# Cisco UCS CLI System Monitoring Guide for Cisco UCS Mini, Release 3.0

**First Published:** July 21, 2014

**Last Modified:** March 09, 2015

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

# CONTENTS


Preface

Preface ix

Audience ix

Conventions ix

Related Cisco UCS Documentation xi

Documentation Feedback xi

CHAPTER 1

Monitoring Traffic 1

Traffic Monitoring 1

Guidelines and Recommendations for Traffic Monitoring 2

Creating an Ethernet Traffic Monitoring Session 3

Creating a Fibre Channel Traffic Monitoring Session 4

Adding Traffic Sources to a Monitoring Session 5

Adding an Uplink Source Port to a Monitoring Session 5

Adding a vNIC or vHBA Source to a Monitoring Session 6

Adding a VLAN or VSAN Source to a Monitoring Session 8

Adding a Storage Port Source to a Monitoring Session 9

Activating a Traffic Monitoring Session 9

Deleting a Traffic Monitoring Session 10

SPAN restrictions for Cisco UCS Mini 11

CHAPTER 2

Monitoring Hardware 13

Monitoring Fan Modules 13

Monitoring Management Interfaces 15

Management Interfaces Monitoring Policy 15

Configuring the Management Interfaces Monitoring Policy 16

Local Storage Monitoring 18

Support for Local Storage Monitoring 18

Prerequisites for Local Storage Monitoring 19
Legacy Disk Drive Monitoring 19
Flash Life Wear Level Monitoring 19
Viewing Flash Life Status 20
Viewing the Status of Local Storage Components 21
Viewing the Status of a Disk Drive 22
Viewing RAID Controller Operations 23
Graphics Cards Monitoring 24
Monitoring Graphics Cards 24
Viewing Graphics Card Properties 24
Viewing Graphics Controller Properties 25
Managing Transportable Flash Module and Supercapacitor 25
TFM and Supercap Guidelines and Limitations 25
Monitoring RAID Battery Status 26
TPM Monitoring 26
Viewing TPM Properties 27

CHAPTER 3 **Configuring Statistics-Related Policies** 29
Configuring Statistics Collection Policies 29
Statistics Collection Policy 29
Configuring a Statistics Collection Policy 30
Configuring Statistics Threshold Policies 30
Statistics Threshold Policy 30
Server and Server Component Statistics Threshold Policy Configuration 31
Configuring a Server and Server Component Statistics Threshold Policy 31
Deleting a Server and Server Component Statistics Threshold Policy 32
Configuring a Server and Server Component Statistics Threshold Policy Class 32
Deleting a Server and Server Component Statistics Threshold Policy Class 34
Uplink Ethernet Port Statistics Threshold Policy Configuration 34
Configuring an Uplink Ethernet Port Statistics Threshold Policy 34
Configuring an Uplink Ethernet Port Statistics Threshold Policy Class 35
Deleting an Uplink Ethernet Port Statistics Threshold Policy Class 37
Server Port, Chassis, and Fabric Interconnect Statistics Threshold Policy Configuration 37
Configuring a Server Port, Chassis, and Fabric Interconnect Statistics Threshold Policy 37

Configuring a Server Port, Chassis, and Fabric Interconnect Statistics Threshold Policy Class 38
Deleting a Server Port, Chassis, and Fabric Interconnect Statistics Threshold Policy Class 40
Fibre Channel Port Statistics Threshold Policy Configuration 40
Configuring a Fibre Channel Port Statistics Threshold Policy 40
Configuring a Fibre Channel Port Statistics Threshold Policy Class 41
Deleting an Uplink Fibre Channel Port Statistics Threshold Policy Class 43

CHAPTER 4 **Configuring Call Home** 45
Call Home 45
Call Home Considerations and Guidelines 47
Cisco UCS Faults and Call Home Severity Levels 48
Cisco Smart Call Home 49
Anonymous Reporting 50
Configuring Call Home 50
Disabling Call Home 52
Enabling Call Home 53
Configuring System Inventory Messages 53
Configuring System Inventory Messages 53
Sending a System Inventory Message 54
Configuring Call Home Profiles 55
Call Home Profiles 55
Call Home Alert Groups 55
Configuring a Call Home Profile 56
Deleting a Call Home Profile 57
Sending a Test Call Home Alert 58
Configuring Call Home Policies 59
Call Home Policies 59
Configuring a Call Home Policy 59
Disabling a Call Home Policy 60
Enabling a Call Home Policy 60
Deleting a Call Home Policy 61
Configuring Anonymous Reporting 61
Enabling Anonymous Reporting 61

Disabling Anonymous Reporting 62
Viewing Anonymous Reports 63
Example: Configuring Call Home for Smart Call Home 64
Configuring Smart Call Home 64
Configuring the Default Cisco TAC-1 Profile 66
Configuring a System Inventory Message for Smart Call Home 67
Registering Smart Call Home 68

CHAPTER 5 Managing the System Event Log 69
System Event Log 69
Viewing the System Event Log for a Server 70
Viewing the System Event Log for an Individual Server 70
Viewing the System Event Log for All of the Servers in a Chassis 70
Configuring the SEL Policy 71
Backing Up the System Event Log for a Server 73
Backing Up the System Event Log for an Individual Server 73
Backing Up the System Event Log for All of the Servers in a Chassis 73
Clearing the System Event Log for a Server 74
Clearing the System Event Log for an Individual Server 74
Clearing the System Event Log for All of the Servers in a Chassis 74

CHAPTER 6 Configuring Settings for Faults, Events, and Logs 77
Configuring Settings for the Fault Collection Policy 77
Global Fault Policy 77
Configuring the Fault Collection Policy 78
Configuring Fault Suppression 79
Fault Suppression 79
Configuring Fault Suppression for a Chassis 80
Configuring Fault Suppression Tasks for a Chassis Using a Fixed Time Interval 80
Configuring Fault Suppression Tasks for a Chassis Using a Schedule 81
Deleting Fault Suppression Tasks for a Chassis 82
Modifying Fault Suppression Tasks for a Chassis 82
Viewing Suppressed Faults and Fault Suppression Tasks for a Chassis 84
Configuring Fault Suppression for a Server 84
Configuring Fault Suppression Tasks for a Server Using a Fixed Time Interval 84

Configuring Fault Suppression Tasks for a Server using a Schedule 85
Deleting Fault Suppression Tasks for a Server 86
Modifying Fault Suppression Tasks for a Server 87
Viewing Suppressed Faults and Fault Suppression Tasks for a Server 88
Configuring Fault Suppression for a Service Profile 89
Configuring Fault Suppression Tasks for a Service Profile Using a Fixed Time Interval 89
Configuring Fault Suppression Tasks for a Service Profile Using a Schedule 90
Deleting Fault Suppression Tasks for a Service Profile 91
Modifying Fault Suppression Tasks for a Service Profile 92
Viewing Suppressed Faults and Fault Suppression Tasks for a Service Profile 94
Configuring Fault Suppression for an Organization 95
Configuring Fault Suppression Tasks for an Organization Using a Fixed Time Interval 95
Configuring Fault Suppression Tasks for an Organization Using a Schedule 96
Deleting Fault Suppression Tasks for an Organization 96
Modifying Fault Suppression Tasks for an Organization 97
Viewing Suppressed Faults and Fault Suppression Tasks for an Organization 98
Configuring Settings for the Core File Exporter 99
Core File Exporter 99
Configuring the Core File Exporter 99
Disabling the Core File Exporter 100
Configuring the Syslog 101
Viewing Audit Logs 103
Configuring the Log File Exporter 104
Log File Exporter 104
Exporting Log Files to a Remote Server 104

CHAPTER 7 **NetFlow Monitoring** 107
NetFlow Monitoring 107
NetFlow Limitations 108
Configuring a Flow Record Definition 109
Configuring an Exporter Profile 110
Configuring a Netflow Collector 111
Configuring a Flow Exporter 111
Configuring a Flow Monitor 112
Configuring a Flow Monitor Session 113

Configuring a NetFlow Cache Active and Inactive Timeout 114
Associating a Flow Monitor Session to a vNIC 114

# Preface

This preface includes the following sections:


- Audience, page ix
- Conventions, page ix
- Related Cisco UCS Documentation, page xi
- Documentation Feedback, 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

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

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

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

**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.

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

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

**Warning** IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

# Related 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: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

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

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

### Other Documentation Resources

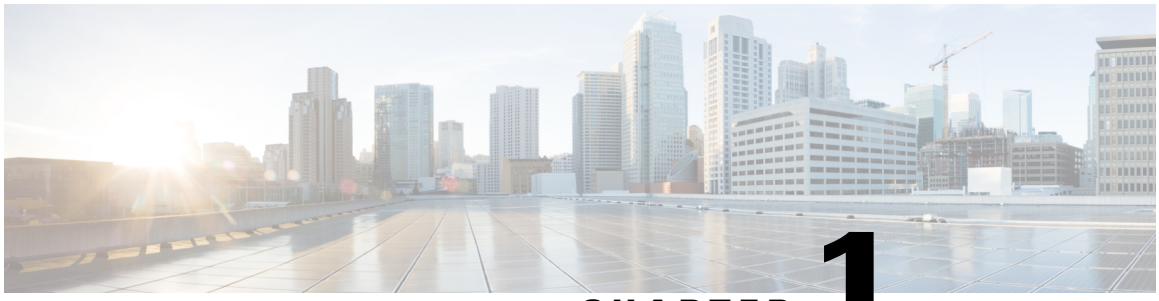
An ISO file containing all B and C-Series documents is available at the following URL: http://www.cisco.com/cisco/software/type.html?mdfid=283853163&flowid=25821. From this page, click **Unified Computing System (UCS) Documentation Roadmap Bundle**.

The ISO file is updated after every major documentation release.

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@cisco.com. We appreciate your feedback.



CHAPTER 1

# Monitoring Traffic

This chapter includes the following sections:


- Traffic Monitoring, page 1
- Guidelines and Recommendations for Traffic Monitoring, page 2
- Creating an Ethernet Traffic Monitoring Session, page 3
- Creating a Fibre Channel Traffic Monitoring Session, page 4
- Adding Traffic Sources to a Monitoring Session, page 5
- Activating a Traffic Monitoring Session, page 9
- Deleting a Traffic Monitoring Session, page 10
- SPAN restrictions for Cisco UCS Mini, page 11


## Traffic Monitoring

Traffic monitoring copies traffic from one or more sources 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).

**Important** You can monitor or use SPAN on port channels only for ingress traffic.

### Type of Session

When you create a traffic monitoring session, you can choose either an Ethernet or Fibre Channel destination port to receive the traffic. The type of destination port determines the type of session, which in turn determines the types of available traffic sources. 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.

### Traffic Sources

An Ethernet traffic monitoring session can monitor any of the following traffic sources:

- Uplink Ethernet port
- Ethernet port channel
- VLAN
- Service profile vNIC
- Service profile vHBA
- FCoE port
- Port channels
- Unified uplink port

A Fibre Channel traffic monitoring session can monitor any of the following traffic sources:

- Uplink Fibre Channel port
- SAN port channel
- VSAN
- Service profile vHBA
- Fibre Channel storage port

# Guidelines and Recommendations for Traffic Monitoring

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

- You can create and store up to 16 traffic monitoring sessions, but only two can be active at the same time.
- A traffic monitoring session is disabled by default when created. To begin monitoring traffic, you must activate the session.
- A traffic monitoring session must be unique on any fabric interconnect within the Cisco UCS pod. Therefore, you must 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.
- You can monitor Fibre Channel traffic using either a Fibre Channel traffic analyzer or an Ethernet traffic analyzer. When Fibre Channel traffic is monitored using an Ethernet traffic monitoring session, with an Ethernet destination port, the destination traffic will be FCoE.
- 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, you must create two sessions—one per fabric—and connect two analyzers. Add the vNIC as the traffic source for both sessions.
- 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 vHBA can be a source for either an Ethernet or Fibre Channel monitoring session, but it cannot be a source for both simultaneously.
- A server port can be a source only if it is a non-virtualized rack server adapter-facing port.
- A Fibre Channel port on a Cisco UCS 6248 fabric interconnect cannot be configured as a source port.
- 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.
- SPAN traffic is rate-limited to 1 Gbps on Cisco UCS 6200 Series fabric interconnects.

**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.

# Creating an Ethernet Traffic Monitoring Session

This procedure describes creating an Ethernet traffic monitoring session.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-traffic-mon** | Enters Ethernet traffic monitoring command mode. |
| **Step 2** | UCS-A /eth-traffic-mon # **scope fabric** {**a** \| **b**} | Enters traffic monitoring command mode for the specified fabric. |
| **Step 3** | UCS-A /eth-traffic-mon/fabric # **create eth-mon-session** *session-name* | Creates a traffic monitoring session with the specified name. |
| **Step 4** | UCS-A /eth-traffic-mon/fabric/eth-mon-session # **create dest-interface** *slot-num port-num* | Configures the interface at the specified slot and port number to be the destination for the traffic monitoring session. Enters the command mode for the interface. |
| **Step 5** | UCS-A /eth-traffic-mon/fabric/eth-mon-session/dest-interface # **set speed***admin-speed* | Sets the data transfer rate of the port channel to be monitored. This can be:<br>• 1gbps—1 Gbps<br>• 10gbps—10 Gbps |
| **Step 6** | UCS-A /eth-traffic-mon/fabric/eth-mon-session/dest-interface # **commit-buffer** | Commits the transaction to the system configuration. |

The following example creates an Ethernet traffic monitoring session to copy and forward traffic to the destination port at slot 2, port 12, sets the admin speed to 20 Gbps, and commits the transaction:

```
UCS-A# scope eth-traffic-mon
UCS-A /eth-traffic-mon # scope fabric a
UCS-A /eth-traffic-mon/fabric # create eth-mon-session EthMonitor33
UCS-A /eth-traffic-mon/fabric/eth-mon-session* # create dest-interface 2 12
UCS-A /eth-traffic-mon/fabric/eth-mon-session/dest-interface* # set speed 20gbps
UCS-A /eth-traffic-mon/fabric/eth-mon-session/dest-interface* # commit-buffer
UCS-A /eth-traffic-mon/fabric/eth-mon-session/dest-interface #
```

### What to Do Next

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

# Creating a Fibre Channel Traffic Monitoring Session

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope fc-traffic-mon** | Enters Fibre Channel traffic monitoring command mode. |
| **Step 2** | UCS-A /fc-traffic-mon # **scope fabric** {**a** \| **b**} | Enters Fibre Channel traffic monitoring command mode for the specified fabric. |
| **Step 3** | UCS-A /fc-traffic-mon/fabric # **create fc-mon-session** *session-name* | Creates a Fibre Channel traffic monitoring session with the specified name. |
| **Step 4** | UCS-A /fc-traffic-mon/fabric/fc-mon-session # **create dest-interface** *slot-num port-num* | Creates and enters the command mode of the destination slot and port for the Fibre Channel traffic monitoring session. |
| **Step 5** | UCS-A /fc-traffic-mon/fabric/fc-mon-session/dest-interface # **set speed***admin-speed* | Sets the data transfer rate of the port channel to be monitored. This can be:<br>• 1gbps—1 Gbps<br>• 2gbps—2 Gbps<br>• 4gbps—4 Gbps<br>• 8gbps—8 Gbps<br>• auto—Cisco UCS determines the data transfer rate. |
| **Step 6** | UCS-A /fc-traffic-mon/fabric/fc-mon-session/dest-interface # **commit-buffer** | Commits the transaction to the system configuration. |

The following example creates a Fibre channel traffic monitoring session to copy and forward traffic to the destination port at slot 1, port 10, sets the admin speed to 8 Gbps, and commits the transaction:

```
UCS-A# scope fc-traffic-mon
UCS-A /fc-traffic-mon # scope fabric a
UCS-A /fc-traffic-mon/fabric # create fc-mon-session FCMonitor
UCS-A /fc-traffic-mon/fabric/fc-mon-session* # create dest-interface 1 10
UCS-A /fc-traffic-mon/fabric/fc-mon-session/dest-interface* # set speed 8gbps
UCS-A /fc-traffic-mon/fabric/fc-mon-session/dest-interface* # commit-buffer
UCS-A /fc-traffic-mon/fabric/fc-mon-session/dest-interface #
```

### What to Do Next

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

# Adding Traffic Sources to a Monitoring Session

## Adding an Uplink Source Port to a Monitoring Session

**Note** This procedure describes adding an Ethernet uplink port as a source for a traffic monitoring session. To add a Fibre Channel uplink port as a source, enter the **scope fc-uplink** command instead of the **scope eth-uplink** command in Step 1.

### Before You Begin

A traffic monitoring session must be created.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-uplink** | Enters Ethernet uplink command mode. |
| **Step 2** | UCS-A /eth-uplink # **scope fabric** {**a** \| **b**} | Enters uplink fabric mode for the specified fabric. |
| **Step 3** | UCS-A /eth-uplink/fabric # **scope interface** *slot-num port-num* | Enters the interface command mode for the specified uplink port. |
| **Step 4** | UCS-A /eth-uplink/fabric/interface # **create mon-src** *session-name* | Adds the uplink port as a source to the specified monitoring session. |
| **Step 5** | UCS-A /eth-uplink/fabric/interface/mon-src # **set direction** {**both** \| **receive** \| **transmit**} | (Optional)<br>Specifies the traffic direction to be monitored.<br>**Note** If you do not select any direction, the default direction is Rx. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | UCS-A /eth-uplink/fabric/interface/mon-src # **commit-buffer** | Commits the transaction to the system configuration. |

The following example adds the ingress traffic on Ethernet uplink port 3 on slot 2 of fabric A as a source for a monitoring session and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # scope interface 2 3
UCS-A /eth-uplink/fabric/interface # create mon-src Monitor23
UCS-A /eth-uplink/fabric/interface/mon-src* # set direction receive
UCS-A /eth-uplink/fabric/interface/mon-src* # commit-buffer
UCS-A /eth-uplink/fabric/interface/mon-src #
```

### What to Do Next

You can add additional sources to the traffic monitoring session.

# Adding a vNIC or vHBA Source to a Monitoring Session

**Note** This procedure describes adding a vNIC as a source for a traffic monitoring session. To add a vHBA as a source, enter the **scope vhba** command instead of the **scope vnic** command in Step 2.

### Before You Begin

A traffic monitoring session must be created.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Switch-A# **scope system** | Enters system mode. |
| **Step 2** | Switch-A /system # **scope vm-mgmt** | Enters VM management mode. |
| **Step 3** | Switch-A /system/vm-mgmt # **show virtual-machine** | (Optional)<br>Displays the running virtual machines. |
| **Step 4** | Switch-A /system/vm-mgmt # **scope virtual-machine** *uuid* | Enters command mode for the virtual machine that contains the dynamic vNIC. |
| **Step 5** | Switch-A /system/vm-mgmt/virtual-machine # **show expand** | (Optional)<br>Displays the virtual machine details, including the vNIC MAC address. |
| **Step 6** | Switch-A /system/vm-mgmt/virtual-machine # **scope vnic** *mac-address* | Enters the command mode for the vNIC at the specified MAC address. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | Switch-A /system/vm-mgmt/virtual-machine/vnic # **create mon-src** *session-name* | Adds the vNIC as a source to the specified monitoring session. |
| **Step 8** | Switch-A /system/vm-mgmt/virtual-machine/vnic/mon-src # **set direction** {**both** \| **receive** \| **transmit**} | (Optional)<br>Specifies the traffic direction to be monitored. |
| **Step 9** | Switch-A /system/vm-mgmt/virtual-machine/vnic/mon-src # **commit-buffer** | Commits the transaction to the system configuration. |

The following example adds the ingress traffic on a dynamic vNIC as a source for a monitoring session and commits the transaction:

```
Switch-A# scope system
Switch-A /system # scope vm-mgmt
Switch-A /system/vm-mgmt # show virtual-machine
Virtual Machine:
    UUID: 42327c42-e00c-886f-e3f7-e615906f51e9
    Service Profile: org-root/ls-dsw-bld1-esx
    Server: sys/chassis-1/blade-1
    Status: Online
.
.
.
Switch-A /system/vm-mgmt # scope virtual-machine 42327c42-e00c-886f-e3f7-e615906f51e9
Switch-A /system/vm-mgmt/virtual-machine # show expand
Virtual Machine:
    UUID: 42327c42-e00c-886f-e3f7-e615906f51e9
    Service Profile: org-root/ls-dsw-bld1-esx
    Server: sys/chassis-1/blade-1
    Status: Online

    vNIC:
        Name:
        Status: Online
        MAC Address: 00:50:56:B2:00:00

        VIF:
            Vif Id: 32772
            Status: Online
            Phys Fabric ID: B
            Virtual Fabric:
Switch-A /system/vm-mgmt/virtual-machine # scope vnic 00:50:56:B2:00:00
Switch-A /system/vm-mgmt/virtual-machine/vnic # create mon-src Monitor23
Switch-A /system/vm-mgmt/virtual-machine/vnic/mon-src* # set direction receive
Switch-A /system/vm-mgmt/virtual-machine/vnic/mon-src* # commit-buffer

Switch-A /system/vm-mgmt/virtual-machine/vnic/mon-src #
```

## What to Do Next

You can add additional sources to the traffic monitoring session.

# Adding a VLAN or VSAN Source to a Monitoring Session

**Note** This procedure describes adding a VLAN as a source for a traffic monitoring session. To add a VSAN as a source, the following changes are required:

- Enter the **scope fc-uplink** command instead of the **scope eth-uplink** command in Step 1.
- Enter the **create vsan** command instead of the **create vlan** command in Step 3.

### Before You Begin

A traffic monitoring session must be created.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-uplink** | Enters Ethernet uplink command mode. |
| **Step 2** | UCS-A /eth-uplink # **scope fabric** {**a** \| **b**} | Enters uplink fabric mode for the specified fabric.<br>**Note** This step is required when adding a local VLAN as a source. To add a global VLAN as a source, omit this step. |
| **Step 3** | UCS-A /eth-uplink/fabric # **create vlan** *vlan-name vlan-id* | Creates a named VLAN, specifies the VLAN name and VLAN ID, and enters uplink VLAN mode. |
| **Step 4** | UCS-A /eth-uplink/fabric/vlan # **create mon-src** *session-name* | Adds the VLAN as a source to the specified monitoring session. |
| **Step 5** | UCS-A /eth-uplink/fabric/vlan/mon-src # **commit-buffer** | Commits the transaction to the system configuration. |

The following example adds a local VLAN as a source for an Ethernet monitoring session and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # create vlan vlan23 23
UCS-A /eth-uplink/fabric/vlan # create mon-src Monitor23
UCS-A /eth-uplink/fabric/vlan/mon-src* # commit-buffer
UCS-A /eth-uplink/fabric/vlan/mon-src #
```

### What to Do Next

You can add additional sources to the traffic monitoring session.

# Adding a Storage Port Source to a Monitoring Session

**Note** This procedure describes adding a Fibre Channel storage port as a source for a Fibre Channel traffic monitoring session. To add an FCoE storage port as a source for an Ethernet traffic monitoring session, enter the **create interface fcoe** command instead of the **create interface fc** command in Step 3.

### Before You Begin

A traffic monitoring session must be created.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope fc-storage** | Enters Fibre Channel storage port command mode. |
| **Step 2** | UCS-A /fc-storage # **scope fabric** {**a** \| **b**} | Enters Fibre Channel storage port fabric mode for the specified fabric. |
| **Step 3** | UCS-A /fc-storage/fabric # **create interface fc** *slot-num port-num* | Creates a Fibre Channel storage port interface and enters the interface command mode. |
| **Step 4** | UCS-A /fc-storage/fabric/fc # **create mon-src** *session-name* | Adds the storage port as a source to the specified monitoring session. |
| **Step 5** | UCS-A /fc-storage/fabric/fc/mon-src # **commit-buffer** | Commits the transaction to the system configuration. |

The following example adds a Fibre Channel storage port on port 3 of slot 2 as a source for a Fibre Channel monitoring session and commits the transaction:

```
UCS-A# scope fc-storage
UCS-A /fc-storage # scope fabric a
UCS-A /fc-storage/fabric # create interface fc 2 3
UCS-A /fc-storage/fabric/fc* # create mon-src Monitor23
UCS-A /fc-storage/fabric/fc/mon-src* # commit-buffer
UCS-A /fc-storage/fabric/fc/mon-src #
```

### What to Do Next

You can add additional sources to the traffic monitoring session.

# Activating a Traffic Monitoring Session

This procedure describes activating an Ethernet traffic monitoring session.

### Before You Begin

Configure a traffic monitoring session.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-traffic-mon** | Enters Ethernet traffic monitoring command mode. |
| **Step 2** | UCS-A /eth-traffic-mon # **scope fabric** {**a** \| **b**} | Enters traffic monitoring command mode for the specified fabric. |
| **Step 3** | UCS-A /eth-traffic-mon/fabric # **scope eth-mon-session** *session-name* | Enters the command mode of the traffic monitoring session with the specified name. |
| **Step 4** | UCS-A /eth-traffic-mon/fabric/eth-mon-session # **disable** \| **enable** | Disables or enables the traffic monitoring session. |
| **Step 5** | UCS-A /eth-traffic-mon/fabric/eth-mon-session # **commit-buffer** | Commits the transaction to the system configuration. |

When activated, the traffic monitoring session begins forwarding traffic to the destination as soon as a traffic source is configured.

The following example activates an Ethernet traffic monitoring session and commits the transaction:

```
UCS-A# scope eth-traffic-mon
UCS-A /eth-traffic-mon # scope fabric a
UCS-A /eth-traffic-mon/fabric # scope eth-mon-session Monitor33
UCS-A /eth-traffic-mon/fabric/eth-mon-session # enable
UCS-A /eth-traffic-mon/fabric/eth-mon-session* # commit-buffer
UCS-A /eth-traffic-mon/fabric/eth-mon-session # show

Ether Traffic Monitoring Session:
    Name       Admin State       Oper State   Oper State Reason
    ---------- ----------------- ------------ -----------------
    Monitor33  Enabled           Up           Active

UCS-A /eth-traffic-mon/fabric/eth-mon-session #
```

# Deleting a Traffic Monitoring Session

This procedure describes deleting an Ethernet traffic monitoring session.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-traffic-mon** | Enters Ethernet traffic monitoring command mode. |
| **Step 2** | UCS-A /eth-traffic-mon # **scope fabric** {**a** \| **b**} | Enters traffic monitoring command mode for the specified fabric. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | UCS-A /eth-traffic-mon/fabric # **delete eth-mon-session** *session-name* | Deletes the traffic monitoring session with the specified name. |
| **Step 4** | UCS-A /eth-traffic-mon/fabric # **commit-buffer** | Commits the transaction to the system configuration. |

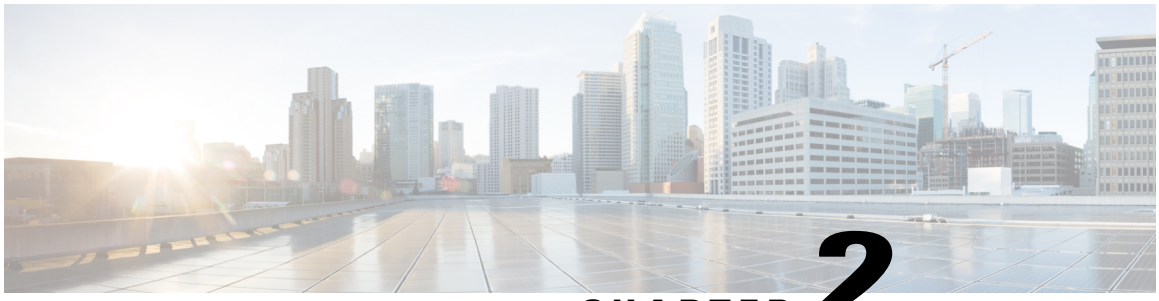
The following example deletes an Ethernet traffic monitoring session and commits the transaction:

```
UCS-A# scope eth-traffic-mon
UCS-A /eth-traffic-mon # scope fabric a
UCS-A /eth-traffic-mon/fabric # delete eth-mon-session Monitor33
UCS-A /eth-traffic-mon/fabric* # commit-buffer
UCS-A /eth-traffic-mon/fabric #
```

# SPAN restrictions for Cisco UCS Mini

Consider the following guidelines and restrictions when configuring the SPAN feature on Cisco UCS Mini

- FC port as SPAN destination is not supported.
- VSAN as SPAN source is not supported.
- FC uplink ports as SPAN source is not supported.



CHAPTER 2

# Monitoring Hardware

This chapter includes the following sections:


- Monitoring Fan Modules, page 13
- Monitoring Management Interfaces, page 15
- Local Storage Monitoring, page 18
- Graphics Cards Monitoring, page 24
- Managing Transportable Flash Module and Supercapacitor, page 25
- TPM Monitoring, page 26


## Monitoring Fan Modules

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope chassis** *chassis-num* | Enters chassis mode for the specified chassis. |
| **Step 2** | UCS-A /chassis # **show environment fan** | Displays the environment status for all fans within the chassis.<br>This includes the following information:<br>• Overall status<br>• Operability<br>• Power state<br>• Thermal status<br>• Threshold status<br>• Voltage status |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | UCS-A /chassis # **scope fan-module** *tray-num module-num* | Enters fan module chassis mode for the specified fan module.<br>**Note** Each chassis contains one tray, so the tray number in this command is always 1. |
| **Step 4** | UCS-A /chassis/fan-module # **show** [**detail** \| **expand**] | Displays the environment status for the specified fan module. |

The following example displays information about the fan modules in chassis 1:

```
UCS-A# scope chassis 1
UCS-A /chassis # show environment fan
Chassis 1:
    Overall Status: Power Problem
    Operability: Operable
    Power State: Redundancy Failed
    Thermal Status: Upper Non Recoverable

    Tray 1 Module 1:
        Threshold Status: OK
        Overall Status: Operable
        Operability: Operable
        Power State: On
        Thermal Status: OK
        Voltage Status: N/A

        Fan Module Stats:
             Ambient Temp (C): 25.000000

        Fan 1:
            Threshold Status: OK
            Overall Status: Operable
            Operability: Operable
            Power State: On
            Thermal Status: OK
            Voltage Status: N/A

        Fan 2:
            Threshold Status: OK
            Overall Status: Operable
            Operability: Operable
            Power State: On
            Thermal Status: OK
            Voltage Status: N/A

    Tray 1 Module 2:
        Threshold Status: OK
        Overall Status: Operable
        Operability: Operable
        Power State: On
        Thermal Status: OK
        Voltage Status: N/A

        Fan Module Stats:
             Ambient Temp (C): 24.000000

        Fan 1:
            Threshold Status: OK
            Overall Status: Operable
            Operability: Operable
            Power State: On
            Thermal Status: OK
            Voltage Status: N/A
```

```
    Fan 2:
        Threshold Status: OK
        Overall Status: Operable
        Operability: Operable
        Power State: On
        Thermal Status: OK
        Voltage Status: N/A
```

The following example displays information about fan module 2 in chassis 1:

```
UCS-A# scope chassis 1
UCS-A /chassis # scope fan-module 1 2
UCS-A /chassis/fan-module # show detail
Fan Module:
    Tray: 1
    Module: 2
    Overall Status: Operable
    Operability: Operable
    Threshold Status: OK
    Power State: On
    Presence: Equipped
    Thermal Status: OK
    Product Name: Fan Module for UCS 5108 Blade Server Chassis
    PID: N20-FAN5
    VID: V01
    Vendor: Cisco Systems Inc
    Serial (SN): NWG14350B6N
    HW Revision: 0
    Mfg Date: 1997-04-01T08:41:00.000
```

# Monitoring Management Interfaces

## Management Interfaces Monitoring Policy

This policy defines how the mgmt0 Ethernet interface on the fabric interconnect should be monitored. If Cisco UCS 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 disabled.

If the affected management interface belongs to a fabric interconnect which is the managing instance, Cisco UCS confirms that the subordinate fabric interconnect's status is up, that there are no current failure reports logged against it, and then modifies the managing instance for the endpoints.

If the affected fabric interconnect is currently the primary inside of a high availability setup, a failover of the management plane is triggered. The data plane is not affected by this failover.

You can set the following properties related to monitoring the management interface:

- Type of mechanism used to monitor the management interface.
- Interval at which the management interface's status is monitored.
- Maximum number of monitoring attempts that can fail before the system assumes that the management is unavailable and generates a fault message.

**Important** In the event of a management interface failure 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** Enter monitoring mode.
UCS-A# **scope monitoring**

**Step 2** Enable or disable the management interfaces monitoring policy.
UCS-A /monitoring # **set mgmt-if-mon-policy admin-state** {**enabled** | **disabled**}

**Step 3** Specify the number of seconds that the system should wait between data recordings.
UCS-A /monitoring # **set mgmt-if-mon-policy poll-interval**

Enter an integer between 90 and 300.

**Step 4** Specify the maximum number of monitoring attempts that can fail before the system assumes that the management interface is unavailable and generates a fault message.
UCS-A /monitoring # **set mgmt-if-mon-policy max-fail-reports** *num-mon-attempts*

Enter an integer between 2 and 5.

**Step 5** Specify the monitoring mechanism that you want the system to use.
UCS-A /monitoring # **set mgmt-if-mon-policy monitor-mechanism** {**mii-status** | **ping-arp-targets** | **ping-gateway**

- **mii-status —**The system monitors the availability of the Media Independent Interface (MII).
- **ping-arp-targets —**The system pings designated targets using the Address Resolution Protocol (ARP).
- **ping-gateway —**The system pings the default gateway address specified for this Cisco UCS domain in the management interface.

**Step 6** If you selected **mii-status** as your monitoring mechanism, configure the following properties:

a) Specify the number of seconds that the system should wait before requesting another response from the MII if a previous attempt fails.
UCS-A /monitoring # **set mgmt-if-mon-policy mii-retry-interval** *num-seconds*

Enter an integer between 3 and 10.

b) Specify the number of times that the system polls the MII until the system assumes that the interface is unavailable.
UCS-A /monitoring # **set mgmt-if-mon-policy mii-retry-count** *num-retries*

Enter an integer between 1 and 3.

**Step 7** If you selected **ping-arp-targets** as your monitoring mechanism, configure the following properties:

a) Specify the first IPv4 or IPv6 address the system pings.
UCS-A /monitoring # **set mgmt-if-mon-policy** {*arp-target1*|*ndisc-target1*} {*ipv4-addr*|*ipv6-addr*}

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.

b) Specify the second IPv4 or IPv6 address the system pings.
UCS-A /monitoring # **set mgmt-if-mon-policy** {*arp-target2*|*ndisc-target2*} {*ipv4-addr* |*ipv6-addr*}

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.

c) Specify the third IPv4 or IPv6 address the system pings.
UCS-A /monitoring # **set mgmt-if-mon-policy** {*arp-target3*|*ndisc-target3*} {*ipv4-addr* |*ipv6-addr*}

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.

**Note** The ping IPv4 ARP or IPv6 N-disc targets must be in the same subnet or prefix, respectively, as the fabric interconnect.

d) Specify the number of ARP requests to send to the target IP addresses.
UCS-A /monitoring # **set mgmt-if-mon-policy arp-requests** *num-requests*

Enter an integer between 1 and 5.

e) Specify the number of seconds to wait for responses from the ARP targets before the system assumes that they are unavailable.
UCS-A /monitoring # **set mgmt-if-mon-policy arp-deadline** *num-seconds*

Enter a number between 5 and 15.

**Step 8** If you selected **ping-gateway** as your monitoring mechanism, configure the following properties:

a) Specify the number of times the system should ping the gateway.
UCS-A /monitoring # **set mgmt-if-mon-policy ping-requests**

Enter an integer between 1 and 5.

b) Specify the number of seconds to wait for a response from the gateway until the system assumes that the address is unavailable.
UCS-A /monitoring # **set mgmt-if-mon-policy ping-deadline**

Enter an integer between 5 and 15.

**Step 9** UCS-A /monitoring # **commit-buffer**
Commits the transaction to the system configuration.

---

The following example creates a monitoring interface management policy using the Media Independent Interface (MII) monitoring mechanism and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # set mgmt-if-mon-policy admin-state enabled
UCS-A /monitoring* # set mgmt-if-mon-policy poll-interval 250
UCS-A /monitoring* # set mgmt-if-mon-policy max-fail-reports 2
UCS-A /monitoring* # set mgmt-if-mon-policy monitor-mechanism set mii-status
UCS-A /monitoring* # set mgmt-if-mon-policy mii-retry-count 3
```

```
UCS-A /monitoring* # set mgmt-if-mon-policy mii-retry-interval 7
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

# 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 (BBU), Transportable Flash Modules (TFM) and super-capacitors, FlexFlash controllers, and SD cards.

Cisco UCS Manager communicates directly with the LSI MegaRAID controllers and FlexFlash controllers using an out-of-band (OOB) 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.

  LSI storage controllers use a Transportable Flash Module (TFM) powered by a super-capacitor 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 might 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 C220 M3 rack server

- Cisco UCS C240 M3 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.

# 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/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 Flash Life Status

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** *chassis-id* / *server-id* | Enters chassis server mode for the specified server. |
| **Step 2** | UCS-A /chassis/server # **show raid-controller detail expand** | Displays details for the RAID controller. |

The following example shows how to display the flash life status for server 3:

```
UCS-A# scope server 1/3
UCS-A /chassis/server # show raid-controller detail expand

RAID Controller:
    ID: 1
    Type: FLASH
    PCI Addr: 131:00.0
    Vendor: Cisco Systems Inc
    Model: UCSC-F-FIO-1205M
    Serial: 1315D2B52
    HW Rev: FLASH
    Raid Support: No
    OOB Interface Supported: No
    Rebuild Rate: N/A
    Controller Status: Unknown

    Flash Life:
    Flash Percentage: N/A
    FLash Status: Error(244)

UCS-A /chassis/server #
```

# Viewing the Status of Local Storage Components

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** *chassis-id* / *server-id* | Enters chassis server mode for the specified server. |
| **Step 2** | UCS-A /chassis/server # **show inventory storage** | Displays the local and virtual storage information for the server. |

The following example shows how to display the local disk status for server 2:

```
UCS-A# scope server 1/2
UCS-A /chassis/server # show inventory storage
Server 1/2:
    Name:
    User Label:
    Equipped PID: UCSB-B200-M3
    Equipped VID: V01
    Equipped Serial (SN): FCH16207KXG
    Slot Status: Equipped
    Acknowledged Product Name: Cisco UCS B200 M3
    Acknowledged PID: UCSB-B200-M3
    Acknowledged VID: V01
    Acknowledged Serial (SN): FCH16207KXG
    Acknowledged Memory (MB): 98304
    Acknowledged Effective Memory (MB): 98304
    Acknowledged Cores: 12
    Acknowledged Adapters: 1
    Motherboard:
        Product Name: Cisco UCS B200 M3
        PID: UCSB-B200-M3
        VID: V01
        Vendor: Cisco Systems Inc
        Serial (SN): FCH16207KXG
        HW Revision: 0

        RAID Controller 1:
            Type: SAS
            Vendor: LSI Logic   Symbios Logic
            Model: LSI MegaRAID SAS 2004 ROMB
            Serial: LSIROMB-0
            HW Revision: B2
            PCI Addr: 01:00.0
            Raid Support: RAID0, RAID1
            OOB Interface Supported: Yes
            Rebuild Rate: 31
            Controller Status: Optimal

          Local Disk 1:
                Product Name: 146GB 6Gb SAS 10K RPM SFF HDD/hot plug/drive sled mounted
                PID: A03-D146GA2
                VID: V01
                Vendor: SEAGATE
                Model: ST9146803SS
                Vendor Description: Seagate Technology LLC
                Serial: 3SD31S4X
                HW Rev: 0
                Block Size: 512
                Blocks: 285155328
                Operability: Operable
```

```
            Oper Qualifier Reason: N/A
            Presence: Equipped
            Size (MB): 139236
            Drive State: Online
            Power State: Active
            Link Speed: 6 Gbps
            Device Type: HDD

        Local Disk 2:
            Product Name: 600G AL12SE SAS Hard Disk Drive
            PID: A03-D600GA2
            VID: V01
            Vendor: TOSHIBA
            Model: MBF2600RC
            Vendor Description: Toshiba Corporation
            Serial: EA00PB109T4A
            HW Rev: 0
            Block Size: 512
            Blocks: 1169920000
            Operability: Operable
            Oper Qualifier Reason: N/A
            Presence: Equipped
            Size (MB): 571250
            Drive State: Online
            Power State: Active
            Link Speed: 6 Gbps
            Device Type: HDD

        Local Disk Config Definition:
            Mode: RAID 1 Mirrored
            Description:
            Protect Configuration: No

        Virtual Drive 0:
            Type: RAID 1 Mirrored
            Block Size: 512
            Blocks: 285155328
            Operability: Operable
            Presence: Equipped
            Size (MB): 139236
            Lifecycle: Allocated
            Drive State: Optimal
            Strip Size (KB): 64
            Access Policy: Read Write
            Read Policy: Normal
            Configured Write Cache Policy: Write Through
            Actual Write Cache Policy: Write Through
            IO Policy: Direct
            Drive Cache: No Change
            Bootable: False

UCS-A /chassis/server #
```

# Viewing the Status of a Disk Drive

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope chassis** *chassis-num* | Enters chassis mode for the specified chassis. |
| **Step 2** | UCS-A /chassis # **scope server** *server-num* | Enters server chassis mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | UCS-A /chassis/server # **scope raid-controller** *raid-contr-id* {**sas** \| **sata**} | Enters RAID controller server chassis mode. |
| **Step 4** | UCS-A /chassis/server/raid-controller # **show local-disk** [*local-disk-id* \| **detail** \| **expand**] | |

The following example shows the status of a disk drive:

```
UCS-A# scope chassis 1
UCS-A /chassis # scope server 6
UCS-A /chassis/server # scope raid-controller 1 sas
UCS-A /chassis/server/raid-controller # show local-disk 1

Local Disk:
    ID: 1
    Block Size: 512
    Blocks: 60545024
    Size (MB): 29563
    Operability: Operable
    Presence: Equipped
```

# Viewing RAID Controller Operations

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** *chassis-id* / *server-id* | Enters chassis server mode for the specified server. |
| **Step 2** | UCS-A /chassis/server # **show raid-controller operation** | Displays the long running operations for the RAID controller. |

The following example shows how to display the RAID controller operations for server 3:

```
UCS-A# scope server 1/3
UCS-A /chassis/server # show raid-controller operation

    Name: Rebuild
    Affected Object: sys/chassis-1/blade-3/board/storage-SAS-1/disk-1
    State: In Progress
    Progress: 4
    Start Time: 2013-11-05T12:02:10.000
    End Time: N/A

UCS-A /chassis/server #
```

# Graphics Cards Monitoring

## Monitoring Graphics Cards

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

## Viewing Graphics Card Properties

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** *blade-id* | Enters server mode for the specified server. |
| **Step 2** | UCS-A /server # **show graphics-card detail** | Displays information about the graphics card. |

The following example shows how to display the graphics card properties on server 1:

```
UCS-A# scope server 1
UCS-A /server # show graphics-card

Graphics Card:
ID  Slot Id    Is Supported Firmware Version
--- ---------- ------------ ----------------
1   5          Yes          80.07.6D.00.13|2401.0502.00.02

UCS-A /server # show graphics-card detail

Graphics Card:
ID: 1
Slot Id: 5
Is Supported: Yes
Vendor: nVidia Corporation
Model: Nvidia GRID K1 P2401-502
Serial: NA
Firmware Version: 80.07.6D.00.13|2401.0502.00.02

UCS-A /server #
```

# Viewing Graphics Controller Properties

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** *blade-id* | Enters server mode for the specified server. |
| **Step 2** | UCS-A /server # **scope graphics-card** *card-id* | Enters graphics card mode for the specified graphics card. |
| **Step 3** | UCS-A /server/graphics-card # **show graphics-controller detail** | Displays information about the graphics controllers. |

The following example shows how to display the graphics controller properties for graphics card 1 on server 1:

```
UCS-A# scope server 1
UCS-A /server # scope graphics-card 1
UCS-A /server/graphics-card # show graphics-controller detail
Graphics Controller:
    ID: 1
    Pci Address: 07:00.0

    ID: 2
    Pci Address: 08:00.0
UCS-A /server/graphics-card #
```

# 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

### Supported Cisco UCS Servers for TFM and Supercap

The following Cisco UCS servers support TFM and supercap:

- Cisco UCS C220 M3 rack server
- Cisco UCS C240 M3 rack server

# 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

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A # **scope chassis** *chassis-num* | Enters chassis mode for the specified chassis. |
| **Step 2** | UCS-A /chassis #**scope server** *server-num* | Enters server chassis mode. |
| **Step 3** | UCS-A /chassis/server # **scope raid-controller** *raid-contr-id* {**flash** \| **sas** \| **sata** \| **sd** \| **unknown**} | Enters RAID controller server chassis mode. |
| **Step 4** | UCS-A /chassis/server/raid-controller # **show raid-battery expand** | Displays the RAID battery status. |

This example shows how to view information on the battery backup unit of a server:

```
UCS-A # scope chassis 1
UCS-A /chassis #scope server 3
UCS-A /chassis/server #scope raid-controller 1 sas
UCS-A /chassis/server/raid-controller # show raid-battery expand
RAID Battery:
    Battery Type: Supercap
    Presence: Equipped
    Operability: Operable
    Oper Qualifier Reason:
    Vendor: LSI
    Model: SuperCaP
    Serial: 0
    Capacity Percentage: Full
    Battery Temperature (C): 54.000000

    Transportable Flash Module:
        Presence: Equipped
        Vendor: Cisco Systems Inc
        Model: UCSB-RAID-1GBFM
        Serial: FCH164279W6
```

# TPM Monitoring

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

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

# Viewing TPM Properties

### Procedure

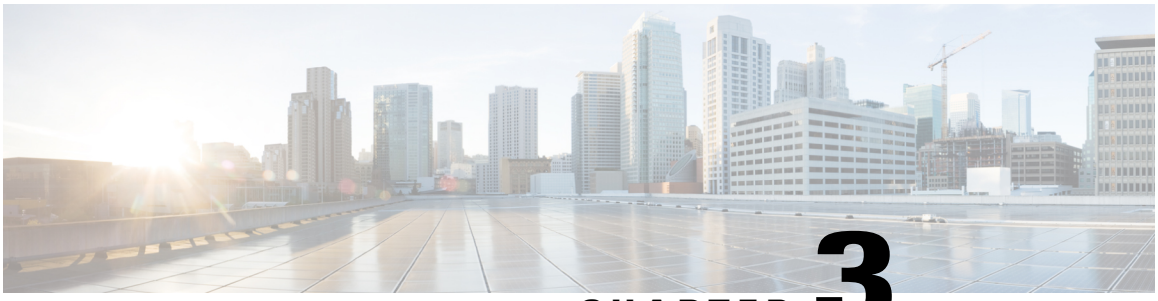
| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** *chassis-id* / *server-id* | Enters chassis server mode for the specified server. |
| **Step 2** | UCS-A /chassis/server # **scope tpm** *tpm-id* | Enters TPM mode for the specified TPM ID. |
| **Step 3** | UCS-A /chassis/server/tpm # **show** | Displays the TPM properties. |
| **Step 4** | UCS-A /chassis/server/tpm # **show detail** | Displays detailed TPM properties. |

The following example shows how to display the TPM properties for blade 3 in chassis 1:

```
UCS-A# scope server 1/3
UCS-A /chassis/server # scope tpm 1
UCS-A /chassis/server/tpm # show

Trusted Platform Module:
    Presence: Equipped
    Enabled Status: Enabled
    Active Status: Activated
    Ownership: Unowned
UCS-A /chassis/server/tpm # show detail

Trusted Platform Module:
    Enabled Status: Enabled
    Active Status: Activated
    Ownership: Unowned
    Tpm Revision: 1
    Model: UCSX-TPM1-001
    Vendor: Cisco Systems Inc
    Serial: FCH16167DBJ
UCS-A /chassis/server/tpm #
```



CHAPTER 3

# Configuring Statistics-Related Policies

This chapter includes the following sections:


- Configuring Statistics Collection Policies, page 29
- Configuring Statistics Threshold Policies, page 30


# Configuring Statistics Collection Policies

## Statistics Collection Policy

A statistics collection policy defines how frequently statistics are to be collected (collection interval) and how frequently the statistics are to be reported (reporting interval). Reporting intervals are longer than collection intervals so that multiple statistical data points can be collected during the reporting interval, which 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.

## Configuring a Statistics Collection Policy

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A/monitoring # **scope stats-collection-policy** {**adapter** \| **chassis** \| **host** \| **port** \| **server**} | Enters statistics collection policy mode for the specified policy type. |
| **Step 3** | UCS-A /monitoring/stats-collection-policy # **set collection-interval** {**1minute** \| **2minutes** \| **30seconds** \| **5minutes**} | Specifies the interval at which statistics are collected from the system. |
| **Step 4** | UCS-A /monitoring/stats-collection-policy # **set reporting-interval** {**15minutes** \| **30minutes** \| **60minutes**} | Specifies the interval at which collected statistics are reported. |
| **Step 5** | UCS-A /monitoring/stats-collection-policy # **commit-buffer** | Commits the transaction to the system configuration. |

The following example creates a statistics collection policy for ports, sets the collection interval to one minute, the reporting interval to 30 minutes, and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # scope stats-collection-policy port
UCS-A /monitoring/stats-collection-policy* # set collection-interval 1minute
UCS-A /monitoring/stats-collection-policy* # set reporting-interval 30minutes
UCS-A /monitoring/stats-collection-policy* # commit-buffer
UCS-A /monitoring/stats-collection-policy #
```

# 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.

# Server and Server Component Statistics Threshold Policy Configuration

## Configuring a Server and Server Component Statistics Threshold Policy

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | Enters organization mode for the specified organization. To enter the root organization mode, type **/** as the *org-name* . |
| **Step 2** | UCS-A /org # **create stats-threshold-policy** *policy-name* | Creates the specified statistics threshold policy and enters organization statistics threshold policy mode. |
| **Step 3** | UCS-A /org/stats-threshold-policy # **set descr** *description* | (Optional)<br>Provides a description for the policy.<br>**Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output. |
| **Step 4** | UCS-A /org/stats-threshold-policy # **commit-buffer** | Commits the transaction to the system configuration. |

The following example creates the server and server component statistics threshold policy named ServStatsPolicy, provides a description for the policy, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # create stats-threshold-policy ServStatsPolicy
UCS-A /org/stats-threshold-policy* # set descr "Server stats threshold policy."
UCS-A /org/stats-threshold-policy* # commit-buffer
UCS-A /org/stats-threshold-policy #
```

### What to Do Next

Configure one or more policy classes for the statistics threshold policy. For more information, see "Configuring a Server and Server Component Statistics Threshold Policy Class, on page 32."

# Deleting a Server and Server Component Statistics Threshold Policy

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* . |
| **Step 2** | UCS-A /org # **delete stats-threshold-policy** *policy-name* | Deletes the specified statistics threshold policy. |
| **Step 3** | UCS-A /org # **commit-buffer** | Commits the transaction to the system configuration. |

The following example deletes the server and server component statistics threshold policy named ServStatsPolicy and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # delete stats-threshold-policy ServStatsPolicy
UCS-A /org* # commit-buffer
UCS-A /org #
```

# Configuring a Server and Server Component Statistics Threshold Policy Class

### Before You Begin

Configure or identify the server and server component statistics threshold policy that will contain the policy class. For more information, see "Configuring a Server and Server Component Statistics Threshold Policy, on page 31."

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* . |
| **Step 2** | UCS-A /org # **scope stats-threshold-policy** *policy-name* | Enters organization statistics threshold policy mode. |
| **Step 3** | UCS-A /org/stats-threshold-policy # **create class** *class-name* | Creates the specified statistics threshold policy class and enters organization statistics threshold policy class mode. The *class-name* argument can be any of the class name keywords available for the particular statistics threshold policy being configured. To see a list of the available class name keywords, enter the **create class ?** command in organization statistics threshold policy mode.<br>**Note** You can configure multiple classes for the statistics threshold policy. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | UCS-A /org/stats-threshold-policy /class # **create property** *property-name* | Creates the specified statistics threshold policy class property and enters organization statistics threshold policy class property mode. The *property-name* argument can be any of the property name keywords available for the particular policy class being configured. To see a list of the available property name keywords, enter the **create property ?** command in organization statistics threshold policy class mode.<br>**Note** You can configure multiple properties for the policy class. |
| **Step 5** | UCS-A /org/stats-threshold-policy/class/property # **set normal-value** *value* | Specifies the normal value for the class property. The *value* format can vary depending on the class property being configured. To see the required format, enter the **set normal-value ?** command in organization statistics threshold policy class property mode. |
| **Step 6** | UCS-A /org/stats-threshold-policy /class/property # **create threshold-value** {**above-normal** \| **below-normal**} {**cleared** \| **condition** \| **critical** \| **info** \| **major** \| **minor** \| **warning**} | Creates the specified threshold value for the class property and enters organization statistics threshold policy class property threshold value mode.<br>**Note** You can configure multiple threshold values for the class property. |
| **Step 7** | UCS-A /org/stats-threshold-policy /class/property/threshold-value # **set** {**deescalating** \| **escalating**} *value* | Specifies the de-escalating or escalating class property threshold value. The *value* format can vary depending on the class property threshold value being configured. To see the required format, enter the **set deescalating ?** or **set escalating ?** command in organization statistics threshold policy class property threshold value mode.<br>**Note** You can specify both de-escalating and escalating class property threshold values. |
| **Step 8** | UCS-A /org/stats-threshold-policy /class/property/threshold-value # **commit-buffer** | Commits the transaction to the system configuration. |

The following example creates the server and server component statistics threshold policy class for CPU statistics, creates a CPU temperature property, specifies that the normal CPU temperature is 48.5° C, creates an above normal warning threshold of 50° C, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # scope stats-threshold-policy ServStatsPolicy
UCS-A /org/stats-threshold-policy* # create class cpu-stats
UCS-A /org/stats-threshold-policy/class* # create property cpu-temp
UCS-A /org/stats-threshold-policy/class/property* # set normal-value 48.5
UCS-A /org/stats-threshold-policy/class/property* # create threshold-value above-normal
warning
UCS-A /org/stats-threshold-policy/class/property/threshold-value* # set escalating 50.0
UCS-A /org/stats-threshold-policy/class/property/threshold-value* # commit-buffer
UCS-A /org/stats-threshold-policy/class/property/threshold-value #
```

## Deleting a Server and Server Component Statistics Threshold Policy Class

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* . |
| **Step 2** | UCS-A /org # **scope stats-threshold-policy** *policy-name* | Enters the specified statistics threshold policy. |
| **Step 3** | UCS-A /org/stats-threshold-policy # **delete class** *class-name* | Deletes the specified statistics threshold policy class from the policy. |
| **Step 4** | UCS-A /org/stats-threshold-policy # **commit-buffer** | Commits the transaction to the system configuration. |

The following example deletes the server and server component statistics threshold policy class for CPU statistics and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # scope stats-threshold-policy ServStatsPolicy
UCS-A /org/stats-threshold-policy* # delete class cpu-stats
UCS-A /org/stats-threshold-policy* # commit-buffer
UCS-A /org/stats-threshold-policy #
```

# Uplink Ethernet Port Statistics Threshold Policy Configuration

## Configuring an Uplink Ethernet Port Statistics Threshold Policy

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-uplink** | Enters Ethernet uplink mode. |
| **Step 2** | UCS-A /eth-uplink # **scope stats-threshold-policy default** | Enters Ethernet uplink statistics threshold policy mode.<br>**Note** You cannot create (or delete) an uplink Ethernet port statistics threshold policy. You can only enter (scope to) the existing default policy. |
| **Step 3** | UCS-A /eth-uplink/stats-threshold-policy # **set descr** *description* | (Optional)<br>Provides a description for the policy. |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output. |
| **Step 4** | UCS-A /eth-uplink/stats-threshold-policy # **commit-buffer** | Commits the transaction to the system configuration. |

The following example enters the default uplink Ethernet port threshold policy, provides a description for the policy, and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink* # scope stats-threshold-policy default
UCS-A /eth-uplink/stats-threshold-policy* # set descr "Uplink Ethernet port stats threshold
 policy."
UCS-A /eth-uplink/stats-threshold-policy* # commit-buffer
UCS-A /eth-uplink/stats-threshold-policy #
```

### What to Do Next

Configure one or more policy classes for the statistics threshold policy. For more information, see "Configuring an Uplink Ethernet Port Statistics Threshold Policy Class, on page 35."

## Configuring an Uplink Ethernet Port Statistics Threshold Policy Class

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-uplink** | Enters Ethernet uplink mode. |
| **Step 2** | UCS-A /eth-uplink # **scope stats-threshold-policy default** | Enters Ethernet uplink statistics threshold policy mode. |
| **Step 3** | UCS-A /eth-uplink/stats-threshold-policy # **create class** *class-name* | Creates the specified statistics threshold policy class and enters Ethernet uplink statistics threshold policy class mode. The *class-name* argument can be any of the class name keywords available for the particular statistics threshold policy being configured. To see a list of the available class name keywords, enter the **create class ?** command in Ethernet uplink statistics threshold policy mode.<br>**Note** You can configure multiple classes for the statistics threshold policy. |
| **Step 4** | UCS-A /eth-uplink/stats-threshold-policy /class # **create property** *property-name* | Creates the specified statistics threshold policy class property and enters Ethernet uplink statistics threshold policy class property mode. The *property-name* argument can be any of the property name keywords available for the particular policy class being configured. To see a list of the available property |

| | Command or Action | Purpose |
|---|---|---|
| | | name keywords, enter the **create property ?** command in Ethernet uplink statistics threshold policy class mode.<br>**Note** You can configure multiple properties for the policy class. |
| **Step 5** | UCS-A /eth-uplink/stats-threshold-policy /class/property # **set normal-value** *value* | Specifies the normal value for the class property. The *value* format can vary depending on the class property being configured. To see the required format, enter the **set normal-value ?** command in Ethernet uplink statistics threshold policy class property mode. |
| **Step 6** | UCS-A /eth-uplink/stats-threshold-policy /class/property # **create threshold-value** {**above-normal** \| **below-normal**} {**cleared** \| **condition** \| **critical** \| **info** \| **major** \| **minor** \| **warning**} | Creates the specified threshold value for the class property and enters Ethernet uplink statistics threshold policy class property threshold value mode.<br>**Note** You can configure multiple threshold values for the class property. |
| **Step 7** | UCS-A /eth-uplink/stats-threshold-policy /class/property/threshold-value # **set** {**deescalating** \| **escalating**} *value* | Specifies the de-escalating or escalating class property threshold value. The *value* format can vary depending on the class property threshold value being configured. To see the required format, enter the **set deescalating ?** or **set escalating ?** command in Ethernet uplink statistics threshold policy class property threshold value mode.<br>**Note** You can specify both de-escalating and escalating class property threshold values. |
| **Step 8** | UCS-A /eth-uplink/stats-threshold-policy /class/property/threshold-value # **commit-buffer** | Commits the transaction to the system configuration. |

The following example creates the uplink Ethernet port statistics threshold policy class for Ethernet error statistics, creates a cyclic redundancy check (CRC) error count property, specifies that the normal CRC error count for each polling interval is 1000, creates an above normal warning threshold of 1250, and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink* # scope stats-threshold-policy default
UCS-A /eth-uplink/stats-threshold-policy* # create class ether-error-stats
UCS-A /eth-uplink/stats-threshold-policy/class* # create property crc-delta
UCS-A /eth-uplink/stats-threshold-policy/class/property* # set normal-value 1000
UCS-A /eth-uplink/stats-threshold-policy/class/property* # create threshold-value above-normal
 warning
UCS-A /eth-uplink/stats-threshold-policy/class/property/threshold-value* # set escalating
1250
UCS-A /eth-uplink/stats-threshold-policy/class/property/threshold-value* # commit-buffer
UCS-A /eth-uplink/stats-threshold-policy/class/property/threshold-value #
```

### Deleting an Uplink Ethernet Port Statistics Threshold Policy Class

#### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-uplink** | Enters Ethernet uplink mode. |
| **Step 2** | UCS-A /eth-uplink # **scope stats-threshold-policy default** | Enters Ethernet uplink statistics threshold policy mode. |
| **Step 3** | UCS-A /eth-uplink/stats-threshold-policy # **delete class** *class-name* | Deletes the specified statistics threshold policy class from the policy. |
| **Step 4** | UCS-A /eth-uplink/stats-threshold-policy # **commit-buffer** | Commits the transaction to the system configuration. |

The following example deletes the uplink Ethernet port statistics threshold policy class for Ethernet error statistics and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope stats-threshold-policy default
UCS-A /eth-uplink/stats-threshold-policy # delete class ether-error-stats
UCS-A /eth-uplink/stats-threshold-policy* # commit-buffer
UCS-A /eth-uplink/stats-threshold-policy #
```

## Server Port, Chassis, and Fabric Interconnect Statistics Threshold Policy Configuration

### Configuring a Server Port, Chassis, and Fabric Interconnect Statistics Threshold Policy

#### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-server** | Enters Ethernet server mode. |
| **Step 2** | UCS-A /eth-server # **scope stats-threshold-policy default** | Enters Ethernet server statistics threshold policy mode.<br>**Note** You cannot create (or delete) a server port, chassis, and fabric interconnect statistics threshold policy. You can only enter (scope to) the existing default policy. |
| **Step 3** | UCS-A /eth-server/stats-threshold-policy # **set descr** *description* | (Optional)<br>Provides a description for the policy. |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output. |
| **Step 4** | UCS-A /eth-server/stats-threshold-policy # **commit-buffer** | Commits the transaction to the system configuration. |

The following example enters the default server port, chassis, and fabric interconnect statistics threshold policy, provides a description for the policy, and commits the transaction:

```
UCS-A# scope eth-server
UCS-A /eth-server* # scope stats-threshold-policy default
UCS-A /eth-server/stats-threshold-policy* # set descr "Server port, chassis, and fabric
interconnect stats threshold policy."
UCS-A /eth-server/stats-threshold-policy* # commit-buffer
UCS-A /eth-server/stats-threshold-policy #
```

### What to Do Next

Configure one or more policy classes for the statistics threshold policy. For more information, see "Configuring a Server Port, Chassis, and Fabric Interconnect Statistics Threshold Policy Class, on page 38."

## Configuring a Server Port, Chassis, and Fabric Interconnect Statistics Threshold Policy Class

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-server** | Enters Ethernet server mode. |
| **Step 2** | UCS-A /eth-server # **scope stats-threshold-policy default** | Enters Ethernet server statistics threshold policy mode. |
| **Step 3** | UCS-A /eth-server/stats-threshold-policy # **create class** *class-name* | Creates the specified statistics threshold policy class and enters Ethernet server statistics threshold policy class mode. The *class-name* argument can be any of the class name keywords available for the particular statistics threshold policy being configured. To see a list of the available class name keywords, enter the **create class ?** command in Ethernet server statistics threshold policy mode.<br>**Note** You can configure multiple classes for the statistics threshold policy. |
| **Step 4** | UCS-A /eth-server/stats-threshold-policy /class # **create property** *property-name* | Creates the specified statistics threshold policy class property and enters Ethernet server statistics threshold policy class property mode. The *property-name* argument can be any of the property name keywords available for the particular policy class being configured. To see a list of the available property |

| | Command or Action | Purpose |
|---|---|---|
| | | name keywords, enter the **create property ?** command in Ethernet server statistics threshold policy class mode.<br>**Note** You can configure multiple properties for the policy class. |
| **Step 5** | UCS-A /eth-server/stats-threshold-policy /class/property # **set normal-value** *value* | Specifies the normal value for the class property. The *value* format can vary depending on the class property being configured. To see the required format, enter the **set normal-value ?** command in Ethernet server statistics threshold policy class property mode. |
| **Step 6** | UCS-A /eth-server/stats-threshold-policy /class/property # **create threshold-value** {**above-normal** \| **below-normal**} {**cleared** \| **condition** \| **critical** \| **info** \| **major** \| **minor** \| **warning**} | Creates the specified threshold value for the class property and enters Ethernet server statistics threshold policy class property threshold value mode.<br>**Note** You can configure multiple threshold values for the class property. |
| **Step 7** | UCS-A /eth-server/stats-threshold-policy /class/property/threshold-value # **set** {**deescalating** \| **escalating**} *value* | Specifies the de-escalating or escalating class property threshold value. The *value* format can vary depending on the class property threshold value being configured. To see the required format, enter the **set deescalating ?** or **set escalating ?** command in Ethernet server statistics threshold policy class property threshold value mode.<br>**Note** You can specify both de-escalating and escalating class property threshold values. |
| **Step 8** | UCS-A /eth-server/stats-threshold-policy /class/property/threshold-value # **commit-buffer** | Commits the transaction to the system configuration. |

The following example creates the server port, chassis, and fabric interconnect statistics threshold policy class for chassis statistics, creates an input power (Watts) property, specifies that the normal power is 8kW, creates an above normal warning threshold of 11kW, and commits the transaction:

```
UCS-A# scope eth-server
UCS-A /eth-server* # scope stats-threshold-policy default
UCS-A /eth-server/stats-threshold-policy* # create class chassis-stats
UCS-A /eth-server/stats-threshold-policy/class* # create property input-power
UCS-A /eth-server/stats-threshold-policy/class/property* # set normal-value 8000.0
UCS-A /eth-server/stats-threshold-policy/class/property* # create threshold-value above-normal
 warning
UCS-A /eth-server/stats-threshold-policy/class/property/threshold-value* # set escalating
11000.0
UCS-A /eth-server/stats-threshold-policy/class/property/threshold-value* # commit-buffer
UCS-A /eth-server/stats-threshold-policy/class/property/threshold-value #
```

## Deleting a Server Port, Chassis, and Fabric Interconnect Statistics Threshold Policy Class

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-server** | Enters Ethernet server mode. |
| **Step 2** | UCS-A /eth-server # **scope stats-threshold-policy default** | Enters Ethernet server statistics threshold policy mode. |
| **Step 3** | UCS-A /eth-server/stats-threshold-policy # **delete class** *class-name* | Deletes the specified statistics threshold policy class from the policy. |
| **Step 4** | UCS-A /eth-server/stats-threshold-policy # **commit-buffer** | Commits the transaction to the system configuration. |

The following example deletes the server port, chassis, and fabric interconnect statistics threshold policy class for chassis statistics and commits the transaction:

```
UCS-A# scope eth-server
UCS-A /eth-server* # scope stats-threshold-policy default
UCS-A /eth-server/stats-threshold-policy* # delete class chassis-stats
UCS-A /eth-server/stats-threshold-policy* # commit-buffer
UCS-A /eth-server/stats-threshold-policy #
```

# Fibre Channel Port Statistics Threshold Policy Configuration

## Configuring a Fibre Channel Port Statistics Threshold Policy

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope fc-uplink** | Enters Fibre Channel uplink mode. |
| **Step 2** | UCS-A /fc-uplink # **scope stats-threshold-policy default** | Enters Fibre Channel uplink statistics threshold policy mode.<br>**Note** You cannot create (or delete) an uplink Fibre Channel port statistics threshold policy. You can only enter (scope to) the existing default policy. |
| **Step 3** | UCS-A /fc-uplink/stats-threshold-policy # **set descr** *description* | (Optional)<br>Provides a description for the policy.<br>**Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | UCS-A /fc-uplink/stats-threshold-policy # **commit-buffer** | Commits the transaction to the system configuration. |

The following example enters the default uplink Fibre Channel port statistics threshold policy, provides a description for the policy, and commits the transaction:

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink* # scope stats-threshold-policy default
UCS-A /fc-uplink/stats-threshold-policy* # set descr "Uplink Fibre Channel stats threshold
 policy."
UCS-A /fc-uplink/stats-threshold-policy* # commit-buffer
UCS-A /fc-uplink/stats-threshold-policy #
```

### What to Do Next

Configure one or more policy classes for the statistics threshold policy. For more information, see "Configuring a Fibre Channel Port Statistics Threshold Policy Class, on page 41."

## Configuring a Fibre Channel Port Statistics Threshold Policy Class

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope fc-uplink** | Enters Fibre Channel uplink mode. |
| **Step 2** | UCS-A /fc-uplink # **scope stats-threshold-policy default** | Enters Fibre Channel uplink statistics threshold policy mode. |
| **Step 3** | UCS-A /fc-uplink/stats-threshold-policy # **create class** *class-name* | Creates the specified statistics threshold policy class and enters Fibre Channel uplink statistics threshold policy class mode. The *class-name* argument can be any of the class name keywords available for the particular statistics threshold policy being configured. To see a list of the available class name keywords, enter the **create class ?** command in Fibre Channel uplink statistics threshold policy mode.<br>**Note** You can configure multiple classes for the statistics threshold policy. |
| **Step 4** | UCS-A /fc-uplink/stats-threshold-policy /class # **create property** *property-name* | Creates the specified statistics threshold policy class property and enters Fibre Channel uplink statistics threshold policy class property mode. The *property-name* argument can be any of the property name keywords available for the particular policy class being configured. To see a list of the available property name keywords, enter the **create property ?** command in Fibre Channel uplink statistics threshold policy class mode.<br>**Note** You can configure multiple properties for the policy class. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | UCS-A /fc-uplink/stats-threshold-policy /class/property # **set normal-value** *value* | Specifies the normal value for the class property. The *value* format can vary depending on the class property being configured. To see the required format, enter the **set normal-value ?** command in Fibre Channel uplink statistics threshold policy class property mode. |
| **Step 6** | UCS-A /fc-uplink/stats-threshold-policy /class/property # **create threshold-value** {**above-normal** \| **below-normal**} {**cleared** \| **condition** \| **critical** \| **info** \| **major** \| **minor** \| **warning**} | Creates the specified threshold value for the class property and enters Fibre Channel uplink statistics threshold policy class property threshold value mode.<br>**Note** You can configure multiple threshold values for the class property. |
| **Step 7** | UCS-A /fc-uplink/stats-threshold-policy /class/property/threshold-value # **set** {**deescalating** \| **escalating**} *value* | Specifies the de-escalating or escalating class property threshold value. The *value* format can vary depending on the class property threshold value being configured. To see the required format, enter the **set deescalating ?** or **set escalating ?** command in Fibre Channel uplink statistics threshold policy class property threshold value mode.<br>**Note** You can specify both de-escalating and escalating class property threshold values. |
| **Step 8** | UCS-A /fc-uplink/stats-threshold-policy /class/property/threshold-value # **commit-buffer** | Commits the transaction to the system configuration. |

The following example creates the uplink Fibre Channel port statistics threshold policy class for Fibre Channel statistics, creates an average bytes received property, specifies that the normal average number of bytes received for each polling interval is 150MB, creates an above normal warning threshold of 200MB, and commits the transaction:

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink* # scope stats-threshold-policy default
UCS-A /fc-uplink/stats-threshold-policy* # create class fc-stats
UCS-A /fc-uplink/stats-threshold-policy/class* # create property bytes-rx-avg
UCS-A /fc-uplink/stats-threshold-policy/class/property* # set normal-value 150000000
UCS-A /fc-uplink/stats-threshold-policy/class/property* # create threshold-value above-normal
 warning
UCS-A /fc-uplink/stats-threshold-policy/class/property/threshold-value* # set escalating
200000000
UCS-A /fc-uplink/stats-threshold-policy/class/property/threshold-value* # commit-buffer
UCS-A /fc-uplink/stats-threshold-policy/class/property/threshold-value #
```

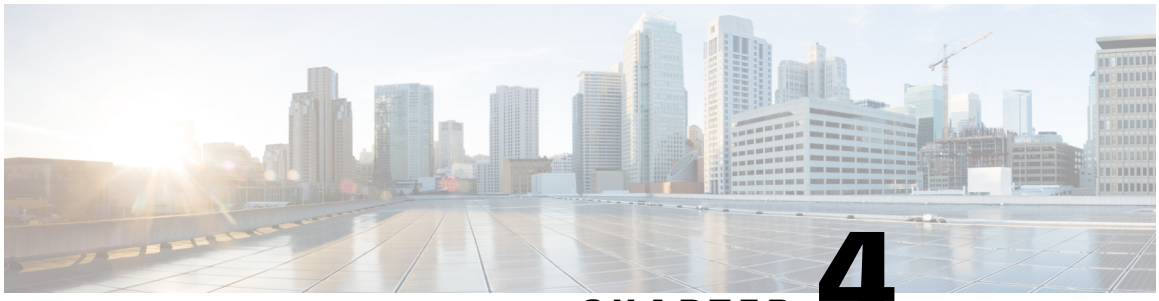
# Deleting an Uplink Fibre Channel Port Statistics Threshold Policy Class

## Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope fc-uplink** | Enters Fibre Channel uplink mode. |
| **Step 2** | UCS-A /fc-uplink # **scope stats-threshold-policy default** | Enters Fibre Channel uplink statistics threshold policy mode. |
| **Step 3** | UCS-A /fc-uplink/stats-threshold-policy # **delete class** *class-name* | Deletes the specified statistics threshold policy class from the policy. |
| **Step 4** | UCS-A /fc-uplink/stats-threshold-policy # **commit-buffer** | Commits the transaction to the system configuration. |

The following example deletes the uplink Fibre Channel port statistics threshold policy class for Fibre Channel statistics and commits the transaction:

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope stats-threshold-policy default
UCS-A /fc-uplink/stats-threshold-policy # delete class fc-stats
UCS-A /fc-uplink/stats-threshold-policy* # commit-buffer
UCS-A /fc-uplink/stats-threshold-policy #
```



CHAPTER 4

# Configuring Call Home

This chapter includes the following sections:


- Call Home, page 45
- Call Home Considerations and Guidelines, page 47
- Cisco UCS Faults and Call Home Severity Levels, page 48
- Cisco Smart Call Home, page 49
- Anonymous Reporting, page 50
- Configuring Call Home, page 50
- Disabling Call Home, page 52
- Enabling Call Home, page 53
- Configuring System Inventory Messages, page 53
- Configuring Call Home Profiles, page 55
- Sending a Test Call Home Alert, page 58
- Configuring Call Home Policies, page 59
- Configuring Anonymous Reporting, page 61
- Example: Configuring Call Home for Smart Call Home, page 64


## Call Home

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.

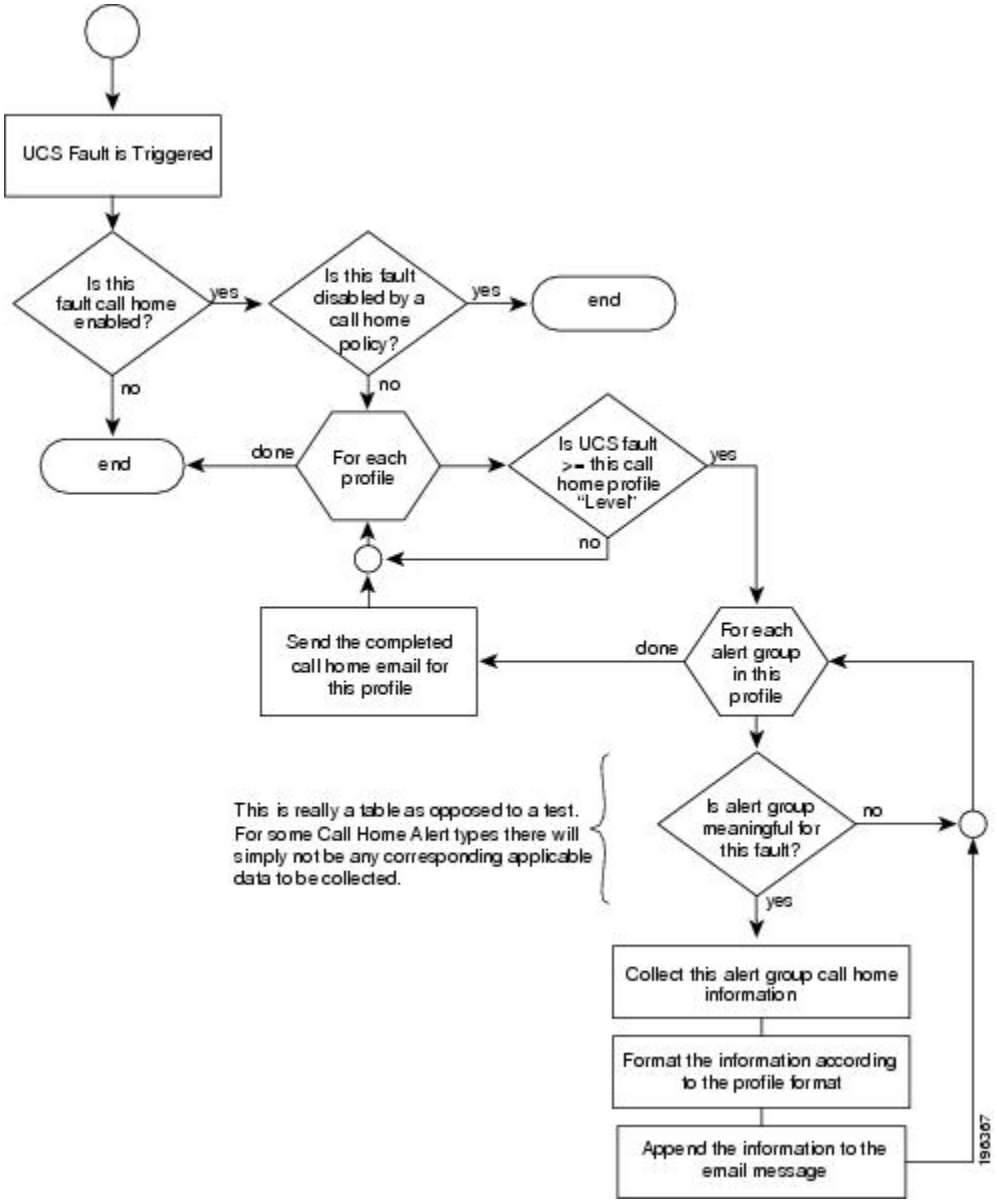
Cisco UCS delivers Call Home messages in the following formats:

- 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:

***Figure 1: Flow of Events after a Fault is Triggered***




# 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 depend 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 may 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 Cisco UCS Manager in a cluster configuration is never the source of the email.

### 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 developed 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 1: Mapping of Faults and Call Home Severity Levels***

| Call Home Severity | Cisco UCS Fault | Call Home Meaning |
|---|---|---|
| (9) Catastrophic | N/A | Network-wide catastrophic failure. |
| (8) Disaster | N/A | Significant network impact. |
| (7) Fatal | N/A | System is unusable. |

| Call Home Severity | Cisco UCS Fault | Call Home Meaning |
|---|---|---|
| (6) Critical | Critical | Critical conditions, immediate attention needed. |
| (5) Major | Major | Major conditions. |
| (4) Minor | Minor | Minor conditions. |
| (3) Warning | Warning | Warning conditions. |
| (2) Notification | Info | Basic notifications and informational messages. Possibly independently insignificant. |
| (1) Normal | Clear | Normal event, signifying a return to normal state. |
| (0) debug | N/A | Debugging messages. |

# 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.

**Note** Using Smart Call Home requires the following:

- A CCO ID associated with a corresponding Cisco Unified Computing Support Service or Cisco Unified Computing Mission Critical Support Service contract for your company.
- 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.

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

To configure Smart Call Home, you must 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 CCO 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 CCO.

# Anonymous Reporting

After you upgrade to the latest release of Cisco UCS Manger, 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.

# Configuring Call Home

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **enable** | Enables Call Home. |
| **Step 4** | UCS-A /monitoring/callhome # **set contact** *name* | Specifies the name of the main Call Home contact person. |
| **Step 5** | UCS-A /monitoring/callhome # **set email** *email-addr* | Specifies the email address of the main Call Home contact person.<br>**Note** If an email address includes special characters, such as # (hash), spaces, or & (ampersand), the email server may 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. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | UCS-A /monitoring/callhome # **set phone-contact** *phone-num* | Specifies the phone number of the main Call Home contact person. The phone number must be in international format, starting with a + (plus sign) and a country code. |
| **Step 7** | UCS-A /monitoring/callhome # **set street-address** *street-addr* | Specifies the street address of the main Call Home contact person.<br>Enter up to 255 ASCII characters. |
| **Step 8** | UCS-A /monitoring/callhome # **set customer-id** *id-num* | Specifies the CCO identification number that includes the contract numbers for the support contract in its entitlements. The number can be up to 255 alphanumeric characters in free format. |
| **Step 9** | UCS-A /monitoring/callhome # **set contract-id** *id-num* | Specifies the contract identification number from the service agreement. The number can be up to 255 alphanumeric characters in free format. |
| **Step 10** | UCS-A /monitoring/callhome # **set site-id** *id-num* | Specifies the site identification number from the service agreement. The number can be up to 255 alphanumeric characters in free format. |
| **Step 11** | UCS-A /monitoring/callhome # **set from-email** *email-addr* | Specifies the email address to use for the From field in Call Home messages. |
| **Step 12** | UCS-A /monitoring/callhome # **set reply-to-email** *email-addr* | Specifies the email address to use for the Reply To field in Call Home messages. |
| **Step 13** | UCS-A /monitoring/callhome # **set hostname** {*hostname* \| *ip-addr*\|*ip6-addr*} | Specifies the hostname, IPv4 or IPv6 address of the SMTP server that Call Home uses to send email messages. |
| **Step 14** | UCS-A /monitoring/callhome # **set port** *port-num* | Specifies the SMTP server port that Call Home uses to send email messages. Valid port numbers are 1 to 65535. |
| **Step 15** | UCS-A /monitoring/callhome # **set throttling** {**off** \| **on**} | Enables or disables Call Home throttling. When enabled, throttling prevents too many Call Home email messages from being sent for the same event. By default, throttling is enabled. |
| **Step 16** | UCS-A /monitoring/callhome # **set urgency** {**alerts** \| **critical** \| **debugging** \| **emergencies** \| **errors** \| **information** \| **notifications** \| **warnings**} | Specifies the urgency level for Call Home email messages. In the context of a large UCS deployment with several pairs of fabric interconnects, the urgency level potentially allows you to attach significance to Call Home messages from one particular Cisco UCS domain versus another. In the context of a small UCS deployment involving only two fabric interconnects, the urgency level holds little meaning. |
| **Step 17** | UCS-A /monitoring/callhome # **commit-buffer** | Commits the transaction to the system configuration. |

The following example configures Call Home with and IPv4 hostname and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring* # scope callhome
UCS-A /monitoring/callhome* # enable
UCS-A /monitoring/callhome* # set contact "Steve Jones"
UCS-A /monitoring/callhome* # set email admin@MyCompany.com
UCS-A /monitoring/callhome* # set phone-contact +1-001-408-555-1234
UCS-A /monitoring/callhome* # set street-address "123 N. Main Street, Anytown, CA, 99885"
UCS-A /monitoring/callhome* # set customer-id 1234567
UCS-A /monitoring/callhome* # set contract-id 99887766
UCS-A /monitoring/callhome* # set site-id 5432112
UCS-A /monitoring/callhome* # set from-email person@MyCompany.com
UCS-A /monitoring/callhome* # set reply-to-email person@MyCompany.com
UCS-A /monitoring/callhome* # set hostname 192.168.100.12
UCS-A /monitoring/callhome* # set port 25
UCS-A /monitoring/callhome* # set throttling on
UCS-A /monitoring/callhome* # set urgency information
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

The following example configures Call Home with and IPv6 hostname and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring* # scope callhome
UCS-A /monitoring/callhome* # enable
UCS-A /monitoring/callhome* # set contact "Steve Jones"
UCS-A /monitoring/callhome* # set email admin@MyCompany.com
UCS-A /monitoring/callhome* # set phone-contact +1-001-408-555-1234
UCS-A /monitoring/callhome* # set street-address "123 N. Main Street, Anytown, CA, 99885"
UCS-A /monitoring/callhome* # set customer-id 1234567
UCS-A /monitoring/callhome* # set contract-id 99887766
UCS-A /monitoring/callhome* # set site-id 5432112
UCS-A /monitoring/callhome* # set from-email person@MyCompany.com
UCS-A /monitoring/callhome* # set reply-to-email person@MyCompany.com
UCS-A /monitoring/callhome* # set hostname 2001::25
UCS-A /monitoring/callhome* # set port 25
UCS-A /monitoring/callhome* # set throttling on
UCS-A /monitoring/callhome* # set urgency information
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

# Disabling Call Home

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **disable** | Enables Call Home. |
| **Step 4** | UCS-A /monitoring/callhome # **commit-buffer** | Commits the transaction to the system configuration. |

The following example disables Call Home and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # disable
```

```
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

# Enabling Call Home

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **enable** | Enables Call Home. |
| **Step 4** | UCS-A /monitoring/callhome # **commit-buffer** | Commits the transaction to the system configuration. |

The following example enables Call Home and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # enable
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

# Configuring System Inventory Messages

## Configuring System Inventory Messages

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **scope inventory** | Enters monitoring call home inventory mode. |
| **Step 4** | UCS-A /monitoring/callhome/inventory # **set send-periodically** {**off** \| **on**} | Enables or disables the sending of inventory messages. When the **on** keyword is specified, inventory messages are automatically sent to the Call Home database. |
| **Step 5** | UCS-A /monitoring/callhome/inventory # **set interval-days** *interval-num* | Specifies the time interval (in days) at which inventory messages will be sent. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | UCS-A /monitoring/callhome/inventory # **set timeofday-hour** *hour* | Specifies the hour (using 24-hour format) that inventory messages are sent. |
| **Step 7** | UCS-A /monitoring/callhome/inventory # **set timeofday-minute** *minute* | Specifies the number of minutes after the hour that inventory messages are sent. |
| **Step 8** | UCS-A /monitoring/callhome/inventory # **commit-buffer** | Commits the transaction to the system configuration. |

The following example configures Call Home system inventory messages and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring* # scope callhome
UCS-A /monitoring/callhome* # scope inventory
UCS-A /monitoring/callhome/inventory* # set send-periodically on
UCS-A /monitoring/callhome/inventory* # set interval-days 15
UCS-A /monitoring/callhome/inventory* # set timeofday-hour 21
UCS-A /monitoring/callhome/inventory* # set timeofday-minute 30
UCS-A /monitoring/callhome/inventory* # commit-buffer
UCS-A /monitoring/callhome/inventory #
```

# 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

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **scope inventory** | Enters monitoring call home inventory mode. |
| **Step 4** | UCS-A /monitoring/callhome/inventory # **send** | Sends the system inventory message to the Call Home database. |

The following example sends the system inventory message to the Call Home database:

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # scope inventory
UCS-A /monitoring/callhome/inventory* # send
```

# 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. However, 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 sends Call Home alerts to e-mail destinations in a destination profile only if that Call Home alert belongs to one of the alert groups associated with that destination profile and 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 generates fits into a category represented by an alert group. The following table describes those alert groups:

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

# Configuring 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

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **create profile** *profile-name* | Enters monitoring call home profile mode. |
| **Step 4** | UCS-A /monitoring/callhome/profile # **set level** {**critical** \| **debug** \| **disaster** \| **fatal** \| **major** \| **minor** \| **normal** \| **notification** \| **warning**} | Specifies the event level for the profile. Each profile can have its own unique event level.<br>Cisco UCS faults that are greater than or equal to the event level will trigger this profile. |
| **Step 5** | UCS-A /monitoring/callhome/profile # **set alertgroups** *group-name*<br>• **ciscotac**<br>• **diagnostic**<br>• **environmental**<br>• **inventory**<br>• **license**<br>• **lifecycle**<br>• **linecard**<br>• **supervisor**<br>• **syslogport**<br>• **system**<br>• **test** | Specifies one or more groups that are alerted based on the profile. The *group-name* argument can be one or more of the following keywords entered on the same command line: |
| **Step 6** | UCS-A /monitoring/callhome/profile # **add alertgroups** *group-names* | (Optional)<br>Adds one or more groups to the existing list of groups that are alerted based on the Call Home profile.<br>**Note** You must use the **add alertgroups** command to add more alert groups to the existing alert group list. Using the **set alertgroups** command will replace any pre-existing alert groups with a new group list. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | UCS-A /monitoring/callhome/profile # **set format** {**shorttxt** \| **xml**} | Specifies the formatting method to use for the e-mail messages. |
| **Step 8** | UCS-A /monitoring/callhome/profile # **set maxsize** *id-num* | Specifies the maximum size (in characters) of the email message. |
| **Step 9** | UCS-A /monitoring/callhome/profile # **create destination** *email-addr* | Specifies the email address to which Call Home alerts should be sent. Use multiple **create destination** commands in monitoring call home profile mode to specify multiple email recipients. Use the **delete destination** command in monitoring call home profile mode to delete a specified email recipient. |
| **Step 10** | UCS-A /monitoring/callhome/profile/destination # **commit-buffer** | Commits the transaction to the system configuration. |

The following example configures a Call Home profile and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring* # scope callhome
UCS-A /monitoring/callhome* # create profile TestProfile
UCS-A /monitoring/callhome/profile* # set level normal
UCS-A /monitoring/callhome/profile* # set alertgroups test diagnostic
UCS-A /monitoring/callhome/profile* # set format xml
UCS-A /monitoring/callhome/profile* # set maxsize 100000
UCS-A /monitoring/callhome/profile* # create destination admin@MyCompany.com
UCS-A /monitoring/callhome/profile/destination* # commit-buffer
UCS-A /monitoring/callhome/profile/destination #
```

# Deleting a Call Home Profile

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **delete profile** *profile-name* | Deletes the specified profile. |
| **Step 4** | UCS-A /monitoring/callhome # **commit-buffer** | Commits the transaction to the system configuration. |

The following example deletes the Call Home profile named TestProfile and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
```

```
UCS-A /monitoring/callhome # delete profile TestProfile
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

# Sending a Test Call Home Alert

### Before You Begin

Configure Call Home and a Call Home Profile.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **send-test-alert** {[**alert-group** {**diagnostic** \| **environmental**}] [**alert-level** {**critical** \| **debug** \| **fatal** \| **major** \| **minor** \| **normal** \| **notify** \| **warning**}] [**alert-message-type** {**conf** \| **diag** \| **env** \| **inventory** \| **syslog** \| **test**}] [**alert-message-subtype** {**delta** \| **full** \| **goldmajor** \| **goldminor** \| **goldnormal** \| **major** \| **minor** \| **nosubtype** \| **test**}] [**alert-description** *description*]} | Sends a test Call Home alert. The test Call Home alert must specify all **alert-*** parameters or Cisco UCS Manager cannot generate the test message. The **alert-*** parameters include the following:<br>• **alert-description—**Alert description<br>• **alert-group—**Alert group<br>• **alert-level—**Event severity level<br>• **alert-message-type—**Message type<br>• **alert-message-subtype—**Message subtype<br>When a test Call Home alert is sent, Call Home responds as it would to any other alert and delivers it to the configured destination email addresses. |

The following example sends a test Call Home alert to the configured destination email address of the environmental alert group:

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # send-test-alert alert-group diagnostic
alert-level critical alert-message-type test alert-message-subtype major
alert-description "This is a test alert"
```

# 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. However, you can configure Cisco UCS not to process certain types.

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

## Configuring a Call Home Policy

**Tip** By default, email alerts are sent for all critical system events. However, you can optionally configure Call Home policies to enable or disable sending email alerts for other critical system events.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **create policy** {**equipment-inoperable** \| **fru-problem** \| **identity-unestablishable** \| **thermal-problem** \| **voltage-problem**} | Creates the specified policy and enters monitoring call home policy mode. |
| **Step 4** | UCS-A /monitoring/callhome/policy # {**disabled** \| **enabled**} | Disables or enables the sending of email alerts for the specified policy. |
| **Step 5** | UCS-A /monitoring/callhome/policy # **commit-buffer** | Commits the transaction to the system configuration. |

The following example creates a Call Home policy that disables the sending of email alerts for system events pertaining to voltage problems and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring* # scope callhome
UCS-A /monitoring/callhome* # create policy voltage-problem
UCS-A /monitoring/callhome/policy* # disabled
UCS-A /monitoring/callhome/policy* # commit-buffer
UCS-A /monitoring/callhome/policy #
```

# Disabling a Call Home Policy

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **scope policy** {**equipment-inoperable** \| **fru-problem** \| **identity-unestablishable** \| **thermal-problem** \| **voltage-problem**} | Enters monitoring call home policy mode for the specified policy. |
| **Step 4** | UCS-A /monitoring/callhome/policy # **disable** | Disables the specified policy. |
| **Step 5** | UCS-A /monitoring/callhome/policy # **commit-buffer** | Commits the transaction to the system configuration. |

The following example disables the Call Home policy named voltage-problem and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # scope policy voltage-problem
UCS-A /monitoring/callhome/policy # disable
UCS-A /monitoring/callhome/policy* # commit-buffer
UCS-A /monitoring/callhome/policy #
```

# Enabling a Call Home Policy

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **scope policy** {**equipment-inoperable** \| **fru-problem** \| **identity-unestablishable** \| **thermal-problem** \| **voltage-problem**} | Enters monitoring call home policy mode for the specified policy. |
| **Step 4** | UCS-A /monitoring/callhome/policy # **enable** | Enables the specified policy. |
| **Step 5** | UCS-A /monitoring/callhome/policy # **commit-buffer** | Commits the transaction to the system configuration. |

The following example enables the Call Home policy named voltage-problem and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # scope policy voltage-problem
UCS-A /monitoring/callhome/policy # enable
UCS-A /monitoring/callhome/policy* # commit-buffer
UCS-A /monitoring/callhome/policy #
```

## Deleting a Call Home Policy

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **delete policy** {**equipment-inoperable** \| **fru-problem** \| **identity-unestablishable** \| **thermal-problem** \| **voltage-problem**} | Deletes the specified policy |
| **Step 4** | UCS-A /monitoring/callhome # **commit-buffer** | Commits the transaction to the system configuration. |

The following example deletes the Call Home policy named voltage-problem and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # delete policy voltage-problems
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

# Configuring Anonymous Reporting

## Enabling Anonymous Reporting

You can enable anonymous reporting on the call home server.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A # **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A/monitoring # **scope callhome** | Enters monitoring call home mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | UCS-A/monitoring/callhome # **show anonymous-reporting** | (Optional)<br>Displays if anonymous reporting is enabled or disabled. |
| **Step 4** | UCS-A/monitoring/callhome # **enable anonymous-reporting** | Enables anonymous reporting on Smart Call Home. |
| **Step 5** | UCS-A/monitoring/callhome # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to enable anonymous reporting on the Call Home server:

```
UCS-A # scope monitoring
UCS-A/monitoring #scope callhome
UCS-A/mnitoring/callhome # show anonymous-reporting
Anonymous Reporting:
    Admin State
    -----------
    Off
UCS-A/monitoring/callhome* # enable anonymous-reporting
UCS-A/monitoring/callhome # commit-buffer
UCS-A/monitoring/callhome # show anonymous-reporting
Anonymous Reporting:
    Admin State
    -----------
    On
```

# Disabling Anonymous Reporting

You can disable anonymous reporting on the Call Home server.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A # **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A/monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A/monitoring/callhome # **show anonymous-reporting** | (Optional)<br>Displays if anonymous reporting is enabled or disabled. |
| **Step 4** | UCS-A/monitoring/callhome # **disable anonymous-reporting** | Disables anonymous reporting on the Smart Call Home server. |
| **Step 5** | UCS-A/monitoring/callhome # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to disable anonymous reporting on the Call Home server:

```
UCS-A # scope monitoring
UCS-A/monitoring # scope callhome
UCS-A/mnitoring/callhome # show anonymous-reporting
Anonymous Reporting:
    Admin State
    -----------
    On
UCS-A/monitoring/callhome* # disable anonymous-reporting
UCS-A/monitoring/callhome # commit-buffer
UCS-A/monitoring/callhome # show anonymous-reporting
Anonymous Reporting:
    Admin State
    -----------
    Off
```

# Viewing Anonymous Reports

You can view the anonymous reports from the Call Home server.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A # **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A/monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A/monitoring/callhome # **scope anonymous-reporting** | Enters anonymous reporting mode. |
| **Step 4** | UCS-A/monitoring/callhome/anonymous-reporting # **show detail** | Displays the SMTP server address and server port. |
| **Step 5** | UCS-A/monitoring/callhome/anonymous-reporting # **show inventory** | Displays the anonymous reporting information. |
| **Step 6** | UCS-A/monitoring/callhome/anonymous-reporting # **show content** | Displays the anonymous report sample information. |

The following example shows how to display anonymous reports from the Call Home server:

```
UCS-A # scope monitoring
UCS-A/monitoring # scope callhome
UCS-A/monitoring/callhome # scope anonymous-reporting
UCS-A/monitoring/callhome/anonymous-reporting # show detail
UCS-A/monitoring/callhome/anonymous-reporting # show inventory
UCS-A/monitoring/callhome/anonymous-reporting # show content
<anonymousData>
<discreteData
smartCallHomeContract="false"
ethernetMode="EndHost"
fcMode="EndHost"
disjointL2Used="false"
fabricFailoverUsed="false"
numVnicAdaptTempl="3"
numServiceProfiles="7"
updatingSPtemplUsed="false"
```

```
initialSPtemplUsed="true"
lanConnPolicyUsed="true"
sanConnPolicyUsed="false"
updatingAdaptTemplUsed="false"
initialAdaptTemplUsed="true"
numMsoftVMnets="10"
numOfVMs="3"
discreteFEX="false"
ucsCentralConnected="false"/>
<bladeUnit
chassisId="1"
slotId="4"
…..
```

# Example: Configuring Call Home for Smart Call Home

## Configuring Smart Call Home

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **enable** | Enables Call Home. |
| **Step 4** | UCS-A /monitoring/callhome # **set contact** *name* | Cisco Smart Call Home sends the registration email to this email address. |
| **Step 5** | UCS-A /monitoring/callhome # **set email** *email-addr* | Specifies the email address of the main Call Home contact person.<br>Cisco Smart Call Home sends the registration email to this email address. |
| **Step 6** | UCS-A /monitoring/callhome # **set phone-contact** *phone-num* | Specifies the phone number of the main Call Home contact person. The phone number must be in international format, starting with a + (plus sign) and a country code. |
| **Step 7** | UCS-A /monitoring/callhome # **set street-address** *street-addr* | Specifies the street address of the main Call Home contact person. |
| **Step 8** | UCS-A /monitoring/callhome # **set customer-id** *id-num* | Specifies the CCO identification number that includes the contract numbers for the support contract in its entitlements. The number can be up to 255 alphanumeric characters in free format. |
| **Step 9** | UCS-A /monitoring/callhome # **set contract-id** *id-num* | Specifies the contract identification number from the service agreement. The number can be up to 255 alphanumeric characters in free format. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 10** | UCS-A /monitoring/callhome # **set site-id** *id-num* | Specifies the site identification number from the service agreement. The number can be up to 255 alphanumeric characters in free format. |
| **Step 11** | UCS-A /monitoring/callhome # **set from-email** *email-addr* | Specifies the email address to use for the From field in Call Home messages. |
| **Step 12** | UCS-A /monitoring/callhome # **set reply-to-email** *email-addr* | Specifies the email address to use for the Reply To field in Call Home messages. |
| **Step 13** | UCS-A /monitoring/callhome # **set hostname** {*hostname* \| *ip-addr*} | Specifies the hostname or IP address of the SMTP server that Call Home uses to send email messages. |
| **Step 14** | UCS-A /monitoring/callhome # **set port** *port-num* | Specifies the SMTP server port that Call Home uses to send email messages. Valid port numbers are 1 to 65535. |
| **Step 15** | UCS-A /monitoring/callhome # **set throttling** {**off** \| **on**} | Enables or disables Call Home throttling. When enabled, throttling prevents too many Call Home email messages from being sent for the same event. By default, throttling is enabled. |
| **Step 16** | UCS-A /monitoring/callhome # **set urgency** {**alerts** \| **critical** \| **debugging** \| **emergencies** \| **errors** \| **information** \| **notifications** \| **warnings**} | Specifies the urgency level for Call Home email messages. |
| **Step 17** | UCS-A /monitoring/callhome # **commit-buffer** | Commits the transaction to the system configuration. |

The following example configures Call Home and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring* # scope callhome
UCS-A /monitoring/callhome* # enable
UCS-A /monitoring/callhome* # set contact "Steve Jones"
UCS-A /monitoring/callhome* # set email admin@MyCompany.com
UCS-A /monitoring/callhome* # set phone-contact +1-001-408-555-1234
UCS-A /monitoring/callhome* # set street-address "123 N. Main Street, Anytown, CA, 99885"
UCS-A /monitoring/callhome* # set customer-id 1234567
UCS-A /monitoring/callhome* # set contract-id 99887766
UCS-A /monitoring/callhome* # set site-id 5432112
UCS-A /monitoring/callhome* # set from-email person@MyCompany.com
UCS-A /monitoring/callhome* # set reply-to-email person@MyCompany.com
UCS-A /monitoring/callhome* # set hostname 192.168.100.12
UCS-A /monitoring/callhome* # set port 25
UCS-A /monitoring/callhome* # set throttling on
UCS-A /monitoring/callhome* # set urgency information
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

## What to Do Next

Continue to "Configuring the Default Cisco TAC-1 Profile, on page 66" to configure a Call Home profile for use with Smart Call Home.

# 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

### Before You Begin

Complete the "Configuring Smart Call Home, on page 64" section.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A /monitoring/callhome # **scope profile CiscoTac-1** | Enters monitoring call home profile mode for the default Cisco TAC-1 profile. |
| **Step 2** | UCS-A /monitoring/callhome/profile # **set level normal** | Specifies the **normal** event level for the profile. |
| **Step 3** | UCS-A /monitoring/callhome/profile # **set alertgroups ciscotac** | Specifies the **ciscotac** alert group for the profile. |
| **Step 4** | UCS-A /monitoring/callhome/profile # **set format xml** | Specifies the e-mail message format to **xml** . |
| **Step 5** | UCS-A /monitoring/callhome/profile # **set maxsize 5000000** | Specifies the maximum size of **5000000** for email messages. |
| **Step 6** | UCS-A /monitoring/callhome/profile # **create destination callhome@cisco.com** | Specifies the email recipient to **callhome@cisco.com** . |
| **Step 7** | UCS-A /monitoring/callhome/profile/destination # **exit** | Exits to monitoring call home profile mode. |
| **Step 8** | UCS-A /monitoring/callhome/profile # **exit** | Exits to monitoring call home mode. |

The following example configures the default Cisco TAC-1 profile for use with Smart Call Home:

```
UCS-A /monitoring/callhome* # scope profile CiscoTac-1
UCS-A /monitoring/callhome/profile* # set level normal
UCS-A /monitoring/callhome/profile* # set alertgroups ciscotac
UCS-A /monitoring/callhome/profile* # set format xml
UCS-A /monitoring/callhome/profile* # set maxsize 5000000
UCS-A /monitoring/callhome/profile* # create destination callhome@cisco.com
UCS-A /monitoring/callhome/profile/destination* # exit
UCS-A /monitoring/callhome/profile* # exit
UCS-A /monitoring/callhome* #
```

### What to Do Next

Continue to "Configuring a System Inventory Message for Smart Call Home, on page 67" to configure system inventory messages for use with Smart Call Home.

# Configuring a System Inventory Message for Smart Call Home

### Before You Begin

Complete the "Configuring the Default Cisco TAC-1 Profile, on page 66" section.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A /monitoring/callhome # **scope inventory** | Enters monitoring call home inventory mode. |
| **Step 2** | UCS-A /monitoring/callhome/inventory # **set send-periodically** {**off** \| **on**} | Enables or disables the sending of inventory messages. When the **on** keyword is specified, inventory messages are automatically sent to the Call Home database. |
| **Step 3** | UCS-A /monitoring/callhome/inventory # **set interval-days** *interval-num* | Specifies the the time interval (in days) at which inventory messages will be sent. |
| **Step 4** | UCS-A /monitoring/callhome/inventory # **set timeofday-hour** *hour* | Specifies the hour (using 24-hour format) that inventory messages are sent. |
| **Step 5** | UCS-A /monitoring/callhome/inventory # **set timeofday-minute** *minute* | Specifies the number of minutes after the hour that inventory messages are sent. |
| **Step 6** | UCS-A /monitoring/callhome/inventory # **commit-buffer** | Commits the transaction to the system configuration. |

The following example configures Call Home system inventory messages and commits the transaction:

```
UCS-A /monitoring/callhome* # scope inventory
UCS-A /monitoring/callhome/inventory* # set send-periodically on
UCS-A /monitoring/callhome/inventory* # set interval-days 15
UCS-A /monitoring/callhome/inventory* # set timeofday-hour 21
UCS-A /monitoring/callhome/inventory* # set timeofday-minute 30
UCS-A /monitoring/callhome/inventory* # commit-buffer
UCS-A /monitoring/callhome/inventory #
```

### What to Do Next

Continue to "Registering Smart Call Home, on page 68" to send an inventory message that starts the Smart Call Home registration process.

# Registering Smart Call Home

### Before You Begin

Complete the "Configuring a System Inventory Message for Smart Call Home, on page 67" section.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A /monitoring/callhome/inventory # **send** | Sends the system inventory message to the Smart Call Home database.<br>When Cisco receives the system inventory, a Smart Call Home registration email is sent to the email address that you configured as the email address for the main Smart Call Home contact. |

The following example sends the system inventory message to the Smart Call Home database:

```
UCS-A /monitoring/callhome/inventory # send
```

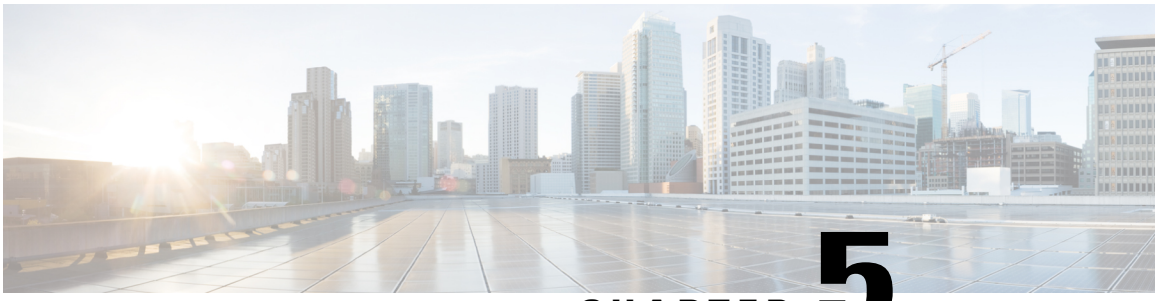
### What to Do Next

When you receive the registration email from Cisco, do the following to complete registration for Smart Call Home:

1. Click the link in the email.

   The link opens the Cisco Smart Call Home portal in your web browser.
2. Log into the Cisco Smart Call Home portal.
3. 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.



CHAPTER 5

# Managing the System Event Log

This chapter includes the following sections:


- System Event Log, page 69
- Viewing the System Event Log for a Server, page 70
- Configuring the SEL Policy, page 71
- Backing Up the System Event Log for a Server, page 73
- Clearing the System Event Log for a Server, page 74


## System Event Log

The system event log (SEL) resides on the CIMC in NVRAM. It records most server-related events, such as over and under voltage, temperature events, fan events, and events from BIOS. The SEL is mainly used for troubleshooting purposes.

The SEL file is approximately 40KB in size, and no further events can be recorded when it is full. It must be cleared before additional events can be recorded.

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

## Viewing the System Event Log for an Individual Server

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **show sel** *chassis-id* / *blade-id* | Displays the system event log for the specified server. |

The following example displays the system event log for blade 3 in chassis 1.

```
UCS-A# show sel 1/3
     1 | 01/01/1970 01:23:27 | System Event 0x83 | Timestamp clock synch | SEL timestamp
clock updated, event is f
irst of pair | Asserted
     2 | 01/01/1970 01:23:28 | Drive slot(Bay) SAS0_LINK_STATUS | Transition to Degraded |
 Asserted
     3 | 01/01/1970 01:23:28 | Drive slot(Bay) SAS0_LINK_STATUS | Transition to On Line |
Deasserted
     4 | 01/01/1970 01:23:28 | Platform alert LED_SAS0_FAULT | LED is blinking fast |
Asserted
     5 | 01/01/1970 01:23:28 | Platform alert LED_SAS0_FAULT | LED is on | Deasserted
     6 | 01/01/1970 01:23:28 | Platform alert LED_FPID | LED is on | Asserted
     7 | 01/01/1970 01:23:28 | Platform alert LED_FPID | LED is off | Deasserted
     8 | 01/01/1970 01:23:29 | Entity presence MAIN_POWER | Device Absent | Asserted
     9 | 01/01/1970 01:23:29 | Entity presence MAIN_POWER | Device Present | Deasserted
     a | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED is on | Asserted
    b | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED color is green | Asserted

     c | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED is blinking fast |
Deasserted
    d | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED color is amber | Deasserted

     e | 01/01/1970 00:00:22 | Drive slot(Bay) SAS0_LINK_STATUS | Transition to Degraded |
 Asserted
     f | 01/01/1970 00:00:22 | Entity presence MEZZ_PRS | Device Present | Asserted
    10 | 01/01/1970 00:00:22 | Entity presence HDD1_PRS | Device Absent | Asserted
```

## Viewing the System Event Log for All of the Servers in a Chassis

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** *chassis-id* / *blade-id* | Enters chassis server mode for the specified server. |
| **Step 2** | UCS-A /chassis/server # **show sel** | Displays the system event log. |

The following example displays the system event log from chassis server mode for blade 3 in chassis 1.

```
UCS-A# scope server 1/3
UCS-A /chassis/server # show sel
     1 | 01/01/1970 01:23:27 | System Event 0x83 | Timestamp clock synch | SEL timestamp
clock updated, event is f
irst of pair | Asserted
     2 | 01/01/1970 01:23:28 | Drive slot(Bay) SAS0_LINK_STATUS | Transition to Degraded |
 Asserted
     3 | 01/01/1970 01:23:28 | Drive slot(Bay) SAS0_LINK_STATUS | Transition to On Line |
Deasserted
     4 | 01/01/1970 01:23:28 | Platform alert LED_SAS0_FAULT | LED is blinking fast |
Asserted
     5 | 01/01/1970 01:23:28 | Platform alert LED_SAS0_FAULT | LED is on | Deasserted
     6 | 01/01/1970 01:23:28 | Platform alert LED_FPID | LED is on | Asserted
     7 | 01/01/1970 01:23:28 | Platform alert LED_FPID | LED is off | Deasserted
     8 | 01/01/1970 01:23:29 | Entity presence MAIN_POWER | Device Absent | Asserted
     9 | 01/01/1970 01:23:29 | Entity presence MAIN_POWER | Device Present | Deasserted
     a | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED is on | Asserted
    b | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED color is green | Asserted

     c | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED is blinking fast |
Deasserted
    d | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED color is amber | Deasserted

     e | 01/01/1970 00:00:22 | Drive slot(Bay) SAS0_LINK_STATUS | Transition to Degraded |
 Asserted
     f | 01/01/1970 00:00:22 | Entity presence MEZZ_PRS | Device Present | Asserted
    10 | 01/01/1970 00:00:22 | Entity presence HDD1_PRS | Device Absent | Asserted
```

# Configuring the SEL Policy

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* . |
| **Step 2** | UCS-A /org # **scope ep-log-policy sel** | Enters organization endpoint log policy mode and scopes the SEL policy. |
| **Step 3** | UCS-A /org/ep-log-policy # **set description** *description* | (Optional)<br>Provides a description for the policy.<br>**Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output. |
| **Step 4** | UCS-A /org/ep-log-policy # **set backup action** [**log-full**] [**on-change-of-association**] [**on-clear**] [**timer**] [**none**] | Specifies an action or actions that will trigger a backup operation. |
| **Step 5** | UCS-A /org/ep-log-policy # **set backup clear-on-backup** {**no** \| **yes**} | Specifies whether to clear the system event log after a backup operation occurs. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | UCS-A /org/ep-log-policy # **set backup destination** *URL* | Specifies the protocol, user, password, remote hostname, and remote path for the backup operation. Depending on the protocol used, specify the URL using one of the following syntax:<br>• **ftp://** *username@hostname* / *path*<br>• **scp://** *username* **@** *hostname* / *path*<br>• **sftp://** *username* **@** *hostname* / *path*<br>• **tftp://** *hostname* **:** *port-num* / *path*<br>**Note** You can also specify the backup destination by using the **set backup hostname** , **set backup password** , **set backup protocol** , **set backup remote-path** , **set backup user** commands, or by using the **set backup destination** command. Use either method to specify the backup destination. |
| **Step 7** | UCS-A /org/ep-log-policy # **set backup format** {*ascii* \| *binary*} | Specifies the format for the backup file. |
| **Step 8** | UCS-A /org/ep-log-policy # **set backup hostname** {*hostname* \| *ip-addr*} | Specifies the hostname or IP address of the remote server. |
| **Step 9** | UCS-A /org/ep-log-policy # **set backup interval** {**1-hour** \| **2-hours** \| **4-hours** \| **8-hours** \| **24-hours** \| **never**} | Specifies the time interval for the automatic backup operation. Specifying the **never** keyword means that automatic backups will not be made. |
| **Step 10** | UCS-A /org/ep-log-policy # **set backup password** *password* | Specifies the password for the username. This step does not apply if the TFTP protocol is used. |
| **Step 11** | UCS-A /org/ep-log-policy # **set backup protocol** {**ftp** \| **scp** \| **sftp** \| **tftp**} | Specifies the protocol to use when communicating with the remote server. |
| **Step 12** | UCS-A /org/ep-log-policy # **set backup remote-path** *path* | Specifies the path on the remote server where the backup file is to be saved. |
| **Step 13** | UCS-A /org/ep-log-policy # **set backup user** *username* | Specifies the username the system should use to log in to the remote server. This step does not apply if the TFTP protocol is used. |
| **Step 14** | UCS-A /org/ep-log-policy # **commit-buffer** | Commits the transaction. |

The following example configures the SEL policy to back up the system event log (in ascii format) every 24 hours or when the log is full and clear the system event log after a backup operation occurs and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope ep-log-policy sel
UCS-A /org/ep-log-policy # set backup destination scp://user@192.168.1.10/logs
Password:
UCS-A /org/ep-log-policy* # set backup action log-full
UCS-A /org/ep-log-policy* # set backup clear-on-backup yes
UCS-A /org/ep-log-policy* # set backup format ascii
UCS-A /org/ep-log-policy* # set backup interval 24-hours
UCS-A /org/ep-log-policy* # commit-buffer
UCS-A /org/ep-log-policy #
```

# Backing Up the System Event Log for a Server

## Backing Up the System Event Log for an Individual Server

### 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

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A /chassis/server # **backup sel** *chassis-id* / *blade-id* | Clears the system event log. |
| **Step 2** | UCS-A# **commit-buffer** | Commits the transaction. |

The following example backs up the system event log for blade 3 in chassis 1 and commits the transaction.

```
UCS-A# backup sel 1/3
UCS-A* # commit-buffer
UCS-A#
```

## Backing Up the System Event Log for All of the Servers in 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

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** *chassis-id* / *blade-id* | Enters chassis server mode for the specified server. |
| **Step 2** | UCS-A /chassis/server # **backup sel** | Clears the system event log. |
| **Step 3** | UCS-A /chassis/server # **commit-buffer** | Commits the transaction. |

The following example backs up the system event log from chassis server mode for blade 3 in chassis 1 and commits the transaction.

```
UCS-A# scope server 1/3
UCS-A /chassis/server # backup sel
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```

# Clearing the System Event Log for a Server

## Clearing the System Event Log for an Individual Server

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **clear sel** *chassis-id* / *blade-id* | Clears the system event log. |
| **Step 2** | UCS-A# **commit-buffer** | Commits the transaction. |

The following example clears the system event log for blade 3 in chassis 1 and commits the transaction:

```
UCS-A# clear sel 1/3
UCS-A* # commit-buffer
UCS-A#
```

## Clearing the System Event Log for All of the Servers in a Chassis

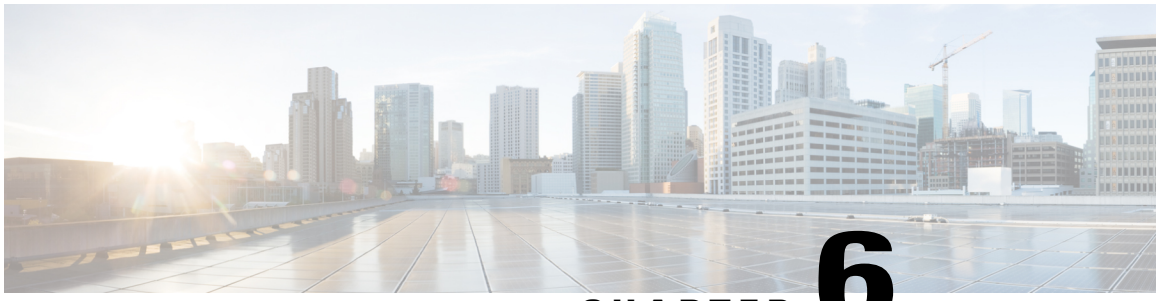
### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** *chassis-id* / *blade-id* | Enters chassis server mode for the specified server. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | UCS-A /chassis/server # **clear sel** | Clears the system event log. |
| **Step 3** | UCS-A /chassis/server # **commit-buffer** | Commits the transaction. |

The following example clears the system event log from chassis server mode for blade 3 in chassis 1 and commits the transaction:

```
UCS-A# scope server 1/3
UCS-A /chassis/server # clear sel
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```



CHAPTER 6

# Configuring Settings for Faults, Events, and Logs

This chapter includes the following sections:


- Configuring Settings for the Fault Collection Policy, page 77
- Configuring Fault Suppression, page 79
- Configuring Settings for the Core File Exporter, page 99
- Configuring the Syslog, page 101
- Viewing Audit Logs, page 103
- Configuring the Log File Exporter, page 104


# 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 Fault Collection Policy

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope fault policy** | Enters monitoring fault policy mode. |
| **Step 3** | UCS-A /monitoring/fault-policy # **set clear-action** {**delete** \| **retain**} | Specifies whether to retain or delete all cleared messages. If the **retain** option is specified, then the length of time that the messages are retained is determined by the **set retention-interval** command. |
| **Step 4** | UCS-A /monitoring/fault-policy # **set flap-interval** *seconds* | Specifies the time interval (in seconds) the system waits before changing a fault state. Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, the system does not allow a fault to change state until the flapping interval has elapsed after the last state change. If the fault is raised again during the flapping interval, it returns to the active state, otherwise, the fault is cleared. |
| **Step 5** | UCS-A /monitoring/fault-policy # **set retention-interval** {*days hours minutes seconds* \| **forever**} | Specifies the time interval the system retains all cleared fault messages before deleting them. The system can retain cleared fault messages forever, or for the specified number of days, hours, minutes, and seconds. |
| **Step 6** | UCS-A /monitoring/fault-policy # **commit-buffer** | Commits the transaction. |

This example configures the fault collection policy to retain cleared fault messages for 30 days, sets the flapping interval to 10 seconds, and commits the transaction.

```
UCS-A# scope monitoring
UCS-A /monitoring # scope fault policy
UCS-A /monitoring/fault-policy # set clear-action retain
UCS-A /monitoring/fault-policy* # set flap-interval 10
UCS-A /monitoring/fault-policy* # set retention-interval 30 0 0 0
UCS-A /monitoring/fault-policy* # commit-buffer
UCS-A /monitoring/fault-policy #
```

# Configuring Fault Suppression

## Fault Suppression

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

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

Fault suppression uses the following:

### 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 and 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 blade servers, power supplies, and fan modules.

  This policy applies only to chassis.

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

  This policy applies only to chassis.

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

  This policy applies only to FEXes.

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

  This policy applies only to FEXes.

- **default-server-maint—**Suppresses faults for blade servers and/or rack servers.

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

**Note** When applied to a chassis, only blade servers are affected.

### 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.

# Configuring Fault Suppression for a Chassis

## Configuring Fault Suppression Tasks for a Chassis Using a Fixed Time Interval

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope chassis** *chassis-num* | Enters chassis mode for the specified chassis. |
| **Step 2** | UCS-A/chassis # **create fault-suppress-task** *name* | Creates a fault-suppress-task on the chassis, and enters fault-suppress-task mode.<br>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 has been saved. |
| **Step 3** | UCS-A/chassis/fault-suppress-task # **set fault-suppress-policy** *policy-name* | Specifies the fault suppression policy that you want to apply. |
| **Step 4** | UCS-A/chassis/fault-suppress-task # **create local-schedule** | Creates a local schedule and enters local-schedule mode. |
| **Step 5** | UCS-A/chassis/fault-suppress-task/local-schedule # **create occurrence single-one-time** | Creates a one-time occurrence, and enters single-one-time mode. |
| **Step 6** | UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds* | Specifies the date and time that this occurrence should run. |
| **Step 7** | UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **set max-duration** {**none** \| *num-of-days num-of-hours num-of-minutes num-of-seconds*} | Specifies the maximum length of time that this task can run. To run the task until it is manually stopped, enter none or omit this step. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to create a fault suppression task called task2 for the chassis, apply the default-chassis-all-maint policy to the task, set the start date to January 1, 2013 at 11:00, and commit the transaction:

```
UCS-A# scope chassis 1
UCS-A/chassis # create fault-suppress-task task2
UCS-A/chassis/fault-suppress-task* # set fault-suppress-policy default-chassis-all-maint
UCS-A/chassis/fault-suppress-task* # create local-schedule
UCS-A/chassis/fault-suppress-task/local-schedule* # create occurrence single-one-time
UCS-A/chassis/fault-suppress-task/local-schedule* # set date jan 1 2013 11 00 00
UCS-A/chassis/fault-suppress-task/local-schedule* # commit-buffer
```

## Configuring Fault Suppression Tasks for a Chassis Using a Schedule

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope chassis** *chassis-num* | Enters chassis mode for the specified chassis. |
| **Step 2** | UCS-A/chassis # **create fault-suppress-task** *name* | Creates a fault-suppress-task on the chassis, and enters the fault-suppress-task mode.<br>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 has been saved. |
| **Step 3** | UCS-A/chassis/fault-suppress-task # **set schedule** *name* | Specifies the schedule that you want to use.<br>**Note** The schedule must exist before you can use it in a fault suppression task. For more information about creating schedules, see Creating a Schedule. |
| **Step 4** | UCS-A/chassis/fault-suppress-task # **set fault-suppress-policy** *policy-name* | Selects the fault suppression policy you want to apply. |
| **Step 5** | UCS-A/chassis/fault-suppress-task # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to create a fault suppression task called task1 for the chassis, apply the scheduler called weekly_maint and the default-chassis-all-maint policy to the task, and commit the transaction:

```
UCS-A# scope chassis 2
UCS-A/chassis # create fault-suppress-task task1
UCS-A/chassis/fault-suppress-task* # set schedule weekly_maint
```

```
UCS-A/chassis/fault-suppress-task* # set fault-suppress-policy default-chassis-all-maint
UCS-A/chassis/fault-suppress-task* # commit-buffer
```

## Deleting Fault Suppression Tasks for a Chassis

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope chassis** *chassis-num* | Enters chassis mode for the specified chassis. |
| **Step 2** | UCS-A/chassis # **delete fault-suppress-task** *name* | Deletes the specified fault suppression task. |
| **Step 3** | UCS-A/chassis # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to delete the fault suppression task called task1:

```
UCS-A# scope chassis 1
UCS-A/chassis # delete fault-suppress-task task1
UCS-A/chassis* # commit-buffer
```

## Modifying Fault Suppression Tasks for a Chassis

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope chassis** *chassis-num* | Enters chassis mode for the specified chassis. |
| **Step 2** | UCS-A/chassis # **scope fault-suppress-task** *name* | Enters fault-suppress-task mode. |
| **Step 3** | UCS-A/chassis/fault-suppress-task # **set fault-suppress-policy** *policy-name* | Modifies the fault suppression policy.<br>**Note** To apply a different schedule to the fault suppression task, go to Step 4. To change the fixed time interval of the fault suppression task, go to Step 5. |
| **Step 4** | UCS-A/chassis/fault-suppress-task # **set schedule** *name* | Applies the schedule you want to use. |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note** If you change from a fixed time interval to a schedule, the fixed time interval is deleted when you commit.<br>If you change from a schedule to a fixed time interval, the reference to the schedule is cleared when you commit. |
| **Step 5** | UCS-A/chassis/fault-suppress-task # **scope local-schedule** | Enters local-schedule mode. |
| **Step 6** | UCS-A/chassis/fault-suppress-task/local-schedule # **scope occurrence single-one-time** | Enters single-one-time mode. |
| **Step 7** | UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds* | Specifies the date and time that this occurrence should run. |
| **Step 8** | UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **set max-duration** {**none** \| *num-of-days num-of-hours num-of-minutes num-of-seconds*} | Specifies the maximum length of time that this task can run. To run the task until it is manually stopped, enter none or omit this step. |
| **Step 9** | UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to change the date and the fault suppression policy of the fault suppression task called task2:

```
UCS-A# scope chassis 1
UCS-A/chassis # scope fault-suppress-task task2
UCS-A/chassis/fault-suppress-task # set fault-suppress-policy default-server-maint
UCS-A/chassis/fault-suppress-task* # scope local-schedule
UCS-A/chassis/fault-suppress-task/local-schedule* # scope occurrence single-one-time
UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time* # set date dec 31 2013
11 00 00
UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time* # commit-buffer
```

The following example shows how to apply a different schedule to the fault suppression task called task1:

```
UCS-A# scope chassis 1
UCS-A/chassis # scope fault-suppress-task task1
UCS-A/chassis/fault-suppress-task # set schedule monthly-maint
UCS-A/chassis/fault-suppress-task* # commit-buffer
```

## Viewing Suppressed Faults and Fault Suppression Tasks for a Chassis

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope chassis** *chassis-num* | Enters chassis mode for the specified chassis. |
| **Step 2** | UCS-A/chassis # **show fault suppressed** | Displays the suppressed faults for the chassis.<br>**Note** Only faults owned by the selected component are displayed. |
| **Step 3** | UCS-A/chassis # **scope fault-suppress-task** *name* | Enters fault-suppress-task mode. |
| **Step 4** | UCS-A/chassis/fault-suppress-task # **show detail expand** | Displays the schedule or fixed time interval for the task. |

The following example shows how to display the suppressed faults for a chassis:

```
UCS-A# scope chassis 1
UCS-A/chassis # show fault suppressed
Fault Suppress Task:

Name               Status             Global Schedule Suppress Policy Name
------------------ ------------------ --------------- --------------------
task1              Active             test_schedule1  Default Chassis Phys Maint

UCS-A/chassis #
```

The following example shows how to display the fault suppression task called task1:

```
UCS-A# scope chassis 1
UCS-A/chassis # scope fault-suppress-task task1
UCS-A/chassis/fault-suppress-task # show detail expand
Fault Suppress Task:
    Name: task1
    Status: Active
    Global Schedule: test_schedule1
    Suppress Policy Name: Default Chassis Phys Maint

UCS-A/chassis/fault-suppress-task #
```

# Configuring Fault Suppression for a Server

## Configuring Fault Suppression Tasks for a Server Using a Fixed Time Interval

The **default-server-maint** suppression policy is selected by default.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** [*chassis-num*/*server-num* \| *dynamic-uuid*] | Enters server mode for the specified server. |
| **Step 2** | UCS-A/server # **create fault-suppress-task** *name* | Creates a fault-suppress-task on the server, and enters the fault-suppress-task mode.<br>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 has been saved. |
| **Step 3** | UCS-A/server/fault-suppress-task # **create local-schedule** | Creates a local schedule and enters local-schedule mode. |
| **Step 4** | UCS-A/server/fault-suppress-task/local-schedule # **create occurrence single-one-time** | Creates a one-time occurrence, and enters single-one-time mode. |
| **Step 5** | UCS-A/server/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds* | Specifies the date and time that this occurrence should run. |
| **Step 6** | UCS-A/server/fault-suppress-task/local-schedule/single-one-time # **set max-duration** {**none** \| *num-of-days num-of-hours num-of-minutes num-of-seconds*} | Specifies the maximum length of time that this task can run. To run the task until it is manually stopped, enter none or omit this step. |
| **Step 7** | UCS-A/server/fault-suppress-task/local-schedule/single-one-time # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to create a fault suppression task called task2 for the server, set the start date to January 1, 2013 at 11:00, and commit the transaction:

```
UCS-A# scope server 1/1
UCS-A/server # create fault-suppress-task task2
UCS-A/server/fault-suppress-task* # create local-schedule
UCS-A/server/fault-suppress-task/local-schedule* # create occurrence single-one-time
UCS-A/server/fault-suppress-task/local-schedule/single-one-time* # set date jan 1 2013 11
00 00
UCS-A/server/fault-suppress-task/local-schedule/single-one-time* # commit-buffer
```

## Configuring Fault Suppression Tasks for a Server using a Schedule

The **default-server-maint** suppression policy is selected by default.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** [*chassis-num*/*server-num* \| *dynamic-uuid*] | Enters server mode for the specified server. |
| **Step 2** | UCS-A/server # **create fault-suppress-task** *name* | Creates a fault-suppress-task on the server, and enters the fault-suppress-task mode.<br>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 has been saved. |
| **Step 3** | UCS-A/server/fault-suppress-task # **set schedule** *name* | Specifies the schedule that you want to use.<br>**Note** The schedule must exist before you can use it in a fault suppression task. For more information about creating schedules, see Creating a Schedule. |
| **Step 4** | UCS-A/server/fault-suppress-task # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to creates a fault suppression task called task1 for the server, apply the scheduler called weekly_maint to the task, and commit the transaction:

```
UCS-A# scope server 1/1
UCS-A/server # create fault-suppress-task task1
UCS-A/server/fault-suppress-task* # set schedule weekly_maint
UCS-A/server/fault-suppress-task* # commit-buffer
```

## Deleting Fault Suppression Tasks for a Server

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** [*chassis-num*/*server-num* \| *dynamic-uuid*] | Enters server mode for the specified server. |
| **Step 2** | UCS-A/server # **delete fault-suppress-task** *name* | Deletes the specified fault suppression task. |
| **Step 3** | UCS-A/server # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to delete the fault suppression task called task1:

```
UCS-A# scope server 1/1
UCS-A/server # delete fault-suppress-task task1
UCS-A/server* # commit-buffer
```

## Modifying Fault Suppression Tasks for a Server

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** [*chassis-num*/*server-num* \| *dynamic-uuid*] | Enters server mode for the specified server. |
| **Step 2** | UCS-A/server # **scope fault-suppress-task** *name* | Enters fault-suppress-task mode.<br>**Note** To apply a different schedule to the fault suppression task, go to Step 3. To change the fixed time interval of the fault suppression task, go to Step 4. |
| **Step 3** | UCS-A/server/fault-suppress-task # **set schedule** *name* | Applies a different schedule.<br>**Note** If you change from a fixed time interval to a schedule, the fixed time interval is deleted when you commit.<br>If you change from a schedule to a fixed time interval, the reference to the schedule is cleared when you commit. |
| **Step 4** | UCS-A/server/fault-suppress-task # **scope local-schedule** | Enters local-schedule mode. |
| **Step 5** | UCS-A/server/fault-suppress-task/local-schedule # **scope occurrence single-one-time** | Enters single-one-time mode. |
| **Step 6** | UCS-A/server/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds* | Specifies the date and time that this occurrence should run. |
| **Step 7** | UCS-A/server/fault-suppress-task/local-schedule/single-one-time # **set max-duration** {**none** \| *num-of-days num-of-hours num-of-minutes num-of-seconds*} | Specifies the maximum length of time that this task can run. To run the task until it is manually stopped, enter none or omit this step. |
| **Step 8** | UCS-A/server/fault-suppress-task/local-schedule/single-one-time # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to change the date and the fault suppression policy of the fault suppression task called task2:

```
UCS-A# scope server 1/1
UCS-A/server # scope fault-suppress-task task2
UCS-A/server/fault-suppress-task # scope local-schedule
UCS-A/server/fault-suppress-task/local-schedule # scope occurrence single-one-time
UCS-A/server/fault-suppress-task/local-schedule/single-one-time # set date dec 31 2013 11
00 00
UCS-A/server/fault-suppress-task/local-schedule/single-one-time* # commit-buffer
```

The following example shows how to apply a different schedule to the fault suppression task called task1:

```
UCS-A# scope server 1/1
UCS-A/server # scope fault-suppress-task task1
UCS-A/server/fault-suppress-task # set schedule monthly-maint
UCS-A/server/fault-suppress-task* # commit-buffer
```

## Viewing Suppressed Faults and Fault Suppression Tasks for a Server

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** [*chassis-num*/*server-num* \| *dynamic-uuid*] | Enters server mode for the specified server. |
| **Step 2** | UCS-A/server # **show fault suppressed** | Displays the suppressed faults for the server.<br>**Note** Only faults owned by the selected component are displayed. |
| **Step 3** | UCS-A/server # **scope fault-suppress-task** *name* | Enters fault-suppress-task mode. |
| **Step 4** | UCS-A/server/fault-suppress-task # **show detail expand** | Displays the schedule or fixed time interval for the task. |

The following example shows how to display the suppressed faults for a server:

```
UCS-A# scope server 1/1
UCS-A/server # show fault suppressed
Fault Suppress Task:

Name               Status             Global Schedule Suppress Policy Name
------------------ ------------------ --------------- --------------------
task1              Active             test_schedule1  Default Server Maint

UCS-A/server #
```

The following example shows how to display the fault suppression task called task1:

```
UCS-A# scope server 1/1
UCS-A/server # scope fault-suppress-task task1
UCS-A/server/fault-suppress-task # show detail expand
Fault Suppress Task:
    Name: task1
    Status: Active
    Global Schedule: test_schedule1
```

```
    Suppress Policy Name: Default Server Maint

UCS-A/server/fault-suppress-task #
```

# Configuring Fault Suppression for a Service Profile

## Configuring Fault Suppression Tasks for a Service Profile Using a Fixed Time Interval

The **default-server-maint** suppression policy is selected by default.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*. |
| **Step 2** | UCS-A /org # **scope service-profile** *profile-name* | Enters service profile organization mode for the service profile. |
| **Step 3** | UCS-A /org/service-profile # **create fault-suppress-task** *name* | Creates a fault-suppress-task on the chassis, and enters the fault-suppress-task mode.<br>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 has been saved. |
| **Step 4** | UCS-A/org/service-profile/fault-suppress-task # **create local-schedule** | Creates a local schedule and enters local-schedule mode. |
| **Step 5** | UCS-A/org/service-profile/fault-suppress-task/local-schedule # **create occurrence single-one-time** | Creates a one-time occurrence, and enters single-one-time mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds* | Specifies the date and time that this occurrence should run. |
| **Step 7** | UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **set max-duration** {**none** \| *num-of-days num-of-hours num-of-minutes num-of-seconds*} | Specifies the maximum length of time that this task can run. To run the task until it is manually stopped, enter none or omit this step. |
| **Step 8** | UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to create a fault suppression task called task2 under the accounting service profile, set the start date to January 1, 2013 at 11:00, and commit the transaction:

```
UCS-A# scope org /
UCS-A/org # scope service-profile accounting
UCS-A/org/service-profile # create fault-suppress-task task2
UCS-A/org/service-profile/fault-suppress-task* # create local-schedule
UCS-A/org/service-profile/fault-suppress-task/local-schedule* # create occurrence
single-one-time
UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time* # set date
jan 1 2013 11 00 00
UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time* # commit-buffer
```

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

The **default-server-maint** suppression policy is selected by default.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*. |
| **Step 2** | UCS-A /org # **scope service-profile** *profile-name* | Enters service profile organization mode for the service profile. |
| **Step 3** | UCS-A /org/service-profile # **create fault-suppress-task** *name* | Creates a fault-suppress-task on the chassis, and enters the fault-suppress-task mode.<br>This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : |

| | Command or Action | Purpose |
|---|---|---|
| | | (colon), and . (period), and you cannot change this name after the object has been saved. |
| **Step 4** | UCS-A/org/service-profile/fault-suppress-task # **set schedule** *name* | Specifies the schedule that you want to use.<br>**Note** The schedule must exist before you can use it in a fault suppression task. For more information about creating schedules, see Creating a Schedule. |
| **Step 5** | UCS-A/org/service-profile/fault-suppress-task # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to create a fault suppression task called task1 under the accounting service profile, apply the scheduler called weekly_maint to the task, and commit the transaction:

```
UCS-A# scope org /
UCS-A/org # scope service-profile accounting
UCS-A/org/service-profile # create fault-suppress-task task1
UCS-A/org/service-profile/fault-suppress-task* # set schedule weekly_maint
UCS-A/org/service-profile/fault-suppress-task* # commit-buffer
```

## Deleting Fault Suppression Tasks for a Service Profile

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*. |
| **Step 2** | UCS-A /org # **scope service-profile** *profile-name* | Enters service profile organization mode for the service profile. |
| **Step 3** | UCS-A/org/service-profile # **delete fault-suppress-task** *name* | Deletes the specified fault suppression task. |
| **Step 4** | UCS-A/org/service-profile # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to delete the fault suppression task called task1:

```
UCS-A# scope org /
UCS-A/org # scope service-profile accounting
UCS-A/org/service-profile # delete fault-suppress-task task1
UCS-A/org/service-profile* # commit-buffer
```

## Modifying Fault Suppression Tasks for a Service Profile

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*. |
| **Step 2** | UCS-A /org # **scope service-profile** *profile-name* | Enters service profile organization mode for the service profile. |
| **Step 3** | UCS-A/org/service-profile # **scope fault-suppress-task** *name* | Enters fault-suppress-task mode.<br>**Note** To apply a different schedule to the fault suppression task, go to Step 4. To change the fixed time interval of the fault suppression task, go to Step 5. |
| **Step 4** | UCS-A/org/service-profile/fault-suppress-task # **set schedule** *name* | Applies a different schedule. |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note** If you change from a fixed time interval to a schedule, the fixed time interval is deleted when you commit.<br>If you change from a schedule to a fixed time interval, the reference to the schedule is cleared when you commit. |
| **Step 5** | UCS-A/org/service-profile/fault-suppress-task # **scope local-schedule** | Enters local-schedule mode. |
| **Step 6** | UCS-A/org/service-profile/fault-suppress-task/local-schedule # **scope occurrence single-one-time** | Enters single-one-time mode. |
| **Step 7** | UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds* | Specifies the date and time that this occurrence should run. |
| **Step 8** | UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **set max-duration** {**none** \| *num-of-days num-of-hours num-of-minutes num-of-seconds*} | Specifies the maximum length of time that this task can run. To run the task until it is manually stopped, enter none or omit this step. |
| **Step 9** | UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to change the date and the fault suppression policy of the fault suppression task called task2:

```
UCS-A# scope org /
UCS-A/org # scope service-profile accounting
UCS-A/org/service-profile # scope fault-suppress-task task2
UCS-A/org/service-profile/fault-suppress-task # scope local-schedule
UCS-A/org/service-profile/fault-suppress-task/local-schedule # scope occurrence
single-one-time
UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # set date dec
 31 2013 11 00 00
```

```
UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time* # commit-buffer
```

The following example shows how to apply a different schedule to the fault suppression task called task1:

```
UCS-A# scope org /
UCS-A/org # scope service-profile accounting
UCS-A/org/service-profile # scope fault-suppress-task task1
UCS-A/org/service-profile/fault-suppress-task # set schedule monthly-maint
UCS-A/org/service-profile/fault-suppress-task* # commit-buffer
```

## Viewing Suppressed Faults and Fault Suppression Tasks for a Service Profile

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*. |
| **Step 2** | UCS-A /org # **scope service-profile** *profile-name* | Enters service profile organization mode for the service profile. |
| **Step 3** | UCS-A/org/service-profile # **show fault suppressed** | Displays the suppressed faults for the server.<br>**Note** Only faults owned by the selected component are displayed. |
| **Step 4** | UCS-A/org/service-profile # **scope fault-suppress-task** *name* | Enters fault-suppress-task mode. |
| **Step 5** | UCS-A/org/service-profile/fault-suppress-task # **show detail expand** | Displays the schedule or fixed time interval for the task. |

The following example shows how to display the suppressed faults for a service profile:

```
UCS-A# scope org /
UCS-A/org # scope service-profile accounting
UCS-A/org/service-profile # show fault suppressed
UCS-A/org/service-profile #
Fault Suppress Task:

Name               Status             Global Schedule Suppress Policy Name
------------------ ------------------ --------------- --------------------
task1              Active             test_schedule1  Default Server Maint

UCS-A/org/service-profile #
```

The following example shows how to display the fault suppression task called task1:

```
UCS-A# scope org /
UCS-A/org # scope service-profile accounting
UCS-A/org/service-profile # scope fault-suppress-task task1
UCS-A/org/service-profile/fault-suppress-task # show detail expand
Fault Suppress Task:
    Name: task1
    Status: Active
    Global Schedule: test_schedule1
    Suppress Policy Name: Default Server Maint

UCS-A/org/service-profile/fault-suppress-task #
```

# Configuring Fault Suppression for an Organization

## Configuring Fault Suppression Tasks for an Organization Using a Fixed Time Interval

The **default-server-maint** suppression policy is selected by default.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*. |
| **Step 2** | UCS-A/org # **create fault-suppress-task** *name* | Creates a fault-suppress-task for the organization, and enters fault-suppress-task mode.<br>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 has been saved. |
| **Step 3** | UCS-A/org/fault-suppress-task # **create local-schedule** | Creates a local schedule and enters local-schedule mode. |
| **Step 4** | UCS-A/org/fault-suppress-task/local-schedule # **create occurrence single-one-time** | Creates a one-time occurrence, and enters single-one-time mode. |
| **Step 5** | UCS-A/org/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds* | Specifies the date and time that this occurrence should run. |
| **Step 6** | UCS-A/org/fault-suppress-task/local-schedule/single-one-time # **set max-duration** {**none** \| *num-of-days num-of-hours num-of-minutes num-of-seconds*} | Specifies the maximum length of time that this task can run. To run the task until it is manually stopped, enter none or omit this step. |
| **Step 7** | UCS-A/org/fault-suppress-task/local-schedule/single-one-time # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to create a fault suppression task called task2 under the Root organization, set the start date to January 1, 2013 at 11:00, and commit the transaction:

```
UCS-A# scope org /
UCS-A/org # create fault-suppress-task task2
UCS-A/org/fault-suppress-task* # create local-schedule
UCS-A/org/fault-suppress-task/local-schedule* # create occurrence single-one-time
UCS-A/org/fault-suppress-task/local-schedule/single-one-time* # set date jan 1 2013 11 00
```

```
OO
UCS-A/org/fault-suppress-task/local-schedule/single-one-time* # commit-buffer
```

## Configuring Fault Suppression Tasks for an Organization Using a Schedule

The **default-server-maint** suppression policy is selected by default.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*. |
| **Step 2** | UCS-A/org # **create fault-suppress-task** *name* | Creates a fault-suppress-task for the organization, and enters the fault-suppress-task mode.<br>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 has been saved. |
| **Step 3** | UCS-A/org/fault-suppress-task # **set schedule** *name* | Specifies the schedule that you want to use.<br>**Note** The schedule must exist before you can use it in a fault suppression task. For more information about creating schedules, see Creating a Schedule. |
| **Step 4** | UCS-A/org/fault-suppress-task # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to create a fault suppression task called task1 under the Root organization, apply the scheduler called weekly_maint to the task, and commit the transaction:

```
UCS-A# scope org /
UCS-A/org # create fault-suppress-task task1
UCS-A/org/fault-suppress-task* # set schedule weekly_maint
UCS-A/org/fault-suppress-task* # commit-buffer
```

## Deleting Fault Suppression Tasks for an Organization

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*. |
| **Step 2** | UCS-A/org # **delete fault-suppress-task** *name* | Deletes the specified fault suppression task. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | UCS-A/org # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to delete the fault suppression task called task1:

```
UCS-A# scope org /
UCS-A/org # delete fault-suppress-task task1
UCS-A/org* # commit-buffer
```

## Modifying Fault Suppression Tasks for an Organization

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*. |
| **Step 2** | UCS-A/org # **scope fault-suppress-task** *name* | Enters fault-suppress-task mode.<br>**Note** To apply a different schedule to the fault suppression task, go to Step 3. To change the fixed time interval of the fault suppression task, go to Step 4. |
| **Step 3** | UCS-A/org/fault-suppress-task # **set schedule** *name* | Applies a different schedule.<br>**Note** If you change from a fixed time interval to a schedule, the fixed time interval is deleted when you commit.<br>If you change from a schedule to a fixed time interval, the reference to the schedule is cleared when you commit. |
| **Step 4** | UCS-A/org/fault-suppress-task # **scope local-schedule** | Enters local-schedule mode. |
| **Step 5** | UCS-A/org/fault-suppress-task/local-schedule # **scope occurrence single-one-time** | Enters single-one-time mode. |
| **Step 6** | UCS-A/org/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds* | Specifies the date and time that this occurrence should run. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | UCS-A/org/fault-suppress-task/local-schedule/single-one-time # **set max-duration** {**none** \| *num-of-days num-of-hours num-of-minutes num-of-seconds*} | Specifies the maximum length of time that this task can run. To run the task until it is manually stopped, enter none or omit this step. |
| **Step 8** | UCS-A/org/fault-suppress-task/local-schedule/single-one-time # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to change the date and the fault suppression policy of the fault suppression task called task2:

```
UCS-A# scope org /
UCS-A/org # scope fault-suppress-task task2
UCS-A/org/fault-suppress-task* # scope local-schedule
UCS-A/org/fault-suppress-task/local-schedule # scope occurrence single-one-time
UCS-A/org/fault-suppress-task/local-schedule/single-one-time # set date dec 31 2013 11 00
00
UCS-A/org/fault-suppress-task/local-schedule/single-one-time* # commit-buffer
```

The following example shows how to apply a different schedule to the fault suppression task called task1:

```
UCS-A# scope org
UCS-A/org # scope fault-suppress-task task1
UCS-A/org/fault-suppress-task # set schedule monthly-maint
UCS-A/org/fault-suppress-task* # commit-buffer
```

## Viewing Suppressed Faults and Fault Suppression Tasks for an Organization

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*. |
| **Step 2** | UCS-A/org # **show fault suppressed** | Displays the suppressed faults for the organization<br>**Note** Only faults owned by the selected component are displayed. |
| **Step 3** | UCS-A/org # **scope fault-suppress-task** *name* | Enters fault-suppress-task mode. |
| **Step 4** | UCS-A/org/fault-suppress-task # **show detail expand** | Displays the schedule or fixed time interval for the task. |

The following example shows how to display the suppressed faults for an organization:

```
UCS-A# scope org Finance
UCS-A/org # show fault suppressed
UCS-A/org #
```

```
Fault Suppress Task:

Name                Status              Global Schedule Suppress Policy Name
------------------- ------------------- --------------- --------------------
task1               Active              test_schedule1  Default Server Maint

UCS-A/org #
```

The following example shows how to display the fault suppression task called task1:

```
UCS-A# scope org Finance
UCS-A/org # scope fault-suppress-task task1
UCS-A/org/fault-suppress-task # show detail expand
Fault Suppress Task:
    Name: task1
    Status: Active
    Global Schedule: test_schedule1
    Suppress Policy Name: Default Server Maint

UCS-A/org/fault-suppress-task #
```

# Configuring Settings for the Core File Exporter

## Core File Exporter

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

## Configuring the Core File Exporter

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope sysdebug** | Enters monitoring system debug mode. |
| **Step 3** | UCS-A /monitoring/sysdebug # **enable core-export-target** | Enables the core file exporter. When the core file exporter is enabled and an error causes the server to perform a core dump, the system exports the core file via TFTP to the specified remote server. |
| **Step 4** | UCS-A /monitoring/sysdebug # **set core-export-target path** *path* | Specifies the path to use when exporting the core file to the remote server. |
| **Step 5** | UCS-A /monitoring/sysdebug # **set core-export-target port** *port-num* | Specifies the port number to use when exporting the core file via TFTP. The range of valid values is 1 to 65,535. |
| **Step 6** | UCS-A /monitoring/sysdebug # **set core-export-target server-description** *description* | Provides a description for the remote server used to store the core file. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | UCS-A /monitoring/sysdebug # **set core-export-target server-name** *hostname* | Specifies the hostname of the remote server to connect with via TFTP. |
| **Step 8** | UCS-A /monitoring/sysdebug # **commit-buffer** | Commits the transaction. |

The following example enables the core file exporter, specifies the path and port to use when sending the core file, specifies the remote server hostname, provides a description for the remote server, and commits the transaction.

```
UCS-A# scope monitoring
UCS-A /monitoring # scope sysdebug
UCS-A /monitoring/sysdebug # enable core-export-target
UCS-A /monitoring/sysdebug* # set core-export-target path /root/CoreFiles/core
UCS-A /monitoring/sysdebug* # set core-export-target port 45000
UCS-A /monitoring/sysdebug* # set core-export-target server-description CoreFile102.168.10.10
UCS-A /monitoring/sysdebug* # set core-export-target server-name 192.168.10.10
UCS-A /monitoring/sysdebug* # commit-buffer
UCS-A /monitoring/sysdebug #
```

# Disabling the Core File Exporter

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope sysdebug** | Enters monitoring system debug mode. |
| **Step 3** | UCS-A /monitoring/sysdebug # **disable core-export-target** | Disables the core file exporter. When the core file exporter is disabled core files are not automatically exported. |
| **Step 4** | UCS-A /monitoring/sysdebug # **commit-buffer** | Commits the transaction. |

The following example disables the core file exporter and commits the transaction.

```
UCS-A# scope monitoring
UCS-A /monitoring # scope sysdebug
UCS-A /monitoring/sysdebug # disable core-export-target
UCS-A /monitoring/sysdebug* # commit-buffer
UCS-A /monitoring/sysdebug #
```

# Configuring the Syslog

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # {**enable** \| **disable**} **syslog console** | Enables or disables the sending of syslogs to the console. |
| **Step 3** | UCS-A /monitoring # **set syslog console level** {**emergencies** \| **alerts** \| **critical**} | (Optional)<br>Select the lowest message level that you want displayed. If syslogs are enabled, the system displays that level and above on the console. The level options are listed in order of decreasing urgency.The default level is Critical. |
| **Step 4** | UCS-A /monitoring # {**enable** \| **disable**} **syslog monitor** | Enables or disables the monitoring of syslog information by the operating system. |
| **Step 5** | UCS-A /monitoring # **set syslog monitor level** {**emergencies** \| **alerts** \| **critical** \| **errors** \| **warnings** \| **notifications** \| **information** \| **debugging**} | (Optional)<br>Select the lowest message level that you want displayed. If the monitor state is enabled, the system displays that level and above. The level options are listed in order of decreasing urgency.The default level is Critical.<br>**Note** Messages at levels below Critical are displayed on the terminal monitor only if you have entered the **terminal monitor** command. |
| **Step 6** | UCS-A /monitoring # {**enable** \| **disable**} **syslog file** | Enables or disables the writing of syslog information to a syslog file. |
| **Step 7** | UCS-A /monitoring # **set syslog file name** *filename* | The name of the file in which the messages are logged. Up to 16 characters are allowed in the file name. |
| **Step 8** | UCS-A /monitoring # **set syslog file level** {**emergencies** \| **alerts** \| **critical** \| **errors** \| **warnings** \| **notifications** \| **information** \| **debugging**} | (Optional)<br>Select the lowest message level that you want stored to a file. If the file state is enabled, the system stores that level and above in the syslog file. The level options are listed in order of decreasing urgency.The default level is Critical. |
| **Step 9** | UCS-A /monitoring # **set syslog file size** *filesize* | (Optional)<br>The maximum file size, in bytes, before the system begins to write over the oldest messages with the newest ones. The range is 4096 to 4194304 bytes. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 10** | UCS-A /monitoring # {**enable** \| **disable**} **syslog remote-destination** {**server-1** \| **server-2** \| **server-3**} | Enables or disables the sending of syslog messages to up to three external syslog servers. |
| **Step 11** | UCS-A /monitoring # **set syslog remote-destination** {**server-1** \| **server-2** \| **server-3**} **level**{**emergencies** \| **alerts** \| **critical** \| **errors** \| **warnings** \| **notifications** \| **information** \| **debugging**} | (Optional)<br>Select the lowest message level that you want stored to the external log. If the remote-destination is enabled, the system sends that level and above to the external server. The level options are listed in order of decreasing urgency.The default level is Critical. |
| **Step 12** | UCS-A /monitoring # **set syslog remote-destination** {**server-1** \| **server-2** \| **server-3**} **hostname** *hostname* | The hostname or IP address of the specified remote syslog server. Up to 256 characters are allowed in the hostname. |
| **Step 13** | UCS-A /monitoring # **set syslog remote-destination** {**server-1** \| **server-2** \| **server-3**} **facility** {**local0** \| **local1** \| **local2** \| **local3** \| **local4** \| **local5** \| **local6** \| **local7**} | (Optional)<br>The facility level contained in the syslog messages sent to the specified remote syslog server. |
| **Step 14** | UCS-A /monitoring # {**enable** \| **disable**} **syslog source** {**audits** \| **events** \| **faults**} | This can be one of the following:<br>• **audits—**Enables or disables the logging of all audit log events.<br>• **events—**Enables or disables the logging of all system events.<br>• **faults—**Enables or disables the logging of all system faults. |
| **Step 15** | UCS-A /monitoring # **commit-buffer** | Commits the transaction. |

This example shows how to enable the storage of syslog messages in a local file and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # disable syslog console
UCS-A /monitoring* # disable syslog monitor
UCS-A /monitoring* # enable syslog file
UCS-A /monitoring* # set syslog file name SysMsgsUCSA
UCS-A /monitoring* # set syslog file level notifications
UCS-A /monitoring* # set syslog file size 4194304
UCS-A /monitoring* # disable syslog remote-destination server-1
UCS-A /monitoring* # disable syslog remote-destination server-2
UCS-A /monitoring* # disable syslog remote-destination server-3
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

# Viewing Audit Logs

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope security** | Enters security mode. |
| **Step 2** | UCS-A /security # **show audit-logs** | Displays the audit logs. |

The following example displays the audit logs:

```
UCS-A# scope security
UCS-A /security # show audit-logs
Audit trail logs:
    Creation Time        User       ID       Action           Description

    -------------------- ---------- -------- ---------------- -----------

    2013-01-04T19:05:36.027
                         internal    1055936 Creation         Fabric A:
local us
er admin logge
    2013-01-03T23:08:37.459
                         admin       1025416 Creation         Uplink FC
VSAN mem
ber port A/1/3
    2013-01-03T23:08:37.459
                         admin       1025417 Deletion         Uplink FC
VSAN mem
ber port A/1/3
    2013-01-03T23:08:02.387
                         admin       1025299 Creation         Uplink FC
VSAN mem
ber port A/1/3
    2013-01-03T23:08:02.387
                         admin       1025300 Deletion         Uplink FC
VSAN mem
ber port A/1/3
    2013-01-03T23:03:23.926
                         admin       1025096 Creation         Uplink FC
VSAN mem
ber port A/1/3
UCS-A /security #
```

# Configuring the Log File Exporter

## Log File Exporter

Cisco UCS Manager generates log files for each executable. The log files can be up to 20 MB in size, and up to five backups can be stored on the server. The log file exporter allows you to export the log files to a remote server before they are deleted. The log file names contain the following information:

- The name of the process
- Timestamp
- The name and ID of the fabric interconnect

**Note** If you do not enable log exporting, the oldest log files are deleted whenever the maximum backup file limit is reached.

### Guidelines and Limitations

- We recommend that you use tftp or password-less scp or sftp for log export. When standard scp or sftp is used, the user password is stored in the configuration file in encrypted format.
- On a HA setup, the log files from each side are exported separately. If one side fails to export logs, the other side does not compensate.

## Exporting Log Files to a Remote Server

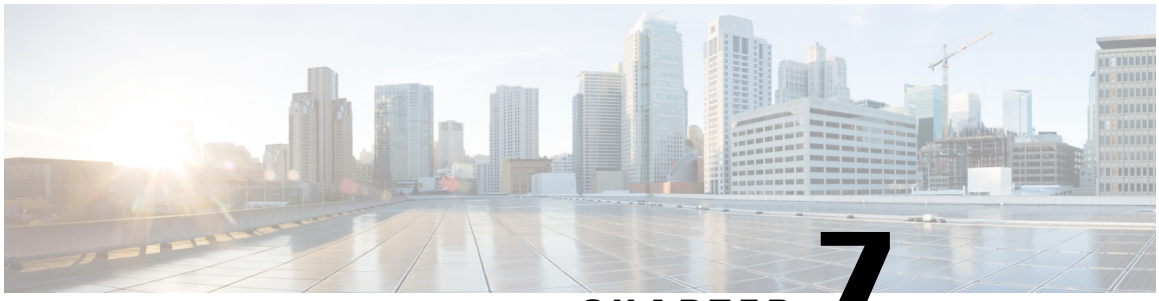
### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope sysdebug** | Enters monitoring system debug mode. |
| **Step 3** | UCS-A /monitoring/sysdebug # **scope log-export-policy** | Enters log file export mode. |
| **Step 4** | UCS-A /monitoring/sysdebug/log-export-policy # **set admin-state** {**disabled** \| **enabled**} | Whether log file exporting is enabled. |
| **Step 5** | UCS-A /monitoring/sysdebug/log-export-policy # **set desc** *description* | (Optional)<br>Provides a description for the log export policy |
| **Step 6** | UCS-A /monitoring/sysdebug/log-export-policy # **set hostname** *hostname* | Specifies the hostname of the remote server. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | UCS-A /monitoring/sysdebug/log-export-policy # **set passwd** | After you press Enter, you are prompted to enter the password.<br>Specifies the password for the remote server username. This step does not apply if the TFTP protocol is used. |
| **Step 8** | UCS-A /monitoring/sysdebug/log-export-policy # **set passwordless-ssh** {**no** \| **yes**} | Enables SSH login without a password. |
| **Step 9** | UCS-A /monitoring/sysdebug/log-export-policy # **set proto** {**scp** \| **ftp** \| **sftp** \| **tftp**} | Specifies the protocol to use when communicating with the remote server. |
| **Step 10** | UCS-A /monitoring/sysdebug/log-export-policy # **set path** *path* | Specifies the path on the remote server where the log file is to be saved. |
| **Step 11** | UCS-A /monitoring/sysdebug/log-export-policy # **set user** *username* | Specifies the username the system should use to log in to the remote server. This step does not apply if the TFTP protocol is used. |
| **Step 12** | UCS-A /monitoring/sysdebug/log-export-policy # **commit-buffer** | Commits the transaction. |

The following example shows how to enable the log file exporter, specify the remote server hostname, set the protocol to scp, enable passwordless login, and commit the transaction.

```
UCS-A# scope monitoring
UCS-A /monitoring # scope sysdebug
UCS-A /monitoring/sysdebug # scope log-export-policy
UCS-A /monitoring/sysdebug/log-export-policy # set admin-state enable
UCS-A /monitoring/sysdebug/log-export-policy* # set hostname 10.10.1.1
UCS-A /monitoring/sysdebug/log-export-policy* # set path /
UCS-A /monitoring/sysdebug/log-export-policy* # set user testuser
UCS-A /monitoring/sysdebug/log-export-policy* # set proto scp
UCS-A /monitoring/sysdebug/log-export-policy* # set passwd
password:
UCS-A /monitoring/sysdebug/log-export-policy* # set passwordless-ssh yes
UCS-A /monitoring/sysdebug/log-export-policy* # commit-buffer
UCS-A /monitoring/sysdebug/log-export-policy #
```



CHAPTER 7

# NetFlow Monitoring

This chapter includes the following sections:


- NetFlow Monitoring, page 107
- NetFlow Limitations, page 108
- Configuring a Flow Record Definition, page 109
- Configuring an Exporter Profile, page 110
- Configuring a Netflow Collector, page 111
- Configuring a Flow Exporter, page 111
- Configuring a Flow Monitor, page 112
- Configuring a Flow Monitor Session, page 113
- Configuring a NetFlow Cache Active and Inactive Timeout, page 114
- Associating a Flow Monitor Session to a vNIC, page 114


# NetFlow Monitoring

**Note** 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 then 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, or the protocol used. Flows are collected when they match the definitions in the flow record definition.

### Flow Record Definitions

A flow record definition contains all 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 nonkeys, are values that you can measure, 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. You can use the following type of flow record definitions:

- **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 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. First generation or non-Cisco VIC adapters are not supported.

  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.
- You can have up to 64 flow record definitions, flow exporters, and flow monitors.
- NetFlow is not supported in vNIC template objects.
- PVLANs and local VLANs are not supported for service VLANs.
- All VLANs must be public and must be common to both fabric interconnects.
- VLANs must be defined as an exporter interface before they can be used with a flow collector.
- You cannot use NetFlow with usNIC, the Virtual Machine queue, or Linux ARFS.

# Configuring a Flow Record Definition

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-flow-mon** | Enters the ethernet flow monitor mode. |
| **Step 2** | UCS-A /eth-flow-mon # **enter flow-record** *flow-record-name* | Enters flow record mode for the specified flow record. |
| **Step 3** | UCS-A /eth-flow-mon/flow-record # **set keytype** {**ipv4keys** \| **ipv6keys** \| **l2keys**} | Specifies the key type. |
| **Step 4** | UCS-A /eth-flow-mon/flow-record # **set ipv4keys** {**dest-port** \| **ip-protocol** \| **ip-tos** \| **ipv4-dest-address** \| **ipv4-src-address** \| **src-port**} | Specifies the attributes for the key type that you selected in Step 3.<br>**Note** Use this command only if you chose **ipv4keys** in step 3. |
| **Step 5** | UCS-A /eth-flow-mon/flow-record # **set ipv6keys** {**dest-port** \| **ip-protocol** \| **ipv6-dest-address** \| **ipv6-src-address** \| **src-port**} | Specifies the attributes for the key type that you selected in Step 3.<br>**Note** Use this command only if you chose **ipv6keys** in Step 3. |
| **Step 6** | UCS-A /eth-flow-mon/flow-record # **set l2keys** {**dest-mac-address** \| **ethertype** \| **src-mac-address**} | Specifies the attributes for the key type that you chose in Step 3.<br>**Note** Use this command only if you selected **l2keys** in step 3. |
| **Step 7** | UCS-A /eth-flow-mon/flow-record # **set nonkeys** {**counter-bytes-long** \| **counter-packets-long** \| **sys-uptime-first** \| **sys-uptime-last**} | Specifies the nonkey attributes. |
| **Step 8** | UCS-A /eth-flow-mon/flow-record # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to create a flow record definition with Layer 2 keys and commit the transaction:

```
UCS-A# scope eth-flow-mon
UCS-A /eth-flow-mon # enter flow-record r1
UCS-A /eth-flow-mon/flow-record* # set keytype l2keys
UCS-A /eth-flow-mon/flow-record* #set l2keys dest-mac-address src-mac-address
UCS-A /eth-flow-mon/flow-record* # set nonkeys sys-uptime counter-bytes counter-packets
UCS-A /eth-flow-mon/flow-record* # commit-buffer
UCS-A /eth-flow-mon/flow-record #
```

# Configuring an Exporter Profile

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-flow-mon** | Enters the ethernet flow monitor mode. |
| **Step 2** | UCS-A /eth-flow-mon # **scope flow-profile** *profile-name* | Enters the flow profile mode for the specified profile. |
| **Step 3** | UCS-A /eth-flow-mon/flow-profile # **show config** | Displays the flow profile configuration. |
| **Step 4** | UCS-A /eth-flow-mon/flow-profile # **enter vlan** *vlan-name* | Specifies the VLAN associated with the exporter profile. PVLANs and local VLAN are not supported. All VLAN must be public and must be common to both fabric interconnects. |
| **Step 5** | UCS-A /eth-flow-mon/flow-profile/vlan # **enter fabric** {**a** \| **b**} | Enters flow profile mode for the specified fabric. |
| **Step 6** | UCS-A /eth-flow-mon/flow-profile/vlan/fabric/ # **set addr** *ip-addr* **subnet** *ip-addr* | Specifies the source IP and subnet mask for the exporter profile on the fabric. |
| **Step 7** | UCS-A /eth-flow-mon/flow-profile/vlan/fabric/ # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to configure the default exporter profile, set the source IP and subnet mask for the exporter interface on each fabric, and commit the transaction:

```
UCS-A# scope eth-flow-mon
UCS-A /eth-flow-mon # scope flow-profile default
UCS-A /eth-flow-mon/flow-profile # enter vlan 100
UCS-A /eth-flow-mon/flow-profile/vlan* # enter fabric a
UCS-A /eth-flow-mon/flow-profile/vlan/fabric* # set addr 10.10.10.10 subnet 255.255.255.0
UCS-A /eth-flow-mon/flow-profile/vlan/fabric* # up
UCS-A /eth-flow-mon/flow-profile/vlan* # enter fabric b
UCS-A /eth-flow-mon/flow-profile/vlan/fabric* # set addr 10.10.10.11 subnet 255.255.255.0
UCS-A /eth-flow-mon/flow-profile/vlan/fabric* # commit-buffer
UCS-A /eth-flow-mon/flow-profile/vlan/fabric #
```

# Configuring a Netflow Collector

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-flow-mon** | Enters the ethernet flow monitor mode. |
| **Step 2** | UCS-A /eth-flow-mon # **enter flow-collector** *flow-collector-name* | Enters the flow collector mode for the specified flow collector. |
| **Step 3** | UCS-A /eth-flow-mon/flow-collector # **set dest-port** *port_number* | Specifies the destination port for the flow collector. |
| **Step 4** | UCS-A /eth-flow-mon/flow-collector # **set vlan** *vlan_id* | Specifies the VLAN ID for the flow collector. |
| **Step 5** | UCS-A /eth-flow-mon/flow-collector # **enter ip-if** | Enters IPv4 configuration mode. |
| **Step 6** | UCS-A /eth-flow-mon/flow-collector/ip-if # **set addr** *ip-address* | Specifies the exporter IP address. |
| **Step 7** | UCS-A /eth-flow-mon/flow-collector/ip-if # **set exporter-gw** *gw-address* | Specifies the exporter gateway address. |
| **Step 8** | UCS-A /eth-flow-mon/flow-collector/ip-if # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to configure a NetFlow collector, set the exporter IP and gateway address, and commit the transaction:

```
UCS-A# scope eth-flow-mon
UCS-A /eth-flow-mon # enter flow-collector c1
UCS-A /eth-flow-mon/flow-collector* # set dest-port 9999
UCS-A /eth-flow-mon/flow-collector* # set vlan vlan100
UCS-A /eth-flow-mon/flow-collector* # enter ip-if
UCS-A /eth-flow-mon/flow-collector/ip-if* # set addr 20.20.20.20
UCS-A /eth-flow-mon/flow-collector/ip-if* # set exporter-gw 10.10.10.1
UCS-A /eth-flow-mon/flow-collector/ip-if* # commit-buffer
UCS-A /eth-flow-mon/flow-collector/ip-if #
```

# Configuring a Flow Exporter

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-flow-mon** | Enters the ethernet flow monitor mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | UCS-A /eth-flow-mon # **enter flow-exporter** *flow-exporter-name* | Enters the flow exporter mode for the specified flow exporter. |
| **Step 3** | UCS-A /eth-flow-mon/flow-exporter # **set dscp** *dscp_number* | Specifies the differentiated services code point. |
| **Step 4** | UCS-A /eth-flow-mon/flow-exporter # **set flow-collector** *flow-collector_name* | Specifies the flow collector. |
| **Step 5** | UCS-A /eth-flow-mon/flow-exporter # **set exporter-stats-timeout** *timeout_number* | Specifies the timeout period for resending NetFlow flow exporter data. |
| **Step 6** | UCS-A /eth-flow-mon/flow-exporter # **set interface-table-timeout** *timeout_number* | Specifies the time period for resending the NetFlow flow exporter interface table. |
| **Step 7** | UCS-A /eth-flow-mon/flow-exporter # **set template-data-timeout** *timeout_number* | Specifies the timeout period for resending NetFlow template data. |
| **Step 8** | UCS-A /eth-flow-mon/flow-exporter # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to configure a flow exporter, set the timeout values, and commit the transaction:

```
UCS-A# scope eth-flow-mon
UCS-A /eth-flow-mon # enter flow-exporter ex1
UCS-A /eth-flow-mon/flow-exporter* # set dscp 6
UCS-A /eth-flow-mon/flow-exporter* # set flow-collector c1
UCS-A /eth-flow-mon/flow-exporter* # set exporter-stats-timeout 600
UCS-A /eth-flow-mon/flow-exporter* # set interface-table-timeout 600
UCS-A /eth-flow-mon/flow-exporter* # set template-data-timeout 600
UCS-A /eth-flow-mon/flow-exporter* # commit-buffer
UCS-A /eth-flow-mon/flow-exporter #
```

# Configuring a Flow Monitor

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-flow-mon** | Enters the ethernet flow monitor mode. |
| **Step 2** | UCS-A /eth-flow-mon # **enter flow-monitor** *flow-monitor-name* | Enters the flow monitor mode for the specified flow monitor. |
| **Step 3** | UCS-A /eth-flow-mon/flow-monitor # **set flow-record** *flow-record-name* | Specifies the flow record. |
| **Step 4** | UCS-A /eth-flow-mon/flow-monitor # **create flow-exporter** *flow-exporter-name* | Specifies the first flow exporter. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | UCS-A /eth-flow-mon/flow-monitor # **create flow-exporter** *flow-exporter-name* | Specifies the second flow exporter. |
| **Step 6** | UCS-A /eth-flow-mon/flow-monitor # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to create a flow monitor and commit the transaction:

```
UCS-A# scope eth-flow-mon
UCS-A /eth-flow-mon # enter flow-monitor m1
UCS-A /eth-flow-mon/flow-monitor* # set flow-record r1
UCS-A /eth-flow-mon/flow-monitor* # create flow-exporter ex1
UCS-A /eth-flow-mon/flow-monitor* # create flow-exporter ex2
UCS-A /eth-flow-mon/flow-monitor* # commit-buffer
UCS-A /eth-flow-mon/flow-monitor #
```

# Configuring a Flow Monitor Session

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-flow-mon** | Enters the ethernet flow monitor mode. |
| **Step 2** | UCS-A /eth-flow-mon # **enter flow-mon-session** *flow-monitor-session-name* | Enters the flow monitor session mode for the specified flow monitor session. |
| **Step 3** | UCS-A /eth-flow-mon/flow-mon-session # **create flow-monitor** *flow-monitor-1* | Specifies the first flow monitor. |
| **Step 4** | UCS-A /eth-flow-mon/flow-mon-session # **create flow-monitor** *flow-monitor-2* | Specifies the second flow monitor. |
| **Step 5** | UCS-A /eth-flow-mon/flow-mon-session # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to create a flow monitor session with two flow monitors:

```
UCS-A# scope eth-flow-mon
UCS-A /eth-flow-mon # enter flow-mon-session s1
UCS-A /eth-flow-mon/flow-mon-session* # create flow-monitor m1
UCS-A /eth-flow-mon/flow-mon-session* # create flow-monitor m2
UCS-A /eth-flow-mon/flow-mon-session* # commit-buffer
UCS-A /eth-flow-mon/flow-mon-session #
```

# Configuring a NetFlow Cache Active and Inactive Timeout

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-flow-mon** | Enters the ethernet flow monitor mode. |
| **Step 2** | UCS-A /eth-flow-mon # **scope flow-timeout** *timeout-name* | Enters the flow timeout mode for the specified flow timeout. |
| **Step 3** | UCS-A /eth-flow-mon/flow-timeout # **set cache-timeout-active** *timeout-value* | Specifies the active timeout value. This value can be between 60 and 4092 seconds. The default value is 120 seconds. |
| **Step 4** | UCS-A /eth-flow-mon/flow-timeout # **set cache-timeout-inactive** *timeout-value* | Specifies the inactive timeout value. This value can be between 15 and 4092 seconds. The default value is 15 seconds. |
| **Step 5** | UCS-A /eth-flow-mon/flow-timeout # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to change the NetFlow timeout values and commit the transaction:

```
UCS-A# scope eth-flow-mon
UCS-A /eth-flow-mon # scope flow-timeout default
UCS-A /eth-flow-mon/flow-timeout # set cache-timeout-active 1800
UCS-A /eth-flow-mon/flow-timeout* # set cache-timeout-inactive 20
UCS-A /eth-flow-mon/flow-timeout* # commit-buffer
UCS-A /eth-flow-mon/flow-timeout #
```

# Associating a Flow Monitor Session to a vNIC

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*. |
| **Step 2** | UCS-A /org # **scope service-profile** *profile-name* | Enters the organization service profile mode for the specified service profile. |
| **Step 3** | UCS-A /org/service-profile # **scope vnic** *vnic-name* | Enters the organization service profile mode for the specified vNIC. |
| **Step 4** | UCS-A /org/service-profile/vnic # **enter flow-mon-src** *flow-monitor-session-name* | Associates the flow monitor session to the vNIC. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | UCS-A /org/service-profile/vnic # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to associate the flow monitor session s1 to the vNIC eth5:

```
UCS-A# scope org /
UCS-A /org # scope service-profile sp1
UCS-A /org/service-profile # scope vnic eth5
UCS-A /org/service-profile/vnic # enter flow-mon-src s1
UCS-A /org/service-profile/vnic # commit-buffer
```