Viewing Faults and Logs

This chapter includes the following sections:

Fault Summary

Viewing the Faults and Logs Summary

Procedure

	Command or Action	Purpose
Step 1	Server # **scope fault**	Enters fault command mode.
Step 2	Server # **show fault-entries**	Displays a log of all the faults.

Example

This example displays a summary of faults:

```
Server # scope fault
Server /fault # show fault-entries
Time                     Severity      Description
------------------------ ------------ -----------------
Sun Jun 27 04:00:52 2013  info        Storage Local disk 12 missing
Sat Jun 26 05:00:22 2013  warning     Power Supply redundancy is lost

Server /fault #
```

Fault History

Viewing the Fault History

Procedure

	Command or Action	Purpose
Step 1	Server # **scope fault**	Enters fault command mode.
Step 2	Server # **show fault-history**	Displays the faults' history.

Example

This example displays the faults' history:

```
Server # scope fault
Server /fault # show fault-history
Time                Severity  Source  Cause                 Description
------------------- --------- ------  --------------------
----------------------------------------
2014 Feb 6 23:24:49 error     %CIMC   PSU_REDUNDANCY-FAIL
"[F0743][major][psu-redundancy-fail].....
2014 Feb 6 23:24:49 error     %CIMC   EQUIPMENT_INOPERABLE
"[F0374][major][equipment-inoperable]...
2014 Feb 6 23:24:19 debug     %CIMC   2014 Feb 6 23        "24:19:7:%CIMC::: SEL INIT DONE"


Server /fault #
```

Cisco IMC Log

Viewing the Cisco IMC Log

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the Cisco IMC command mode.
Step 2	Server /cimc # **scope log**	Enters the Cisco IMC log command mode.
Step 3	Server /cimc/log # **show entries** [**detail**]	Displays Cisco IMC events, including timestamp, the software module that logged the event, and a description of the event.

Example

This example displays the log of Cisco IMC events:

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # show entries
Time                Severity      Source           Description

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

2012 Jan 30 05:20:45 Informational BMC:ciscoNET:961 " rpc_aim_callback_function_1_svc() -
result == SUCCESS, callbackData size: 600 "
2012 Jan 30 05:20:45 Informational BMC:ciscoNET:961 rpc_aim_callback_function_1_svc() -
returned from pFunctionCallback result:0
2012 Jan 30 05:20:45 Informational BMC:ciscoNET:961 " rpc_aim_callback_function_1_svc() -
szFunctionName:netGetCurrentIfConfig nSize:0 nMaxSize: 600 "
--More--

Server /cimc/log # show entries detail
Trace Log:
    Time: 2012 Jan 30 05:20:45
    Severity: Informational
    Source: BMC:ciscoNET:961
   Description: " rpc_aim_callback_function_1_svc() - result == SUCCESS, callbackData size:
 600 "
    Order: 0
Trace Log:
    Time: 2012 Jan 30 05:20:45
    Severity: Informational
    Source: BMC:ciscoNET:961
   Description: rpc_aim_callback_function_1_svc() - returned from pFunctionCallback result:0

    Order: 1
Trace Log:
    Time: 2012 Jan 30 05:20:45
    Severity: Informational
    Source: BMC:ciscoNET:961
   Description: " rpc_aim_callback_function_1_svc() - szFunctionName:netGetCurrentIfConfig
 nSize:0 nMaxSize: 600 "
    Order: 2
--More--

Server /cimc/log #
```

Clearing the Cisco IMC Log

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the Cisco IMC command mode.
Step 2	Server /cimc # **scope log**	Enters the Cisco IMC log command mode.
Step 3	Server /cimc/log # **clear**	Clears the Cisco IMC log.

Example

The following example clears the log of Cisco IMC events:

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # clear
```

Configuring the Cisco IMC Log Threshold

You can specify the lowest level of messages that will be included in the Cisco IMC log.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the Cisco IMC command mode.
Step 2	Server /cimc # **scope log**	Enters the Cisco IMC log command mode.
Step 3	Server /cimc/log # **set local-syslog-severity** *level*	The severity *level* can be one of the following, in decreasing order of severity: • emergency • alert • critical • error • warning • notice • informational • debug **Note** Cisco IMC does not log any messages with a severity below the selected severity. For example, if you select **error**, then the Cisco IMC log will contain all messages with the severity Emergency, Alert, Critical, or Error. It will not show Warning, Notice, Informational, or Debug messages.
Step 4	Server /cimc/log # **commit**	Commits the transaction to the system configuration.

	Command or Action	Purpose
Step 5	(Optional) Server /cimc/log # **show local-syslog-severity**	Displays the configured severity level.

Example

This example shows how to configure the logging of messages with a minimum severity of Warning:

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # set local-syslog-severity warning
Server /cimc/log *# commit
Server /cimc/log # show local-syslog-severity
    Local Syslog Severity: warning

Server /cimc/log #
```

Sending the Cisco IMC Log to a Remote Server

You can configure profiles for one or two remote syslog servers to receive Cisco IMC log entries.

Before you begin

- The remote syslog server must be configured to receive logs from a remote host.
- The remote syslog server must be configured to receive all types of logs, including authentication-related logs.
- The remote syslog server's firewall must be configured to allow syslog messages to reach the syslog server.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the Cisco IMC command mode.
Step 2	Server /cimc # **scope log**	Enters the Cisco IMC log command mode.
Step 3	(Optional) Server /cimc/log # **set remote-syslog-severity** *level*	The severity *level* can be one of the following, in decreasing order of severity: • emergency • alert • critical • error • warning • notice

	Command or Action	Purpose
		• informational • debug **Note** Cisco IMC does not remotely log any messages with a severity below the selected severity. For example, if you select **error**, then the remote syslog server will receive all Cisco IMC log messages with the severity Emergency, Alert, Critical, or Error. It will not show Warning, Notice, Informational, or Debug messages.
Step 4	Server /cimc/log # **scope server** {**1** | **2**}	Selects one of the two remote syslog server profiles and enters the command mode for configuring the profile.
Step 5	Server /cimc/log/server # **set server-ip** *ipv4 or ipv6 address or domain name*	Specifies the remote syslog server address. **Note** You can set an IPv4 or IPv6 address or a domain name as the remote server address.
Step 6	Server /cimc/log/server # **set server-port** *port number*	Sets the destination port number of the remote syslog server.
Step 7	Server /cimc/log/server # **set enabled** {**yes** | **no**}	Enables the sending of Cisco IMC log entries to this syslog server.
Step 8	Server /cimc/log/server # **commit**	Commits the transaction to the system configuration.

Example

This example shows how to configure a remote syslog server profile and enable the sending of Cisco IMC log entries with a minimum severity level of Warning:

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # set remote-syslog-severity warning
Server /cimc/log *# scope server 1
Server /cimc/log/server *# set server-ip www.abc.com
Server /cimc/log/server *# set server-port 514
Server /cimc/log/server *# set enabled yes
Server /cimc/log/server *# commit
Server /cimc/log/server # exit
Server /cimc/log # show server
Syslog Server 1:
    Syslog Server Address: www.abc.com
    Syslog Server Port: 514
    Enabled: yes
```

```
Server /cimc/log # show remote-syslog-severity
    Remote Syslog Severity: warning

Server /cimc/log #
```

Sending a Test Cisco IMC Log to a Remote Server

Before you begin

- The remote syslog server must be configured to receive logs from a remote host.
- The remote syslog server must be configured to receive all types of logs, including authentication-related logs.
- The remote syslog server's firewall must be configured to allow syslog messages to reach the syslog server.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the Cisco IMC command mode.
Step 2	Server /cimc # **scope log**	Enters the Cisco IMC log command mode.
Step 3	Server /cimc/log # **send-test-syslog**	Sends a test Cisco IMC log to the configured remote servers.

Example

This example shows how to send a test Cisco IMC syslog to the configured remote servers:

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # send-test-syslog

Syslog Test message will be sent to configured Syslog destinations.
If no Syslog destinations configured, this command will be silently ignored.
Syslog Test message has been requested.

Server /cimc/log #
```

Enabling the Logging of Invalid Usernames

Perform this procedure to enable logging of invalid usernames in case of failed logging attempts.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the Cisco IMC command mode.

	Command or Action	Purpose
Step 2	Server /cimc # **scope log**	Enters the Cisco IMC log command mode.
Step 3	Server /cimc/log #**set log-username-on-auth-fail enabled**	Enables logging of invalid usernames.
Step 4	Server /cimc/log* #**commit**	Commits the transaction to the system configuration.

Example

This example displays how to enable logging invalid usernames:

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # set log-username-on-auth-fail enabled
Server /cimc/log* #commit
Server /cimc/log
```

System Event Log

Viewing the System Event Log

Procedure

	Command or Action	Purpose
Step 1	Server# **scope sel**	Enters the system event log (SEL) command mode.
Step 2	Server /sel # **show entries** [**detail**]	For system events, displays timestamp, the severity of the event, and a description of the event. The **detail** keyword displays the information in a list format instead of a table format.

Example

This example displays the system event log:

```
Server# scope sel
Server /sel # show entries
Time                 Severity      Description
-------------------- ------------- ----------------------------------------
[System Boot]       Informational " LED_PSU_STATUS: Platform sensor, OFF event was asserted"

[System Boot]        Informational " LED_HLTH_STATUS: Platform sensor, GREEN was asserted"
[System Boot]        Normal        " PSU_REDUNDANCY: PS Redundancy sensor, Fully Redundant
was asserted"
[System Boot]        Normal        " PSU2 PSU2_STATUS: Power Supply sensor for PSU2, Power
```

```
Supply input lost (AC/DC) was deasserted"
[System Boot]       Informational " LED_PSU_STATUS: Platform sensor, ON event was asserted"

[System Boot]       Informational " LED_HLTH_STATUS: Platform sensor, AMBER was asserted"
[System Boot]       Critical      " PSU_REDUNDANCY: PS Redundancy sensor, Redundancy Lost
was asserted"
[System Boot]       Critical      " PSU2 PSU2_STATUS: Power Supply sensor for PSU2, Power
Supply input lost (AC/DC) was asserted"
[System Boot]       Normal        " HDD_01_STATUS: Drive Slot sensor, Drive Presence was
asserted"
[System Boot]       Critical      " HDD_01_STATUS: Drive Slot sensor, Drive Presence was
deasserted"
[System Boot]       Informational " DDR3_P2_D1_INFO: Memory sensor, OFF event was asserted"

2001-01-01 08:30:16 Warning       " PSU2 PSU2_VOUT: Voltage sensor for PSU2, failure event
 was deasserted"
2001-01-01 08:30:16 Critical     " PSU2 PSU2_VOUT: Voltage sensor for PSU2, non-recoverable
 event was deasserted"
2001-01-01 08:30:15 Informational " LED_PSU_STATUS: Platform sensor, ON event was asserted"

2001-01-01 08:30:15 Informational " LED_HLTH_STATUS: Platform sensor, AMBER was asserted"
2001-01-01 08:30:15 Informational " LED_HLTH_STATUS: Platform sensor, FAST BLINK event was
 asserted"
2001-01-01 08:30:14 Non-Recoverable " PSU2 PSU2_VOUT: Voltage sensor for PSU2, non-recoverable
 event was asserted"
2001-01-01 08:30:14 Critical      " PSU2 PSU2_VOUT: Voltage sensor for PSU2, failure event
 was asserted"
--More--
```

Clearing the System Event Log

Procedure

	Command or Action	Purpose
Step 1	Server# **scope sel**	Enters the system event log command mode.
Step 2	Server /sel # **clear**	You are prompted to confirm the action. If you enter **y** at the prompt, the system event log is cleared.

Example

This example clears the system event log:

```
Server# scope sel
Server /sel # clear
This operation will clear the whole sel.
Continue?[y|N]y
```