks for an IOM

**Procedure**

**Step 1** In the **Navigation** pane, click **Equipment**.
**Step 2** (Optional) To select IOM modules in a chassis, expand **Equipment > Chassis > Chassis Number > IO Modules**.
### Fault Collection and Suppression

#### Viewing Fault Suppression Tasks for an IOM

**Procedure**

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

**Step 2** (Optional) To select IOM modules in a chassis, expand **Equipment > Chassis > Chassis Number > IO Modules**.

---

**Step 3** (Optional) To select IOM modules in a FEX, expand **Equipment > FEX > FEX Number > IO Modules**.

**Step 4** Click the IOM for which you want to create a fault suppression task.

**Step 5** In the **Work** pane, click the **General** tab.

**Step 6** In the **Actions** area, click **Start Fault Suppression**.

**Tip** To configure fault suppression tasks for multiple IOMs, use the **Ctrl** key to select multiple IOMs in the **Navigation** pane. Right-click one of the selected IOMs and choose **Start Fault Suppression**.

You can select IOMs in either chassis, FEXes, or both.

**Step 7** In the **Start Fault Suppression** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong> field</td>
<td>The name of the fault suppression task. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.</td>
</tr>
<tr>
<td><strong>Select Fixed Time Interval/Schedule</strong> field</td>
<td>Specify when the fault suppression task will run. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Fixed Time Interval</strong>—Choose this option to specify the start time and duration for the fault suppression task.</td>
</tr>
<tr>
<td></td>
<td>Specify the day and time the fault suppression task should start in the <strong>Start Time</strong> field. Click the down arrow at the end of this field to select the start time from a pop-up calendar.</td>
</tr>
<tr>
<td></td>
<td>Specify the length of time this task should run in the <strong>Task Duration</strong> field. To specify that this task should run until it is manually stopped, enter <strong>00:00:00:00</strong> in this field.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Schedule</strong>—Choose this option to configure the start time and duration using a pre-defined schedule.</td>
</tr>
<tr>
<td></td>
<td>Choose the schedule from the <strong>Schedule</strong> drop-down list. To create a new schedule, click <strong>Create Schedule</strong>.</td>
</tr>
<tr>
<td><strong>Policy</strong> drop-down list</td>
<td>The following suppression policy is selected by default:</td>
</tr>
<tr>
<td></td>
<td>• <strong>default-iom-maint</strong>—Suppresses faults for IOMs in a chassis or FEX.</td>
</tr>
</tbody>
</table>

**Step 8** Click **OK**.

---

---

---
Step 3  (Optional) To select IOM modules in a FEX, expand Equipment > FEX > FEX Number > IO Modules.
Step 4  Click the IOM for which you want to view fault suppression task properties.
Step 5  In the Work pane, click the General tab.
Step 6  In the Actions area, click Suppression Task Properties.

In the Suppression Tasks dialog box, you can add new fault suppression tasks, delete existing fault suppression tasks, or modify existing fault suppression tasks.

Deleting Fault Suppression Tasks for an IOM

This procedure deletes all fault suppression tasks for an IOM. To delete individual tasks, use the Delete button on the Suppression Tasks dialog box. See Viewing Fault Suppression Tasks for an IOM, on page 33.

Procedure

Step 1  In the Navigation pane, click Equipment.
Step 2  (Optional) To select IOM modules in a chassis, expand Equipment > Chassis > Chassis Number > IO Modules.
Step 3  (Optional) To select IOM modules in a FEX, expand Equipment > FEX > FEX Number > IO Modules.
Step 4  Click the IOM for which you want to delete all fault suppression tasks.
Step 5  In the Work pane, click the General tab.
Step 6  In the Actions area, click Stop Fault Suppression.

Tip  To delete fault suppression tasks for multiple IOMs, use the Ctrl key to select multiple IOMs in the Navigation pane. Right-click one of the selected IOMs and choose Stop Fault Suppression.

You can select IOMs in either chassis, FEXes, or both.

Step 7  If a confirmation dialog box displays, click Yes.

Configuring Fault Suppression for a FEX

Configuring Fault Suppression Tasks for a FEX

Procedure

Step 1  In the Navigation pane, click Equipment.
Step 2  Expand Equipment > Rack Mounts > FEX.
Step 3  Click the FEX for which you want to create a fault suppression task.
Step 4  In the Work pane, click the General tab.
Step 5  In the Actions area, click Start Fault Suppression.
To configure fault suppression tasks for multiple FEXes, use the Ctrl key to select multiple FEXes in the Navigation pane. Right-click one of the selected FEXes and choose Start Fault Suppression.

**Tip**

To configure fault suppression tasks for multiple FEXes, use the Ctrl key to select multiple FEXes in the Navigation pane. Right-click one of the selected FEXes and choose Start Fault Suppression.

**Step 6**

In the **Start Fault Suppression** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>The name of the fault suppression task.</td>
</tr>
<tr>
<td></td>
<td>This name can be between 1 and 16 alphanumeric characters. You cannot use</td>
</tr>
<tr>
<td></td>
<td>spaces or any special characters other than -(hyphen), _ (underscore), :</td>
</tr>
<tr>
<td></td>
<td>(colon), and . (period), and you cannot change this name after the object</td>
</tr>
<tr>
<td></td>
<td>is saved.</td>
</tr>
<tr>
<td>Select Fixed Time Interval/Schedule field</td>
<td>Specify when the fault suppression task will run. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Fixed Time Interval</strong>—Choose this option to specify the start time and duration for the fault suppression task.</td>
</tr>
<tr>
<td></td>
<td>Specify the day and time the fault suppression task should start in the <strong>Start Time</strong> field. Click the down arrow at the end of this field to select the start time from a pop-up calendar.</td>
</tr>
<tr>
<td></td>
<td>Specify the length of time this task should run in the <strong>Task Duration</strong> field. To specify that this task should run until it is manually stopped, enter <strong>00:00:00</strong> in this field.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Schedule</strong>—Choose this option to configure the start time and duration using a pre-defined schedule.</td>
</tr>
<tr>
<td></td>
<td>Choose the schedule from the <strong>Schedule</strong> drop-down list. To create a new schedule, click <strong>Create Schedule</strong>.</td>
</tr>
<tr>
<td>Policy drop-down list</td>
<td>Choose the suppression policy from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• <strong>default-fex-all-maint</strong>—Suppresses faults for the FEX, all power supplies, fan modules, and IOMs in the FEX.</td>
</tr>
<tr>
<td></td>
<td>• <strong>default-fex-phys-maint</strong>—Suppresses faults for the FEX, all fan modules and power supplies in the FEX.</td>
</tr>
<tr>
<td></td>
<td>• <strong>default-iom-maint</strong>—Suppresses faults for IOMs in a chassis or FEX.</td>
</tr>
</tbody>
</table>

**Step 7**

Click **OK**.

---

**Viewing Fault Suppression Tasks for a FEX**

**Procedure**

**Step 1**

In the **Navigation** pane, click **Equipment**.

**Step 2**

Expand **Equipment** > **Rack Mounts** > **FEX**.

**Step 3**

Click the FEX for which you want to view fault suppression task properties.

**Step 4**

In the **Work** pane, click the **General** tab.
Deleting Fault Suppression Tasks for a FEX

This procedure deletes all fault suppression tasks for a FEX. To delete individual tasks, use the Delete button on the Suppression Tasks dialog box. See Viewing Fault Suppression Tasks for a FEX, on page 35.

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Expand Equipment > Rack Mounts > FEX.
Step 3 Click the FEX for which you want to delete all fault suppression tasks.
Step 4 In the Work pane, click the General tab.
Step 5 In the Actions area, click Stop Fault Suppression.

Tip To delete fault suppression tasks for multiple FEXes, use the Ctrl key to select multiple FEXes in the Navigation pane. Right-click one of the selected FEXes and choose Stop Fault Suppression.

Step 6 If a confirmation dialog box displays, click Yes.

Configuring Fault Suppression for Servers

Configuring Fault Suppression Tasks for a Blade Server

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Expand Equipment > Chassis > Chassis Number > Servers.
Step 3 Click the server for which you want to create a fault suppression task.
Step 4 In the Work pane, click the General tab.
Step 5 In the Actions area, click Start Fault Suppression.

Tip To configure fault suppression tasks for multiple blade servers, use the Ctrl key to select multiple blade servers in the Navigation pane. Right-click one of the selected servers and choose Start Fault Suppression.

Step 6 In the Start Fault Suppression dialog box, complete the following fields:
Viewing Fault Suppression Tasks for a Blade Server

**Procedure**

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

**Step 2**
Expand Equipment > Chassis > Chassis Number > Servers.

**Step 3**
Click the server for which you want to view fault suppression task properties.

**Step 4**
In the Work pane, click the General tab.

**Step 5**
In the Actions area, click Suppression Task Properties.

In the Suppression Tasks dialog box, you can add new fault suppression tasks, delete existing fault suppression tasks, or modify existing fault suppression tasks.
Deleting Fault Suppression Tasks for a Blade Server

This procedure deletes all fault suppression tasks for a blade server. To delete individual tasks, use the **Delete** button on the **Suppression Tasks** dialog box. See Viewing Fault Suppression Tasks for a Blade Server, on page 37.

**Procedure**

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

**Step 2**  Expand **Equipment > Chassis > Chassis Number > Servers**.

**Step 3**  Click the server for which you want to delete all fault suppression tasks.

**Step 4**  In the **Work** pane, click the **General** tab.

**Step 5**  In the **Actions** area, click **Stop Fault Suppression**.

**Tip**  To delete fault suppression tasks for multiple blade servers, use the **Ctrl** key to select multiple blade servers in the **Navigation** pane. Right-click one of the selected servers and choose **Stop Fault Suppression**.

**Step 6**  If a confirmation dialog box displays, click **Yes**.

Configuring Fault Suppression Tasks for a Rack Server

**Procedure**

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

**Step 2**  Expand **Equipment > Rack Mounts > Servers**.

**Step 3**  Click the server for which you want to create a fault suppression task.

**Step 4**  In the **Work** pane, click the **General** tab.

**Step 5**  In the **Actions** area, click **Start Fault Suppression**.

**Tip**  To configure fault suppression tasks for multiple rack servers, use the **Ctrl** key to select multiple rack servers in the **Navigation** pane. Right-click one of the selected servers and choose **Start Fault Suppression**.

**Step 6**  In the **Start Fault Suppression** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name field</th>
<th>The name of the fault suppression task.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.</td>
</tr>
</tbody>
</table>
Select Fixed Time Interval/Schedule field | Specify when the fault suppression task will run. This can be one of the following:

- **Fixed Time Interval**—Choose this option to specify the start time and duration for the fault suppression task.

  Specify the day and time the fault suppression task should start in the **Start Time** field. Click the down arrow at the end of this field to select the start time from a pop-up calendar.

  Specify the length of time this task should run in the **Task Duration** field. To specify that this task should run until it is manually stopped, enter `00:00:00:00` in this field.

- **Schedule**—Choose this option to configure the start time and duration using a pre-defined schedule.

  Choose the schedule from the **Schedule** drop-down list. To create a new schedule, click **Create Schedule**.

| Policy drop-down list | The following suppression policy is selected by default:

  - **default-server-maint**—Suppresses faults for servers. |

**Step 7** Click **OK**.

### Viewing Fault Suppression Tasks for a Rack Server

**Procedure**

1. **Step 1** In the **Navigation** pane, click **Equipment**.
2. **Step 2** Expand **Equipment > Rack Mounts > Servers**.
3. **Step 3** Click the server for which you want to view fault suppression task properties.
4. **Step 4** In the **Work** pane, click the **General** tab.
5. **Step 5** In the **Actions** area, click **Suppression Task Properties**.

   In the **Suppression Tasks** dialog box, you can add new fault suppression tasks, delete existing fault suppression tasks, or modify existing fault suppression tasks.

### Deleting Fault Suppression Tasks for a Rack Server

This procedure deletes all fault suppression tasks for a rack server. To delete individual tasks, use the **Delete** button on the **Suppression Tasks** dialog box. See **Viewing Fault Suppression Tasks for a Rack Server**, on page 39.
Procedure

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

**Step 2**  
Expand Equipment > Rack Mounts > Servers.

**Step 3**  
Click the server for which you want to delete all fault suppression tasks.

**Step 4**  
In the Work pane, click the General tab.

**Step 5**  
In the Actions area, click Stop Fault Suppression.

**Tip**  
To delete fault suppression tasks for multiple rack servers, use the Ctrl key to select multiple rack servers in the Navigation pane. Right-click one of the selected servers and choose Stop Fault Suppression.

**Step 6**  
If a confirmation dialog box displays, click Yes.

### Configuring Fault Suppression for a Service Profile

#### Configuring Fault Suppression Tasks for a Service Profile

**Procedure**

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

**Step 2**  
Expand Servers > Service Profiles.

**Step 3**  
Click the service profile for which you want to create a fault suppression task.

**Step 4**  
In the Work pane, click the General tab.

**Step 5**  
In the Actions area, click Start Fault Suppression.

**Tip**  
To configure fault suppression tasks for multiple service profiles, use the Ctrl key to select multiple service profiles in the Navigation pane. Right-click one of the selected service profiles and choose Start Fault Suppression.

**Step 6**  
In the Start Fault Suppression dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name field</th>
<th>The name of the fault suppression task.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.</td>
</tr>
</tbody>
</table>
Select Fixed Time Interval/Schedule field

Specify when the fault suppression task will run. This can be one of the following:

- **Fixed Time Interval**—Choose this option to specify the start time and duration for the fault suppression task.

  Specify the day and time the fault suppression task should start in the **Start Time** field. Click the down arrow at the end of this field to select the start time from a pop-up calendar.

  Specify the length of time this task should run in the **Task Duration** field. To specify that this task should run until it is manually stopped, enter `00:00:00:00` in this field.

- **Schedule**—Choose this option to configure the start time and duration using a pre-defined schedule.

  Choose the schedule from the **Schedule** drop-down list. To create a new schedule, click **Create Schedule**.

Policy drop-down list

The following suppression policy is selected by default:

- **default-server-maint**—Suppresses faults for servers.

---

**Deleting Fault Suppression Tasks for a Service Profile**

This procedure deletes all fault suppression tasks for a service profile. To delete individual tasks, use the **Delete** button on the **Suppression Tasks** dialog box. See **Viewing Fault Suppression Tasks for a Service Profile**, on page 42.

**Procedure**

1. **Step 1** In the **Navigation** pane, click **Servers**.
2. **Step 2** Expand **Servers > Service Profiles**.
3. **Step 3** Click the service profile for which you want to delete all fault suppression tasks.
4. **Step 4** In the **Work** pane, click the **General** tab.
5. **Step 5** In the **Actions** area, click **Stop Fault Suppression**.

   **Tip** To delete fault suppression tasks for multiple service profiles, use the `Ctrl` key to select multiple service profiles in the **Navigation** pane. Right-click one of the selected service profiles and choose **Stop Fault Suppression**.

6. **Step 6** If a confirmation dialog box displays, click **Yes**.
### Viewing Fault Suppression Tasks for a Service Profile

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the <strong>Navigation</strong> pane, click <strong>Servers</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Expand <strong>Servers &gt; Service Profiles</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Click the service profile for which you want to view fault suppression task properties.</td>
</tr>
<tr>
<td>4</td>
<td>In the <strong>Work</strong> pane, click the <strong>General</strong> tab.</td>
</tr>
<tr>
<td>5</td>
<td>In the <strong>Actions</strong> area, click <strong>Suppression Task Properties</strong>. In the <strong>Suppression Tasks</strong> dialog box, you can add new fault suppression tasks, delete existing fault suppression tasks, or modify existing fault suppression tasks.</td>
</tr>
</tbody>
</table>

---

### Configuring Fault Suppression for an Organization

**Configuring Fault Suppression Tasks for an Organization**

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the <strong>Navigation</strong> pane, click <strong>Servers</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Expand <strong>Servers &gt; Policies &gt; Organization_Name</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Click the organization for which you want to create a fault suppression task.</td>
</tr>
<tr>
<td>4</td>
<td>In the <strong>Work</strong> pane, click the <strong>General</strong> tab.</td>
</tr>
<tr>
<td>5</td>
<td>In the <strong>Actions</strong> area, click <strong>Start Fault Suppression</strong>.</td>
</tr>
<tr>
<td>6</td>
<td>In the <strong>Start Fault Suppression</strong> dialog box, complete the following fields:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>The name of the fault suppression task. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.</td>
</tr>
</tbody>
</table>
Specify when the fault suppression task will run. This can be one of the following:

- **Fixed Time Interval**—Choose this option to specify the start time and duration for the fault suppression task.
  
  Specify the day and time the fault suppression task should start in the **Start Time** field. Click the down arrow at the end of this field to select the start time from a pop-up calendar.
  
  Specify the length of time this task should run in the **Task Duration** field. To specify that this task should run until it is manually stopped, enter **00:00:00:00** in this field.
  
- **Schedule**—Choose this option to configure the start time and duration using a pre-defined schedule.
  
  Choose the schedule from the **Schedule** drop-down list. To create a new schedule, click **Create Schedule**.

**Policy** drop-down list

The following suppression policy is selected by default:

- **default-server-maint**—Suppresses faults for servers.

**Step 7**  
Click **OK**.

---

**Deleting Fault Suppression Tasks for an Organization**

This procedure deletes all fault suppression tasks for an organization. To delete individual tasks, use the **Delete** button on the **Suppression Tasks** dialog box. See **Viewing Fault Suppression Tasks for an Organization**, on page 43.

**Procedure**

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

**Step 2**  
Expand **Servers > Policies > Organization_Name**.

**Step 3**  
Click the organization for which you want to delete all fault suppression tasks.

**Step 4**  
In the **Work** pane, click the **General** tab.

**Step 5**  
In the **Actions** area, click **Stop Fault Suppression**.

**Step 6**  
If a confirmation dialog box displays, click **Yes**.

---

**Viewing Fault Suppression Tasks for an Organization**

**Procedure**

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

**Step 2**  
Expand **Servers > Policies > Organization_Name**.
Step 3  Click the organization for which you want to view fault suppression task properties.
Step 4  In the Work pane, click the General tab.
Step 5  In the Actions area, click Suppression Task Properties.  

In the Suppression Tasks dialog box, you can add new fault suppression tasks, delete existing fault suppression tasks, or modify existing fault suppression tasks.
SNMP Configuration

- SNMP Overview, on page 45
- Enabling SNMP and Configuring SNMP Properties, on page 48
- Creating an SNMP Trap, on page 49
- Deleting an SNMP Trap, on page 50
- Creating an SNMPv3 user, on page 50
- Deleting an SNMPv3 User, on page 51

SNMP Overview

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language for monitoring and managing devices in a network.

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, the managed device that maintains the data for Cisco UCS, and reports the data as needed to the SNMP manager. Cisco UCS 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 Manager.

- A managed information base (MIB)—The collection of managed objects on the SNMP agent. Cisco UCS release 1.4(1) and higher supports a larger number of MIBs than earlier releases.

Cisco UCS supports SNMPv1, SNMPv2c and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security. SNMP is defined in the following:

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 Manager generates SNMP notifications as either traps or informs. Traps are less reliable than informs because the SNMP manager does not send any acknowledgment when it receives a trap, and Cisco UCS Manager cannot determine if the trap was received. An SNMP manager that receives an inform request acknowledges the message with an SNMP response Protocol Data Unit (PDU). If the Cisco UCS Manager does not receive the PDU, it can send the inform request again.

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 requires protection from disclosure or whether the message is authenticated. The supported security level depends on 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.

Supported Combinations of SNMP Security Models and Levels

The following table identifies the combinations of security models and levels.
Table 1: SNMP Security Models and Levels

<table>
<thead>
<tr>
<th>Model</th>
<th>Level</th>
<th>Authentication</th>
<th>Encryption</th>
<th>What Happens</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1</td>
<td>noAuthNoPriv</td>
<td>Community string</td>
<td>No</td>
<td>Uses a community string match for authentication.</td>
</tr>
<tr>
<td>v2c</td>
<td>noAuthNoPriv</td>
<td>Community string</td>
<td>No</td>
<td>Uses a community string match for authentication.</td>
</tr>
<tr>
<td>v3</td>
<td>noAuthNoPriv</td>
<td>Username</td>
<td>No</td>
<td>Uses a username match for authentication.</td>
</tr>
<tr>
<td>v3</td>
<td>authNoPriv</td>
<td>HMAC-MD5 or HMAC-SHA</td>
<td>No</td>
<td>Provides authentication based on the Hash-Based Message Authentication Code</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(HMAC) Message Digest 5 (MD5) algorithm or the HMAC Secure Hash Algorithm (SHA).</td>
</tr>
<tr>
<td>v3</td>
<td>authPriv</td>
<td>HMAC-MD5 or HMAC-SHA</td>
<td>DES</td>
<td>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.</td>
</tr>
</tbody>
</table>

SNMPv3 Security Features

SNMPv3 provides secure access to devices through a combination of authenticating and encrypting frames over the network. SNMPv3 authorizes only configured users to perform management operations 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 are not altered or destroyed in an unauthorized manner, and that data sequences are not altered beyond what can occur non-maliciously.
- **Message origin authentication**—Ensures that the identity of a message originator is verifiable.
- **Message confidentiality and encryption**—Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

SNMP Support in Cisco UCS

Cisco UCS provides the following support for SNMP:

**Support for MIBs**

Cisco UCS supports read-only access to MIBs.


**Authentication Protocols for SNMPv3 Users**

Cisco UCS supports the following authentication protocols for SNMPv3 users:
- HMAC-MD5-96 (MD5)
- HMAC-SHA-96 (SHA)

**AES Privacy Protocol for SNMPv3 Users**

Cisco UCS uses Advanced Encryption Standard (AES) as one of the privacy protocols for SNMPv3 message encryption and conforms with RFC 3826.

The privacy password, or priv option, offers a choice of DES or 128-bit AES encryption for SNMP security encryption. If you enable AES-128 configuration and include a privacy password for an SNMPv3 user, Cisco UCS Manager 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.

To deploy such a user, enable **AES-128** encryption.

---

**Enabling SNMP and Configuring SNMP Properties**

SNMP messages from a Cisco UCS domain display the fabric interconnect name rather than the system name.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click Admin.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Expand All &gt; Communication Management &gt; Communication Services.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select the Communication Services tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the SNMP area, complete the following fields:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State field</td>
<td>This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Enabled</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
</tr>
<tr>
<td></td>
<td>Enable this service only if your system includes integration with an SNMP server.</td>
</tr>
<tr>
<td></td>
<td>If Admin State is enabled, Cisco UCS Manager GUI displays the remaining fields in this section.</td>
</tr>
</tbody>
</table>

| Step 5 | Click Save Changes. |

**What to do next**

Create SNMP traps and users.
Creating an SNMP Trap

Procedure

Step 1  In the Navigation pane, click Admin.
Step 2  Expand All > Communication Management > Communication Services.
Step 3  Select the Communication Services tab.
Step 4  In the SNMP Traps area, click +.
Step 5  In the Create SNMP Trap dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hostname (or IP Address) field</strong></td>
<td>The host name or IP address of the SNMP host to which Cisco UCS Manager should send the trap. You can use an IPv4 address, or an IPv6 address for the SNMP host. The host name can also be a fully qualified domain name of an IPv4 address.</td>
</tr>
<tr>
<td><strong>Community/Username field</strong></td>
<td>The SNMP v1 or v2c community name or the SNMP v3 username Cisco UCS Manager includes when it sends the trap to the SNMP host. This must be the same as the community or username that is configured for the SNMP service. Enter an alphanumeric string between 1 and 32 characters. Do not use @ (at sign), \ (backslash), &quot; (double quote), ? (question mark), &amp; (ampersand), or an empty space.</td>
</tr>
<tr>
<td><strong>Port field</strong></td>
<td>The port on which Cisco UCS Manager communicates with the SNMP host for the trap. Enter an integer between 1 and 65535. The default port is 162.</td>
</tr>
<tr>
<td><strong>Version field</strong></td>
<td>The SNMP version and model used for the trap. This can be one of the following: • V1 • V2c • V3</td>
</tr>
<tr>
<td><strong>Type field</strong></td>
<td>The type of trap to send. If you select V2c or V3 for the version, the type of trap to be sent can be one of the following: • Traps • Informs</td>
</tr>
</tbody>
</table>
### Deleting an SNMP Trap

**Procedure**

- **Step 1** In the Navigation pane, click Admin.
- **Step 2** Expand All > Communication Management > Communication Services.
- **Step 3** Select the Communication Services tab.
- **Step 4** In the SNMP Traps area, click the row in the table that corresponds to the user you want to delete.
- **Step 5** Click the Delete icon to the right of the table.
- **Step 6** If a confirmation dialog box displays, click Yes.
- **Step 7** Click Save Changes.

### Creating an SNMPv3 user

**Procedure**

- **Step 1** In the Navigation pane, click Admin.
- **Step 2** Expand All > Communication Management > Communication Services.
- **Step 3** Select the Communication Services tab.
- **Step 4** In the SNMP Users area, click +.
- **Step 5** In the Create SNMP User dialog box, complete the following fields:

---

**Table: v3 Privilege field**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>v3 Privilege field</td>
<td>If you select V3 for the version, the privilege associated with the trap. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Auth—Authentication but no encryption</td>
</tr>
<tr>
<td></td>
<td>• Noauth—No authentication or encryption</td>
</tr>
<tr>
<td></td>
<td>• Priv—Authentication and encryption</td>
</tr>
</tbody>
</table>
### SNMP Configuration

#### Name field
- **Description:** The username assigned to the SNMP user.
- **Note:** 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).

#### Auth Type field
- **Description:** The authorization type. This can be only be SHA.

#### Use AES-128 field
- **Description:** Whether the user uses AES-128 encryption.

#### Password field
- **Description:** The password for this user.

#### Confirm Password field
- **Description:** The password again for confirmation purposes.

#### Privacy Password field
- **Description:** The privacy password for this user.

#### Confirm Privacy Password field
- **Description:** The privacy password again for confirmation purposes.

---

### Deleting an SNMPv3 User

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

#### Step 7
Click **Save Changes**.

---

## Deleting an SNMPv3 User

### Procedure

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

#### Step 2
Expand **All > Communication Management > Communication Services**.

#### Step 3
Select the **Communication Services** tab.

#### Step 4
In the **SNMP Users** area, click the row in the table that corresponds to the user you want to delete.

#### Step 5
Click the **Delete** icon to the right of the table.

#### Step 6
If a confirmation dialog box displays, click **Yes**.

#### Step 7
Click **Save Changes**.
Deleting an SNMPv3 User
Statistics Collection Policy Configuration

- Configuring Statistics Collection Policies, on page 53
- Configuring Statistics Threshold Policies, on page 56

Configuring Statistics Collection Policies

Statistics Collection Policy

A statistics collection policy defines how frequently statistics are collected (collection interval) and how frequently the statistics are reported (reporting interval). Reporting intervals are longer than collection intervals so that multiple statistical data points can be collected during the reporting interval. This provides Cisco UCS Manager with sufficient data to calculate and report minimum, maximum, and average values.

For NIC statistics, Cisco UCS Manager displays the average, minimum, and maximum of the change since the last collection of statistics. If the values are 0, there has been no change since the last collection.

Statistics can be collected and reported for the following five functional areas of the Cisco UCS system:

- Adapter — Statistics related to the adapters
- Chassis — Statistics related to the chassis
- Host — This policy is a placeholder for future support
- Port — Statistics related to the ports, including server ports, uplink Ethernet ports, and uplink Fibre Channel ports
- Server — Statistics related to servers

Note

Cisco UCS Manager has one default statistics collection policy for each of the five functional areas. You cannot create additional statistics collection policies and you cannot delete the existing default policies. You can only modify the default policies.

The values that are displayed for delta counter in Cisco UCS Manager are calculated as the difference between the last two samples in a collection interval. In addition, Cisco UCS Manager displays the average, minimum, and maximum delta values of the samples in the collection interval.
Modifying a Statistics Collection Policy

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click Admin.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Expand All &gt; Stats Management &gt; Collection Policies.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the work pane, right-click the policy that you want to modify and select Modify Collection Policy.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Modify Collection Policy dialog box, complete the following fields:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>The name of the collection policy. This name is assigned by Cisco UCS and cannot be changed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Collection Interval field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection Interval field</td>
<td>The length of time the fabric interconnect should wait between data recordings. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• 30 Seconds</td>
</tr>
<tr>
<td></td>
<td>• 1 Minute</td>
</tr>
<tr>
<td></td>
<td>• 2 Minutes</td>
</tr>
<tr>
<td></td>
<td>• 5 Minutes</td>
</tr>
</tbody>
</table>
The length of time the fabric interconnect should wait before sending any data collected for the counter to Cisco UCS Manager. This can be one of the following:

- 2 Minutes
- 15 Minutes
- 30 Minutes
- 60 Minutes
- 2 Hours
- 4 Hours
- 8 Hours

When this time has elapsed, the fabric interconnect groups all data collected since the last time it sent information to Cisco UCS Manager, and it extracts four pieces of information from that group and sends them to Cisco UCS Manager:

- The most recent statistic collected
- The average of this group of statistics
- The maximum value within this group
- The minimum value within this group

For example, if the collection interval is set to 1 minute and the reporting interval is 15 minutes, the fabric interconnect collects 15 samples in that 15 minute reporting interval. Instead of sending 15 statistics to Cisco UCS Manager, it sends only the most recent recording along with the average, minimum, and maximum values for the entire group.

The task that is executing on behalf of this component. For details, see the associated FSM tab.

Note: If there is no current task, this field is not displayed.

**Step 5**

Click **OK**.
Configuring Statistics Threshold Policies

Statistics Threshold Policy

A statistics threshold policy monitors statistics about certain aspects of the system and generates an event if the threshold is crossed. You can set both minimum and maximum thresholds. For example, you can configure the policy to raise an alarm if the CPU temperature exceeds a certain value, or if a server is overutilized or underutilized.

These threshold policies do not control the hardware or device-level thresholds enforced by endpoints, such as the CIMC. Those thresholds are burned in to the hardware components at manufacture.

Cisco UCS enables you to configure statistics threshold policies for the following components:

• Servers and server components
• Uplink Ethernet ports
• Ethernet server ports, chassis, and fabric interconnects
• Fibre Channel port

Note

You cannot create or delete a statistics threshold policy for Ethernet server ports, uplink Ethernet ports, or uplink Fibre Channel ports. You can only configure the existing default policy.

Cisco UCS enables you to configure statistics threshold policies for servers and server components.

Creating a Server and Server Component Threshold Policy

Tip

This procedure documents how to create a server and server component threshold policy on the Server tab. You can also create and configure these threshold policies within the appropriate organization in the Policies node on the LAN tab, SAN tab, and under the Stats Management node of the Admin tab.

Procedure

Step 1  In the Navigation pane, click Servers.
Step 2  Expand Servers > Policies.
Step 3  Expand the node for the organization where you want to create the policy.
        If the system does not include multitenancy, expand the root node.
Step 4  Right-click Threshold Policies and choose Create Threshold Policy.
Step 5  In the Define Name and Description page of the Create Threshold Policy wizard, do the following:
        a) Complete the following fields:
### Name field
The name of the policy.

This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.

### Description field
A description of the policy. Cisco recommends including information about where and when to use the policy.

Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).

### Owner field
This can be one of the following:

- **Local**—This policy is available only to service profiles and service profile templates in this Cisco UCS domain.

- **Pending Global**—Control of this policy is being transferred to Cisco UCS Central. Once the transfer is complete, this policy will be available to all Cisco UCS domains registered with Cisco UCS Central.

- **Global**—This policy is managed by Cisco UCS Central. Any changes to this policy must be made through Cisco UCS Central.

---

**Step 6**

In the **Threshold Classes** page of the **Create Threshold Policy** wizard, do the following:

a) Click **Add**.

b) In the **Choose Statistics Class** dialog box, choose the statistics class for which you want to configure a custom threshold from the **Stat Class** drop-down list.

c) Click **Next**.

**Step 7**

In the **Threshold Definitions** page, do the following:

a) Click **Add**.

The **Create Threshold Definition** dialog box opens.

b) From the **Property Type** field, choose the threshold property that you want to define for the class.

c) In the **Normal Value** field, enter the desired value for the property type.

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

- **Critical**
- **Major**
- **Minor**
- **Warning**
- **Condition**
- **Info**
e) In the Up and Down fields, enter the range of values that should trigger the alarm.

f) In the Alarm Triggers (Below Normal Value) fields, check one or more of the following check boxes:
   - Info
   - Condition
   - Warning
   - Minor
   - Major
   - Critical

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

h) Click Finish Stage.

i) Do one of the following:
   - To define another threshold property for the class, repeat Step 7.
   - If you have defined all required properties for the class, click Finish Stage.

Step 8 In the Threshold Classes page of the Create Threshold Policy wizard, do one the following:
   - To configure another threshold class for the policy, repeat Steps 6 and 7.
   - If you have configured all required threshold classes for the policy, click Finish.

Step 9 Click OK.

Deleting a Server and Server Component Threshold Policy

Procedure

Step 1 In the Navigation pane, click Servers.
Step 2 Expand Servers > Policies > Organization_Name.
Step 3 Expand the Threshold Policies node.
Step 4 Right-click the policy you want to delete and select Delete.
Step 5 If a confirmation dialog box displays, click Yes.
Adding a Threshold Class to an Existing Server and Server Component Threshold Policy

Tip
This procedure documents how to add a threshold class to a server and server component threshold policy in the Server tab. You can also create and configure these threshold policies within the appropriate organization in the Policies node on the LAN tab, SAN tab, and under the Stats Management node of the Admin tab.

Procedure

Step 1 In the Navigation pane, click Servers.
Step 2 Expand Servers > Policies > Organization_Name.
Step 3 Expand the Threshold Policies node.
Step 4 Right-click the policy to which you want to add a threshold class and choose Create Threshold Class.
Step 5 In the Choose Statistics Class page of the Create Threshold Class wizard, do the following:
   a) From the Stat Class drop-down list, choose the statistics class for which you want to configure a custom threshold.
   b) Click Next.
Step 6 In the Threshold Definitions page, do the following:
   a) Click Add.

      The Create Threshold Definition dialog box opens.

   b) From the Property Type field, choose the threshold property that you want to define for the class.
   c) In the Normal Value field, enter the desired value for the property type.
   d) In the Alarm Triggers (Above Normal Value) field, check one or more of the following check boxes:
      • Critical
      • Major
      • Minor
      • Warning
      • Condition
      • Info

   e) In the Up and Down fields, enter the range of values that should trigger the alarm.
   f) In the Alarm Triggers (Below Normal Value) field, check one or more of the following check boxes:
      • Info
      • Condition
      • Warning
      • Minor
• Major
• Critical

g) In the Up and Down fields, enter the range of values that should trigger the alarm.
h) Click Finish Stage.
i) Do one of the following:
   • To define another threshold property for the class, repeat Step 6.
   • If you have defined all required properties for the class, click Finish Stage.

**Step 7**
In the Choose Statistics Class page of the Create Threshold Class wizard, do one the following:
   • To configure another threshold class for the policy, repeat Steps 5 and 6.
   • If you have configured all required threshold classes for the policy, click Finish.

**Step 8**
Click OK.

---

### Adding a Threshold Class to the Uplink Ethernet Port Threshold Policy

**Tip**
You cannot create an uplink Ethernet port threshold policy. You can only modify or delete the default policy.

**Procedure**

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

**Step 2**
Expand LAN > LAN Cloud.

**Step 3**
Expand the Threshold Policies node.

**Step 4**
Right-click Thr-policy-default and choose the Create Threshold Class.

**Step 5**
In the Choose Statistics Class page of the Create Threshold Class wizard, do the following:
   a) From the Stat Class drop-down list, choose the statistics class for which you want to configure a custom threshold.
   b) Click Next.

**Step 6**
In the Threshold Definitions page, do the following:
   a) Click Add.
      The Create Threshold Definition dialog box opens.
   b) From the Property Type field, choose the threshold property that you want to define for the class.
   c) In the Normal Value field, enter the desired value for the property type.
   d) In the Alarm Triggers (Above Normal Value) field, check one or more of the following check boxes:
      • Critical
      • Major
Step 7 In the Create Threshold Class page of the Create Threshold Policy wizard, do one of the following:
   • To configure another threshold class for the policy, repeat Steps 5 and 6.
   • If you have configured all required threshold classes for the policy, click Finish.

Adding a Threshold Class to the Ethernet Server Port, Chassis, and Fabric Interconnect Threshold Policy

You cannot create an ethernet server port, chassis, and fabric interconnect threshold policy. You can only modify or delete the default policy.

Procedure

Step 1 In the Navigation pane, click LAN.
Step 2 Expand LAN > Internal LAN.
Step 3 Expand the Threshold Policies node.
Step 4  Right-click Thr-policy-default and choose the Create Threshold Class.

Step 5  In the Choose Statistics Class page of the Create Threshold Class wizard, do the following:
   a) From the Stat Class drop-down list, choose the statistics class for which you want to configure a custom threshold.
   b) Click Next.

Step 6  In the Threshold Definitions page, do the following:
   a) Click Add.
      The Create Threshold Definition dialog box opens.
   b) From the Property Type field, choose the threshold property that you want to define for the class.
   c) In the Normal Value field, enter the desired value for the property type.
   d) In the Alarm Triggers (Above Normal Value) field, check one or more of the following check boxes:
      • Critical
      • Major
      • Minor
      • Warning
      • Condition
      • Info
   e) In the Up and Down fields, enter the range of values that should trigger the alarm.
   f) In the Alarm Triggers (Below Normal Value) field, check one or more of the following check boxes:
      • Info
      • Condition
      • Warning
      • Minor
      • Major
      • Critical
   g) In the Up and Down fields, enter the range of values that should trigger the alarm.
   h) Click Finish Stage.
   i) Do one of the following:
      • To define another threshold property for the class, repeat Step 6.
      • If you have defined all required properties for the class, click Finish Stage.

Step 7  In the Create Threshold Class page of the Create Threshold Policy wizard, do one the following:
   • To configure another threshold class for the policy, repeat Steps 5 and 6.
   • If you have configured all required threshold classes for the policy, click Finish.
Adding a Threshold Class to the Fibre Channel Port Threshold Policy

You cannot create a Fibre Channel port threshold policy. You can only modify or delete the default policy.

Procedure

Step 1  In the Navigation pane, click SAN.
Step 2  Expand SAN > SAN Cloud.
Step 3  Expand the Threshold Policies node.
Step 4  Right-click Thr-policy-default and choose the Create Threshold Class.
Step 5  In the Choose Statistics Class page of the Create Threshold Class wizard, do the following:
   a) From the Stat Class drop-down list, choose the statistics class for which you want to configure a custom threshold.
   b) Click Next.
Step 6  In the Threshold Definitions page, do the following:
   a) Click Add.
      The Create Threshold Definition dialog box opens.
   b) From the Property Type field, choose the threshold property that you want to define for the class.
   c) In the Normal Value field, enter the desired value for the property type.
   d) In the Alarm Triggers (Above Normal Value) field, check one or more of the following check boxes:
      • Critical
      • Major
      • Minor
      • Warning
      • Condition
      • Info
   e) In the Up and Down fields, enter the range of values that should trigger the alarm.
   f) In the Alarm Triggers (Below Normal Value) field, check one or more of the following check boxes:
      • Info
      • Condition
      • Warning
      • Minor
      • Major
      • Critical
   g) In the Up and Down fields, enter the range of values that should trigger the alarm.
   h) Click Finish Stage.
i) Do one of the following:
   • To define another threshold property for the class, repeat Step 6.
   • If you have defined all required properties for the class, click Finish Stage.

**Step 7**

In the Create Threshold Class page of the Create Threshold Policy wizard, do one the following:
   • To configure another threshold class for the policy, repeat Steps 5 and 6.
   • If you have configured all required threshold classes for the policy, click Finish.
 CHAPTER 10

Call Home and Smart Call Home Configuration

Call Home in UCS Overview

Call Home provides an email-based notification for critical system policies. A range of message formats are available for compatibility with pager services or XML-based automated parsing applications. You can use this feature to page a network support engineer, email a Network Operations Center, or use Cisco Smart Call Home services to generate a case with the Technical Assistance Center.

The Call Home feature can deliver alert messages containing information about diagnostics and environmental faults and events.

The Call Home feature can deliver alerts to multiple recipients, referred to as Call Home destination profiles. Each profile includes configurable message formats and content categories. A predefined destination profile is provided for sending alerts to the Cisco TAC, but you also can define your own destination profiles.

When you configure Call Home to send messages, Cisco UCS Manager executes the appropriate CLI `show` command and attaches the command output to the message.

Cisco UCS delivers Call Home messages in the following formats:

- Short text format which provides a one or two line description of the fault that is suitable for pagers or printed reports.

- Full text format which provides fully formatted message with detailed information that is suitable for human reading.

- XML machine-readable format that uses Extensible Markup Language (XML) and Adaptive Messaging Language (AML) XML Schema Definition (XSD). The AML XSD is published on the Cisco.com website. The XML format enables communication with the Cisco Systems Technical Assistance Center.

For information about the faults that can trigger Call Home email alerts, see the Cisco UCS Faults and Error Messages Reference.

The following figure shows the flow of events after a Cisco UCS fault is triggered in a system with Call Home configured:
Call Home Considerations and Guidelines

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

Destination Profile

You must configure at least one destination profile. The destination profile or profiles that you use depends upon whether the receiving entity is a pager, email, or automated service such as Cisco Smart Call Home.
If the destination profile uses email message delivery, you must specify a Simple Mail Transfer Protocol (SMTP) server when you configure Call Home.

Contact Information

The contact email, phone, and street address information should be configured so that the receiver can determine the origin of messages received from the Cisco UCS domain.
Cisco Smart Call Home sends the registration email to this email address after you send a system inventory to begin the registration process.

If an email address includes special characters, such as # (hash), spaces, or & (ampersand), the email server might not be able to deliver email messages to that address. Cisco recommends that you use email addresses which comply with RFC2821 and RFC2822 and include only 7bit ASCII characters.

**IP Connectivity to Email Server or HTTP Server**

The fabric interconnect must have IP connectivity to an email server or the destination HTTP server. In a cluster configuration, both fabric interconnects must have IP connectivity. This connectivity ensures that the current, active fabric interconnect can send Call Home email messages. The source of these email messages is always the IP address of a fabric interconnect. The virtual IP address assigned to Cisco UCS Manager in a cluster configuration is never the source of the email.

---

**Note**

Ensure that you add each fabric interconnect IP in the SMTP server. Call Home email messages cannot be delivered if the fabric interconnect IPs are not configured in the SMTP server.

**Smart Call Home**

If Cisco Smart Call Home is used, the following are required:

- An active service contract must cover the device being configured.
- The customer ID associated with the Smart Call Home configuration in Cisco UCS must be the CCO (Cisco.com) account name associated with a support contract that includes Smart Call Home.

---

**Cisco UCS Faults and Call Home Severity Levels**

Because Call Home is present across several Cisco product lines, Call Home has its own standardized severity levels. The following table describes how the underlying Cisco UCS fault levels map to the Call Home severity levels. You need to understand this mapping when you configure the Level setting for Call Home profiles.

*Table 2: Mapping of Faults and Call Home Severity Levels*

<table>
<thead>
<tr>
<th>Call Home Severity</th>
<th>Cisco UCS Fault</th>
<th>Call Home Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>(9) Catastrophic</td>
<td>N/A</td>
<td>Network-wide catastrophic failure.</td>
</tr>
<tr>
<td>(8) Disaster</td>
<td>N/A</td>
<td>Significant network impact.</td>
</tr>
<tr>
<td>(7) Fatal</td>
<td>N/A</td>
<td>System is unusable.</td>
</tr>
<tr>
<td>(6) Critical</td>
<td>Critical</td>
<td>Critical conditions, immediate attention needed.</td>
</tr>
<tr>
<td>(5) Major</td>
<td>Major</td>
<td>Major conditions.</td>
</tr>
<tr>
<td>(4) Minor</td>
<td>Minor</td>
<td>Minor conditions.</td>
</tr>
<tr>
<td>(3) Warning</td>
<td>Warning</td>
<td>Warning conditions.</td>
</tr>
</tbody>
</table>
### Anonymous Reporting

After you upgrade to the latest release of Cisco UCS Manager, by default, you are prompted with a dialog box to enable anonymous reporting.

To enable anonymous reporting, you need to enter details about the SMTP server and the data file that is stored on the fabric switch. This report is generated every seven days and is compared with the previous version of the same report. When Cisco UCS Manager identifies changes in the report, the report is sent as an e-mail.

### Enabling Anonymous Reporting

**Note**

Anonymous reporting can be enabled even when Call Home is disabled.

**Procedure**

**Step 1**

In the **Navigation** pane, click **Admin**.

**Step 2**

Expand **All > Communication Management > Call Home**.

**Step 3**

In the **Work** pane, click the **Anonymous Reporting** tab.

**Step 4**

In the **Actions** area, click **Anonymous Reporting Data** to view the sample or existing report.

**Step 5**

In the **Properties** pane, click one of the following radio buttons in the **Anonymous Reporting** field:

- **On**—Enables the server to send anonymous reports.
- **Off**—Disables the server to send anonymous reports.

**Step 6**

In the **SMTP Server** area, complete the following fields with the information about the SMTP server where anonymous reporting should send email messages:

- **Host (IP Address or Hostname)**—The IPv4 or IPv6 address, or the hostname of the SMTP server.
- **Port**—The port number that the system should use to talk to the SMTP server.

Enter an integer between 1 and 65535. The default is 25.

**Step 7**

Click **Save Changes**.

---

<table>
<thead>
<tr>
<th>Call Home Severity</th>
<th>Cisco UCS Fault</th>
<th>Call Home Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2) Notification</td>
<td>Info</td>
<td>Basic notifications and informational messages. Possibly independently insignificant.</td>
</tr>
<tr>
<td>(1) Normal</td>
<td>Clear</td>
<td>Normal event, signifying a return to normal state.</td>
</tr>
<tr>
<td>(0) debug</td>
<td>N/A</td>
<td>Debugging messages.</td>
</tr>
</tbody>
</table>
Configuring Call Home

Procedure

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

**Step 2**  
Expand **All > Communication Management > Call Home**.

**Step 3**  
In the **Work** pane, click the **General** tab.

**Step 4**  
In the **Admin** area, complete the following fields to enable Call Home:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State field</td>
<td>This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Off—Call Home is not used for this Cisco UCS domain.</td>
</tr>
<tr>
<td></td>
<td>• On—Cisco UCS generates Call Home alerts based on the Call Home policies and profiles defined in the system.</td>
</tr>
<tr>
<td>Note</td>
<td>If this field is set to <strong>On</strong>, Cisco UCS Manager GUI displays the rest of the fields on this tab.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch Priority</td>
<td>This can be one of the following:</td>
</tr>
<tr>
<td>drop-down list</td>
<td>• Alerts</td>
</tr>
<tr>
<td></td>
<td>• Critical</td>
</tr>
<tr>
<td></td>
<td>• Debugging</td>
</tr>
<tr>
<td></td>
<td>• Emergencies</td>
</tr>
<tr>
<td></td>
<td>• Errors</td>
</tr>
<tr>
<td></td>
<td>• Information</td>
</tr>
<tr>
<td></td>
<td>• Notifications</td>
</tr>
<tr>
<td></td>
<td>• Warnings</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throttling field</td>
<td>Indicates whether the system limits the number of duplicate messages received for the same event. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• On—If the number of duplicate messages sent exceeds 30 messages within a 2-hour timeframe, then the system discards further messages for that alert type.</td>
</tr>
<tr>
<td></td>
<td>• Off—The system sends all duplicate messages, regardless of how many are encountered.</td>
</tr>
</tbody>
</table>

a) In the **State** field, click **On**.  
**Note**  
If this field is set to **On**, Cisco UCS Manager GUI displays the rest of the fields on this tab.

b) From the **Switch Priority** drop-down list, select one of the following levels:
* Alerts
* Critical
* Debugging
* Emergencies
* Errors
* Information
* Notifications
* Warnings

For a large Cisco UCS deployment with several pairs of fabric interconnects, this field enables you to attach significance to messages from one particular Cisco UCS domain, so that message recipients can gauge the priority of the message. This field may not be as useful for a small Cisco UCS deployment, such as a single Cisco UCS domain.

### Step 5
In the **Contact Information** area, complete the following fields with the required contact information:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contact field</strong></td>
<td>The main Call Home contact person.</td>
</tr>
<tr>
<td></td>
<td>Enter up to 255 ASCII characters.</td>
</tr>
<tr>
<td><strong>Phone field</strong></td>
<td>The telephone number for the main contact.</td>
</tr>
<tr>
<td></td>
<td>Enter the number in international format, starting with a + (plus sign) and a country code. You can use hyphens but not parentheses.</td>
</tr>
<tr>
<td><strong>Email field</strong></td>
<td>The email address for the main contact.</td>
</tr>
<tr>
<td></td>
<td>Cisco Smart Call Home sends the registration email to this email address.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If an email address includes special characters, such as # (hash), spaces, or &amp; (ampersand), the email server might not be able to deliver email messages to that address. Cisco recommends that you use email addresses which comply with RFC2821 and RFC2822 and include only 7bit ASCII characters.</td>
</tr>
<tr>
<td><strong>Address field</strong></td>
<td>The mailing address for the main contact.</td>
</tr>
<tr>
<td></td>
<td>Enter up to 255 ASCII characters.</td>
</tr>
</tbody>
</table>

### Step 6
In the **Ids** area, complete the following fields with the identification information that Call Home should use:

**Tip** If you are not configuring Smart Call Home, this step is optional.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Id field</td>
<td>The Cisco.com ID that includes the contract numbers for the support contract in its entitlements. Enter up to 510 ASCII characters.</td>
</tr>
<tr>
<td>Contract Id field</td>
<td>The Call Home contract number for the customer. Enter up to 510 ASCII characters.</td>
</tr>
<tr>
<td>Site Id field</td>
<td>The unique Call Home identification number for the customer site. Enter up to 510 ASCII characters.</td>
</tr>
</tbody>
</table>

**Step 7**

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

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

**Step 8**

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host (IP Address or Hostname)</td>
<td>The IPv4 or IPv6 address, or the hostname of the SMTP server. If you use a hostname rather than an IPv4 or IPv6 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.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number the system should use to talk to the SMTP server. Enter an integer between 1 and 65535. The default is 25.</td>
</tr>
</tbody>
</table>

**Step 9**

Click **Save Changes**.

---

**Disabling Call Home**

This step is optional.

When you upgrade a Cisco UCS domain, Cisco UCS Manager restarts the components to complete the upgrade process. This restart causes events that are identical to service disruptions and component failures that trigger...
Enabling Call Home

Call Home alerts to be sent. If you do not disable Call Home before you begin the upgrade, you can ignore the alerts generated by the upgrade-related component restarts.

**Procedure**

**Step 1** In the Navigation pane, click Admin.
**Step 2** Expand All > Communication Management > Call Home.
**Step 3** In the Work pane, click the General tab.
**Step 4** In the Admin area, click Off in the State field.

**Note** If this field is set to Off, Cisco UCS Manager hides the rest of the fields on this tab.

**Step 5** Click Save Changes.

---

Enabling Call Home

This step is optional. You only need to enable Call Home if you disabled it before you began the firmware upgrades.

**Procedure**

**Step 1** In the Navigation pane, click Admin.
**Step 2** Expand All > Communication Management > Call Home.
**Step 3** In the Work pane, click the General tab.
**Step 4** In the Admin area, click On in the State field.

**Note** If this field is set to On, Cisco UCS Manager GUI displays the rest of the fields on this tab.

**Step 5** Click Save Changes.

---

**What to do next**

Ensure that Call Home is fully configured.

---

Configuring System Inventory Messages

**Procedure**

**Step 1** In the Navigation pane, click Admin.
**Step 2** Expand All > Communication Management > Call Home.
**Step 3** In the Work pane, click the System Inventory tab.
**Step 4** In the Properties area, complete the following fields:
**Sending a System Inventory Message**

Use this procedure if you need to manually send a system inventory message outside of the scheduled messages.

**Note**
The system inventory message is sent only to those recipients defined in CiscoTAC-1 profile.

**Procedure**

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

**Step 2** Expand All > Communication Management > Call Home.

**Step 3** In the Work pane, click the System Inventory tab.

**Step 4** In the Actions area, click Send System Inventory Now.

Cisco UCS Manager immediately sends a system inventory message to the recipient configured for Call Home.

**Configuring Call Home Profiles**

**Call Home Profiles**

Call Home profiles determine which alerts are sent to designated recipients. You can configure the profiles to send email alerts for events and faults at a desired severity level and for specific alert groups that represent...
categories of alerts. You can also use these profiles to specify the format of the alert for a specific set of recipients and alert groups.

Alert groups and Call Home profiles enable you to filter the alerts and ensure that a specific profile only receives certain categories of alerts. For example, a data center may have a hardware team that handles issues with fans and power supplies. This hardware team does not care about server POST failures or licensing issues. To ensure that the hardware team only receives relevant alerts, create a Call Home profile for the hardware team and check only the "environmental" alert group.

By default, you must configure the Cisco TAC-1 profile. You can also create additional profiles to send email alerts to one or more alert groups, when events occur at the level that you specify and provide the recipients with the appropriate amount of information about those alerts.

For example, you may want to configure two profiles for faults with a major severity:

- A profile that sends an alert to the Supervisor alert group in the short text format. Members of this group receive a one- or two-line description of the fault that they can use to track the issue.

- A profile that sends an alert to the CiscoTAC alert group in the XML format. Members of this group receive a detailed message in the machine-readable format preferred by the Cisco Systems Technical Assistance Center.

### Call Home Alert Groups

An alert group is a predefined subset of Call Home alerts. Alert groups allow you to select the set of Call Home alerts that you want to send to a predefined or custom Call Home profile. Cisco UCS Manager sends Call Home alerts to e-mail destinations in a destination profile only under the following conditions:

- If the Call Home alert belongs to one of the alert groups associated with that destination profile.
- If the alert has a Call Home message severity at or above the message severity set in the destination profile.

Each alert that Cisco UCS Manager generates fits into a category represented by an alert group. The following table describes those alert groups:

<table>
<thead>
<tr>
<th>Alert Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco TAC</td>
<td>All critical alerts from the other alert groups destined for Smart Call Home.</td>
</tr>
<tr>
<td>Diagnostic</td>
<td>Events generated by diagnostics, such as the POST completion on a server.</td>
</tr>
<tr>
<td>Environmental</td>
<td>Events related to power, fan, and environment-sensing elements such as temperature alarms.</td>
</tr>
</tbody>
</table>

**Note**: A Call Home alert is not generated when fans or PSUs are manually removed from the chassis. This is by design.

### Creating a Call Home Profile

By default, you must configure the Cisco TAC-1 profile. However, you can also create additional profiles to send email alerts to one or more specified groups when events occur at the level that you specify.
**Procedure**

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

**Step 2**  Expand **All > Communication Management > Call Home**.

**Step 3**  In the **Work** pane, click the **Profiles** tab.

**Step 4**  On the icon bar to the right of the table, click +.

If the + icon is disabled, click an entry in the table to enable it.

**Step 5**  In the **Create Call Home Profile** dialog box, complete the following information fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>A user-defined name for this profile. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.</td>
</tr>
<tr>
<td>Level field</td>
<td>Cisco UCS faults that are greater than or equal to this level trigger the profile. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>- Critical</td>
</tr>
<tr>
<td></td>
<td>- Debug</td>
</tr>
<tr>
<td></td>
<td>- Disaster</td>
</tr>
<tr>
<td></td>
<td>- Fatal</td>
</tr>
<tr>
<td></td>
<td>- Major</td>
</tr>
<tr>
<td></td>
<td>- Minor</td>
</tr>
<tr>
<td></td>
<td>- Normal</td>
</tr>
<tr>
<td></td>
<td>- Notification</td>
</tr>
<tr>
<td></td>
<td>- Warning</td>
</tr>
<tr>
<td>Alert Groups field</td>
<td>The group or groups that are alerted based on this Call Home profile. This can be one or more of the following:</td>
</tr>
<tr>
<td></td>
<td>- Cisco Tac—Cisco TAC recipients</td>
</tr>
<tr>
<td></td>
<td>- Diagnostic—POST completion server failure notification recipients</td>
</tr>
<tr>
<td></td>
<td>- Environmental—Recipients of notifications about problems with PSUs, fans, etc.</td>
</tr>
</tbody>
</table>

**Step 6**  In the **Email Configuration** area, complete the following fields to configure the email alerts:
Deleting a Call Home Profile

### Format field
This can be one of the following:
- **Xml**—A machine readable format that uses Extensible Markup Language (XML) and Adaptive Messaging Language (AML) XML schema definition (XSD). This format enables communication with the Cisco Systems Technical Assistance Center.
- **Full Txt**—A fully formatted message with detailed information that is suitable for human reading.
- **Short Txt**—A one or two line description of the fault that is suitable for pagers or printed reports.

### Max Message Size field
The maximum message size that is sent to the designated Call Home recipients.
- Enter an integer between 1 and 5000000. The default is 5000000.
- For full text and XML messages, the maximum recommended size is 5000000. For short text messages, the maximum recommended size is 1000000. For the Cisco TAC alert group, the maximum message size must be 5000000.

### Step 7
In the **Recipients** area, do the following to add one or more email recipients for the email alerts:

a) On the icon bar to the right of the table, click +.
b) In the **Add Email Recipients** dialog box, enter the email address to which Call Home alerts should be sent in the **Email** field.

   This email address receives Callhome Alerts/Faults.

   After you save this email address, it can be deleted but it cannot be changed.

c) Click **OK**.

### Step 8
Click **OK**.

---

Deleting a Call Home Profile

### Procedure

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

**Step 2**
Expand **All > Communication Management > Call Home**.

**Step 3**
In the **Work** pane, click the **Profiles** tab.

**Step 4**
Right-click the profile you want to delete and choose **Delete**.

**Step 5**
Click **Save Changes**.
Configuring Call Home Policies

Call Home Policies

Call Home policies determine whether or not Call Home alerts are sent for a specific type of fault or system event. By default, Call Home is enabled to send alerts for certain types of faults and system events.

Note

You can configure Cisco UCS Manager not to process the default faults and system events.

To disable alerts for a type of fault or event, you must first create a Call Home policy for that type and then disable the policy.

Configuring a Call Home Policy

Tip

By default, all Call Home policies are enabled to ensure that email alerts are sent for all critical system events.

Procedure

Step 1
In the Navigation pane, click Admin.

Step 2
Expand All > Communication Management > Call Home.

Step 3
In the Work pane, click the Call Home Policies tab.

Step 4
On the icon bar to the right of the table, click +.

If the + icon is disabled, click an entry in the table to enable it.

Step 5
In the Create Call Home Policy dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State field</td>
<td>If this field is <strong>Enabled</strong>, the system uses this policy when an error matching the associated cause is encountered. Otherwise, the system ignores this policy even if a matching error occurs. By default, all policies are enabled.</td>
</tr>
<tr>
<td>Cause field</td>
<td>The event that triggers the alert. Each policy defines whether an alert is sent for one type of event.</td>
</tr>
</tbody>
</table>

Step 6
Click OK.

Step 7
Repeat Steps 4 and 5 if you want to configure a Call Home policy for a different type of fault or event.
Disabling a Call Home Policy

**Procedure**

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

**Step 2** Expand All > Communication Management > Call Home.

**Step 3** In the Work pane, click the Call Home Policies tab.

**Step 4** Click the policy that you want to disable and choose Show Navigator.

**Step 5** In the State field, click Disabled.

**Step 6** Click OK.

Enabling a Call Home Policy

**Procedure**

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

**Step 2** Expand All > Communication Management > Call Home.

**Step 3** In the Work pane, click the Call Home Policies tab.

**Step 4** Click the policy that you want to enable and choose Show Navigator.

**Step 5** In the State field, click Enabled.

**Step 6** Click OK.

Deleting a Call Home Policy

**Procedure**

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

**Step 2** Expand All > Communication Management > Call Home.

**Step 3** In the Work pane, click the Call Home Policies tab.

**Step 4** Right-click the policy that you want to disable and choose Delete.

**Step 5** Click Save Changes.

Cisco Smart Call Home

Cisco Smart Call Home is a web application which leverages the Call Home feature of Cisco UCS. Smart Call Home offers proactive diagnostics and real-time email alerts of critical system events, which results in higher network availability and increased operational efficiency. Smart Call Home is a secure connected service offered by Cisco Unified Computing Support Service and Cisco Unified Computing Mission Critical Support Service for Cisco UCS.
Using Smart Call Home requires the following:


- Cisco Unified Computing Support Service or Cisco Unified Computing Mission Critical Support Service for the device to be registered.

You can configure and register Cisco UCS Manager to send Smart Call Home email alerts to either the Smart Call Home System or the secure Transport Gateway. Email alerts sent to the secure Transport Gateway are forwarded to the Smart Call Home System using HTTPS.

For security reasons, we recommend using the Transport Gateway option. The Transport Gateway can be downloaded from Cisco.com.

To configure Smart Call Home, do the following:

- Enable the Smart Call Home feature.

- Configure the contact information.

- Configure the email information.
• Configure the SMTP server information.
• Configure the default CiscoTAC-1 profile.
• Send a Smart Call Home inventory message to start the registration process.
• Ensure that the Cisco.com ID you plan to use as the Call Home Customer ID for the Cisco UCS domain has the contract numbers from the registration added to its entitlements. You can update the ID in the Account Properties under Additional Access in the Profile Manager on Cisco.com.

Configuring Smart Call Home

Procedure

Step 1
In the Navigation pane, click Admin.

Step 2
Expand All > Communication Management > Call Home.

Step 3
In the Work pane, click the General tab.

Step 4
In the Admin area, do the following to enable Call Home:

   a) In the State field, click On.

   Note If this field is set to On, Cisco UCS Manager GUI displays the rest of the fields on this tab.

   b) From the Switch Priority drop-down list, select one of the following urgency levels:

       • Alerts
       • Critical
       • Debugging
       • Emergencies
       • Errors
       • Information
       • Notifications
       • Warnings

Step 5
In the Contact Information area, complete the following fields with the required contact information:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contact</strong>  field</td>
<td>The main Call Home contact person. Enter up to 255 ASCII characters.</td>
</tr>
<tr>
<td><strong>Phone</strong> field</td>
<td>The telephone number for the main contact. Enter the number in international format, starting with a + (plus sign) and a country code. You can use hyphens but not parentheses.</td>
</tr>
</tbody>
</table>
### Step 6
In the **Ids** area, complete the following fields with the Smart Call Home identification information:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Customer Id</strong></td>
<td>The Cisco.com ID that includes the contract numbers for the support contract in its entitlements. Enter up to 510 ASCII characters.</td>
</tr>
<tr>
<td><strong>Contract Id</strong></td>
<td>The Call Home contract number for the customer. Enter up to 510 ASCII characters.</td>
</tr>
<tr>
<td><strong>Site Id</strong></td>
<td>The unique Call Home identification number for the customer site. Enter up to 510 ASCII characters.</td>
</tr>
</tbody>
</table>

### Step 7
In the **Email Addresses** area, complete the following fields with the email information for Smart Call Home alert messages:

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

### Step 8
In the **SMTP Server** area, complete the following fields with information about the SMTP server that Call Home should use to send email messages:
The IPv4 or IPv6 address, or the hostname of the SMTP server. If you use a hostname rather than an IPv4 or IPv6 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host (IP Address or Hostname) field</td>
<td>The IPv4 or IPv6 address, or the hostname of the SMTP server.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you use a hostname rather than an IPv4 or IPv6 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.</td>
</tr>
<tr>
<td>Port field</td>
<td>The port number the system should use to talk to the SMTP server. Enter an integer between 1 and 65535. The default is 25.</td>
</tr>
</tbody>
</table>

**Step 9** Click **Save Changes**.

---

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

The following are the default settings for the CiscoTAC-1 profile:

- Level is normal
- Only the CiscoTAC alert group is selected
- Format is xml
- Maximum message size is 5000000

**Procedure**

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

**Step 2** Expand **All > Communication Management > Call Home**.

**Step 3** In the **Work** pane, click the **Profiles** tab.

**Step 4** Right-click the Cisco TAC-1 profile and choose **Recipient**.

**Step 5** In the **Add Email Recipients** dialog box, do the following:

- a) In the **Email** field, enter the email address to which Call Home alerts should be sent.

  For example, enter callhome@cisco.com.

  After you save this email address, it can be deleted but it cannot be changed.

- b) Click **OK**.
Configuring System Inventory Messages for Smart Call Home

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click Admin.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Expand All &gt; Communication Management &gt; Call Home.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Work pane, click the System Inventory tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Properties area, complete the following fields to specify how system inventory messages will be sent to Smart Call Home:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Periodically</td>
<td>If this field is set to On, Cisco UCS sends the system inventory to the Call Home database. When the information is sent depends on the other fields in this area.</td>
</tr>
<tr>
<td>Send Interval</td>
<td>The number of days that should pass between automatic system inventory data collection. Enter an integer between 1 and 30.</td>
</tr>
<tr>
<td>Hour of Day to Send</td>
<td>The hour that the data should be sent using the 24-hour clock format.</td>
</tr>
<tr>
<td>Minute of Hour</td>
<td>The number of minutes after the hour that the data should be sent.</td>
</tr>
<tr>
<td>Time Last Sent</td>
<td>The date and time the information was last sent. Note: This field is displayed after the first inventory has been sent.</td>
</tr>
<tr>
<td>Next Scheduled</td>
<td>The date and time for the upcoming data collection. Note: This field is displayed after the first inventory has been sent.</td>
</tr>
</tbody>
</table>

| Step 5 | Click Save Changes. |

Registering Smart Call Home

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click Admin.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Expand All &gt; Communication Management &gt; Call Home.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Work pane, click the System Inventory tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Actions area, click Send System Inventory Now to start the registration process.</td>
</tr>
</tbody>
</table>

When Cisco receives the system inventory, a Smart Call Home registration email is sent to the email address that you configured in the Contact Information area on the General tab.
Step 5  When you receive the registration email from Cisco, do the following to complete registration for Smart Call Home:

a) Click the link in the email.
   The link opens the Cisco Smart Call Home portal in your web browser.

b) Log into the Cisco Smart Call Home portal.

c) Follow the steps provided by Cisco Smart Call Home.

   After you agree to the terms and conditions, the Cisco Smart Call Home registration for the Cisco UCS domain is complete.
Database Health Monitoring

- Cisco UCS Manager Database Health Monitoring, on page 85
- Changing Internal Backup Interval, on page 85
- Triggering Health Check, on page 86
- Changing Health Check Interval, on page 86

Cisco UCS Manager Database Health Monitoring

Cisco UCS Manager uses a SQLite database stored on the Fabric Interconnects to persist configuration and inventory. Data corruption on both the Flash and NVRAM storage devices can cause failures and loss of customer configuration data. Cisco UCS Manager provides several proactive health check and recovery mechanisms to improve the integrity of the Cisco UCS Manager database. These mechanisms enable active monitoring of the database health.

- **Periodic Health Check**—A periodic check of database integrity ensures that any corruption is caught and recovered proactively. See Triggering Health Check, on page 86, and Changing Health Check Interval, on page 86.

- **Periodic Backup**—A periodic internal full state backup of the system ensures a smoother route to recovery in the case of any unrecoverable errors. See Changing Internal Backup Interval, on page 85.

Changing Internal Backup Interval

You can change the interval at which the internal backup is done. To disable the backup the value can be set to 0.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> UCS-A# scope system</td>
<td>Enters the system.</td>
</tr>
<tr>
<td><strong>Step 2</strong> UCS-A /system# set mgmt-db-check-policy internal-backup-interval days</td>
<td>Specifies the time interval (in days) at which the integrity backup is done.</td>
</tr>
<tr>
<td><strong>Step 3</strong> UCS-A /system# commit-buffer</td>
<td>Commits the transaction.</td>
</tr>
</tbody>
</table>
Example

This example changes the time interval at which the check runs to two days, and commits the transaction.

```
UCS-A# scope system
UCS-A /system # set mgmt-db-check-policy health-check-interval 2
UCS-A /system* # commit-buffer
```

Triggering Health Check

Use the following commands to trigger an immediate full database integrity check.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>UCS-A# scope system</td>
<td>Enters the system.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>UCS-A /system # start-db-check</td>
<td>Triggers health check.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>UCS-A /system # commit-buffer</td>
<td>Commits the transaction.</td>
</tr>
</tbody>
</table>

Changing Health Check Interval

You can change the interval at which the integrity check runs. To disable the periodic check entirely set the value for to 0.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>UCS-A# scope system</td>
<td>Enters the system.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>UCS-A /system# set mgmt-db-check-policy health-check-interval hours</td>
<td>Specifies the time interval (in hours) at which the integrity check runs.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>UCS-A /system* # commit-buffer</td>
<td>Commits the transaction.</td>
</tr>
</tbody>
</table>

Example

This example changes the time interval at which the check runs to two hours, and commits the transaction.

```
UCS-A# scope system
UCS-A /system# set mgmt-db-check-policy health-check-interval 2
UCS-A /system* # commit-buffer
UCS-A /system #
```
CHAPTER 12

Hardware Monitoring

- Monitoring a Fabric Interconnect, on page 87
- Monitoring a Blade Server, on page 88
- Monitoring a Rack-Mount Server, on page 90
- Monitoring an IO Module, on page 92
- Monitoring Crypto Cards, on page 93
- Monitoring NVMe PCIe SSD Devices, on page 95
- Health Monitoring, on page 98
- Management Interfaces Monitoring Policy, on page 102
- Local Storage Monitoring, on page 105
- Graphics Card Monitoring, on page 109
- Managing Transportable Flash Module and Supercapacitor, on page 111
- TPM Monitoring, on page 113

Monitoring a Fabric Interconnect

Procedure

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

**Step 2**
Expand Equipment > Fabric Interconnects.

**Step 3**
Click the node for the fabric interconnect that you want to monitor.

**Step 4**
In the Work pane, click one of the following tabs to view the status of the fabric interconnect:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General tab</strong></td>
<td>Provides an overview of the status of the fabric interconnect, including a summary of any faults, a summary of the fabric interconnect properties, and a physical display of the fabric interconnect and its components.</td>
</tr>
</tbody>
</table>
| **Physical Ports** tab | Displays the status of all ports on the fabric interconnect. This tab includes the following subtabs:  
  • Uplink Ports tab  
  • Server Ports tab |
Monitoring a Blade Server

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Expand Equipment > Chassis > Chassis Number > Servers.
Step 3 Click the server that you want to monitor.
Step 4 In the Work pane, click one of the following tabs to view the status of the server:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General tab</td>
<td>Provides an overview of the status of the server, including a summary of any faults, a summary of the server properties, and a physical display of the server and its components.</td>
</tr>
</tbody>
</table>

Note Enable Info Policy to view Neighbors details.

Step 5 Click the following tabs to view the status of the server:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fibre Channel Ports tab</td>
<td>Displays the status of all fan modules in the fabric interconnect.</td>
</tr>
<tr>
<td>Unconfigured Ports tab</td>
<td>Displays the status of all power supply units in the fabric interconnect.</td>
</tr>
<tr>
<td>Fans tab</td>
<td>Provides a graphical view of the fabric interconnect and all ports and other components. If a component has a fault, the fault icon is displayed next to that component.</td>
</tr>
<tr>
<td>PSUs tab</td>
<td>Provides details about the current FSM task running on the server, including the status of that task. You can use this information to diagnose errors with those tasks.</td>
</tr>
<tr>
<td>Faults tab</td>
<td>Provides details of faults generated by the fabric interconnect.</td>
</tr>
<tr>
<td>Events tab</td>
<td>Provides details of events generated by the fabric interconnect.</td>
</tr>
<tr>
<td>Neighbors tab</td>
<td>Provides details about the LAN, SAN, and LLDP neighbors of the fabric interconnect.</td>
</tr>
<tr>
<td>Statistics tab</td>
<td>Provides statistics about the fabric interconnect and its components. You can view these statistics in tabular or chart format.</td>
</tr>
</tbody>
</table>
### Option | Description
--- | ---
- **Motherboard** | Information about the motherboard and information about the server BIOS settings. You can also recover corrupt BIOS firmware from this subtab.
- **CIMC** | Information about the CIMC and its firmware, and provides access to the SEL for the server. You can also assign a static or pooled management IP address, and update and activate the CIMC firmware from this subtab.
- **CPUs** | Information about each CPU in the server.
- **Memory** | Information about each memory slot in the server and the DIMM in that slot.
- **Adapters** | Information about each adapter installed in the server.
- **HBAs** | Properties of each HBA and the configuration of that HBA in the service profile associated with the server.
- **NICs** | Properties of each NIC and the configuration of that NIC in the service profile associated with the server. You can expand each row to view information about the associated VIFs and vNICs.
- **iSCSI vNICs** | Properties of each iSCSI vNIC and the configuration of that vNIC in the service profile associated with the server.
- **Storage** | Properties of the storage controller, the local disk configuration policy in the service profile associated with the server, and for each hard disk in the server.

**Tip**

If the server contains one or more SATA devices, such as a hard disk drive or solid state drive, Cisco UCS Manager GUI displays the vendor name for the SATA device in the **Vendor** field.

However, Cisco UCS Manager CLI displays ATA in the **Vendor** field and includes the vendor information, such as the vendor name, in a **Vendor Description** field. This second field does not exist in Cisco UCS Manager GUI.

<table>
<thead>
<tr>
<th>Virtual Machines tab</th>
<th>Displays details about any virtual machines hosted on the server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed Firmware tab</td>
<td>Displays the firmware versions on the CIMC, adapters, and other server components. You can also use this tab to update and activate the firmware on those components.</td>
</tr>
<tr>
<td>CIMC Sessions tab</td>
<td>Provides data about the CIMC sessions on the server.</td>
</tr>
<tr>
<td>SEL Logs tab</td>
<td>Displays the system event log for the server.</td>
</tr>
<tr>
<td>VIF Paths tab</td>
<td>Displays the VIF paths for the adapters on the server.</td>
</tr>
<tr>
<td>Faults tab</td>
<td>Displays an overview of the faults generated by the server. You can click any fault to view additional information.</td>
</tr>
<tr>
<td>Events tab</td>
<td>Displays an overview of the events generated by the server. You can click any event to view additional information.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>FSM tab</td>
<td>Provides details about the current FSM task running on the server, including the status of that task. You can use this information to diagnose errors with those tasks.</td>
</tr>
<tr>
<td>Health tab</td>
<td>Displays details about the health status of the server and its components.</td>
</tr>
<tr>
<td>Statistics tab</td>
<td>Displays statistics about the server and its components. You can view these statistics in tabular or chart format.</td>
</tr>
<tr>
<td>Temperatures tab</td>
<td>Displays temperature statistics for the components of the server. You can view these statistics in tabular or chart format.</td>
</tr>
<tr>
<td>Power tab</td>
<td>Displays power statistics for the components of the server. You can view these statistics in tabular or chart format.</td>
</tr>
</tbody>
</table>

**Step 5**
In the **Navigation** pane, expand `Server_ID > Adapters > Adapter_ID`.

**Step 6**
In the **Navigation** pane, click on one or more of the following components of the adapter to open the navigator and view the status of the component:

- DCE interfaces
- HBAs
- NICs
- iSCSI vNICs

**Tip**
Expand the nodes in the table to view the child nodes. For example, if you expand a NIC node, you can view each VIF created on that NIC.

---

### Monitoring a Rack-Mount Server

**Procedure**

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

**Step 2**
Expand **Equipment > Rack Mounts > Servers**.

**Step 3**
Click the server that you want to monitor.

**Step 4**
In the **Work** pane, click one of the following tabs to view the status of the server:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General tab</td>
<td>Provides an overview of the status of the server, including a summary of any faults, a summary of the server properties, and a physical display of the server and its components.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Inventory tab</td>
<td>Provides details about the properties and status of the components of the server on the following subtabs:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Motherboard</strong> — Information about the motherboard and information about the server BIOS settings. You can also recover corrupt BIOS firmware from this subtab.</td>
</tr>
<tr>
<td></td>
<td>• <strong>CIMC</strong> — Information about the CIMC and its firmware, and provides access to the SEL for the server. You can also assign a static or pooled management IP address, and update and activate the CIMC firmware from this subtab.</td>
</tr>
<tr>
<td></td>
<td>• <strong>CPU</strong> — Information about each CPU in the server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Memory</strong> — Information about each memory slot in the server and the DIMM in that slot.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Adapters</strong> — Information about each adapter installed in the server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>HBAs</strong> — Properties of each HBA and the configuration of that HBA in the service profile associated with the server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>NICs</strong> — Properties of each NIC and the configuration of that NIC in the service profile associated with the server. You can expand each row to view information about the associated VIFs and vNICs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>iSCSI vNICs</strong> — Properties of each iSCSI vNIC and the configuration of that vNIC in the service profile associated with the server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Storage</strong> — Properties of the storage controller, the local disk configuration policy in the service profile associated with the server, and for each hard disk in the server.</td>
</tr>
<tr>
<td>Note</td>
<td>If the firmware of C-Series/S-Series servers is upgraded from Cisco UCSM release 2.2(6) to 3.1(2) or later release, the Platform Controller Hub (PCH) storage controller (along with the SSD boot drives) does not appear in UCSM GUI.</td>
</tr>
<tr>
<td>Tip</td>
<td>If the server contains one or more SATA devices, such as a hard disk drive or solid state drive, Cisco UCS Manager GUI displays the vendor name for the SATA device in the <strong>Vendor</strong> field. However, Cisco UCS Manager CLI displays ATA in the <strong>Vendor</strong> field and includes the vendor information, such as the vendor name, in a <strong>Vendor Description</strong> field. This second field does not exist in Cisco UCS Manager GUI.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Virtual Machines tab</th>
<th>Displays details about any virtual machines hosted on the server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed Firmware tab</td>
<td>Displays the firmware versions on the CIMC, adapters, and other server components. You can also use this tab to update and activate the firmware on those components.</td>
</tr>
<tr>
<td>SEL Logs tab</td>
<td>Displays the system event log for the server.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>VIF Paths</td>
<td>Displays the VIF paths for the adapters on the server.</td>
</tr>
<tr>
<td>Faults tab</td>
<td>Displays an overview of the faults generated by the server. You can click any fault to view additional information.</td>
</tr>
<tr>
<td>Events tab</td>
<td>Displays an overview of the events generated by the server. You can click any event to view additional information.</td>
</tr>
<tr>
<td>FSM tab</td>
<td>Provides details about the current FSM task running on the server, including the status of that task. You can use this information to diagnose errors with those tasks.</td>
</tr>
<tr>
<td>Statistics tab</td>
<td>Displays statistics about the server and its components. You can view these statistics in tabular or chart format.</td>
</tr>
<tr>
<td>Temperatures tab</td>
<td>Displays temperature statistics for the components of the server. You can view these statistics in tabular or chart format.</td>
</tr>
<tr>
<td>Power tab</td>
<td>Displays power statistics for the components of the server. You can view these statistics in tabular or chart format.</td>
</tr>
</tbody>
</table>

**Step 5**
In the **Navigation** pane, expand `Server_ID > Adapters > Adapter_ID`.

**Step 6**
In the **Work** pane, right-click one or more of the following components of the adapter to open the navigator and view the status of the component:
- Adapters
- DCE interfaces
- HBAs
- NICs

**Tip**
Expand the nodes in the table to view the child nodes. For example, if you expand a NIC node, you can view each VIF created on that NIC.

---

**Monitoring an IO Module**

**Procedure**

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

**Step 2**
Expand **Equipment > Chassis > Chassis Number > IO Modules**.

**Step 3**
Click the module that you want to monitor.

**Step 4**
Click one of the following tabs to view the status of the module:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General tab</td>
<td>Provides an overview of the status of the IO module, including a summary</td>
</tr>
<tr>
<td></td>
<td>of any faults, a summary of the module properties, and a physical display of</td>
</tr>
<tr>
<td></td>
<td>the module and its components.</td>
</tr>
<tr>
<td>Fabric Ports</td>
<td>Displays the status and selected properties of all fabric ports in the I/O</td>
</tr>
<tr>
<td></td>
<td>module.</td>
</tr>
<tr>
<td>Backplane Ports</td>
<td>Displays the status and selected properties of all backplane ports in the</td>
</tr>
<tr>
<td></td>
<td>module.</td>
</tr>
<tr>
<td>Faults tab</td>
<td>Provides details of faults generated by the module.</td>
</tr>
<tr>
<td>Events tab</td>
<td>Provides details of events generated by the module.</td>
</tr>
<tr>
<td>FSM tab</td>
<td>Provides details about and the status of FSM tasks related to the module.</td>
</tr>
<tr>
<td></td>
<td>You can use this information to diagnose errors with those tasks.</td>
</tr>
<tr>
<td>Health tab</td>
<td>Provides details about the health status of the module.</td>
</tr>
<tr>
<td>Statistics tab</td>
<td>Provides statistics about the module and its components. You can view these</td>
</tr>
<tr>
<td></td>
<td>statistics in tabular or chart format.</td>
</tr>
</tbody>
</table>

## Monitoring Crypto Cards

### Cisco Crypto Card Management for Blade Servers

Cisco UCS Manager provides inventory management for the Cisco Mezzanine Crypto Card (UCSB-MEZ-INT8955) for the Cisco UCSB-B200-M4 Blade Server. The main function of Cisco Crypto Card is to provide hardware based encryption capability to UCS blade server for certain applications.

The Cisco B200 M4 Blade Server includes two optional, hot-pluggable, SAS, SATA hard disk drives (HDDs) or solid-state drives (SSDs) and is suited for a broad spectrum of IT workloads. Place the Crypto Card in slot 2 of the blade server.

Cisco UCS Manager discovers the Crypto Card present in a blade server and displays the model, revision, vendor, serial number on the Equipment > Chassis > Server_Number > Inventory > Security subtab. Discovery of the Crypto Card fails if you add the Crypto Card to an unsupported blade server.

Cisco UCS Manager does not support firmware management for the Crypto Card.

Insertion and removal of a Crypto Card triggers deep discovery. Replacing the Crypto Card with another Crypto Card, Adaptor or Fusion I/O, or pass through card triggers deep discovery for commissioned servers. The following are the various Crypto Card replacement scenarios:

- Replacing a Crypto Card with another Crypto Card
- Replacing a Crypto Card with an adaptor
- Replacing a Crypto Card with a Fusion I/O
• Replacing a Crypto Card with a GPU card
• Replacing Crypto Card with a pass through card
• Replacing an adaptor with a Crypto Card
• Replacing a storage Mezzanine with a Crypto Card
• Replacing a GPU card with a Crypto Card

No cleanup is necessary for the downgrade of Cisco UCS Manager to an earlier version. If you upgrade UCS Manager after a downgrade, rediscovery of the card is necessary to inventory the card. For servers that do not support crypto cards, discovery proceeds uninterrupted.

Cisco UCS Manager discovers, associates, disassociates, and decommissions Crypto Cards.

**Viewing Crypto Card Properties**

**Procedure**

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

**Step 2** Expand Equipment > Chassis > Chassis Number > Servers.

**Step 3** On the Work pane, click the Inventory tab, then click the Security subtab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID field</td>
<td></td>
</tr>
<tr>
<td>Slot ID field</td>
<td>Specifies the Slot ID where the Mezzanine card is placed.</td>
</tr>
<tr>
<td>Magma Expander Slot Id field</td>
<td>Specifies the ID number of the PCI slot.</td>
</tr>
<tr>
<td>Is Supported field</td>
<td>Specifies whether the card is supported.</td>
</tr>
<tr>
<td>Vendor field</td>
<td>Specifies the vendor of the card.</td>
</tr>
<tr>
<td>Model field</td>
<td>Specifies the model number of the card.</td>
</tr>
<tr>
<td>Serial field</td>
<td>Specifies the serial number of the card.</td>
</tr>
<tr>
<td>Firmware Version field</td>
<td>Specifies the Crypto card serial number.</td>
</tr>
</tbody>
</table>
Monitoring NVMe PCIe SSD Devices

NVMe PCIe SSD Storage Device Inventory

Cisco UCS Manager GUI discovers, identifies, and displays the inventory of Non-Volatile Memory Express (NVMe) Peripheral Component Interconnect Express (PCIe) SSD storage devices. You can view the health of the storage devices in the server. NVMe with PCIe SSD storage devices reduce latency, increased Input/Output Operations Per Second (IOPS), and lower power consumption compared to SAS or SATA SSDs.

Viewing NVMe PCIe SSD Storage Inventory

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Expand Equipment > Rack Mounts > Servers > Server Number.
Step 3 Click the Inventory tab.
Step 4 Do one of the following:
   a) Click the Storage tab.
      The list of NVMe PCIe SSD storage devices named Storage Controller NVME ID number is displayed. You can view the name, size, serial number, operating status, state and other details.
   b) Click the NVMe PCIe SSD storage device.
      The following inventory details are displayed:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actions Area</td>
<td></td>
</tr>
<tr>
<td>ID field</td>
<td>The NVMe PCIe SSD storage device configured on the server.</td>
</tr>
<tr>
<td>Description field</td>
<td>Brief description of the NVMe PCIe SSD storage device configured on the server.</td>
</tr>
<tr>
<td>Model field</td>
<td>The NVMe PCIe SSD storage device model.</td>
</tr>
<tr>
<td>Revision field</td>
<td>The NVMe PCIe SSD storage device revision.</td>
</tr>
<tr>
<td>Subtype field</td>
<td>The vendor name of the NVMe PCIe SSD storage device.</td>
</tr>
<tr>
<td>RAID Support field</td>
<td>Indicated whether the NVMe PCIe SSD storage device is RAID enabled.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OOB Interface Support</td>
<td>Indicates if the NVMe PCIe SSD storage device supports out-of-band management.</td>
</tr>
<tr>
<td>PCIe Address</td>
<td>The NVMe PCIe SSD storage device on the virtual interface card (VIC).</td>
</tr>
<tr>
<td>Number of Local Disks</td>
<td>The number of disks contained in the NVMe PCIe SSD storage device.</td>
</tr>
<tr>
<td>Rebuild Rate</td>
<td>The time it takes the storage device to rebuild RAID when a disk fails.</td>
</tr>
<tr>
<td>SubOemID</td>
<td>The OME ID for the NVMe PCIe SSD storage device on the virtual interface card (VIC).</td>
</tr>
<tr>
<td>Supported Strip Sizes</td>
<td>The strip size supported by the NVMe PCIe SSD storage device.</td>
</tr>
<tr>
<td>Sub Device ID</td>
<td>The sub device ID of the controller</td>
</tr>
<tr>
<td>Sub Vendor ID</td>
<td>The sub vendor ID of the controller</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the controller.</td>
</tr>
<tr>
<td>PID</td>
<td>The NVMe PCIe SSD storage device product ID, also known as product name, model name, product number</td>
</tr>
<tr>
<td>Serial</td>
<td>The storage device serial number.</td>
</tr>
<tr>
<td>Vendor</td>
<td>The vendor that manufactured the NVMe PCIe SSD storage device.</td>
</tr>
<tr>
<td>PCI Slot</td>
<td>The PCI slot of the storage device.</td>
</tr>
</tbody>
</table>
### Hardware Monitoring

**Viewing NVMe PCIe SSD Storage Inventory**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Controller Status</strong></td>
<td>The current status of the controller as reported by CIMC. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Optimal—The controller is functioning properly.</td>
</tr>
<tr>
<td></td>
<td>• Failed—The controller is not functioning.</td>
</tr>
<tr>
<td></td>
<td>• Unresponsive—The CIMC is unable to communicate with the controller.</td>
</tr>
<tr>
<td><strong>Pinned Cache Status</strong></td>
<td>The pin cache status of the storage device.</td>
</tr>
<tr>
<td><strong>Default Strip Size</strong></td>
<td>The default strip size the storage device can support.</td>
</tr>
<tr>
<td><strong>Device ID</strong></td>
<td>The ID of the storage device.</td>
</tr>
<tr>
<td><strong>Vendor ID</strong></td>
<td>The ID of the manufacturer.</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>The device security applied to the storage device.</td>
</tr>
</tbody>
</table>

**Embedded Storage Area**

| Presence field          | Whether the storage is embedded or not.                                    |
| Block Size field        | The memory of the device.                                                   |
| Size (MB) field         | The fractional memory of the device in MB.                                  |
| Connection Protocol field | The connection protocol followed.                                          |
| Oper Qualified Reason   | The operability reason of the device                                        |
| Number of Blocks field  | The number of memory blocks.                                                |

**Firmware Area**

| Boot-loader Version field | Displays the firmware version that is associated with the boot-loader software on the component. |
### Health Monitoring

#### Monitoring Fabric Interconnect Low Memory Statistics and Correctable Parity Errors

You can monitor Cisco UCS fabric interconnect system statistics and faults that allow you to manage overall system health, such as:

- **Low kernel memory**—This is the segment that the Linux kernel addresses directly. Cisco UCS Manager raises a major fault on a fabric interconnect when kernel memory falls below 100 MB. See Monitoring Fabric Interconnect Low Memory Faults, on page 99. Two statistics KernelMemFree and KernelMemTotal alarm, when low memory thresholds are met. KernelMemFree and KernelMemTotal statistics are added to the threshold policy for system statistics where you can define your own thresholds.

Low memory faults are supported on the following Cisco UCS fabric interconnects:

- UCS 6248-UP
- UCS 6296-UP

---

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Running Version</strong></td>
<td>The firmware version used by the component.</td>
</tr>
<tr>
<td><strong>Package Version</strong></td>
<td>The firmware package version in which the firmware was included.</td>
</tr>
<tr>
<td><strong>Startup Version</strong></td>
<td>The version of the firmware that takes effect the next time that the component reboots.</td>
</tr>
<tr>
<td><strong>Activate Status</strong></td>
<td>This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Ready—Activation succeeded and the component is running the new version.</td>
</tr>
<tr>
<td></td>
<td>• Activating—The system is activating the new firmware version.</td>
</tr>
<tr>
<td></td>
<td>• Failed—The firmware activation failed. For more information, double-click the failed component to view its status properties.</td>
</tr>
</tbody>
</table>
• UCS Mini
• UCS-FI-6332
• UCS-FI-6332-16UP

• **Correctable Parity Errors**—(For UCS 6300 fabric interconnects only) The system collects and reports these errors for the fabric interconnect under **Statistics > sysstats > CorrectableParityError**.

• **Uncorrectable Parity Errors**—(For UCS 6300 fabric interconnects only) These errors raise a major fault on fabric interconnects under the **Faults** tab and triggers CallHome. These major faults may cause you to reboot the fabric interconnect. See **Monitoring Fabric Interconnect Uncorrectable Parity Error Major Faults**, on page 100.

To view fabric interconnect low memory statistics and correctable memory statistics:

**Procedure**

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

**Step 2** Expand **Equipment > Fabric Interconnects > Fabric_Interconnect_Name**.

**Step 3** In the **Work** pane, click the **Statistics** tab.

**Step 4** On the **Statistics** tab, expand the **sysstats** node to monitor fabric interconnect low memory statistics and correctable parity errors.

A major fault is raised when kernel memory free (KernelMemFree) goes below 100 MB. The system also raises a major fault when an Uncorrectable Parity Error occurs.

---

**Monitoring Fabric Interconnect Low Memory Faults**

Cisco UCS Manager system raises a major severity fault on a fabric interconnect when kernel memory free falls below 100 MB.

Low memory faults are supported on the following Cisco UCS fabric interconnects:

• UCS 6248-UP
• UCS 6296-UP
• UCS Mini
• UCS-FI-6332
• UCS-FI-6332-16UP

To view fabric interconnect low memory faults:

**Procedure**

**Step 1** In the **Navigation** pane, click **Equipment**.
Monitoring Fabric Interconnect Uncorrectable Parity Error Major Faults

Uncorrectable Parity Errors raise a major fault on fabric interconnects under the Faults tab and triggers CallHome. Major faults may cause you to reboot the fabric interconnect.

**Note**

This applies for UCS 6300 fabric interconnects only.

To monitor Uncorrectable Parity Error faults:

**Procedure**

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

**Step 2**
Expand Equipment > Fabric Interconnects > Fabric_Interconnect_Name.

**Step 3**
In the Work pane, click the Faults tab.

**Step 4**
On the Faults tab, look for a major severity fault with the description: Fabric Interconnect_Name kernel low memory free reached critical level: ## (MB)

**Step 5**
Reboot the fabric interconnect.

Monitoring CIMC Memory Usage for Blade, and Rack-Mount Servers

The Cisco Integrated Management Controller (CIMC) reports the following memory usage events for blade, and rack-mount servers:

- When memory falls below 1MB, CIMC has fatal memory usage. Reset is imminent.
- When memory falls below 5 MB, CIMC has extremely high memory usage.
- When memory falls below 10 MB, CIMC has high memory usage.

To view CIMC memory usage events:

**Procedure**

Do one of the following:

- For Blade Servers:
1. On the Equipment tab, expand Equipment > Chassis > Chassis Number > Servers.
2. Click Server_Number.
3. In the Work pane, click the Health tab.

For Rack-Mount Servers:
2. Click Server_Number.
3. In the Work pane, click the Health tab.

If CIMC reports two health events, one with major severity, the other with minor severity, the system raises a major severity fault and displays details under the Health tab Management Services subtab. Every health event does not translate to a fault. The highest severity health event translates to a fault. Faults appear under Server_Number > Faults tab.

---

**Monitoring CMC Memory Usage for Input/Output Modules**

The Cisco Chassis Management Controller (CMC) reports memory usage events for IOMs and chassis. The system raises a fault on the aggregation of reported health status.

To view CMC memory usage events:

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Navigation pane, click Equipment.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Expand Equipment &gt; Chassis &gt; Chassis Number &gt; IO Modules.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click IO Module_Number.</td>
</tr>
</tbody>
</table>

The Health tab Management Services subtab appears.

Every event does not translate to a fault. The highest severity events translate to fault. Faults appear under IO Module_Number > Faults tab.

---

**Monitoring FEX Statistics**

Cisco UCS Manager reports the following statistics for Cisco Fabric Extenders (FEXs) under the System Stats:

- Load
- Available Memory
- Cached Memory
Cisco 2200 Series and 2300 Series FEX support statistics monitoring.

---

**Note**

FEX stats are not supported on the Cisco UCS Mini platform.

All FEX stats are added to threshold policy as FexSystemStats where users can define their own thresholds.

**Procedure**

**Step 1**
On the **Equipment** tab, expand **Equipment** > **Rack Mounts** > **FEX** > **FEX Number**.

The **Statistics** tab appears. You can view the statistics in tabular or chart format.

**Step 2**
Expand the **sys-stats** node to monitor FEX statistics.

**Management Interfaces Monitoring Policy**

The management interfaces monitoring policy defines how the mgmt0 Ethernet interface on the fabric interconnect is monitored. If Cisco UCS Manager detects a management interface failure, a failure report is generated. If the configured number of failure reports is reached, the system assumes that the management interface is unavailable and generates a fault. By default, the management interfaces monitoring policy is enabled.

When the management interface of a fabric interconnect which is currently the managing instance fails, Cisco UCS Manager first confirms if the status of the subordinate fabric interconnect is up. In addition, if there are no current failure reports logged against the fabric interconnect, Cisco UCS Manager modifies the managing instance for the endpoints.

If the affected fabric interconnect is currently the primary in a high availability setup, a failover of the management plane is triggered. This failover does not affect the data plane. You can set the following properties related to monitoring the management interface:

- The type of mechanism used to monitor the management interface.
- The interval at which the status of the management interface is monitored.
- The maximum number of monitoring attempts that can fail before the system assumes that the management is unavailable and generates a fault message.
When the management interface fails on a fabric interconnect, the managing instance may not change if one of the following occurs:

- A path to the endpoint through the subordinate fabric interconnect does not exist.
- The management interface for the subordinate fabric interconnect has failed.
- The path to the endpoint through the subordinate fabric interconnect has failed.

### Configuring the Management Interfaces Monitoring Policy

**Procedure**

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

**Step 2**  
Expand **All > Communication Management**.

**Step 3**  
Click **Management Interfaces**.

**Step 4**  
In the **Work** pane, click the **Management Interfaces Monitoring Policy** tab.

**Step 5**  
Complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Admin Status</strong> field</td>
<td>Indicates whether the monitoring policy is enabled or disabled for the management interfaces.</td>
</tr>
<tr>
<td><strong>Poll Interval</strong> field</td>
<td>The number of seconds Cisco UCS should wait between data recordings. Enter an integer between 90 and 300.</td>
</tr>
<tr>
<td><strong>Max Fail Report Count</strong></td>
<td>The maximum number of monitoring attempts that can fail before Cisco UCS assumes that the management interface is unavailable and generates a fault message. Enter an integer between 2 and 5.</td>
</tr>
</tbody>
</table>
**Step 6** If you chose **MII Status** for the monitoring mechanism, complete the following fields in the Media Independent Interface Monitoring area:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Retry Interval</strong></td>
<td>The number of seconds Cisco UCS should wait before requesting another response from the MII if a previous attempt fails. Enter an integer between 3 and 10.</td>
</tr>
<tr>
<td><strong>Max Retry Count</strong></td>
<td>The number of times Cisco UCS polls the MII until the system assumes the interface is unavailable. Enter an integer between 1 and 3.</td>
</tr>
</tbody>
</table>

**Step 7** If you chose **Ping Arp Targets** for the monitoring mechanism, complete the fields on the appropriate tab in the ARP Target Monitoring area.

If you are using IPv4 addresses, complete the following fields in the IPv4 subtab:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Target IP 1</strong></td>
<td>The first IPv4 address Cisco UCS pings.</td>
</tr>
<tr>
<td><strong>Target IP 2</strong></td>
<td>The second IPv4 address Cisco UCS pings.</td>
</tr>
<tr>
<td><strong>Target IP 3</strong></td>
<td>The third IPv4 address Cisco UCS pings.</td>
</tr>
<tr>
<td><strong>Number of ARP Requests</strong></td>
<td>The number of ARP requests Cisco UCS sends to the target IP addresses. Enter an integer between 1 and 5.</td>
</tr>
<tr>
<td><strong>Max Deadline Timeout</strong></td>
<td>The number of seconds Cisco UCS waits for responses from the ARP targets until the system assumes they are unavailable. Enter an integer between 5 and 15.</td>
</tr>
</tbody>
</table>

If you are using IPv6 addresses, complete the following fields in the IPv6 subtab:
## Local Storage Monitoring

Local storage monitoring in Cisco UCS provides status information on local storage that is physically attached to a blade or rack server. This includes RAID controllers, physical drives and drive groups, virtual drives, RAID controller batteries (Battery Backup Unit), Transportable Flash Modules (TFM), supercapacitors, FlexFlash controllers, and SD cards.

Cisco UCS Manager communicates directly with the LSI MegaRAID controllers and FlexFlash controllers using an out-of-band interface, which enables real-time updates. Some of the information that is displayed includes:

- RAID controller status and rebuild rate.
- The drive state, power state, link speed, operability, and firmware version of physical drives.
- The drive state, operability, strip size, access policies, drive cache, and health of virtual drives.
- The operability of a BBU, whether it is a supercap or battery, and information about the TFM.

### Hardware Monitoring

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target IP 1 field</td>
<td>The first IPv6 address Cisco UCS pings.</td>
</tr>
<tr>
<td>Target IP 2 field</td>
<td>The second IPv6 address Cisco UCS pings.</td>
</tr>
<tr>
<td>Target IP 3 field</td>
<td>The third IPv6 address Cisco UCS pings.</td>
</tr>
<tr>
<td>Number of ARP Requests field</td>
<td>The number of ARP requests Cisco UCS sends to the target IP addresses. Enter an integer between 1 and 5.</td>
</tr>
<tr>
<td>Max Deadline Timeout field</td>
<td>The number of seconds Cisco UCS waits for responses from the ARP targets until the system assumes they are unavailable. Enter an integer between 5 and 15.</td>
</tr>
</tbody>
</table>

Type 0.0.0.0 for an IPv4 address to remove the ARP target or :: for an IPv6 address to remove the N-disc target.

**Step 8**  
If you chose Ping Gateway for the monitoring mechanism, complete the following fields in the **Gateway Ping Monitoring** area:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Ping Requests field</td>
<td>The number of times Cisco UCS should ping the gateway. Enter an integer between 1 and 5.</td>
</tr>
<tr>
<td>Max Deadline Timeout field</td>
<td>The number of seconds Cisco UCS waits for a response from the gateway until Cisco UCS assumes the address is unavailable. Enter an integer between 5 and 15.</td>
</tr>
</tbody>
</table>

**Step 9**  
Click **Save Changes**.
LSI storage controllers use a Transportable Flash Module (TFM) powered by a supercapacitor to provide RAID cache protection.

- Information on SD cards and FlexFlash controllers, including RAID health and RAID state, card health, and operability.
- Information on operations that are running on the storage component, such as rebuild, initialization, and relearning.

Note
After a CIMC reboot or build upgrades, the status, start time, and end times of operations running on the storage component may not be displayed correctly.

- Detailed fault information for all local storage components.

Note
All faults are displayed on the Faults tab.

Support for Local Storage Monitoring

The type of monitoring supported depends upon the Cisco UCS server.

Supported Cisco UCS Servers for Local Storage Monitoring

Through Cisco UCS Manager, you can monitor local storage components for the following servers:

- Cisco UCS B200 M3 blade server
- Cisco UCS B420 M3 blade server
- Cisco UCS B22 M3 blade server
- Cisco UCS B200 M4 blade server
- Cisco UCS B260 M4 blade server
- Cisco UCS B460 M4 blade server
- Cisco UCS C460 M2 rack server
- Cisco UCS C420 M3 rack server
- Cisco UCS C260 M2 rack server
- Cisco UCS C240 M3 rack server
- Cisco UCS C220 M3 rack server
- Cisco UCS C24 M3 rack server
- Cisco UCS C22 M3 rack server
- Cisco UCS C220 M4 rack server
- Cisco UCS C240 M4 rack server
• Cisco UCS C460 M4 rack server

**Note**
Not all servers support all local storage components. For Cisco UCS rack servers, the onboard SATA RAID 0/1 controller integrated on motherboard is not supported.

**Supported Cisco UCS Servers for Legacy Disk Drive Monitoring**
Only legacy disk drive monitoring is supported through Cisco UCS Manager for the following servers:

• Cisco UCS B200 M1/M2 blade server

• Cisco UCS B250 M1/M2 blade server

**Note**
In order for Cisco UCS Manager to monitor the disk drives, the 1064E storage controller must have a firmware level contained in a Cisco UCS bundle with a package version of 2.0(1) or higher.

**Prerequisites for Local Storage Monitoring**
These prerequisites must be met for local storage monitoring or legacy disk drive monitoring to provide useful status information:

• The drive must be inserted in the server drive bay.

• The server must be powered on.

• The server must have completed discovery.

• The results of the BIOS POST complete must be TRUE.

**Legacy Disk Drive Monitoring**

**Note**
The following information is applicable only for B200 M1/M2 and B250 M1/M2 blade servers.

The legacy disk drive monitoring for Cisco UCS provides Cisco UCS Manager with blade-resident disk drive status for supported blade servers in a Cisco UCS domain. Disk drive monitoring provides a unidirectional fault signal from the LSI firmware to Cisco UCS Manager to provide status information.

The following server and firmware components gather, send, and aggregate information about the disk drive status in a server:

• Physical presence sensor—Determines whether the disk drive is inserted in the server drive bay.

• Physical fault sensor—Determines the operability status reported by the LSI storage controller firmware for the disk drive.

• IPMI disk drive fault and presence sensors—Sends the sensor results to Cisco UCS Manager.
• Disk drive fault LED control and associated IPMI sensors—Controls disk drive fault LED states (on or off) and relays the states to Cisco UCS Manager.

Flash Life Wear Level Monitoring

Flash life wear level monitoring enables you to monitor the life span of solid state drives. You can view both the percentage of the flash life remaining, and the flash life status. Wear level monitoring is supported on the Fusion IO mezzanine card with the following Cisco UCS blade servers:

• Cisco UCS B22 M3 blade server
• Cisco UCS B200 M3 blade server
• Cisco UCS B420 M3 blade server
• Cisco UCS B200 M4 blade server
• Cisco UCS B260 M4 blade server
• Cisco UCS B460 M4 blade server

Note

Wear level monitoring requires the following:

• Cisco UCS Manager must be at release 2.2(2a) or greater.
• The Fusion IO mezzanine card firmware must be at version 7.1.15 or greater.

Viewing the Status of Local Storage Components

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Expand Equipment > Chassis > Chassis Number > Servers.
Step 3 Click the server for which you want to view the status of your local storage components.
Step 4 In the Work pane, click the Inventory tab.
Step 5 Click the Storage subtab to view the status of your RAID controllers and any FlexFlash controllers.
Step 6 Click the down arrows to expand the Local Disk Configuration Policy, Actual Disk Configurations, Disks, and Firmware bars and view additional status information.

Note The Local Disk Configuration Policy and Actual Disk Configurations areas only display data for the Cisco UCS B460 blade server master node. No fields are displayed for the slave node.
RAID 0 Check Consistency Limitation

The Check Consistency operation is not supported for RAID 0 volumes. You must change the local disk configuration policy to run Check Consistency. For more information, see the *UCS Manager Server Management Guide*, Server Related Policies chapter, Changing a Local Disk Policy topic.

Graphics Card Monitoring

Graphics Card Server Support

With Cisco UCS Manager, you can view the properties for certain graphics cards and controllers. Graphics cards are supported on the following servers:

- Cisco UCS C240 M3 Rack Server
- Cisco UCS C460 M4 Rack Server
- Cisco UCS B200 M4 Blade Server

**Note**

Certain NVIDIA Graphics Processing Units (GPU) do not support Error Correcting Code (ECC) and vGPU together. Cisco recommends that you refer to the release notes published by NVIDIA for the respective GPU to know whether it supports ECC and vGPU together.

GPU Mezzanine Graphics Module Management for Blade Servers

Cisco UCS Manager provides inventory and firmware management support for the NVIDIA Graphics Processing Unit (GPU) Mezzanine Graphic Module (N16E-Q5) for Cisco B200 M4 Blade Servers. GPU computing accelerates scientific, analytics, engineering, consumer, and enterprise applications. The Cisco B200 M4 Blade Server includes two optional, hot-pluggable, SAS, SATA hard disk drives (HDDs) or solid-state drives (SSDs) and is suited for a broad spectrum of IT workloads.

Cisco UCS Manager discovers the presence of the GPU Graphics Card in a blade server as a field replaceable unit and collects device inventory information, such as model, vendor, serial number, PCI slot and address, and firmware. Cisco UCS Manager displays GPU Card inventory on the Equipment > Chassis > Server_Number > Inventory > GPUs subtab.

GPU Card firmware management includes firmware upgrade and downgrade. Upgrade the GPU firmware through existing Cisco UCS Manager service profiles. Do not downgrade GPU firmware with older firmware versions, because cleanup is required.

Place the GPU Card in slot 2 of the blade server. GPU Card discovery fails if you insert a card in an unsupported blade.

Replacing a GPU card triggers deep discovery for commissioned servers. The following are the various GPU card replacement scenarios that cause deep discovery:

- Replacing a GPU card with another GPU card
- Replacing a GPU card with an adaptor
- Replacing a GPU card with a storage Mezzanine
- Replacing an adaptor with a GPU card
- Replacing a storage Mezzanine with GPU card
- Replacing a GPU card with Crypto card
- Replacing a Crypto card with a GPU card

Cisco UCS Manager discovers, associates, disassociates, and decommissions GPU Graphics Cards. To view GPU Graphics Cards, see Viewing Graphics Card Properties, on page 110.

---

**Note**

There is a maximum limit on the GPU Graphics Card memory (DIMMS) of 1 TB.

---

**Viewing Graphics Card Properties**

**Procedure**

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

**Step 2**
Do one of the following:
- Expand **Equipment > Chassis > Chassis_Number > Servers > Server_Number**.
- Expand **Equipment > Rack-Mounts > Servers > Server_Number**.

**Step 3**
On the Work pane, click the **Inventory** tab, then click the **GPU** subtab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID field</td>
<td>The unique ID for the graphics card.</td>
</tr>
<tr>
<td>PCI Slot field</td>
<td>The PCI slot number where the graphics card is installed.</td>
</tr>
<tr>
<td>Expander Slot ID field</td>
<td>The expander slot ID.</td>
</tr>
<tr>
<td>PID field</td>
<td>Product Identifier of the graphics card.</td>
</tr>
<tr>
<td>Is Supported field</td>
<td>Whether the graphics card is supported. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Yes</td>
</tr>
<tr>
<td></td>
<td>• No</td>
</tr>
<tr>
<td>Vendor field</td>
<td>The name of the manufacturer.</td>
</tr>
<tr>
<td>Model field</td>
<td>The model number of the graphics card.</td>
</tr>
<tr>
<td>Serial field</td>
<td>The serial number of the component.</td>
</tr>
<tr>
<td>Running Version field</td>
<td>The firmware version of the graphics card.</td>
</tr>
</tbody>
</table>
Managing Transportable Flash Module and Supercapacitor

LSI storage controllers use a Transportable Flash Module (TFM) powered by a supercapacitor to provide RAID cache protection. With Cisco UCS Manager, you can monitor these components to determine the status of the battery backup unit (BBU). The BBU operability status can be one of the following:

- **Operable**—The BBU is functioning successfully.
- **Inoperable**—The TFM or BBU is missing, or the BBU has failed and needs to be replaced.
- **Degraded**—The BBU is predicted to fail.

TFM and supercap functionality is supported beginning with Cisco UCS Manager Release 2.1(2).

TFM and Supercap Guidelines and Limitations

**TFM and Supercap Limitations**

- The CIMC sensors for TFM and supercap on the Cisco UCS B420 M3 blade server are not polled by Cisco UCS Manager.
- If the TFM and supercap are not installed on the Cisco UCS B420 M3 blade server, or are installed and then removed from the blade server, no faults are generated.
- If the TFM is not installed on the Cisco UCS B420 M3 blade server, but the supercap is installed, Cisco UCS Manager reports the entire BBU system as absent. You should physically check to see if both the TFM and supercap is present on the blade server.
Supported Cisco UCS Servers for TFM and Supercap

The following Cisco UCS servers support TFM and supercap:

- Cisco UCS B420 M3 blade server
- Cisco UCS C22 M3 rack server
- Cisco UCS C24 M3 rack server
- Cisco UCS C220 M3 rack server
- Cisco UCS C240 M3 rack server
- Cisco UCS C420 M3 rack server
- Cisco UCS C460 M4 rack server
- Cisco UCS C220 M3 rack server
- Cisco UCS C240 M3 rack server

Viewing the RAID Controller Stats

The following procedure shows how to see RAID controller stats for a server with PCIe\NVMe Flash Storage

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Navigation pane, click Equipment.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Equipment pane, expand Chassis &gt; Chassis Number &gt; Servers &gt; Server Number.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Work pane, click the Inventory tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click the Storage &gt; Controller &gt; General subtab to view the controller stats.</td>
</tr>
</tbody>
</table>

Monitoring RAID Battery Status

This procedure applies only to Cisco UCS servers that support RAID configuration and TFM. If the BBU has failed or is predicted to fail, you should replace the unit as soon as possible.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Navigation pane, click Equipment.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Equipment pane, expand Chassis &gt; Chassis Number &gt; Servers &gt; Server Number.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Work pane, click the Inventory tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click the Storage subtab to view the RAID Battery (BBU) area.</td>
</tr>
</tbody>
</table>
Viewing a RAID Battery Fault

This applies only to Cisco UCS servers that support RAID configuration and TFM.

Procedure

- **Step 1**: In the Navigation pane, click Equipment.
- **Step 2**: In the Equipment pane, expand Chassis > Chassis Number > Servers > Server Number.
- **Step 3**: In the Work pane, click the Faults tab.
- **Step 4**: Select the battery to see more information on its condition.

TPM Monitoring

Trusted Platform Module (TPM) is included on all Cisco UCS M3 and higher blade and rack-mount servers. Operating systems can use TPM to enable encryption. For example, Microsoft's BitLocker Drive Encryption uses the TPM on Cisco UCS servers to store encryption keys.

Cisco UCS Manager enables monitoring of TPM, including whether TPM is present, enabled, or activated.

Viewing TPM Properties

Procedure

- **Step 1**: In the Navigation pane, click Equipment.
- **Step 2**: Expand Equipment > Chassis > Chassis Number > Servers.
- **Step 3**: Choose the server for which you want to view the TPM settings.
- **Step 4**: On the Work pane, click the Inventory tab.
- **Step 5**: Click the Motherboard subtab.
Traffic Monitoring

Traffic monitoring copies traffic from one or more source ports and sends the copied traffic to a dedicated destination port for analysis by a network analyzer. This feature is also known as Switched Port Analyzer (SPAN).

Types of Traffic Monitoring Sessions

There are two types of monitoring sessions:

- Ethernet
- Fibre channel

The type of destination port determines what kind of monitoring session you need. For an Ethernet traffic monitoring session, the destination port must be an unconfigured physical port. For a Fibre Channel traffic monitoring session, the destination port must be a Fibre Channel uplink port except when you are using Cisco UCS 6300 Fabric Interconnects.

Note

For Cisco UCS 6332 and 6332-16UP Fabric Interconnects, you cannot choose Fibre Channel destination ports. The destination port must be an unconfigured physical Ethernet port.
Traffic Monitoring Across Ethernet

An Ethernet traffic monitoring session can monitor any of the following traffic source and destination ports:

<table>
<thead>
<tr>
<th>Source Ports</th>
<th>Destination Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Uplink Ethernet port</td>
<td>Unconfigured Ethernet Port</td>
</tr>
<tr>
<td>• Ethernet port channel</td>
<td></td>
</tr>
<tr>
<td>• VLAN</td>
<td></td>
</tr>
<tr>
<td>• Service profile vNIC</td>
<td></td>
</tr>
<tr>
<td>• Service profile vHBA</td>
<td></td>
</tr>
<tr>
<td>• FCoE port</td>
<td></td>
</tr>
<tr>
<td>• Port channels</td>
<td></td>
</tr>
<tr>
<td>• Unified uplink port</td>
<td></td>
</tr>
<tr>
<td>• VSAN</td>
<td></td>
</tr>
</tbody>
</table>

All traffic sources must be located within the same switch as the destination port. A port configured as a destination port cannot also be configured as a source port. A member port of a port channel cannot be configured individually as a source. If the port channel is configured as a source, all member ports are source ports.

A server port can be a source, only if it is a nonvirtualized rack server adapter-facing port.

Traffic Monitoring for Cisco UCS 6300 Interconnects

• Cisco UCS 6300 Fabric Interconnect supports port-based mirroring.
• Cisco UCS 6300 Fabric Interconnect supports VLAN SPAN only in the Rx or the receive direction.
• Ethernet SPAN is port based on the Cisco UCS 6300 Fabric Interconnect.

Traffic Monitoring for Cisco UCS 6200 Interconnects

• Cisco UCS 6200 and 6324 supports monitoring traffic in the ‘transmit’ direction for up to two sources per Fabric Interconnect.
• Cisco UCS 6200 SPAN traffic is rate-limited by the SPAN destination port speed. This can be either 1 or 10 Gbps.

(For 6200 and 6324 Fabric Interconnects) You can monitor or use SPAN on port channels only for ingress traffic.

Traffic Monitoring Across Fibre Channel

You can monitor Fibre Channel traffic using either a Fibre Channel traffic analyzer or an Ethernet traffic analyzer. When Fibre Channel traffic is monitored with an Ethernet traffic monitoring session, at an Ethernet destination port, the destination traffic is FCoE. The Cisco UCS 6300 Fabric Interconnect supports FC SPAN.
only on the ingress side. A Fibre Channel port on a Cisco UCS 6248 Fabric Interconnect cannot be configured as a source port.

A Fibre Channel traffic monitoring session can monitor any of the following traffic source and destination ports:

<table>
<thead>
<tr>
<th>Source Ports</th>
<th>Destination Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>• FC Port</td>
<td>• Fibre Channel uplink port</td>
</tr>
<tr>
<td>• FC Port Channel</td>
<td>• Unconfigured Ethernet Port (Cisco UCS 6332 and</td>
</tr>
<tr>
<td>• Uplink Fibre Channel port</td>
<td>Cisco UCS 6332-16UP Fabric Interconnects)</td>
</tr>
<tr>
<td>• SAN port channel</td>
<td></td>
</tr>
<tr>
<td>• VSAN</td>
<td></td>
</tr>
<tr>
<td>• Service profile vHBA</td>
<td></td>
</tr>
<tr>
<td>• Fibre Channel storage port</td>
<td></td>
</tr>
</tbody>
</table>

**Guidelines and Recommendations for Traffic Monitoring**

When configuring or activating traffic monitoring, consider the following guidelines:

**Traffic Monitoring Sessions**

A traffic monitoring session is disabled by default when created. To begin monitoring traffic, first activate the session. A traffic monitoring session must be unique on any fabric interconnect within the Cisco UCS pod. Create each monitoring session with a unique name and unique VLAN source. To monitor traffic from a server, add all vNICs from the service profile corresponding to the server.

**Maximum Number of Supported Active Traffic Monitoring Sessions Per Fabric-Interconnect**

You can create and store up to 16 traffic monitoring sessions, but only four can be active at the same time. For each Cisco UCS 6300 Fabric Interconnect, you can only monitor up to four traffic directions. The receive and transmit directions each count as one monitoring session, while the bi-direction monitoring session is counted as 2. For example:

- Four active sessions — If each session is configured to monitor traffic in only one direction
- Two active sessions — If each session is configured to monitor traffic bidirectionally.
- Three active sessions — If one session is unidirectional and the second session is bidirectional.

**Note**

Traffic monitoring can impose a significant load on your system resources. To minimize the load, select sources that carry as little unwanted traffic as possible and disable traffic monitoring when it is not needed.
vNIC

Because a traffic monitoring destination is a single physical port, a traffic monitoring session can monitor only a single fabric. To monitor uninterrupted vNIC traffic across a fabric failover, create two sessions, one per fabric and connect two analyzers. Add the vNIC as the traffic source using the exact same name for both sessions. If you change the port profile of a virtual machine, any associated vNICs being used as source ports are removed from monitoring, and you must reconfigure the monitoring session. If a traffic monitoring session was configured on a dynamic vNIC under a release earlier than Cisco UCS Manager Release 2.0, you must reconfigure the traffic monitoring session after upgrading.

vHBA

A vHBA can be a source for either an Ethernet or Fibre Channel monitoring session, but it cannot be a source for both simultaneously. When a VHBA is set as the SPAN source, the SPAN destination only receives VN-Tagged frames. It does not receive direct FC frames.

Creating an Ethernet Traffic Monitoring Session

Procedure

Step 1  In the Create Traffic Monitoring Session dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the traffic monitoring session. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.</td>
</tr>
<tr>
<td>Admin State field</td>
<td>Indicates whether traffic will be monitored for the physical port selected in the Destination field. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Enabled—Cisco UCS begins monitoring the port activity as soon as some source components are added to the session.</td>
</tr>
<tr>
<td></td>
<td>• Disabled—Cisco UCS does not monitor the port activity.</td>
</tr>
<tr>
<td>Span Control Packets field</td>
<td>Indicates whether outgoing control packets that are sent from the CPU are monitored. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Enabled—Cisco UCS monitors outgoing control packets on the port.</td>
</tr>
<tr>
<td></td>
<td>• Disabled—Cisco UCS does not monitor outgoing control packets on the port.</td>
</tr>
<tr>
<td>Destination drop-down list</td>
<td>The physical port that is being monitored. Click the link in this field to view the port properties.</td>
</tr>
</tbody>
</table>
Step 2 Click OK.

What to do next

• Add traffic sources to the traffic monitoring session.
• Activate the traffic monitoring session.

Setting the Destination for an Existing Ethernet Traffic Monitoring Session

Procedure

Step 1 In the Navigation pane, click LAN.
Step 2 On the LAN tab, expand LAN > Traffic Monitoring Sessions > Fabric_Interconnect_Name > Monitor_Session_Name.
Step 3 In the Work pane, click the General tab.
Step 4 In the Actions area, click Set Destination.
Step 5 In the Set Destination dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destination</strong> drop-down list</td>
<td>The physical port where you want to monitor all the communication from the sources.</td>
</tr>
<tr>
<td><strong>Admin Speed</strong> field</td>
<td>The data transfer rate of the port channel to be monitored. The available data rates depend on the fabric interconnect installed in the Cisco UCS domain. For Ethernet Traffic Monitoring sessions in 6332 and 6332-16UP Fls, you cannot use the 1Gbps speed configuration for the configured Ethernet Destination Port.</td>
</tr>
</tbody>
</table>

Step 6 Click OK.
Clearing the Destination for an Existing Ethernet Traffic Monitoring Session

Procedure

Step 1 In the Navigation pane, click LAN.
Step 2 Expand LAN > Traffic Monitoring Sessions > Fabric_Interconnect_Name > Monitor_Session_Name.
Step 3 In the Work pane, click the General tab.
Step 4 In the Actions area, click Clear Destination.
Step 5 If a confirmation dialog box displays, click Yes.

Creating a Fibre Channel Traffic Monitoring Session

Procedure

Step 1 In the Navigation pane, click SAN.
Step 2 Expand SAN > Traffic Monitoring Sessions > Fabric_Interconnect_Name.
Step 3 Right-click Fabric_Interconnect_Name and choose Create Traffic Monitoring Session.
Step 4 In the Create Traffic Monitoring Session dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the traffic monitoring session. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.</td>
</tr>
<tr>
<td>Admin State</td>
<td>Indicates whether traffic will be monitored for the physical port selected in the Destination field. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Enabled   —Cisco UCS begins monitoring the port activity as soon as some source components are added to the session.</td>
</tr>
<tr>
<td></td>
<td>• Disabled  —Cisco UCS does not monitor the port activity.</td>
</tr>
</tbody>
</table>
### Setting the Destination for an Existing Fibre Channel Traffic Monitoring Session

**Step 1**
In the Navigation pane, click SAN.

**Step 2**
Expand SAN > Traffic Monitoring Sessions > Fabric_Interconnect_Name > Monitor_Session_Name

**Step 3**
In the Work pane, click the General tab.

**Step 4**
In the Actions area, click Set Destination.

**Step 5**
In the Set Destination dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Span Control Packets</strong></td>
<td>Indicates whether outgoing control packets that are sent from the CPU are monitored. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—Cisco UCS monitors outgoing control packets on the port.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—Cisco UCS does not monitor outgoing control packets on the port.</td>
</tr>
<tr>
<td><strong>Destination</strong> drop-down list</td>
<td>Select the physical port where you want to monitor all the communication from the sources.</td>
</tr>
<tr>
<td><strong>Admin Speed</strong> drop-down list</td>
<td>The data transfer rate of the port channel to be monitored. The available data rates depend on the fabric interconnect installed in the Cisco UCS domain. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• 1 Gbps</td>
</tr>
<tr>
<td></td>
<td>• 10 Gbps</td>
</tr>
<tr>
<td></td>
<td>• 25 Gbps</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong>—Cisco UCS determines the data transfer rate.</td>
</tr>
</tbody>
</table>

**What to do next**
- Add traffic sources to the traffic monitoring session.
- Activate the traffic monitoring session.
Clearing the Destination for an Existing Fibre Channel Traffic Monitoring Session

Procedure

**Step 1** In the Navigation pane, click SAN.

**Step 2** Expand SAN > Traffic Monitoring Sessions > Fabric_Interconnect_Name > Monitor_Session_Name

**Step 3** In the Work pane, click the General tab.

**Step 4** In the Actions area, click Clear Destination.

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

Adding Traffic Sources to a Monitoring Session

You can choose multiple sources from more than one source type to be monitored by a traffic monitoring session. The available sources depend on the components configured in the Cisco UCS domain.

*Note*

This procedure describes how to add sources for Ethernet traffic monitoring sessions. To add sources for a Fibre Channel monitoring session, select the SAN tab instead of the LAN tab in Step 2.
Before you begin

A traffic monitoring session must be created.

Procedure

Step 1 In the Navigation pane, click LAN.
Step 2 Expand LAN > Traffic Monitoring Sessions > Fabric_Interconnect_Name.
Step 3 Expand Fabric_Interconnect_Name and click the monitor session that you want to configure.
Step 4 In the Work pane, click the General tab.
Step 5 In the Sources area, expand the section for the type of traffic source that you want to add.
Step 6 To see the components that are available for monitoring, click the + button in the right-hand edge of the table to open the Add Monitoring Session Source dialog box.
Step 7 Select a source component and click OK.

You can repeat the preceding three steps as needed to add multiple sources from multiple source types.

Step 8 Click Save Changes.

What to do next

Activate the traffic monitoring session. If the session is already activated, traffic will be forwarded to the monitoring destination when you add a source.

Activating a Traffic Monitoring Session

Note

This procedure describes how to activate an Ethernet traffic monitoring session. To activate a Fibre Channel monitoring session, select the SAN tab instead of the LAN tab in Step 2.

Before you begin

A traffic monitoring session must be created.

Procedure

Step 1 In the Navigation pane, click LAN.
Step 2 Expand LAN > Traffic Monitoring Sessions > Fabric_Interconnect_Name.
Step 3 Expand Fabric_Interconnect_Name and click the monitor session that you want to activate.
Step 4 In the Work pane, click the General tab.
Step 5 In the Properties area, click the enabled radio button for Admin State.
Deleting a Traffic Monitoring Session

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

If a traffic monitoring source is configured, traffic begins to flow to the traffic monitoring destination port.

---

### Deleting a Traffic Monitoring Session

**Procedure**

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

2. **Step 2**  
   Expand **LAN > Traffic Monitoring Sessions > Fabric_Interconnect_Name**.

3. **Step 3**  
   Expand **Fabric_Interconnect_Name** and click the monitor session that you want to delete.

4. **Step 4**  
   In the *Work* pane, click the **General** tab.

5. **Step 5**  
   In the *Actions* area, click the **Delete** icon.

6. **Step 6**  
   If a confirmation dialog box displays, click **Yes**.
NetFlow Monitoring

For Release 3.0(2), NetFlow monitoring is supported for end-host mode only.

NetFlow is a standard network protocol for collecting IP traffic data. NetFlow enables you to define a flow in terms of unidirectional IP packets that share certain characteristics. All packets that match the flow definition are collected and exported to one or more external NetFlow Collectors, where they can be further aggregated, analyzed, and used for application-specific processing.

Cisco UCS Manager uses NetFlow-capable adapters (Cisco UCS VIC 1240, Cisco UCS VIC 1280, and Cisco UCS VIC 1225) to communicate with the routers and switches that collect and export flow information.

Network Flows

A flow is a set of unidirectional IP packets that have common properties such as, the source or destination of the traffic, routing information, and protocol used. Flows are collected when they match the definitions in the flow record definition.

Flow Record Definitions

A flow record definition contains information about the properties used to define the flow, which can include both characteristic properties or measured properties. Characteristic properties, also called flow keys, are the
properties that define the flow. Cisco UCS Manager supports IPv4, IPv6, and Layer 2 keys. Measured characteristics, also called flow values or non-keys, measurable values such as the number of bytes contained in all packets of the flow, or the total number of packets.

A flow record definition is a specific combination of flow keys and flow values. The two types of flow record definitions are:

- **System-defined**—Default flow record definitions supplied by Cisco UCS Manager.
- **User-defined**—Flow record definitions that you can create yourself.

**Flow Exporters, Flow Exporter Profiles, and Flow Collectors**

Flow exporters transfer the flows to the flow connector based on the information in a flow exporter profile. The flow exporter profile contains the networking properties used to export NetFlow packets. The networking properties include a VLAN, the source IP address, and the subnet mask for each fabric interconnect.

*Note* In the Cisco UCS Manager GUI, the networking properties are defined in an exporter interface that is included in the profile. In the Cisco UCS Manager CLI, the properties are defined in the profile.

Flow collectors receive the flows from the flow exporter. Each flow collector contains an IP address, port, external gateway IP, and VLAN that defines where the flows are sent.

**Flow Monitors and Flow Monitor Sessions**

A flow monitor consists of a flow definition, one or two flow exporters, and a timeout policy. You can use a flow monitor to specify which flow information you want to gather, and where you want to collect it from. Each flow monitor operates in either the egress or ingress direction.

A flow monitor session contains up to four flow monitors: two flow monitors in the ingress direction and two flow monitors in the egress direction. A flow monitor session can also be associated with a vNIC.

---

**NetFlow Monitoring Limitations**

*Note* For Release 3.0(2), NetFlow monitoring is supported for end-host mode only.

The following limitations apply to NetFlow monitoring:

- NetFlow monitoring is not supported on the Cisco UCS 6100 Series Fabric Interconnect.
- NetFlow monitoring is supported only on the Cisco UCS VIC 1240, Cisco UCS VIC 1280, and Cisco UCS VIC 1225 adapters. Beginning with release 2.2(3a), NetFlow monitoring is also supported on the Cisco UCS VIC 1340, Cisco UCS VIC 1380, and Cisco UCS VIC 1227 adapters.

*Note* NetFlow monitoring is not supported on the Cisco UCS VIC 1200 adapters when configured with vHBAs.
Enabling NetFlow Monitoring

You must enable NetFlow monitoring for the feature to work.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Navigation pane, click LAN.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Expand LAN &gt; Netflow Monitoring.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the General tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Admin State field, click the Enabled radio button to enable NetFlow monitoring.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Save Changes to save the configuration change.</td>
</tr>
</tbody>
</table>

Creating a Flow Record Definition

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Navigation pane, click LAN.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Expand LAN &gt; Netflow Monitoring.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Right-click Flow Record Definitions and choose Create Flow Record Definition.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Create Flow Record Definition dialog box, complete the following fields:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the flow record definition. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.</td>
</tr>
<tr>
<td>Description</td>
<td>The user-defined description of the flow record definition.</td>
</tr>
</tbody>
</table>
Viewing Flow Record Definitions

**Procedure**

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

**Step 2** Expand LAN > Netflow Monitoring.

**Step 3** Choose Flow Record Definitions to view the list of all flow definitions.

**Step 4** Double-click the name of a flow definition to view the properties for the selected flow definition.

On the Properties window, you can modify the keys and non-keys used for the flow.

---

Defining the Exporter Profile

**Procedure**

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

**Step 2** Expand LAN > Netflow Monitoring > Flow Exporters > Flow Exporter Profiles.
Creating a Flow Collector

Procedure

Step 1  In the Navigation pane, click LAN.
Step 2  Expand LAN > Netflow Monitoring.
Step 3  In the Work pane, click the Flow Collectors tab.
Step 4  Click Add at the side of the Flow Collectors table.
Step 5  In the Create Flow Collectors dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>Choose the VLAN that you want to associate with the exporter interface, or click Create VLANs to create a new one. PVLAN and local VLANs are not supported. All VLANs must be public and must be common to both fabric interconnects.</td>
</tr>
<tr>
<td>Fabric A Source IP</td>
<td>The source IP for the exporter interface on fabric A. Important Make sure the IP address you specify is unique within the Cisco UCS domain. IP address conflicts can occur if you specify an IP address that is already being used by Cisco UCS Manager.</td>
</tr>
<tr>
<td>Fabric A Subnet Mask</td>
<td>The subnet mask for the exporter interface on fabric A.</td>
</tr>
<tr>
<td>Fabric B Source IP</td>
<td>The source IP for the exporter interface on fabric B. Important Make sure the IP address you specify is unique within the Cisco UCS domain. IP address conflicts can occur if you specify an IP address that is already being used by Cisco UCS Manager.</td>
</tr>
<tr>
<td>Fabric B Subnet Mask</td>
<td>The subnet mask for the exporter interface on fabric B.</td>
</tr>
</tbody>
</table>

Step 6  Click OK.
Creating a Flow Exporter

Procedure

Step 1 In the Navigation pane, click LAN.
Step 2 Expand LAN > Netflow Monitoring.
Step 3 Right-click Flow Exporters and choose Create Flow Exporter.
Step 4 In the Create Flow Exporter dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the flow exporter.</td>
</tr>
<tr>
<td>Description</td>
<td>The user-defined description of the flow exporter.</td>
</tr>
<tr>
<td>DSCP</td>
<td>The differentiated services codepoint (DSCP) value. The range of values is from 0 and 63.</td>
</tr>
<tr>
<td>Version</td>
<td>The exporter version. By default, this is version 9.</td>
</tr>
<tr>
<td>Exporter Profile</td>
<td>The exporter profile that you want to associate with the flow exporter.</td>
</tr>
</tbody>
</table>
Creating a Flow Monitor

Procedure

Step 1  In the Navigation pane, click LAN.
Step 2  Expand LAN > Netflow Monitoring.
Step 3  Right-click Flow Monitors and choose Create Flow Monitor.
Step 4  In the Create Flow Monitor dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow Collector</td>
<td>Choose the flow collector that you want to associate with the flow exporter, or click Create Flow Exporter to create a new one.</td>
</tr>
<tr>
<td>Template Data Timeout</td>
<td>The timeout period for resending NetFlow template data. Enter a value between 1 and 86400.</td>
</tr>
<tr>
<td>Option Exporter Stats Timeout</td>
<td>The timeout period for resending NetFlow flow exporter data. Enter a value between 1 and 86400.</td>
</tr>
<tr>
<td>Option Interface Table Timeout</td>
<td>The time period for resending the NetFlow flow exporter interface table. Enter a value between 1 and 86400.</td>
</tr>
</tbody>
</table>

Step 5  Click OK.
Creating a Flow Monitor Session

Procedure

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

**Step 2** Expand LAN > Netflow Monitoring.

**Step 3** Right-click Flow Monitor Sessions and choose Create Flow Monitor Session.

**Step 4** In the Create Flow Monitor Session dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the flow monitor session. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.</td>
</tr>
<tr>
<td>Description</td>
<td>The user-defined description of the flow monitor session.</td>
</tr>
<tr>
<td>Host Receive Direction Monitor 1</td>
<td>Choose the flow monitor that you want to use from the list of values, or click Create Flow Monitor to create a new one.</td>
</tr>
<tr>
<td>Host Receive Direction Monitor 2</td>
<td>Choose the flow monitor that you want to use from the list of values, or click Create Flow Monitor to create a new one.</td>
</tr>
<tr>
<td>Host Transmit Direction Monitor 1</td>
<td>Choose the flow monitor that you want to use from the list of values, or click Create Flow Monitor to create a new one.</td>
</tr>
<tr>
<td>Host Transmit Direction Monitor 2</td>
<td>Choose the flow monitor that you want to use from the list of values, or click Create Flow Monitor to create a new one.</td>
</tr>
</tbody>
</table>

**Step 5** Click OK.

Associating a Flow Monitor Session to a vNIC

Procedure

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

**Step 2** Expand LAN > Netflow Monitoring > Flow Monitor Sessions.
Step 3  Click the flow monitor session that you want to associate.
Step 4  Click Flow Exporter Profile default.
Step 5  In the Properties area, expand vNICs.
Step 6  Click Add at the side of the table.
Step 7  In the Add Monitoring Session Source dialog box, choose the vNIC that you want to associate with the flow monitor session.
Step 8  Click OK to close the dialog box.
Step 9  Click Save to close the dialog box.
Associating a Flow Monitor Session to a vNIC