



Cisco UCS Manager CLI System Monitoring Guide, Release 2.5

First Published: April 07, 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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.



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 5

Adding Traffic Sources to a Monitoring Session 6

Adding an Uplink Source Port to a Monitoring Session 6

Adding a vNIC or vHBA Source to a Monitoring Session 7

Adding a VLAN or VSAN Source to a Monitoring Session 9

Adding a Storage Port Source to a Monitoring Session 10

Activating a Traffic Monitoring Session 11

Deleting a Traffic Monitoring Session 12

CHAPTER 2

Monitoring Hardware 15

Monitoring Fan Modules 15

Monitoring Management Interfaces 17

Management Interfaces Monitoring Policy 17

Configuring the Management Interfaces Monitoring Policy 18

Local Storage Monitoring 20

Support for Local Storage Monitoring 20

Prerequisites for Local Storage Monitoring 21

Viewing the Status of a Disk Drive	21
Viewing Detailed Information About Virtual Drives	22
Viewing Detailed Information About the Storage Controller	24
Viewing Storage Controller Operations	24

CHAPTER 3

Configuring Statistics-Related Policies 27

Configuring Statistics Collection Policies	27
Statistics Collection Policy	27
Configuring a Statistics Collection Policy	28
Configuring Statistics Threshold Policies	28
Statistics Threshold Policy	28
Server and Server Component Statistics Threshold Policy Configuration	29
Configuring a Server and Server Component Statistics Threshold Policy	29
Deleting a Server and Server Component Statistics Threshold Policy	30
Configuring a Server and Server Component Statistics Threshold Policy Class	31
Deleting a Server and Server Component Statistics Threshold Policy Class	32
Uplink Ethernet Port Statistics Threshold Policy Configuration	33
Configuring an Uplink Ethernet Port Statistics Threshold Policy	33
Configuring an Uplink Ethernet Port Statistics Threshold Policy Class	34
Deleting an Uplink Ethernet Port Statistics Threshold Policy Class	36
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	39
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	53
Enabling Call Home	53
Configuring System Inventory Messages	54
Configuring System Inventory Messages	54
Sending a System Inventory Message	55
Configuring Call Home Profiles	56
Call Home Profiles	56
Call Home Alert Groups	56
Configuring a Call Home Profile	57
Deleting a Call Home Profile	60
Sending a Test Call Home Alert	60
Configuring Call Home Policies	62
Call Home Policies	62
Configuring a Call Home Policy	62
Disabling a Call Home Policy	63
Enabling a Call Home Policy	64
Deleting a Call Home Policy	64
Configuring Anonymous Reporting	65
Enabling Anonymous Reporting	65
Disabling Anonymous Reporting	66
Viewing Anonymous Reports	67
Example: Configuring Call Home for Smart Call Home	69
Configuring Smart Call Home	69
Configuring the Default Cisco TAC-1 Profile	71
Configuring a System Inventory Message for Smart Call Home	72
Registering Smart Call Home	73

CHAPTER 5**Managing the System Event Log 75**

System Event Log	75
Viewing the System Event Log for a Server	75
Configuring the SEL Policy	77

Backing Up the System Event Log for a Server 79

Clearing the System Event Log for a Server 79

CHAPTER 6

Configuring Settings for Faults, Events, and Logs 81

Configuring Settings for the Fault Collection Policy 81

Global Fault Policy 81

Configuring the Fault Collection Policy 82

Configuring Fault Suppression 83

Fault Suppression 83

Configuring Fault Suppression for a Chassis 84

Configuring Fault Suppression Tasks for a Chassis Using a Fixed Time Interval 84

Configuring Fault Suppression Tasks for a Chassis Using a Schedule 86

Deleting Fault Suppression Tasks for a Chassis 87

Modifying Fault Suppression Tasks for a Chassis 88

Viewing Suppressed Faults and Fault Suppression Tasks for a Chassis 89

Configuring Fault Suppression for a Server 90

Configuring Fault Suppression Tasks for a Server Using a Fixed Time Interval 90

Configuring Fault Suppression Tasks for a Server using a Schedule 92

Deleting Fault Suppression Tasks for a Server 93

Modifying Fault Suppression Tasks for a Server 93

Viewing Suppressed Faults and Fault Suppression Tasks for a Server 95

Configuring Fault Suppression for a Service Profile 96

Configuring Fault Suppression Tasks for a Service Profile Using a Fixed Time Interval 96

Configuring Fault Suppression Tasks for a Service Profile Using a Schedule 97

Deleting Fault Suppression Tasks for a Service Profile 98

Modifying Fault Suppression Tasks for a Service Profile 99

Viewing Suppressed Faults and Fault Suppression Tasks for a Service Profile 101

Configuring Fault Suppression for an Organization 102

Configuring Fault Suppression Tasks for an Organization Using a Fixed Time Interval 102

Configuring Fault Suppression Tasks for an Organization Using a Schedule 103

Deleting Fault Suppression Tasks for an Organization 104

Modifying Fault Suppression Tasks for an Organization 105

Viewing Suppressed Faults and Fault Suppression Tasks for an Organization 106

Configuring Settings for the Core File Exporter	107
Core File Exporter	107
Configuring the Core File Exporter	107
Disabling the Core File Exporter	108
Configuring the Syslog	109
Viewing Audit Logs	111
Configuring the Log File Exporter	112
Log File Exporter	112
Exporting Log Files to a Remote Server	113



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 . Main titles such as window, dialog box, and wizard titles appear in this font .
Document titles	Document titles appear in <i>this font</i> .
TUI elements	In a Text-based User Interface, text the system displays appears in <i>this font</i> .
System output	Terminal sessions and information that the system displays appear in <i>this font</i> .

Text Type	Indication
CLI commands	CLI command keywords appear in this font . Variables in a CLI command appear in <i>this font</i> .
[]	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.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_M_Series_Servers_Documentation_Roadmap.html

Other Documentation Resources

Follow [Cisco UCS Docs on Twitter](#) to receive document update notifications.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-docfeedback@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 5](#)
- [Adding Traffic Sources to a Monitoring Session, page 6](#)
- [Activating a Traffic Monitoring Session, page 11](#)
- [Deleting a Traffic Monitoring Session, page 12](#)

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



Important

Fibre Channel, Fibre Channel over Ethernet, vHBA, VSAN, and SAN are not supported in Cisco UCS Release 2.5

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.



Important

Fibre Channel and Fibre Channel over Ethernet are not supported in Cisco UCS Manager Release 2.5.

- 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 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

**Note**

This procedure describes creating an Ethernet traffic monitoring session. To create a Fibre Channel traffic monitoring session, the following changes are required:

- Enter the **scope fc-traffic-mon** command instead of the **scope eth-traffic-mon** command in Step 1.
- Enter the **create fc-mon-session** command instead of the **create eth-mon-session** command in Step 3.

SUMMARY STEPS

1. UCS-A# **scope eth-traffic-mon**
2. UCS-A /eth-traffic-mon # **scope fabric {a | b}**
3. UCS-A /eth-traffic-mon/fabric # **create eth-mon-session** *session-name*
4. UCS-A /eth-traffic-mon/fabric/eth-mon-session # **create dest-interface** *slot-num port-num*
5. UCS-A /eth-traffic-mon/fabric/eth-mon-session/dest-interface # **set speed***admin-speed*
6. UCS-A /eth-traffic-mon/fabric/eth-mon-session/dest-interface # **commit-buffer**

DETAILED STEPS

	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: <ul style="list-style-type: none"> • 1gbps—1 Gbps • 10gbps—10 Gbps • 20gbps—20 Gbps • 40gbps—40 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

SUMMARY STEPS

1. UCS-A# **scope fc-traffic-mon**
2. UCS-A /fc-traffic-mon # **scope fabric {a | b}**
3. UCS-A /fc-traffic-mon/fabric # **create fc-mon-session session-name**
4. UCS-A /fc-traffic-mon/fabric/fc-mon-session # **create dest-interface slot-num port-num**
5. UCS-A /fc-traffic-mon/fabric/fc-mon-session/dest-interface # **set speedadmin-speed**
6. UCS-A /fc-traffic-mon/fabric/fc-mon-session/dest-interface # **commit-buffer**

DETAILED STEPS

	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 speedadmin-speed	Sets the data transfer rate of the port channel to be monitored. This can be: <ul style="list-style-type: none"> • 1gbps—1 Gbps • 2gbps—2 Gbps • 4gbps—4 Gbps • 8gbps—8 Gbps • 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.

SUMMARY STEPS

1. UCS-A# **scope eth-uplink**
2. UCS-A /eth-uplink # **scope fabric {a | b}**
3. UCS-A /eth-uplink/fabric # **scope interface slot-num port-num**
4. UCS-A /eth-uplink/fabric/interface # **create mon-src session-name**
5. (Optional) UCS-A /eth-uplink/fabric/interface/mon-src # **set direction {both | receive | transmit}**
6. UCS-A /eth-uplink/fabric/interface/mon-src # **commit-buffer**

DETAILED STEPS

	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) Specifies the traffic direction to be monitored.

	Command or Action	Purpose
		Note If you do not select any direction, the default direction is Rx.
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 vhma** command instead of the **scope vnic** command in Step 2.

Before You Begin

A traffic monitoring session must be created.

SUMMARY STEPS

1. Switch-A# **scope system**
2. Switch-A /system # **scope vm-mgmt**
3. (Optional) Switch-A /system/vm-mgmt # **show virtual-machine**
4. Switch-A /system/vm-mgmt # **scope virtual-machine** *uuid*
5. (Optional) Switch-A /system/vm-mgmt/virtual-machine # **show expand**
6. Switch-A /system/vm-mgmt/virtual-machine # **scope vnic** *mac-address*
7. Switch-A /system/vm-mgmt/virtual-machine/vnic # **create mon-src** *session-name*
8. (Optional) Switch-A /system/vm-mgmt/virtual-machine/vnic/mon-src # **set direction** {both | receive | transmit}
9. Switch-A /system/vm-mgmt/virtual-machine/vnic/mon-src # **commit-buffer**

DETAILED STEPS

	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) Displays the running virtual machines.
Step 4	Switch-A /system/vm-mgmt # scope virtual-machine <i>uuid</i>	Enters command mode for the virtual machine that contains the dynamic vNIC.
Step 5	Switch-A /system/vm-mgmt/virtual-machine # show expand	(Optional) Displays the virtual machine details, including the vNIC MAC address.
Step 6	Switch-A /system/vm-mgmt/virtual-machine # scope vnic <i>mac-address</i>	Enters the command mode for the vNIC at the specified MAC address.
Step 7	Switch-A /system/vm-mgmt/virtual-machine/vnic # create mon-src <i>session-name</i>	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) 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.

SUMMARY STEPS

1. UCS-A# **scope eth-uplink**
2. UCS-A /eth-uplink # **scope fabric {a | b}**
3. UCS-A /eth-uplink/fabric # **create vlan vlan-name vlan-id**
4. UCS-A /eth-uplink/fabric/vlan # **create mon-src session-name**
5. UCS-A /eth-uplink/fabric/vlan/mon-src # **commit-buffer**

DETAILED STEPS

	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. 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.

	Command or Action	Purpose
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.

SUMMARY STEPS

1. UCS-A# **scope fc-storage**
2. UCS-A /fc-storage # **scope fabric {a | b}**
3. UCS-A /fc-storage/fabric # **create interface fc slot-num port-num**
4. UCS-A /fc-storage/fabric/fc # **create mon-src session-name**
5. UCS-A /fc-storage/fabric/fc/mon-src # **commit-buffer**

DETAILED STEPS

	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.

	Command or Action	Purpose
Step 3	UCS-A /fc-storage/fabric # create interface fc <i>slot-num port-num</i>	Creates a Fibre Channel storage port interface and enters the interface command mode.
Step 4	UCS-A /fc-storage/fabric/fc # create mon-src <i>session-name</i>	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



Note

This procedure describes activating an Ethernet traffic monitoring session. To activate a Fibre Channel traffic monitoring session, the following changes are required:

- Enter the **scope fc-traffic-mon** command instead of the **scope eth-traffic-mon** command in Step 1.
- Enter the **scope fc-mon-session** command instead of the **scope eth-mon-session** command in Step 3.

Before You Begin

Configure a traffic monitoring session.

SUMMARY STEPS

1. UCS-A# **scope eth-traffic-mon**
2. UCS-A /eth-traffic-mon # **scope fabric** {a | b}
3. UCS-A /eth-traffic-mon/fabric # **scope eth-mon-session** *session-name*
4. UCS-A /eth-traffic-mon/fabric/eth-mon-session # **disable** | **enable**
5. UCS-A /eth-traffic-mon/fabric/eth-mon-session # **commit-buffer**

DETAILED STEPS

	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


Note

This procedure describes deleting an Ethernet traffic monitoring session. To delete a Fibre Channel traffic monitoring session, the following changes are required:

- Enter the **scope fc-traffic-mon** command instead of the **scope eth-traffic-mon** command in Step 1.
- Enter the **delete fc-mon-session** command instead of the **delete eth-mon-session** command in Step 3.

SUMMARY STEPS

1. UCS-A# **scope eth-traffic-mon**
2. UCS-A /eth-traffic-mon # **scope fabric {a | b}**
3. UCS-A /eth-traffic-mon/fabric # **delete eth-mon-session *session-name***
4. UCS-A /eth-traffic-mon/fabric # **commit-buffer**

DETAILED STEPS

	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 # delete eth-mon-session <i>session-name</i>	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 #
```




Monitoring Hardware

This chapter includes the following sections:

- [Monitoring Fan Modules, page 15](#)
- [Monitoring Management Interfaces, page 17](#)
- [Local Storage Monitoring, page 20](#)

Monitoring Fan Modules

SUMMARY STEPS

1. UCS-A# **scope chassis** *chassis-num*
2. UCS-A /chassis # **show environment fan**
3. UCS-A /chassis # **scope fan-module** *tray-num module-num*
4. UCS-A /chassis/fan-module # **show** [**detail** | **expand**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope chassis <i>chassis-num</i>	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. This includes the following information: <ul style="list-style-type: none">• Overall status• Operability• Power state• Thermal status• Threshold status

	Command or Action	Purpose
		<ul style="list-style-type: none"> Voltage status
Step 3	UCS-A /chassis # scope fan-module <i>tray-num</i> <i>module-num</i>	Enters fan module chassis mode for the specified fan module. 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 enabled.

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

SUMMARY STEPS

1. Enter monitoring mode.
2. Enable or disable the management interfaces monitoring policy.
3. Specify the number of seconds that the system should wait between data recordings.
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.
5. Specify the monitoring mechanism that you want the system to use.
6. If you selected **mii-status** as your monitoring mechanism, configure the following properties:
7. If you selected **ping-arp-targets** as your monitoring mechanism, configure the following properties:
8. If you selected **ping-gateway** as your monitoring mechanism, configure the following properties:
9. UCS-A /monitoring # **commit-buffer**

DETAILED STEPS

- | | |
|---------------|---|
| 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:

- 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.
- 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:

- 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.
- 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.
- 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.
- 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.
- 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:

- 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.
- 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 chassis. This includes RAID controllers, physical drives and drive groups, virtual drives, and RAID controller batteries (BBU).

Cisco UCS Manager communicates directly with the storage 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.
- Information on 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 CMC 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.

Support for Local Storage Monitoring

Through Cisco UCS Manager, you can monitor local storage components for the Cisco UCSME-142-M4 server:

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 chassis.
- The chassis must be powered on.
- The chassis must have completed discovery.
- The results of the BIOS POST complete must be TRUE.


Note

This prerequisite is not applicable to the chassis

Viewing the Status of a Disk Drive

SUMMARY STEPS

1. UCS-A# **scope chassis** *chassis-num*
2. UCS-A /chassis # **scope raid-controller** *raid-contr-id* {**sas** | **sata**}
3. UCS-A /chassis/raid-controller # **show local-disk** [*local-disk-id* | **detail** | **expand**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope chassis <i>chassis-num</i>	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # scope raid-controller <i>raid-contr-id</i> { sas sata }	Enters RAID controller chassis mode.
Step 3	UCS-A /chassis/raid-controller # show local-disk [<i>local-disk-id</i> detail expand]	Displays the status of the specified disk drive.

The following example shows the status of a disk drive:

```
UCS-A# scope chassis 1
UCS-A /chassis # scope raid-controller 1 sas
UCS-A /chassis/raid-controller # show local-disk 4
```

```
Local Disk:
ID: 4
Block Size: 512
Blocks: 193357824
Size: 94413
Operability: Operable
Presence: Equipped
Connection Protocol: SATA
```

Viewing Detailed Information About Virtual Drives

SUMMARY STEPS

1. UCS-A# **scope chassis** *chassis-num*
2. UCS-A /chassis # **scope raid-controller** *raid-contr-id* {**sas** | **sata**}
3. UCS-A /chassis/raid-controller # **show virtual-drive** [**detail**] [**expand**]
4. (Optional) UCS-A /chassis/raid-controller # **show virtual-drive** *vd-id* [**detail**] [**expand**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope chassis <i>chassis-num</i>	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # scope raid-controller <i>raid-contr-id</i> { sas sata }	Enters RAID controller chassis mode.
Step 3	UCS-A /chassis/raid-controller # show virtual-drive [detail] [expand]	Displays detailed information about the virtual drives controlled by the specified storage controller.
Step 4	UCS-A /chassis/raid-controller # show virtual-drive <i>vd-id</i> [detail] [expand]	(Optional) Displays detailed information about the specified virtual drive controlled by the specified storage controller.

The following example shows how to display detailed information about virtual drives controlled by raid-controller 1:

```
UCS-A# scope chassis 1
UCS-A /chassis # scope raid-controller 1 sas
UCS-A /chassis/raid-controller # show virtual-drive detail expand
```

```
Virtual Drive:
  ID: 1000
  Name: lunb-1
  Block Size: 512
  Blocks: 8388608
  Size (MB): 4096
  Operability: Operable
  Presence: Equipped
  Lifecycle: Allocated
  Drive State: Optimal
  Type: RAID 0 Striped
  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: Unknown
  Oper Device ID: 4
  Change Qualifier: No Change
```

```

Config State: Orphaned
Deploy Action: No Action
Service Profile Lun Reference:
Assigned To Server:
Unique Identifier: 678da6e7-15b0-1400-1c1f-30684b3a3bc6

```

```

VD Members:
  Slot: 4
  Role: Normal
  Presence: Equipped
  Span Id (RAID levels 10, 50, 60): Unspecified
  Oper Qualifier Reason: N/A

```

```

ID: 1001
Name: luna-1
Block Size: 512
Blocks: 8388608
Size (MB): 4096
Operability: Operable
Presence: Equipped
Lifecycle: Allocated
Drive State: Optimal
Type: RAID 0 Striped
Strip Size (KB): 64

```

...

The following example shows how to display detailed information about virtual drive 1001 controlled by raid-controller 1:

```
UCS-A /chassis/raid-controller # show virtual-drive 1001 detail expand
```

```

Virtual Drive:
  ID: 1001
  Name: boot-1
  Block Size: 512
  Blocks: 104857600
  Size (MB): 51200
  Operability: Operable
  Presence: Equipped
  Lifecycle: Allocated
  Drive State: Optimal
  Type: RAID 0 Striped
  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: Unknown
  Oper Device ID: 0
  Change Qualifier: No Change
  Config State: Orphaned
  Deploy Action: No Action
  Service Profile Lun Reference:
  Assigned To Server:
  Available Size On Disk Group (MB): 43213
  Unique Identifier: 678da6e7-15b0-1400-1c53-7f47891e884c

VD Members:
  Slot: 4
  Role: Normal
  Presence: Equipped
  Span Id (RAID levels 10, 50, 60): Unspecified
  Oper Qualifier Reason: N/A

```

Viewing Detailed Information About the Storage Controller

SUMMARY STEPS

1. UCS-A# **scope chassis** *chassis-num*
2. UCS-A /chassis # **scope raid-controller** *raid-contr-id* {**sas** | **sata**}
3. UCS-A /chassis/raid-controller # **show detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope chassis <i>chassis-num</i>	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # scope raid-controller <i>raid-contr-id</i> { sas sata }	Enters RAID controller chassis mode.
Step 3	UCS-A /chassis/raid-controller # show detail	Displays detailed information about the storage controller.

The following example shows how to display detailed information about storage controller 1:

```
UCS-A# scope chassis 1
UCS-A /chassis # scope raid-controller 1 sas
UCS-A /chassis/raid-controller # show detail

RAID Controller:
  ID: 1
  Type: SAS
  PCI Addr:
  Vendor: Cisco Systems Inc
  Model: Cisco 12G SAS Modular Raid Controller
  Serial: SR416P0075
  HW Rev: C0
  Raid Support: RAID0, RAID1, RAID5, RAID6, RAID10, RAID50, RAID60
  OOB Interface Supported: Yes
  Rebuild Rate: 30
  Controller Status: Optimal
  Config State: Applied
  VID: V01
  Part Number:
  Storage Controller Admin State: Unspecified
  Current Task:
```

Viewing Storage Controller Operations

SUMMARY STEPS

1. UCS-A# **scope chassis** *chassis-num*
2. UCS-A /chassis # **show raid-controller operation**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope chassis <i>chassis-num</i>	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # show raid-controller operation	Displays the long running operations for the storage controller.

The following example shows how to display the storage controller operations for chassis 1:

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

Name: Relearning
Affected Object: sys/chassis-1/storage-SAS-1/raid-battery
State: Completed
Progress (%): N/A
Start Time: 2014-12-13T16:05:25.000
End Time: 2014-12-17T14:30:59.000

Name: Initialization
Affected Object: sys/chassis-1/storage-SAS-1/vd-1000
State: Completed
Progress (%): N/A
Start Time: N/A
End Time: N/A

Name: Initialization
Affected Object: sys/chassis-1/storage-SAS-1/vd-1001
State: Completed
Progress (%): N/A
Start Time: N/A
End Time: N/A

UCS-A /chassis #
```




Configuring Statistics-Related Policies

This chapter includes the following sections:

- [Configuring Statistics Collection Policies, page 27](#)
- [Configuring Statistics Threshold Policies, page 28](#)

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

SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A/monitoring # **scope stats-collection-policy {adapter | chassis | host | port | server}**
3. UCS-A /monitoring/stats-collection-policy # **set collection-interval {1minute | 2minutes | 30seconds | 5minutes}**
4. UCS-A /monitoring/stats-collection-policy # **set reporting-interval {15minutes | 30minutes | 60minutes}**
5. UCS-A /monitoring/stats-collection-policy # **commit-buffer**

DETAILED STEPS

	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

SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A /org # **create stats-threshold-policy** *policy-name*
3. (Optional) UCS-A /org/stats-threshold-policy # **set descr** *description*
4. UCS-A /org/stats-threshold-policy # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope org <i>org-name</i>	Enters organization mode for the specified organization. To enter the root organization mode, type <code>/</code> as the <i>org-name</i> .
Step 2	UCS-A /org # create stats-threshold-policy <i>policy-name</i>	Creates the specified statistics threshold policy and enters organization statistics threshold policy mode.
Step 3	UCS-A /org/stats-threshold-policy # set descr <i>description</i>	(Optional) Provides a description for the policy. 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 /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 31."](#)

Deleting a Server and Server Component Statistics Threshold Policy

SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A /org # **delete stats-threshold-policy** *policy-name*
3. UCS-A /org # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope org <i>org-name</i>	Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> .
Step 2	UCS-A /org # delete stats-threshold-policy <i>policy-name</i>	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 29](#)."

SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A /org # **scope stats-threshold-policy** *policy-name*
3. UCS-A /org/stats-threshold-policy # **create class** *class-name*
4. UCS-A /org/stats-threshold-policy /class # **create property** *property-name*
5. UCS-A /org/stats-threshold-policy/class/property # **set normal-value** *value*
6. UCS-A /org/stats-threshold-policy /class/property # **create threshold-value** {*above-normal* | *below-normal*} {*cleared* | *condition* | *critical* | *info* | *major* | *minor* | *warning*}
7. UCS-A /org/stats-threshold-policy /class/property/threshold-value # **set** {*deescalating* | *escalating*} *value*
8. UCS-A /org/stats-threshold-policy /class/property/threshold-value # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope org <i>org-name</i>	Enters organization mode for the specified organization. To enter the root organization mode, type <i>/</i> as the <i>org-name</i> .
Step 2	UCS-A /org # scope stats-threshold-policy <i>policy-name</i>	Enters organization statistics threshold policy mode.
Step 3	UCS-A /org/stats-threshold-policy # create class <i>class-name</i>	Creates the specified statistics threshold policy class and enters organization statistics threshold policy class mode. The <i>class-name</i> 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. Note You can configure multiple classes for the statistics threshold policy.
Step 4	UCS-A /org/stats-threshold-policy /class # create property <i>property-name</i>	Creates the specified statistics threshold policy class property and enters organization statistics threshold policy class property mode. The <i>property-name</i> 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. Note You can configure multiple properties for the policy class.

	Command or Action	Purpose
Step 5	UCS-A /org/stats-threshold-policy/class/property # set normal-value <i>value</i>	Specifies the normal value for the class property. The <i>value</i> 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. 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 } <i>value</i>	Specifies the de-escalating or escalating class property threshold value. The <i>value</i> 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. 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

SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A /org # **scope stats-threshold-policy** *policy-name*
3. UCS-A /org/stats-threshold-policy # **delete class** *class-name*
4. UCS-A /org/stats-threshold-policy # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope org <i>org-name</i>	Enters organization mode for the specified organization. To enter the root organization mode, type <i>/</i> as the <i>org-name</i> .
Step 2	UCS-A /org # scope stats-threshold-policy <i>policy-name</i>	Enters the specified statistics threshold policy.
Step 3	UCS-A /org/stats-threshold-policy # delete class <i>class-name</i>	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

SUMMARY STEPS

1. UCS-A# **scope eth-uplink**
2. UCS-A /eth-uplink # **scope stats-threshold-policy default**
3. (Optional) UCS-A /eth-uplink/stats-threshold-policy # **set descr** *description*
4. UCS-A /eth-uplink/stats-threshold-policy # **commit-buffer**

DETAILED STEPS

	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. 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 <i>description</i>	(Optional) 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 34."](#)

Configuring an Uplink Ethernet Port Statistics Threshold Policy Class

SUMMARY STEPS

1. UCS-A# **scope eth-uplink**
2. UCS-A /eth-uplink # **scope stats-threshold-policy default**
3. UCS-A /eth-uplink/stats-threshold-policy # **create class class-name**
4. UCS-A /eth-uplink/stats-threshold-policy /class # **create property property-name**
5. UCS-A /eth-uplink/stats-threshold-policy /class/property # **set normal-value value**
6. UCS-A /eth-uplink/stats-threshold-policy /class/property # **create threshold-value {above-normal | below-normal} {cleared | condition | critical | info | major | minor | warning}**
7. UCS-A /eth-uplink/stats-threshold-policy /class/property/threshold-value # **set {deescalating | escalating} value**
8. UCS-A /eth-uplink/stats-threshold-policy /class/property/threshold-value # **commit-buffer**

DETAILED STEPS

	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.

	Command or Action	Purpose
Step 3	UCS-A /eth-uplink/stats-threshold-policy # create class <i>class-name</i>	Creates the specified statistics threshold policy class and enters Ethernet uplink statistics threshold policy class mode. The <i>class-name</i> 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. Note You can configure multiple classes for the statistics threshold policy.
Step 4	UCS-A /eth-uplink/stats-threshold-policy /class # create property <i>property-name</i>	Creates the specified statistics threshold policy class property and enters Ethernet uplink statistics threshold policy class property mode. The <i>property-name</i> 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 Ethernet uplink statistics threshold policy class mode. Note You can configure multiple properties for the policy class.
Step 5	UCS-A /eth-uplink/stats-threshold-policy /class/property # set normal-value <i>value</i>	Specifies the normal value for the class property. The <i>value</i> 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. 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 } <i>value</i>	Specifies the de-escalating or escalating class property threshold value. The <i>value</i> 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. 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

SUMMARY STEPS

1. UCS-A# **scope eth-uplink**
2. UCS-A /eth-uplink # **scope stats-threshold-policy default**
3. UCS-A /eth-uplink/stats-threshold-policy # **delete class class-name**
4. UCS-A /eth-uplink/stats-threshold-policy # **commit-buffer**

DETAILED STEPS

	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

SUMMARY STEPS

1. UCS-A# **scope eth-server**
2. UCS-A /eth-server # **scope stats-threshold-policy default**
3. (Optional) UCS-A /eth-server/stats-threshold-policy # **set descr** *description*
4. UCS-A /eth-server/stats-threshold-policy # **commit-buffer**

DETAILED STEPS

	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. 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 <i>description</i>	(Optional) Provides a description for the policy. 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

SUMMARY STEPS

1. UCS-A# **scope eth-server**
2. UCS-A /eth-server # **scope stats-threshold-policy default**
3. UCS-A /eth-server/stats-threshold-policy # **create class class-name**
4. UCS-A /eth-server/stats-threshold-policy /class # **create property property-name**
5. UCS-A /eth-server/stats-threshold-policy /class/property # **set normal-value value**
6. UCS-A /eth-server/stats-threshold-policy /class/property # **create threshold-value {above-normal | below-normal} {cleared | condition | critical | info | major | minor | warning}**
7. UCS-A /eth-server/stats-threshold-policy /class/property/threshold-value # **set {deescalating | escalating} value**
8. UCS-A /eth-server/stats-threshold-policy /class/property/threshold-value # **commit-buffer**

DETAILED STEPS

	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 <i>class-name</i> 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. 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 <i>property-name</i> 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 Ethernet server statistics threshold policy class mode. 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 <i>value</i> 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.

	Command or Action	Purpose
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. 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 } <i>value</i>	Specifies the de-escalating or escalating class property threshold value. The <i>value</i> 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. 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

SUMMARY STEPS

1. UCS-A# **scope eth-server**
2. UCS-A /eth-server # **scope stats-threshold-policy default**
3. UCS-A /eth-server/stats-threshold-policy # **delete class class-name**
4. UCS-A /eth-server/stats-threshold-policy # **commit-buffer**

DETAILED STEPS

	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

SUMMARY STEPS

1. UCS-A# **scope fc-uplink**
2. UCS-A /fc-uplink # **scope stats-threshold-policy default**
3. (Optional) UCS-A /fc-uplink/stats-threshold-policy # **set descr description**
4. UCS-A /fc-uplink/stats-threshold-policy # **commit-buffer**

DETAILED STEPS

	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. 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) 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 /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

SUMMARY STEPS

1. UCS-A# **scope fc-uplink**
2. UCS-A /fc-uplink # **scope stats-threshold-policy default**
3. UCS-A /fc-uplink/stats-threshold-policy # **create class class-name**
4. UCS-A /fc-uplink/stats-threshold-policy /class # **create property property-name**
5. UCS-A /fc-uplink/stats-threshold-policy /class/property # **set normal-value value**
6. UCS-A /fc-uplink/stats-threshold-policy /class/property # **create threshold-value {above-normal | below-normal} {cleared | condition | critical | info | major | minor | warning}**
7. UCS-A /fc-uplink/stats-threshold-policy /class/property/threshold-value # **set {deescalating | escalating} value**
8. UCS-A /fc-uplink/stats-threshold-policy /class/property/threshold-value # **commit-buffer**

DETAILED STEPS

	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.

	Command or Action	Purpose
Step 3	UCS-A /fc-uplink/stats-threshold-policy # create class <i>class-name</i>	Creates the specified statistics threshold policy class and enters Fibre Channel uplink statistics threshold policy class mode. The <i>class-name</i> 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. Note You can configure multiple classes for the statistics threshold policy.
Step 4	UCS-A /fc-uplink/stats-threshold-policy /class # create property <i>property-name</i>	Creates the specified statistics threshold policy class property and enters Fibre Channel uplink statistics threshold policy class property mode. The <i>property-name</i> 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. Note You can configure multiple properties for the policy class.
Step 5	UCS-A /fc-uplink/stats-threshold-policy /class/property # set normal-value <i>value</i>	Specifies the normal value for the class property. The <i>value</i> 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. 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 } <i>value</i>	Specifies the de-escalating or escalating class property threshold value. The <i>value</i> 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. 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

SUMMARY STEPS

1. UCS-A# **scope fc-uplink**
2. UCS-A /fc-uplink # **scope stats-threshold-policy default**
3. UCS-A /fc-uplink/stats-threshold-policy # **delete class** *class-name*
4. UCS-A /fc-uplink/stats-threshold-policy # **commit-buffer**

DETAILED STEPS

	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 <i>class-name</i>	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 #

```




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 53](#)
- [Enabling Call Home, page 53](#)
- [Configuring System Inventory Messages, page 54](#)
- [Configuring Call Home Profiles, page 56](#)
- [Sending a Test Call Home Alert, page 60](#)
- [Configuring Call Home Policies, page 62](#)
- [Configuring Anonymous Reporting, page 65](#)
- [Example: Configuring Call Home for Smart Call Home, page 69](#)

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.

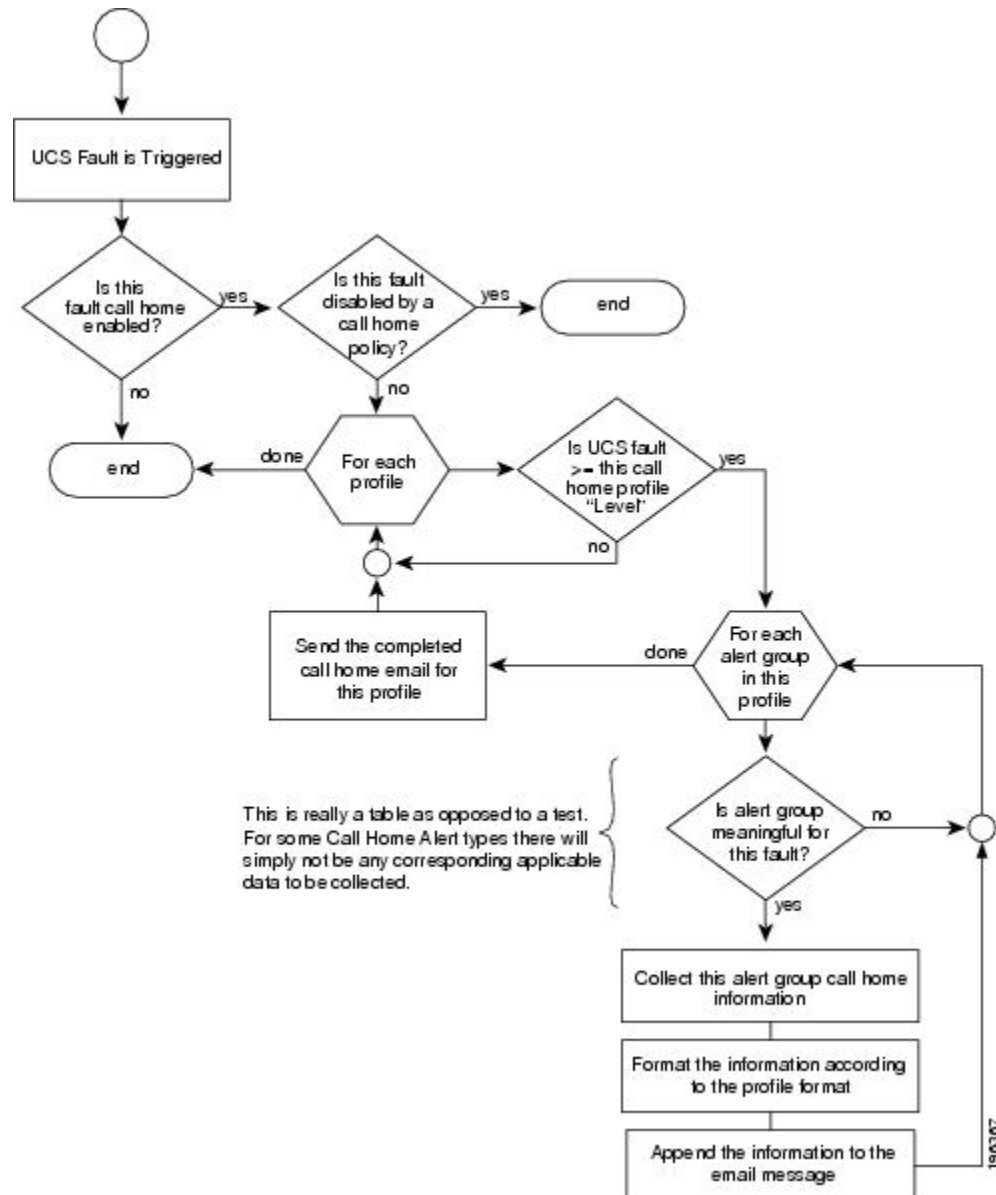
Cisco UCS delivers Call Home messages in the following formats:

- 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](http://Cisco.com). 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 Manager, by default, you are prompted with a dialog box to enable anonymous reporting.

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

Configuring Call Home

SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
3. UCS-A /monitoring/callhome # **enable**
4. UCS-A /monitoring/callhome # **set contact** *name*
5. UCS-A /monitoring/callhome # **set email** *email-addr*
6. UCS-A /monitoring/callhome # **set phone-contact** *phone-num*
7. UCS-A /monitoring/callhome # **set street-address** *street-addr*
8. UCS-A /monitoring/callhome # **set customer-id** *id-num*
9. UCS-A /monitoring/callhome # **set contract-id** *id-num*
10. UCS-A /monitoring/callhome # **set site-id** *id-num*
11. UCS-A /monitoring/callhome # **set from-email** *email-addr*
12. UCS-A /monitoring/callhome # **set reply-to-email** *email-addr*
13. UCS-A /monitoring/callhome # **set hostname** {*hostname* | *ip-addr*|*ip6-addr*}
14. UCS-A /monitoring/callhome # **set port** *port-num*
15. UCS-A /monitoring/callhome # **set throttling** {**off** | **on**}
16. UCS-A /monitoring/callhome # **set urgency** {**alerts** | **critical** | **debugging** | **emergencies** | **errors** | **information** | **notifications** | **warnings**}
17. UCS-A /monitoring/callhome # **commit-buffer**

DETAILED STEPS

	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 <i>name</i>	Specifies the name of the main Call Home contact person.
Step 5	UCS-A /monitoring/callhome # set email <i>email-addr</i>	Specifies the email address of the main Call Home contact person. 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.
Step 6	UCS-A /monitoring/callhome # set phone-contact <i>phone-num</i>	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 <i>street-addr</i>	Specifies the street address of the main Call Home contact person. Enter up to 255 ASCII characters.
Step 8	UCS-A /monitoring/callhome # set customer-id <i>id-num</i>	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 <i>id-num</i>	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 <i>id-num</i>	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 <i>email-addr</i>	Specifies the email address to use for the From field in Call Home messages.
Step 12	UCS-A /monitoring/callhome # set reply-to-email <i>email-addr</i>	Specifies the email address to use for the Reply To field in Call Home messages.
Step 13	UCS-A /monitoring/callhome # set hostname { <i>hostname</i> <i>ip-addr</i> <i>ip6-addr</i> }	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 <i>port-num</i>	Specifies the SMTP server port that Call Home uses to send email messages. Valid port numbers are 1 to 65535.

	Command or Action	Purpose
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

SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
3. UCS-A /monitoring/callhome # **disable**
4. UCS-A /monitoring/callhome # **commit-buffer**

DETAILED STEPS

	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

SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
3. UCS-A /monitoring/callhome # **enable**
4. UCS-A /monitoring/callhome # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope monitoring	Enters monitoring mode.

	Command or Action	Purpose
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

SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
3. UCS-A /monitoring/callhome # **scope inventory**
4. UCS-A /monitoring/callhome/inventory # **set send-periodically {off | on}**
5. UCS-A /monitoring/callhome/inventory # **set interval-days interval-num**
6. UCS-A /monitoring/callhome/inventory # **set timeofday-hour hour**
7. UCS-A /monitoring/callhome/inventory # **set timeofday-minute minute**
8. UCS-A /monitoring/callhome/inventory # **commit-buffer**

DETAILED STEPS

	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.

	Command or Action	Purpose
Step 5	UCS-A /monitoring/callhome/inventory # set interval-days <i>interval-num</i>	Specifies the time interval (in days) at which inventory messages will be sent.
Step 6	UCS-A /monitoring/callhome/inventory # set timeofday-hour <i>hour</i>	Specifies the hour (using 24-hour format) that inventory messages are sent.
Step 7	UCS-A /monitoring/callhome/inventory # set timeofday-minute <i>minute</i>	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.

SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
3. UCS-A /monitoring/callhome # **scope inventory**
4. UCS-A /monitoring/callhome/inventory # **send**

DETAILED STEPS

	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 # 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.

SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
3. UCS-A /monitoring/callhome # **create profile** *profile-name*
4. UCS-A /monitoring/callhome/profile # **set level** {**critical** | **debug** | **disaster** | **fatal** | **major** | **minor** | **normal** | **notification** | **warning**}
5. UCS-A /monitoring/callhome/profile # **set alertgroups** *group-name*
 - **ciscotac**
 - **diagnostic**
 - **environmental**
 - **inventory**
 - **license**
 - **lifecycle**
 - **linecard**
 - **supervisor**
 - **syslogport**
 - **system**
 - **test**
6. (Optional) UCS-A /monitoring/callhome/profile # **add alertgroups** *group-names*
7. UCS-A /monitoring/callhome/profile # **set format** {**shorttxt** | **xml**}
8. UCS-A /monitoring/callhome/profile # **set maxsize** *id-num*
9. UCS-A /monitoring/callhome/profile # **create destination** *email-addr*
10. UCS-A /monitoring/callhome/profile/destination # **commit-buffer**

DETAILED STEPS

	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 <i>profile-name</i>	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. Cisco UCS faults that are greater than or equal to the event level will trigger this profile.

	Command or Action	Purpose
Step 5	UCS-A /monitoring/callhome/profile # set alertgroups <i>group-name</i> <ul style="list-style-type: none"> • ciscotac • diagnostic • environmental • inventory • license • lifecycle • linecard • supervisor • syslogport • system • test 	Specifies one or more groups that are alerted based on the profile. The <i>group-name</i> 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 <i>group-names</i>	(Optional) Adds one or more groups to the existing list of groups that are alerted based on the Call Home profile. 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.
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 <i>id-num</i>	Specifies the maximum size (in characters) of the email message.
Step 9	UCS-A /monitoring/callhome/profile # create destination <i>email-addr</i>	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

SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
3. UCS-A /monitoring/callhome # **delete profile** *profile-name*
4. UCS-A /monitoring/callhome # **commit-buffer**

DETAILED STEPS

	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 <i>profile-name</i>	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.

SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
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*]}

DETAILED STEPS

	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 <i>description</i>]}	<p>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:</p> <ul style="list-style-type: none"> • alert-description—Alert description • alert-group—Alert group • alert-level—Event severity level • alert-message-type—Message type • alert-message-subtype—Message subtype <p>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.</p>

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.

SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
3. UCS-A /monitoring/callhome # **create policy {equipment-inoperable | fru-problem | identity-unestablishable | thermal-problem | voltage-problem}**
4. UCS-A /monitoring/callhome/policy # **{disabled | enabled}**
5. UCS-A /monitoring/callhome/policy # **commit-buffer**

DETAILED STEPS

	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

SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
3. UCS-A /monitoring/callhome # **scope policy {equipment-inoperable | fru-problem | identity-unestablishable | thermal-problem | voltage-problem}**
4. UCS-A /monitoring/callhome/policy # **disable**
5. UCS-A /monitoring/callhome/policy # **commit-buffer**

DETAILED STEPS

	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

SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
3. UCS-A /monitoring/callhome # **scope policy** {equipment-inoperable | fru-problem | identity-unestablishable | thermal-problem | voltage-problem}
4. UCS-A /monitoring/callhome/policy # **enable**
5. UCS-A /monitoring/callhome/policy # **commit-buffer**

DETAILED STEPS

	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

SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
3. UCS-A /monitoring/callhome # **delete policy** {equipment-inoperable | fru-problem | identity-unestablishable | thermal-problem | voltage-problem}
4. UCS-A /monitoring/callhome # **commit-buffer**

DETAILED STEPS

	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.

SUMMARY STEPS

1. UCS-A # **scope monitoring**
2. UCS-A/monitoring # **scope callhome**
3. (Optional) UCS-A/monitoring/callhome # **show anonymous-reporting**
4. UCS-A/monitoring/callhome # **enable anonymous-reporting**
5. UCS-A/monitoring/callhome # **commit-buffer**

DETAILED STEPS

	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) 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/monitoring/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.

SUMMARY STEPS

1. UCS-A # **scope monitoring**
2. UCS-A/monitoring # **scope callhome**
3. (Optional) UCS-A/monitoring/callhome # **show anonymous-reporting**
4. UCS-A/monitoring/callhome # **disable anonymous-reporting**
5. UCS-A/monitoring/callhome # **commit-buffer**

DETAILED STEPS

	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) Displays if anonymous reporting is enabled or disabled.

	Command or Action	Purpose
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/monitoring/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.

SUMMARY STEPS

1. UCS-A # **scope monitoring**
2. UCS-A/monitoring # **scope callhome**
3. UCS-A/monitoring/callhome # **scope anonymous-reporting**
4. UCS-A/monitoring/callhome/anonymous-reporting # **show detail**
5. UCS-A/monitoring/callhome/anonymous-reporting # **show inventory**
6. UCS-A/monitoring/callhome/anonymous-reporting # **show content**

DETAILED STEPS

	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.

	Command or Action	Purpose
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

SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
3. UCS-A /monitoring/callhome # **enable**
4. UCS-A /monitoring/callhome # **set contact** *name*
5. UCS-A /monitoring/callhome # **set email** *email-addr*
6. UCS-A /monitoring/callhome # **set phone-contact** *phone-num*
7. UCS-A /monitoring/callhome # **set street-address** *street-addr*
8. UCS-A /monitoring/callhome # **set customer-id** *id-num*
9. UCS-A /monitoring/callhome # **set contract-id** *id-num*
10. UCS-A /monitoring/callhome # **set site-id** *id-num*
11. UCS-A /monitoring/callhome # **set from-email** *email-addr*
12. UCS-A /monitoring/callhome # **set reply-to-email** *email-addr*
13. UCS-A /monitoring/callhome # **set hostname** {*hostname* | *ip-addr*}
14. UCS-A /monitoring/callhome # **set port** *port-num*
15. UCS-A /monitoring/callhome # **set throttling** {**off** | **on**}
16. UCS-A /monitoring/callhome # **set urgency** {**alerts** | **critical** | **debugging** | **emergencies** | **errors** | **information** | **notifications** | **warnings**}
17. UCS-A /monitoring/callhome # **commit-buffer**

DETAILED STEPS

	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 <i>name</i>	Cisco Smart Call Home sends the registration email to this email address.
Step 5	UCS-A /monitoring/callhome # set email <i>email-addr</i>	Specifies the email address of the main Call Home contact person. Cisco Smart Call Home sends the registration email to this email address.

	Command or Action	Purpose
Step 6	UCS-A /monitoring/callhome # set phone-contact <i>phone-num</i>	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 <i>street-addr</i>	Specifies the street address of the main Call Home contact person.
Step 8	UCS-A /monitoring/callhome # set customer-id <i>id-num</i>	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 <i>id-num</i>	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 <i>id-num</i>	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 <i>email-addr</i>	Specifies the email address to use for the From field in Call Home messages.
Step 12	UCS-A /monitoring/callhome # set reply-to-email <i>email-addr</i>	Specifies the email address to use for the Reply To field in Call Home messages.
Step 13	UCS-A /monitoring/callhome # set hostname <i>{hostname ip-addr}</i>	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 <i>port-num</i>	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 <i>{off on}</i>	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 <i>{alerts critical debugging emergencies errors information notifications warnings}</i>	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 71](#)" 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 69](#)" section.

SUMMARY STEPS

1. UCS-A /monitoring/callhome # **scope profile CiscoTac-1**
2. UCS-A /monitoring/callhome/profile # **set level normal**
3. UCS-A /monitoring/callhome/profile # **set alertgroups ciscotac**
4. UCS-A /monitoring/callhome/profile # **set format xml**
5. UCS-A /monitoring/callhome/profile # **set maxsize 5000000**
6. UCS-A /monitoring/callhome/profile # **create destination callhome@cisco.com**
7. UCS-A /monitoring/callhome/profile/destination # **exit**
8. UCS-A /monitoring/callhome/profile # **exit**

DETAILED STEPS

	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.

	Command or Action	Purpose
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 72](#)" 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 71](#)" section.

SUMMARY STEPS

1. UCS-A /monitoring/callhome # **scope inventory**
2. UCS-A /monitoring/callhome/inventory # **set send-periodically {off | on}**
3. UCS-A /monitoring/callhome/inventory # **set interval-days *interval-num***
4. UCS-A /monitoring/callhome/inventory # **set timeofday-hour *hour***
5. UCS-A /monitoring/callhome/inventory # **set timeofday-minute *minute***
6. UCS-A /monitoring/callhome/inventory # **commit-buffer**

DETAILED STEPS

	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 <i>interval-num</i>	Specifies the the time interval (in days) at which inventory messages will be sent.
Step 4	UCS-A /monitoring/callhome/inventory # set timeofday-hour <i>hour</i>	Specifies the hour (using 24-hour format) that inventory messages are sent.
Step 5	UCS-A /monitoring/callhome/inventory # set timeofday-minute <i>minute</i>	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 73](#)" 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 72](#)" section.

SUMMARY STEPS

1. UCS-A /monitoring/callhome/inventory # **send**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A /monitoring/callhome/inventory # send	Sends the system inventory message to the Smart Call Home database. 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.



Managing the System Event Log

This chapter includes the following sections:

- [System Event Log, page 75](#)
- [Viewing the System Event Log for a Server, page 75](#)
- [Configuring the SEL Policy, page 77](#)
- [Backing Up the System Event Log for a Server, page 79](#)
- [Clearing the System Event Log for a Server, page 79](#)

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

SUMMARY STEPS

1. UCS-A# **scope server** *chassis-id/cartridge-id/server-id*
2. UCS-A /chassis/cartridge/server # **show sel**

DETAILED STEPS

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

The following example displays the system event log from server 2 in cartridge 1 and chassis 1.

```
UCS-A# scope server 1/1/2
UCS-A /chassis/cartridge/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

SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A /org # **scope ep-log-policy sel**
3. (Optional) UCS-A /org/ep-log-policy # **set description** *description*
4. UCS-A /org/ep-log-policy # **set backup action** [**log-full**] [**on-change-of-association**] [**on-clear**] [**timer**] [**none**]
5. UCS-A /org/ep-log-policy # **set backup clear-on-backup** {**no** | **yes**}
6. UCS-A /org/ep-log-policy # **set backup destination** *URL*
7. UCS-A /org/ep-log-policy # **set backup format** {*ascii* | *binary*}
8. UCS-A /org/ep-log-policy # **set backup hostname** {*hostname* | *ip-addr*}
9. UCS-A /org/ep-log-policy # **set backup interval** {**1-hour** | **2-hours** | **4-hours** | **8-hours** | **24-hours** | **never**}
10. UCS-A /org/ep-log-policy # **set backup password** *password*
11. UCS-A /org/ep-log-policy # **set backup protocol** {**ftp** | **scp** | **sftp** | **tftp**}
12. UCS-A /org/ep-log-policy # **set backup remote-path** *path*
13. UCS-A /org/ep-log-policy # **set backup user** *username*
14. UCS-A /org/ep-log-policy # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope org <i>org-name</i>	Enters organization mode for the specified organization. To enter the root organization mode, type <i>/</i> as the <i>org-name</i> .
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 <i>description</i>	(Optional) Provides a description for the policy. 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 <i>URL</i>	<p>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:</p> <ul style="list-style-type: none"> • ftp:// <i>username@hostname</i> / <i>path</i> • scp:// <i>username</i> @ <i>hostname</i> / <i>path</i> • sftp:// <i>username</i> @ <i>hostname</i> / <i>path</i> • tftp:// <i>hostname</i> : <i>port-num</i> / <i>path</i> <p>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.</p>
Step 7	UCS-A /org/ep-log-policy # set backup format { <i>ascii</i> <i>binary</i> }	Specifies the format for the backup file.
Step 8	UCS-A /org/ep-log-policy # set backup hostname { <i>hostname</i> <i>ip-addr</i> }	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 <i>password</i>	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 <i>path</i>	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 <i>username</i>	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

Before You Begin

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

SUMMARY STEPS

1. UCS-A# **scope server** *chassis-id/cartridge-id/server-id*
2. UCS-A /chassis/cartridge/server # **backup sel**
3. UCS-A /chassis/cartridge/server # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope server <i>chassis-id/cartridge-id/server-id</i>	Enters server mode for the specified server.
Step 2	UCS-A /chassis/cartridge/server # backup sel	Backs up the system event log.
Step 3	UCS-A /chassis/cartridge/server # commit-buffer	Commits the transaction.

The following example backs up the system event log for server 2 in cartridge 1 and chassis 1 and commits the transaction.

```
UCS-A# scope server 1/1/2
UCS-A /chassis/cartridge/server # backup sel
UCS-A /chassis/cartridge/server* # commit-buffer
UCS-A /chassis/cartridge/server #
```

Clearing the System Event Log for a Server

SUMMARY STEPS

1. UCS-A# **scope server** *chassis-id/cartridge-id/server-id*
2. UCS-A /chassis/cartridge/server # **clear sel**
3. UCS-A /chassis/cartridge/server # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope server <i>chassis-id/cartridge-id/server-id</i>	Enters server mode for the specified server.
Step 2	UCS-A /chassis/cartridge/server # clear sel	Clears the system event log.
Step 3	UCS-A /chassis/cartridge/server # commit-buffer	Commits the transaction.

The following example clears the system event log from server 2 in cartridge 1 and chassis 1 and commits the transaction:

```
UCS-A# scope server 1/1/2
UCS-A /chassis/cartridge/server # clear sel
UCS-A /chassis/cartridge/server* # commit-buffer
UCS-A /chassis/cartridge/server #
```



Configuring Settings for Faults, Events, and Logs

This chapter includes the following sections:

- [Configuring Settings for the Fault Collection Policy, page 81](#)
- [Configuring Fault Suppression, page 83](#)
- [Configuring Settings for the Core File Exporter, page 107](#)
- [Configuring the Syslog, page 109](#)
- [Viewing Audit Logs, page 111](#)
- [Configuring the Log File Exporter, page 112](#)

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

SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope fault policy**
3. UCS-A /monitoring/fault-policy # **set clear-action {delete | retain}**
4. UCS-A /monitoring/fault-policy # **set flap-interval seconds**
5. UCS-A /monitoring/fault-policy # **set retention-interval {days hours minutes seconds | forever}**
6. UCS-A /monitoring/fault-policy # **commit-buffer**

DETAILED STEPS

	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 servers, power supplies, fan modules, and IOMs.
This policy applies only to chassis.
- **default-chassis-phys-maint**—Suppresses faults for the chassis and all fan modules and power supplies installed into the chassis.
This policy applies only to chassis.
- **default-fex-all-maint**—Suppresses faults for the FEX and all power supplies, fan modules, and IOMs in the FEX.
This policy applies only to FEXes.
- **default-fex-phys-maint**—Suppresses faults for the FEX and all fan modules and power supplies in the FEX.
This policy applies only to FEXes.
- **default-server-maint**—Suppresses faults for servers.
This policy applies to chassis, organizations, and service profiles.

**Note**

When applied to a chassis, only servers are affected.

- **default-iom-maint**—Suppresses faults for IOMs in a chassis or FEX.

This policy applies only to chassis, FEXes, and IOMs.

**Important**

FEX and IO Modules are not supported by Cisco UCS M-Series Servers.

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

SUMMARY STEPS

1. UCS-A# **scope chassis** *chassis-num*
2. UCS-A/chassis # **create fault-suppress-task** *name*
3. UCS-A/chassis/fault-suppress-task # **set fault-suppress-policy** *policy-name*
4. UCS-A/chassis/fault-suppress-task # **create local-schedule**
5. UCS-A/chassis/fault-suppress-task/local-schedule # **create occurrence single-one-time**
6. UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*
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*}
8. UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope chassis <i>chassis-num</i>	Enters chassis mode for the specified chassis.

	Command or Action	Purpose
Step 2	UCS-A/chassis # create fault-suppress-task <i>name</i>	Creates a fault-suppress-task on the chassis, and enters fault-suppress-task mode. 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 <i>policy-name</i>	Specifies the fault suppression policy that you want to apply. This can be one of the following: <ul style="list-style-type: none"> • default-chassis-all-maint—Suppresses faults for the chassis and all components installed into the chassis, including all servers, power supplies, fan modules, and IOMs. • default-chassis-phys-maint—Suppresses faults for the chassis and all fan modules and power supplies installed into the chassis. • default-server-maint—Suppresses faults for servers. <p>Note When applied to a chassis, only servers are affected.</p> <ul style="list-style-type: none"> • default-iom-maint—Suppresses faults for IOMs in a chassis or FEX.
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 <i>month day-of-month year hour minute seconds</i>	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 { <i>none</i> <i>num-of-days num-of-hours num-of-minutes num-of-seconds</i> }	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/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

SUMMARY STEPS

1. UCS-A# **scope chassis** *chassis-num*
2. UCS-A/chassis # **create fault-suppress-task** *name*
3. UCS-A/chassis/fault-suppress-task # **set schedule** *name*
4. UCS-A/chassis/fault-suppress-task # **set fault-suppress-policy** *policy-name*
5. UCS-A/chassis/fault-suppress-task # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope chassis <i>chassis-num</i>	Enters chassis mode for the specified chassis.
Step 2	UCS-A/chassis # create fault-suppress-task <i>name</i>	Creates a fault-suppress-task on the chassis, and enters the fault-suppress-task mode. 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 <i>name</i>	Specifies the schedule that you want to use. 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 <i>policy-name</i>	Selects the fault suppression policy you want to apply. This can be one of the following: <ul style="list-style-type: none"> • default-chassis-all-maint—Suppresses faults for the chassis and all components installed into the chassis, including all servers, power supplies, fan modules, and IOMs. • default-chassis-phys-maint—Suppresses faults for the chassis and all fan modules and power supplies installed into the chassis. • default-server-maint—Suppresses faults for servers. Note When applied to a chassis, only servers are affected. • default-iom-maint—Suppresses faults for IOMs in a chassis or FEX.
Step 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

SUMMARY STEPS

1. UCS-A# **scope chassis** *chassis-num*
2. UCS-A/chassis # **delete fault-suppress-task** *name*
3. UCS-A/chassis # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope chassis <i>chassis-num</i>	Enters chassis mode for the specified chassis.
Step 2	UCS-A/chassis # delete fault-suppress-task <i>name</i>	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

SUMMARY STEPS

1. UCS-A# **scope chassis** *chassis-num*
2. UCS-A/chassis # **scope fault-suppress-task** *name*
3. UCS-A/chassis/fault-suppress-task # **set fault-suppress-policy** *policy-name*
4. UCS-A/chassis/fault-suppress-task # **set schedule** *name*
5. UCS-A/chassis/fault-suppress-task # **scope local-schedule**
6. UCS-A/chassis/fault-suppress-task/local-schedule # **scope occurrence single-one-time**
7. UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*
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*}
9. UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope chassis <i>chassis-num</i>	Enters chassis mode for the specified chassis.
Step 2	UCS-A/chassis # scope fault-suppress-task <i>name</i>	Enters fault-suppress-task mode.
Step 3	UCS-A/chassis/fault-suppress-task # set fault-suppress-policy <i>policy-name</i>	<p>Modifies the fault suppression policy. This can be one of the following:</p> <ul style="list-style-type: none"> • default-chassis-all-maint—Suppresses faults for the chassis and all components installed into the chassis, including all servers, power supplies, fan modules, and IOMs. • default-chassis-phys-maint—Suppresses faults for the chassis and all fan modules and power supplies installed into the chassis. • default-server-maint—Suppresses faults for servers. • default-iom-maint—Suppresses faults for IOMs in a chassis or FEX. <p>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.</p>
Step 4	UCS-A/chassis/fault-suppress-task # set schedule <i>name</i>	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. 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 <i>month day-of-month year hour minute seconds</i>	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 <i>num-of-days num-of-hours num-of-minutes num-of-seconds</i> }	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

SUMMARY STEPS

1. UCS-A# **scope chassis** *chassis-num*
2. UCS-A/chassis # **show fault suppressed**
3. UCS-A/chassis # **scope fault-suppress-task** *name*
4. UCS-A/chassis/fault-suppress-task # **show detail expand**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope chassis <i>chassis-num</i>	Enters chassis mode for the specified chassis.
Step 2	UCS-A/chassis # show fault suppressed	Displays the suppressed faults for the chassis. Note Only faults owned by the selected component are displayed.
Step 3	UCS-A/chassis # scope fault-suppress-task <i>name</i>	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.

SUMMARY STEPS

1. UCS-A# **scope server** *chassis-id/cartridge-id/server-id*
2. UCS-A /chassis/cartridge/server # **create fault-suppress-task** *name*
3. UCS-A /chassis/cartridge/server/fault-suppress-task # **create local-schedule**
4. UCS-A /chassis/cartridge/server/fault-suppress-task/local-schedule # **create occurrence single-one-time**
5. UCS-A /chassis/cartridge/server/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*
6. UCS-A /chassis/cartridge/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*}
7. UCS-A /chassis/cartridge/server/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope server <i>chassis-id/cartridge-id/server-id</i>	Enters server mode for the specified server.
Step 2	UCS-A /chassis/cartridge/server # create fault-suppress-task <i>name</i>	Creates a fault-suppress-task on the server, and enters the fault-suppress-task mode. 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/cartridge/server/fault-suppress-task # create local-schedule	Creates a local schedule and enters local-schedule mode.
Step 4	UCS-A /chassis/cartridge/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 /chassis/cartridge/server/fault-suppress-task/local-schedule/single-one-time # set date <i>month day-of-month year hour minute seconds</i>	Specifies the date and time that this occurrence should run.
Step 6	UCS-A /chassis/cartridge/server/fault-suppress-task/local-schedule/single-one-time # set max-duration { <i>none num-of-days num-of-hours num-of-minutes num-of-seconds</i> }	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 /chassis/cartridge/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, 2015 at 11:00, and commit the transaction:

```
UCS-A# scope server 1/1/1
UCS-A /chassis/cartridge/server # create fault-suppress-task task2
UCS-A /chassis/cartridge/server/fault-suppress-task* # create local-schedule
UCS-A /chassis/cartridge/server/fault-suppress-task/local-schedule* # create occurrence
single-one-time
UCS-A /chassis/cartridge/server/fault-suppress-task/local-schedule/single-one-time* # set
date jan 1 2015 11 00 00
UCS-A /chassis/cartridge/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.

SUMMARY STEPS

1. UCS-A# **scope server** *chassis-id/cartridge-id/server-id*
2. UCS-A /chassis/cartridge/server # **create fault-suppress-task** *name*
3. UCS-A /chassis/cartridge/server/fault-suppress-task # **set schedule** *name*
4. UCS-A /chassis/cartridge/server/fault-suppress-task # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope server <i>chassis-id/cartridge-id/server-id</i>	Enters server mode for the specified server.
Step 2	UCS-A /chassis/cartridge/server # create fault-suppress-task <i>name</i>	Creates a fault-suppress-task on the server, and enters the fault-suppress-task mode. 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/cartridge/server/fault-suppress-task # set schedule <i>name</i>	Specifies the schedule that you want to use. 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/cartridge/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 1/1/1
UCS-A /chassis/cartridge/server # create fault-suppress-task task1
```



```
UCS-A /chassis/cartridge/server/fault-suppress-task* # set schedule weekly_maint
UCS-A /chassis/cartridge/server/fault-suppress-task* # commit-buffer
```

Deleting Fault Suppression Tasks for a Server

SUMMARY STEPS

1. UCS-A# **scope server** *chassis-id/cartridge-id/server-id*
2. UCS-A /chassis/cartridge/server # **delete fault-suppress-task** *name*
3. UCS-A /chassis/cartridge/server # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope server <i>chassis-id/cartridge-id/server-id</i>	Enters server mode for the specified server.
Step 2	UCS-A /chassis/cartridge/server # delete fault-suppress-task <i>name</i>	Deletes the specified fault suppression task.
Step 3	UCS-A /chassis/cartridge/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 1/1/1
UCS-A /chassis/cartridge/server # delete fault-suppress-task task1
UCS-A /chassis/cartridge/server* # commit-buffer
```

Modifying Fault Suppression Tasks for a Server

SUMMARY STEPS

1. UCS-A# **scope server** *chassis-id/cartridge-id/server-id*
2. UCS-A /chassis/cartridge/server # **scope fault-suppress-task** *name*
3. UCS-A /chassis/cartridge/server/fault-suppress-task # **set schedule** *name*
4. UCS-A /chassis/cartridge/server/fault-suppress-task # **scope local-schedule**
5. UCS-A /chassis/cartridge/server/fault-suppress-task/local-schedule # **scope occurrence single-one-time**
6. UCS-A /chassis/cartridge/server/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*
7. UCS-A /chassis/cartridge/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*}
8. UCS-A /chassis/cartridge/server/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope server <i>chassis-id/cartridge-id/server-id</i>	Enters server mode for the specified server.
Step 2	UCS-A /chassis/cartridge/server # scope fault-suppress-task <i>name</i>	Enters fault-suppress-task mode. 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 /chassis/cartridge/server/fault-suppress-task # set schedule <i>name</i>	Applies a different schedule. Note If you change from a fixed time interval to a schedule, the fixed time interval is deleted when you commit. 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 /chassis/cartridge/server/fault-suppress-task # scope local-schedule	Enters local-schedule mode.
Step 5	UCS-A /chassis/cartridge/server/fault-suppress-task/local-schedule # scope occurrence single-one-time	Enters single-one-time mode.
Step 6	UCS-A /chassis/cartridge/server/fault-suppress-task/local-schedule/single-one-time # set date <i>month day-of-month year hour minute seconds</i>	Specifies the date and time that this occurrence should run.
Step 7	UCS-A /chassis/cartridge/server/fault-suppress-task/local-schedule/single-one-time # set max-duration { <i>none num-of-days num-of-hours num-of-minutes num-of-seconds</i> }	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 /chassis/cartridge/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 1/1/1
UCS-A /chassis/cartridge/server # scope fault-suppress-task task2
UCS-A /chassis/cartridge/server/fault-suppress-task # scope local-schedule
UCS-A /chassis/cartridge/server/fault-suppress-task/local-schedule # scope occurrence
single-one-time
UCS-A /chassis/cartridge/server/fault-suppress-task/local-schedule/single-one-time # set
date dec 31 2014 11 00 00
UCS-A /chassis/cartridge/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 1/1/1
UCS-A /chassis/cartridge/server # scope fault-suppress-task task1
UCS-A /chassis/cartridge/server/fault-suppress-task # set schedule monthly-maint
UCS-A /chassis/cartridge/server/fault-suppress-task* # commit-buffer
```

Viewing Suppressed Faults and Fault Suppression Tasks for a Server

SUMMARY STEPS

1. UCS-A# **scope server** *chassis-id/cartridge-id/server-id*
2. UCS-A /chassis/cartridge/server # **show fault suppressed**
3. UCS-A /chassis/cartridge/server # **scope fault-suppress-task** *name*
4. UCS-A /chassis/cartridge/server/fault-suppress-task # **show detail expand**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope server <i>chassis-id/cartridge-id/server-id</i>	Enters server mode for the specified server.
Step 2	UCS-A /chassis/cartridge/server # show fault suppressed	Displays the suppressed faults for the server. Note Only faults owned by the selected component are displayed.
Step 3	UCS-A /chassis/cartridge/server # scope fault-suppress-task <i>name</i>	Enters fault-suppress-task mode.
Step 4	UCS-A /chassis/cartridge/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 1/1/1
UCS-A /chassis/cartridge/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 1/1/1
UCS-A /chassis/cartridge/server # scope fault-suppress-task task1
UCS-A /chassis/cartridge/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 /chassis/cartridge/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.

SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A /org # **scope service-profile** *profile-name*
3. UCS-A /org/service-profile # **create fault-suppress-task** *name*
4. UCS-A/org/service-profile/fault-suppress-task # **create local-schedule**
5. UCS-A/org/service-profile/fault-suppress-task/local-schedule # **create occurrence single-one-time**
6. UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*
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*}
8. UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope org <i>org-name</i>	Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the <i>org-name</i> .
Step 2	UCS-A /org # scope service-profile <i>profile-name</i>	Enters service profile organization mode for the service profile.
Step 3	UCS-A /org/service-profile # create fault-suppress-task <i>name</i>	Creates a fault-suppress-task on the chassis, and enters the fault-suppress-task mode. 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 <i>month day-of-month year hour minute seconds</i>	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 <i>num-of-days num-of-hours num-of-minutes num-of-seconds</i> }	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.

SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A /org # **scope service-profile** *profile-name*
3. UCS-A /org/service-profile # **create fault-suppress-task** *name*
4. UCS-A/org/service-profile/fault-suppress-task # **set schedule** *name*
5. UCS-A/org/service-profile/fault-suppress-task # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope org <i>org-name</i>	Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the <i>org-name</i> .
Step 2	UCS-A /org # scope service-profile <i>profile-name</i>	Enters service profile organization mode for the service profile.
Step 3	UCS-A /org/service-profile # create fault-suppress-task <i>name</i>	Creates a fault-suppress-task on the chassis, and enters the fault-suppress-task mode.

	Command or Action	Purpose
		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 # set schedule <i>name</i>	Specifies the schedule that you want to use. 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

SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A /org # **scope service-profile** *profile-name*
3. UCS-A/org/service-profile # **delete fault-suppress-task** *name*
4. UCS-A/org/service-profile # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope org <i>org-name</i>	Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the <i>org-name</i> .
Step 2	UCS-A /org # scope service-profile <i>profile-name</i>	Enters service profile organization mode for the service profile.
Step 3	UCS-A/org/service-profile # delete fault-suppress-task <i>name</i>	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

SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A /org # **scope service-profile** *profile-name*
3. UCS-A/org/service-profile # **scope fault-suppress-task** *name*
4. UCS-A/org/service-profile/fault-suppress-task # **set schedule** *name*
5. UCS-A/org/service-profile/fault-suppress-task # **scope local-schedule**
6. UCS-A/org/service-profile/fault-suppress-task/local-schedule # **scope occurrence single-one-time**
7. UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*
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*}
9. UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope org <i>org-name</i>	Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the <i>org-name</i> .
Step 2	UCS-A /org # scope service-profile <i>profile-name</i>	Enters service profile organization mode for the service profile.
Step 3	UCS-A/org/service-profile # scope fault-suppress-task <i>name</i>	Enters fault-suppress-task mode. 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 <i>name</i>	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. 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 <i>month day-of-month year hour minute seconds</i>	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 { <i>none num-of-days num-of-hours num-of-minutes num-of-seconds</i> }	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

SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A /org # **scope service-profile** *profile-name*
3. UCS-A/org/service-profile # **show fault suppressed**
4. UCS-A/org/service-profile # **scope fault-suppress-task** *name*
5. UCS-A/org/service-profile/fault-suppress-task # **show detail expand**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope org <i>org-name</i>	Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the <i>org-name</i> .
Step 2	UCS-A /org # scope service-profile <i>profile-name</i>	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. Note Only faults owned by the selected component are displayed.
Step 4	UCS-A/org/service-profile # scope fault-suppress-task <i>name</i>	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.

SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A/org # **create fault-suppress-task** *name*
3. UCS-A/org/fault-suppress-task # **create local-schedule**
4. UCS-A/org/fault-suppress-task/local-schedule # **create occurrence single-one-time**
5. UCS-A/org/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*
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*}
7. UCS-A/org/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope org <i>org-name</i>	Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the <i>org-name</i> .
Step 2	UCS-A/org # create fault-suppress-task <i>name</i>	Creates a fault-suppress-task for the organization, and enters fault-suppress-task mode. 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 <i>month day-of-month year hour minute seconds</i>	Specifies the date and time that this occurrence should run.

	Command or Action	Purpose
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
00
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.

SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A/org # **create fault-suppress-task** *name*
3. UCS-A/org/fault-suppress-task # **set schedule** *name*
4. UCS-A/org/fault-suppress-task # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope org <i>org-name</i>	Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the <i>org-name</i> .
Step 2	UCS-A/org # create fault-suppress-task <i>name</i>	Creates a fault-suppress-task for the organization, and enters the fault-suppress-task mode. 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 <i>name</i>	Specifies the schedule that you want to use. 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 .

	Command or Action	Purpose
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

SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A/org # **delete fault-suppress-task** *name*
3. UCS-A/org # **commit-buffer**

DETAILED STEPS

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

SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A/org # **scope fault-suppress-task** *name*
3. UCS-A/org/fault-suppress-task # **set schedule** *name*
4. UCS-A/org/fault-suppress-task # **scope local-schedule**
5. UCS-A/org/fault-suppress-task/local-schedule # **scope occurrence single-one-time**
6. UCS-A/org/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*
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*}
8. UCS-A/org/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# scope org <i>org-name</i>	Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the <i>org-name</i> .
Step 2	UCS-A/org # scope fault-suppress-task <i>name</i>	Enters fault-suppress-task mode. 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 <i>name</i>	Applies a different schedule. Note If you change from a fixed time interval to a schedule, the fixed time interval is deleted when you commit. 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 <i>month day-of-month year hour minute seconds</i>	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

SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A/org # **show fault suppressed**
3. UCS-A/org # **scope fault-suppress-task** *name*
4. UCS-A/org/fault-suppress-task # **show detail expand**

DETAILED STEPS

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

SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope sysdebug**
3. UCS-A /monitoring/sysdebug # **enable core-export-target**
4. UCS-A /monitoring/sysdebug # **set core-export-target path** *path*
5. UCS-A /monitoring/sysdebug # **set core-export-target port** *port-num*
6. UCS-A /monitoring/sysdebug # **set core-export-target server-description** *description*
7. UCS-A /monitoring/sysdebug # **set core-export-target server-name** *hostname*
8. UCS-A /monitoring/sysdebug # **commit-buffer**

DETAILED STEPS

	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.
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

SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope sysdebug**
3. UCS-A /monitoring/sysdebug # **disable core-export-target**
4. UCS-A /monitoring/sysdebug # **commit-buffer**

DETAILED STEPS

	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

DETAILED STEPS

	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) 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) 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. Note Messages at levels below Critical are displayed on the terminal monitor only if you have entered the terminal monitor command.

	Command or Action	Purpose
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 <i>filename</i>	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) 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 <i>filesize</i>	(Optional) 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.
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) 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 <i>hostname</i>	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) 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: <ul style="list-style-type: none"> • audits—Enables or disables the logging of all audit log events. • events—Enables or disables the logging of all system events. • 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

SUMMARY STEPS

1. UCS-A# **scope security**
2. UCS-A /security # **show audit-logs**

DETAILED STEPS

	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 user admin logge				
2013-01-03T23:08:37.459	admin	1025416	Creation	Uplink FC
VSAN member port A/1/3				
2013-01-03T23:08:37.459	admin	1025417	Deletion	Uplink FC
VSAN member port A/1/3				
2013-01-03T23:08:02.387	admin	1025299	Creation	Uplink FC
VSAN member port A/1/3				
2013-01-03T23:08:02.387	admin	1025300	Deletion	Uplink FC
VSAN member				

```

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

SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope sysdebug**
3. UCS-A /monitoring/sysdebug # **scope log-export-policy**
4. UCS-A /monitoring/sysdebug/log-export-policy # **set admin-state {disabled | enabled}**
5. (Optional) UCS-A /monitoring/sysdebug/log-export-policy # **set desc *description***
6. UCS-A /monitoring/sysdebug/log-export-policy # **set hostname *hostname***
7. UCS-A /monitoring/sysdebug/log-export-policy # **set passwd**
8. UCS-A /monitoring/sysdebug/log-export-policy # **set passwordless-ssh {no | yes}**
9. UCS-A /monitoring/sysdebug/log-export-policy # **set proto {scp | ftp | sftp | tftp}**
10. UCS-A /monitoring/sysdebug/log-export-policy # **set path *path***
11. UCS-A /monitoring/sysdebug/log-export-policy # **set user *username***
12. UCS-A /monitoring/sysdebug/log-export-policy # **commit-buffer**

DETAILED STEPS

	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 <i>description</i>	(Optional) Provides a description for the log export policy
Step 6	UCS-A /monitoring/sysdebug/log-export-policy # set hostname <i>hostname</i>	Specifies the hostname of the remote server.
Step 7	UCS-A /monitoring/sysdebug/log-export-policy # set passwd	After you press Enter, you are prompted to enter the password. 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.

	Command or Action	Purpose
Step 10	UCS-A /monitoring/sysdebug/log-export-policy # set path <i>path</i>	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 <i>username</i>	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 #
```