Monitoring Cisco UCS Manager using Syslog

First Published: April 01, 2013

Last Modified: October 01, 2013

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

Text Part Number: OL-29326-01

© 2013 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

This preface includes the following sections:

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 *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.
System output	Terminal sessions and information that the system displays appear in `this font`.
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Text Type	Indication
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.

Other Documentation Resources

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

The ISO file is updated after every major documentation release.

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

Documentation Feedback

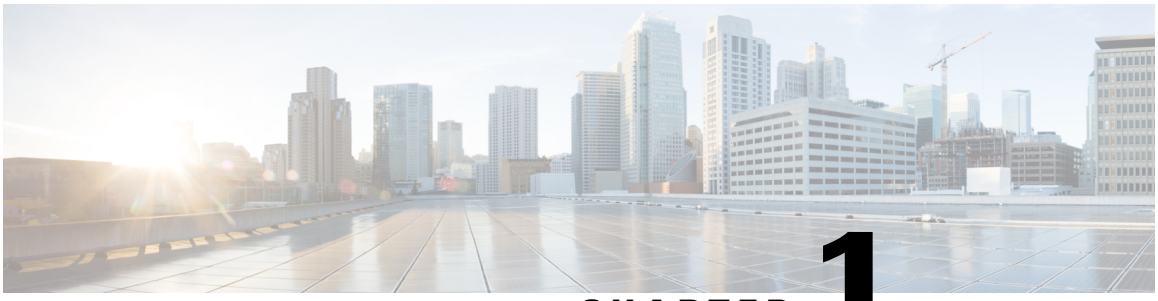
To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation.

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

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



CHAPTER 1

Introduction to Syslog Messages

This chapter includes the following sections:

Syslog Messages

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

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

There are three kinds of syslog entries:

- Faults
- Events
- Audit logs

Each syslog message identifies the Cisco UCS Manager process that generated the message and provides a brief description of the operation or error that occurred.

Cisco UCS Manager Message Severity Terms and Codes

Cisco UCS Manager labels each log entry with a severity term. The following table compares the Cisco UCS Manager severity term label for a log entry to the serverity term label displayed in the syslog in Cisco UCS Manager, release 1.4 and later:

Table 1: Severity Terms

Cisco UCS Manager Severity	Syslog Level, Release 1.4 and Later
info	info
warning	notification
minor	warnings
major	error
crtical	critical

The following table contains the Cisco UCS Manager message severity codes and their descriptions. Severity codes can be used to create filters for monitoring syslog messages.

Table 2: Severity Codes

Code	Severity	Keyword	Description
0	Emergency	emerg (panic)	Emergency messages indicate that the system is unusable. A panic condition usually affects multiple applications, servers, or sites. Emergency messages can be set to notify all technical staff members who are on call.
1	Alert	alert	Alert messages indicate that action must be taken immediately; staff members who can fix the problem must be notified. An example of an alert message would be the loss of a primary ISP connection.
2	Critical	crit	Critical messages indicate conditions that should be corrected immediately, and also indicate failure in a secondary system. An example of a critical message would be the loss of a backup ISP connection.
3	Error	err	Error messages indicate non-urgent failures. Error messages should be relayed to developers or network administrators, and must be resolved within a specific timeframe.
4	Warning	warning (warn)	Warning messages indicate that that an error will occur if action is not taken, for example, the file system is 85% full. Warnings faults also must be resolved within a specific timeframe.

Code	Severity	Keyword	Description
5	Notice	notice	Notice messages indicate events that are unusual but that are not error conditions. They can be summarized in an email to developers or administrators to spot potential problems, but no immediate action is necessary.
6	Informational	info	Informational messages are associated with normal operational behavior. They may be tracked for reporting, measuring throughput, or other purposes, but no action is required.
7	Debug	debug	Debug messages are useful to developers for debugging the application, but are not useful for tracking operations.

Cisco UCS Manager Fault Types

The table below defines the fault types that are available in Cisco UCS Manager, and their usefulness for monitoring purposes:

Table 3: Fault Types in Cisco UCS Manager

Type	Description	Monitoring
fsm	An FSM task has failed to complete successfully, or the Cisco UCS Manager is retrying one of the stages of the FSM.	These faults are not intended for remote syslog or SNMP notification.
equipment	Cisco UCS Manager has detected that a physical component is inoperable or has another functional issue.	These faults are essential for service monitoring.
server	Cisco UCS Manager is unable to complete a server task, such as associating a service profile with a server.	These faults are raised during server provisioning or service profile association.
configuration	Cisco UCS Manager is unable to successfully configure a component.	These faults are essential for service monitoring.
environment	Cisco UCS Manager has detected a power problem, thermal problem, voltage problem, or loss of CMOS settings.	These faults are essential for service monitoring.

Type	Description	Monitoring
management	Cisco UCS Manager has detected a serious management issue, such as one of the following: • Critical services cannot be started. • The primary switch cannot be identified. • A software service has become unresponsive. • Components in the instance include incompatible firmware versions.	These faults are essential for service monitoring.
connectivity	Cisco UCS Manager has detected a connectivity problem, such as an unreachable adapter.	These faults are essential for service monitoring.
network	Cisco UCS Manager has detected a network issue, such as a link down.	These faults are essential for service monitoring.
operational	Cisco UCS Manager has detected an operational issue, such as one of the following: • A log data store has reached its maximum capacity. • Files cannot be transferred. • A server discovery failed.	These faults do not have significant value for remote monitoring.

Syslog Message Example and Format

The following string is an example of a typical Cisco UCS Manager syslog message:

Apr 19 17:11:12 UTC: %UCSM-6-LOG_CAPACITY: [F0461][info][log-capacity][sys/chassis-1/blade-7/mgmt/log-SEL-0] Log capacity on Management Controller on server 1/7 is very-low

The following table lists the Syslog message parts and provides the definition of each part:

Syslog Message	Message Part	Definition
Apr 19 17:11:12 UTC	Date and Time	Provides the date and the time, in UTC format, and indicates when the event or fault occurred.
%UCSM	Facility	Refers to the message source. The message source is usually a hardware device, a protocol, or a module of the system software. **Note** Facility is Cisco-specific and is only relevant within the message string. It is different from facility as defined in RFC 3164 for the syslog protocol. For messages originating from Cisco UCS Manager, the facility will always be %UCSM.

Syslog Message	Message Part	Definition
6	Severity	Refers to the syslog severity code.
LOG_CAPACITY	Mnemonic	A device-specific code that uniquely identifies the message, and maps to a fault type in Cisco UCS Manager.
[F0461]	ID	A unique identifier assigned to the fault.
[info]	UCSM Severity	In this example, a basic notification or informational message, possibly independently insignificant.
[log-capacity]	Mnemonic	A device-specific code that uniquely identifies the message and maps to the fault type in Cisco UCS Manager.
[sys/chassis-1/blade-7/mgmt/log-SEL-0]	System	The specific Cisco UCS device in which the fault occurred.
Log capacity on Management Controller on server 1/7 is very-low	Description	A brief description of the fault.

Note For more information about Cisco UCS Manager faults, refer tohttp://www.cisco.com/en/US/docs/unified_computing/ucs/ts/faults/reference/2.0/UCSFaultsErrorsRef_20.html.

Syslog Messages for Cisco UCS Manager Faults

A fault is an abnormal condition or defect at the component, equipment, or subsystem level which may lead to a failure. Faults are categorized by their severity, and the message part of the syslog entry contains text that lets you see the criticality of the fault. Faults can also be managed using SNMP. For more information about managing faults using SNMP, refer to the http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/b-series/b_UCS_MIBRef.html.

The following are a few examples of syslog messages generated for fault events:

- 2011 Apr 19 17:11:12 UTC: %UCSM-6-LOG_CAPACITY: [F0461][info][log-capacity][sys/chassis-1/blade-7/mgmt/log-SEL-0] Log capacity on Management Controller on server 1/7 is very-low
- 2011 Apr 20 14:33:14 UTC: %UCSM-3-CONFIGURATION_FAILURE: [F0327][major][configuration-failure][org-root/ls-test] Service profile test configuration failed due to insufficient-resources,mac-address-assignment,system-uuid-as
- 2011 Apr 20 20:50:25 UTC: %UCSM-3-THERMAL_PROBLEM: [F0382][major][thermal-problem][sys/chassis-1/fan-module-1-1] Fan module 1/1-1 temperature: lower-critical

- 2011 Apr 20 14:33:14 UTC: %UCSM-5-UNASSOCIATED: [F0334][warning][unassociated][org-root/ls-test] Service profile test is not associated

Syslog Messages for Cisco UCS Manager Events

Event messages are generated when an FSM transitions from one state to another. Event messages notify you of the transitions of all FSMs, and may contain information about a specific user when a user invokes a process that updates the state of an FSM.

Note All FSM event messages are delivered with the info security level in syslog.

The following are a few examples of syslog messages generated by system events:

- 2011 Apr 22 16:53:18 UTC: %UCSM-6-EVENT: [E4195931][456249][transition][ucs-username\username][] [FSM:BEGIN]: Hard-reset server sys/chassis-1/blade-7(FSM:sam:dme:ComputePhysicalHardreset)
- 2011 Apr 22 16:53:18 UTC: %UCSM-6-EVENT: [E4195931][456250][transition][ucs-username\username][] [FSM:STAGE:END]:(FSM-STAGE:sam:dme:ComputePhysicalHardreset:begin)
- 2011 Apr 22 16:53:18 UTC: %UCSM-6-EVENT: [E4195932][456251][transition][ucs-username\username][] [FSM:STAGE:ASYNC]: Preparing to check hardware configuration server sys/chassis-1/blade-7(FSM-STAGE:sam:dme:ComputePhysicalHa
- 2011 Apr 22 16:53:23 UTC: %UCSM-6-EVENT: [E4195932][456252][transition][internal][] [FSM:STAGE:STALE-SUCCESS]: Preparing to check hardware configuration server sys/chassis-1/blade-7(FSM-STAGE:sam:dme:ComputePhysicalHardres
- 2011 Apr 22 16:53:23 UTC: %UCSM-6-EVENT: [E4195932][456253][transition][internal][] [FSM:STAGE:END]: Preparing to check hardware configuration server sys/chassis-1/blade-7(FSM-STAGE:sam:dme:ComputePhysicalHardreset:PreSani
- 2011 Apr 25 18:27:01 UTC: %UCSM-6-EVENT: [E4196181][535831][transition][internal][] [FSM:END]: Hard-reset server sys/chassis-1/blade-7(FSM:sam:dme:ComputePhysicalHardreset)

Syslog Messages for Cisco UCS Manager Audit Logs

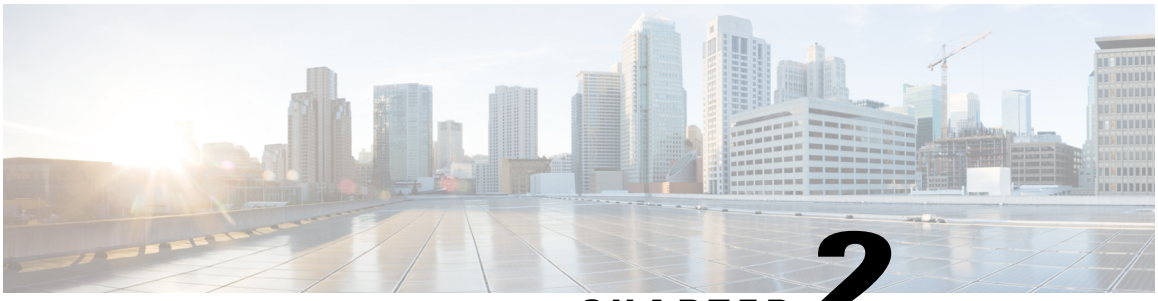
An audit log entry describes an activity that takes place in the Cisco UCS Manager system. It identifies what took place, when it took place, where it took place (in what physical resource), and who was responsible. Audit log entries track actions that are initiated by system users.

Note All audit log messages are delivered with the info security level in syslog.

The following are a few examples of system audit log messages that are logged to syslog:

- 2011 May 15 10:19:14 UTC: %UCSM-6-AUDIT: [session][internal][creation][] Web B: remote user ibm logged in from 172.25.206.73

- 2011 Apr 22 16:53:18 UTC: %UCSM-6-AUDIT: [admin][ucs-username\username][modification][] server 1/7 power-cycle/reset action requested: hard-reset-immediate
- 2011 Apr 20 14:33:14 UTC: %UCSM-6-AUDIT: [admin][username][creation][] service profile test created
- 2011 Apr 20 14:33:14 UTC: %UCSM-6-AUDIT: [admin][username][creation][] service profile Power MO created
- 2011 Apr 20 14:33:14 UTC: %UCSM-6-AUDIT: [admin][username][creation][] Ether vnic eth1 created
- 2011 Apr 20 14:33:14 UTC: %UCSM-6-AUDIT: [admin][username][creation][] Ethernet interface created



CHAPTER 2

Configuring Syslog in Cisco UCS Manager

This chapter contains the following sections:

Syslog Configuration

You can configure syslog in Cisco UCS Manager using both Cisco UCS Manager GUI and the Cisco UCS Manager CLI.

Configuring the Syslog Using Cisco UCS Manager GUI

SUMMARY STEPS

1. In the **Navigation** pane, click the **Admin** tab.
2. On the **Admin** tab, expand **All** > **Faults, Events, and Audit Log**.
3. Click **Syslog**.
4. In the **Work** pane, click the **Syslog** tab.
5. In the **Local Destinations** area, complete the following fields:
6. In the **Remote Destinations** area, complete the following fields to configure up to three external logs that can store messages generated by the Cisco UCS components:
7. In the **Local Sources** area, complete the following fields:
8. Click **Save Changes**.

DETAILED STEPS

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

Step 2 On the **Admin** tab, expand **All** > **Faults, Events, and Audit Log**.

Step 3 Click **Syslog**.

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

Step 5 In the **Local Destinations** area, complete the following fields:

Name	Description
Console Section	
Admin State field	Whether Cisco UCS displays Syslog messages on the console. This can be one of the following: • **Enabled—**Syslog messages are displayed on the console as well as added to the log. • **Disabled—**Syslog messages are added to the log but not displayed on the console.
Level field	If this option is **enabled**, select the lowest message level that you want displayed. Cisco UCS displays that level and above on the console. This can be one of the following: • **Emergencies** • **Alerts** • **Critical**
Monitor Section	
Admin State field	Whether Cisco UCS displays Syslog messages on the monitor. This can be one of the following: • **Enabled—**Syslog messages are displayed on the monitor as well as added to the log. • **Disabled—**Syslog messages are added to the log but not displayed on the monitor. If **Admin State** is enabled, Cisco UCS Manager GUI displays the rest of the fields in this section.

Name	Description
Level drop-down list	If this option is **enabled**, select the lowest message level that you want displayed. The system displays that level and above on the monitor. This can be one of the following: • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information** • **Debugging**
File Section	
Admin State field	Whether Cisco UCS stores messages in a system log file on the fabric interconnect. This can be one of the following: • **Enabled—**Messages are saved in the log file. • **Disabled—**Messages are not saved. If **Admin State** is enabled, Cisco UCS Manager GUI displays the rest of the fields in this section.
Level drop-down list	Select the lowest message level that you want the system to store. Cisco UCS stores that level and above in a file on the fabric interconnect. This can be one of the following: • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information** • **Debugging**

Name	Description
Name field	The name of the file in which the messages are logged. This name can be up to 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period). The default is messages.
Size field	The maximum size, in bytes, the file can be before Cisco UCS Manager begins to write over the oldest messages with the newest ones. Enter an integer between 4096 and 4194304.

Step 6 In the **Remote Destinations** area, complete the following fields to configure up to three external logs that can store messages generated by the Cisco UCS components:

Name	Description
Admin State field	This can be one of the following: • **Enabled** • **Disabled** If **Admin State** is enabled, Cisco UCS Manager GUI displays the rest of the fields in this section.
Level drop-down list	Select the lowest message level that you want the system to store. The system stores that level and above in the remote file. This can be one of the following: • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information** • **Debugging**
Hostname field	The hostname or IP address on which the remote log file resides. **Note** If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.

Name	Description
Facility drop-down list	This is the remote server where the syslog files are sent. You can configure specific log files to reach specific destinations. This can be one of the following: • **Local0** • **Local1** • **Local2** • **Local3** • **Local4** • **Local5** • **Local6** • **Local7**

Step 7 In the **Local Sources** area, complete the following fields:

Name	Description
Faults Admin State field	If this field is **Enabled**, Cisco UCS logs all system faults.
Audits Admin State field	If this field is **Enabled**, Cisco UCS logs all audit log events.
Events Admin State field	If this field is **Enabled**, Cisco UCS logs all system events.

Step 8 Click **Save Changes**.

Configuring the Syslog Using the Cisco UCS Manager CLI

DETAILED STEPS

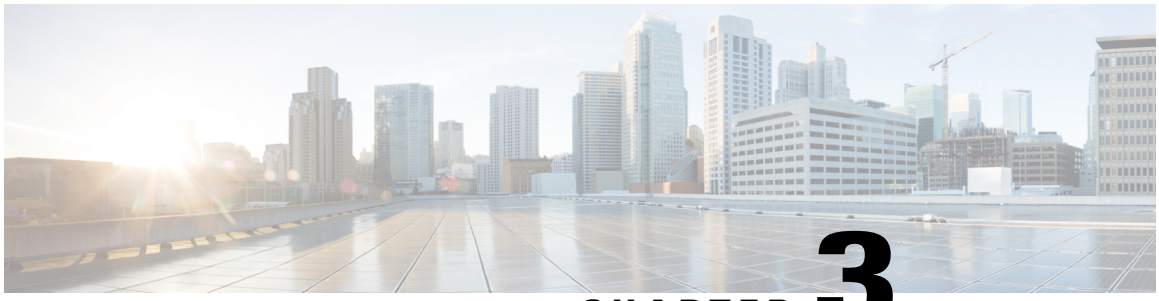
	Command or Action	Purpose
Step 1	UCS-A# **scope monitoring**	Enters monitoring mode.
Step 2	UCS-A /monitoring # {**enable** | **disable**} **syslog console**	Enables or disables the sending of syslogs to the console.
Step 3	UCS-A /monitoring # **set syslog console level** {**emergencies** | **alerts** | **critical**}	(Optional) Select the lowest message level that you want displayed. If syslogs are enabled, the system displays that level and above on the

	Command or Action	Purpose
		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.
Step 6	UCS-A /monitoring # {**enable** | **disable**} **syslog file**	Enables or disables the writing of syslog information to a syslog file.
Step 7	UCS-A /monitoring # **set syslog file name** *filename*	The name of the file in which the messages are logged. Up to 16 characters are allowed in the file name.
Step 8	UCS-A /monitoring # **set syslog file level** {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}	(Optional) Select the lowest message level that you want stored to a file. If the file state is enabled, the system stores that level and above in the syslog file. The level options are listed in order of decreasing urgency.The default level is Critical.
Step 9	UCS-A /monitoring # **set syslog file size** *filesize*	(Optional) 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** *hostname*	The hostname or IP address of the specified remote syslog server. Up to 256 characters are allowed in the hostname.
Step 13	UCS-A /monitoring # **set syslog remote-destination** {**server-1** | **server-2** | **server-3**} **facility** {**local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7**}	(Optional) The facility level contained in the syslog messages sent to the specified remote syslog server.

	Command or Action	Purpose
Step 14	UCS-A /monitoring # {**enable** | **disable**} **syslog source** {**audits** | **events** | **faults**}	This can be one of the following: • **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 #
```



CHAPTER 3

Monitoring Syslog Messages in Cisco UCS Manager

This chapter contains the following sections:

Monitoring Syslog Messages

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

- By **event** or **fault** codes: Define a filter with a parsing rule to include only the specific codes that you intend to monitor. All messages that do not match these criteria will be discarded.
- By **severity** level: Define a filter with a parsing rule to monitor syslog messages with specific severity levels.

Refer to Cisco UCS Manager Message Severity Terms and Codes, on page 1 for more detail.

Syslog Messages to Monitor

The table below lists some syslog messages that you may want to monitor in Cisco UCS Manager:

Failure	Fault Type	Fault Code and Description
DIMM problems	equipment	F0185 - DIMM [id]/[id] on server [chassisId]/[slotId] operability: [operability]

Failure	Fault Type	Fault Code and Description
Equipment failures	equipment	F0291 - Fabric Interconnect [id] operability: [operability] F0313 - Server [chassisId]/[slotId] (service profile: [assignedToDn]) BIOS failed power-on self test F0317 - Server [chassisId]/[slotId] (service profile: [assignedToDn]) health: [operability] F0373 - Fan [id] in Fan Module [id]/[tray]-[id] operability: [operability]Fan [id] in fabric interconnect [id] operability: [operability]Fan [id] in fex [id] operability: [operability]Fan [id] in server [id] operability: [operability] F0374 - Power supply [id] in chassis [id] operability: [operability]Power supply [id] in fabric interconnect [id] operability: [operability]Power supply [id] in fex [id] operability: [operability]Power supply [id] in server [id] operability: [operability] F0376 - [side] IOM [chassisId]/[id] ([switchId]) is removed F0404 - Chassis [id] has a mismatch between FRU identity reported by Fabric/IOM vs. FRU identity reported by CMC F0405 - [side] IOM [chassisId]/[id] ([switchId]) has a malformed FRU F0478 - [side] IOM [chassisId]/[id] ([switchId]) is inaccessible F0481 - [side] IOM [chassisId]/[id] ([switchId]) POST failure F0484 - Fan [id] in Fan Module [id]/[tray]-[id] speed: [perf]Fan [id] in fabric interconnect [id] speed: [perf]Fan [id] in server [id] speed: [perf]

Failure	Fault Type	Fault Code and Description
Thermal problems	environment	F0176/F0177 - Processor [id] on server [chassisId]/[slotId] temperature: [thermal] F0187/F0188 - DIMM [id]/[id] on server [chassisId]/[slotId] temperature: [thermal] F0312/F0313 - Server [chassisId]/[slotId] (service profile: [assignedToDn]) oper state: [operState] F0379 - [side] IOM [chassisId]/[id] ([switchId]) operState: [operState] F0382/F0384 - Fan module [id]/[tray]-[id] temperature: [thermal]Fan module [id]/[tray]-[id] temperature: [thermal] F0383/F0385 - Power supply [id] in chassis [id] temperature: [thermal]Power supply [id] in fabric interconnect [id] temperature:thermal]Power supply [id] in server [id] temperature: [thermal] F0409/F0411 - Temperature on chassis [id] is [thermal] F0539/F0540 - IO Hub on server [chassisId]/[slotId] temperature: [thermal]
Voltage problems	environment	F0179/F0180 - Processor [id] on server [chassisId]/[slotId] voltage: [voltage] F0190/F0191 - Memory array [id] on server [chassisId]/[slotId] voltage: [voltage] F0389/F0391 - Power supply [id] in chassis [id] voltage: [voltage]Power supply [id] in fabric interconnect [id] voltage: [voltage]Power supply [id] in fex [id] voltage: [voltage]Power supply [id] in server [id] voltage: [voltage] F0425 - Possible loss of CMOS settings: CMOS battery voltage on server [chassisId]/[slotId] is [cmosVoltage]
Power problems	environment	F0310 - Motherboard of server [chassisId]/[slotId] (service profile: [assignedToDn]) power: [operPower] F0311 - Server [chassisId]/[slotId] (service profile: [assignedToDn]) oper state: [operState] F0369 - Power supply [id] in chassis [id] power: [power]Power supply [id] in fabric interconnect [id] power: [power]Power supply [id] in fex [id] power: [power]Power supply [id] in server [id] power: [power] F0408 - Power state on chassis [id] is [power]

Failure	Fault Type	Fault Code and Description
HA Cluster failures	management	F0293 - Fabric Interconnect [id], HA Cluster interconnect link failure F0294 - Fabric Interconnect [id], HA Cluster interconnect total link failure F0428 - Fabric Interconnect [id], election of primary managemt instance has failed F0429 - Fabric Interconnect [id], HA functionality not ready F0430 - Fabric Interconnect [id], management services, incompatible versions F0451 - Fabric Interconnect [id], management services have failed F0452 - Fabric Interconnect [id], management services are unresponsive
Link failures	connectivity	F0276 - [transport] port [portId] on chassis [id] oper state: [operState], reason: [stateQual][transport] port [portId] on fabric interconnect [id] oper state: [operState], reason: [stateQual] F0277 - [transport] port [portId] on chassis [id] oper state: [operState], reason: [stateQual][transport] port [portId] on fabric interconnect [id] oper state: [operState], reason: [stateQual] F0367 - No link between IOM port [chassisId]/[slotId]/[portId] and fabric interconnect [switchId]:[peerSlotId]/[peerPortId]