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      Distinguished Name (DN)
--------------      ---------     ----------------------------------------
2015-08-18T06:44:02  major        sys/chassis-1/server-2/board/memarray-1/mem-2
2015-08-18T06:43:48  major        sys/chassis-1/server-2/board/memarray-1/mem-1

Description
------------------------------------------------------------------
"DDR3_P1_A2_ECC: DIMM 2 is inoperable : Check or replace DIMM"
"DDR3_P1_A1_ECC: DIMM 1 is inoperable : Check or replace DIMM"
```

```
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 Cisco IMC Log

Procedure

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope log**	Enters log command mode.
Step 3	Server /chassis/log # **show entries detail**	Displays the CMC trace log details.

Example

This example displays the CMC trace log details:

```
Server# scope chassis
Server /chassis # scope log
Server /chassis/log # show entries detail
Trace Log:
    Time: 2015 Jul 26 06:35:15
    Severity: Notice
    Source: CMC:dropbear:19566
    Description: PAM password auth succeeded for 'cli' from 10.127.148.234:53791
    Order: 0
Trace Log:
    Time: 2015 Jul 26 06:35:15
    Severity: Notice
    Source: CMC:AUDIT:19566
    Description: Session open (user:admin, ip:10.127.148.234, id:6, type:CLI)
    Order: 1
Trace Log:
    Time: 2015 Jul 26 06:35:15
    Severity: Informational
    Source: CMC:dropbear:19566
    Description: " pam_session_manager(sshd:session): session (6) opened for user admin
from 10.127.148.234 by (uid=0) "
    Order: 2
Trace Log:
    Time: 2015 Jul 26 06:35:15
    Severity: Notice
    Source: CMC:AUDIT:1779
.
.
.

Server /chassis/log #
```

Clearing Trace Logs

Procedure

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

Example

The following example clears the log of trace logs:

```
Server# scope chassis
Server /chassis # scope log
Server /chassis/log # clear
```

```
Server /chassis/log #
```

Configuring the Cisco IMC Log Threshold

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

Procedure

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

	Command or Action	Purpose
		• 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 5	Server /chassis/log # **commit**	Commits the transaction to the system configuration.
Step 6	(Optional) Server /chassis/log # **show**	Displays the configured severity level.

Example

This example shows how to configure the logging of messages with a minimum severity of Debug for the local syslogs and error for the remote syslog:

```
Server# scope chassis
Server /chassis # scope log
Server /chassis/log # set local-syslog-severity debug
Server /chassis/log # set remote-syslog-severity error
Server /chassis/log *# commit
Server /chassis/log # show
Local Syslog Severity  Remote Syslog Severity
---------------------- ----------------------
debug                  error

Server /chassis/log #
```

Sending the Cisco IMC Log to a Remote Server

You can configure profiles for one or two remote syslog servers to receive system 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 chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope log**	Enters log command mode.
Step 3	Server /chassis/log # **scope server** {**1** | **2**}	Selects one of the two remote syslog server profiles and enters the command mode for configuring the profile.
Step 4	Server /chassis/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 5	Server /chassis/log/server # **set server-port** *port number*	Sets the destination port number of the remote syslog server.
Step 6	Server /chassis/log/server # **set enabled** {**yes** | **no**}	Enables the sending of system log entries to this syslog server.
Step 7	Server /chassis/log/server # **commit**	Commits the transaction to the system configuration.
Step 8	Server /chassis/log/server # **exit**	Exits to the log command mode.
Step 9	Server /chassis/log/server # **showserver**	Exits to the log command mode.

Example

This example shows how to configure a remote syslog server profile and enable the sending of system log entries:

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--
```

Viewing the System Event Log for Servers

Procedure

	Command or Action	Purpose
Step 1	Server# **scope server** {*1* | *2* }	Enters the server mode for server 1 or 2.
Step 2	Server /server # **scope sel**	Enters the system event log (SEL) command mode.
Step 3	Server /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 server 1
Server/server # scope sel
Server /server/sel # show entries
Time                Severity  Description
------------------- --------- ----------------------------------------
2015-08-18 08:46:03 Normal    "BIOS_POST_CMPLT: Presence sensor, Device Inserted / Device
Present was asserted"
2015-08-18 08:46:00 Normal    "System Software event: System Event sensor, OEM System Boot
 Event was asserted"
2010-03-21 00:17:42 Normal    "System Software event: System Event sensor, Timestamp Clock
 Synch (second of pair) was asserted"
2015-08-18 08:44:34 Normal    "System Software event: System Event sensor, Timestamp Clock
 Synch (first of pair) was asserted"
2015-08-18 08:44:00 Normal    "BIOS_POST_CMPLT: Presence sensor, Device Removed / Device
Absent was asserted"
2015-08-18 08:44:00 Normal    "MAIN_POWER_PRS: Presence sensor, Device Inserted / Device
Present was asserted"
2015-08-18 08:43:39 Normal    "MAIN_POWER_PRS: Presence sensor, Device Removed / Device
Absent was asserted"
2015-08-18 08:16:18 Normal    "BIOS_POST_CMPLT: Presence sensor, Device Inserted / Device
Present was asserted"
2015-08-18 08:16:16 Normal    "System Software event: System Event sensor, OEM System Boot
 Event was asserted"
2010-03-20 23:47:59 Normal    "System Software event: System Event sensor, Timestamp Clock
 Synch (second of pair) was asserted"
2015-08-18 08:14:50 Normal    "System Software event: System Event sensor, Timestamp Clock
 Synch (first of pair) was asserted"
2015-08-18 08:14:20 Normal    "BIOS_POST_CMPLT: Presence sensor, Device Removed / Device
Absent was asserted"
2015-08-18 08:14:20 Normal    "MAIN_POWER_PRS: Presence sensor, Device Inserted / Device
```

```
Present was asserted"
2015-08-18 08:13:44 Normal    "MAIN_POWER_PRS: Presence sensor, Device Removed / Device
Absent was asserted"
2015-08-18 08:12:57 Normal    "FRU_RAM SEL_FULLNESS: Event Log sensor for FRU_RAM, Log Area
 Reset/Cleared was asserted"
```

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
```

Logging Controls

Configuring the Cisco IMC Log Threshold

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

Procedure

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope log**	Enters log command mode.
Step 3	Server /chassis/log # **set local-syslog-severity** *level*	The severity *level* can be one of the following, in decreasing order of severity: • emergency • alert

	Command or Action	Purpose
		• 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 /chassis/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 • 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.

	Command or Action	Purpose
Step 5	Server /chassis/log # **commit**	Commits the transaction to the system configuration.
Step 6	(Optional) Server /chassis/log # **show**	Displays the configured severity level.

Example

This example shows how to configure the logging of messages with a minimum severity of Debug for the local syslogs and error for the remote syslog:

```
Server# scope chassis
Server /chassis # scope log
Server /chassis/log # set local-syslog-severity debug
Server /chassis/log # set remote-syslog-severity error
Server /chassis/log *# commit
Server /chassis/log # show
Local Syslog Severity  Remote Syslog Severity
---------------------- ----------------------
debug                  error

Server /chassis/log #
```

Sending the Cisco IMC Log to a Remote Server

You can configure profiles for one or two remote syslog servers to receive system 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 chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope log**	Enters log command mode.
Step 3	Server /chassis/log # **scope server** {**1** | **2**}	Selects one of the two remote syslog server profiles and enters the command mode for configuring the profile.

	Command or Action	Purpose
Step 4	Server /chassis/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 5	Server /chassis/log/server # **set server-port** *port number*	Sets the destination port number of the remote syslog server.
Step 6	Server /chassis/log/server # **set enabled** {**yes** | **no**}	Enables the sending of system log entries to this syslog server.
Step 7	Server /chassis/log/server # **commit**	Commits the transaction to the system configuration.
Step 8	Server /chassis/log/server # **exit**	Exits to the log command mode.
Step 9	Server /chassis/log/server # **showserver**	Exits to the log command mode.

Example

This example shows how to configure a remote syslog server profile and enable the sending of system log entries:

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 chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope log**	Enters log command mode.
Step 3	Server /chassis/log # **send-test-syslog**	Sends a test log to the remote server.

Example

This example shows how send a test log to a remote server: