Viewing Faults and Logs

This chapter includes the following sections:

Faults

Viewing the Fault Summary

Procedure

	Command or Action	Purpose
Step 1	Server# **scope fault**	Enters fault command mode.
Step 2	Server /fault # **show discrete-alarm** [**detail**]	Displays a summary of faults from discrete sensors.
Step 3	Server /fault # **show threshold-alarm** [**detail**]	Displays a summary of faults from threshold sensors.
Step 4	Server /fault # **show pef** [**detail**]	Displays a summary of platform event filters.

Example

This example displays a summary of faults from discrete sensors:

```
Server# scope fault
Server /fault # show discrete-alarm
Name         Reading              Sensor Status
------------ -------------------- ------------------------------------
PSU2_STATUS  absent               Critical

Server /fault #
```

System Event Log

Viewing the System Event Log

SUMMARY STEPS

1. Server# **scope sel**
2. Server /sel # **show entries** [**detail**]

DETAILED STEPS

	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

SUMMARY STEPS

1. Server# **scope sel**
2. Server /sel # **clear**

DETAILED STEPS

	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
```

Cisco IMC Log

Viewing the CIMC Log

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **scope log**
3. Server /cimc/log # **show entries** [**detail**]

DETAILED STEPS

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

Example

This example displays the log of CIMC events:

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # show entries
Time                Source           Description
------------------- ---------------- ----------------------------------------
1970 Jan 4 18:55:36 BMC:kernel:-
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:306:I2c Controller-4 DAT is stuck-low,
 issuing One Clock Pulse.
1970 Jan 4 18:55:36 BMC:kernel:-
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:301:I2c Controller-4 Loop:[0].
1970 Jan 4 18:55:36 BMC:kernel:-     "
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:422: Controller-4 has a stuck bus,
attempting to clear it now... "
1970 Jan 4 18:55:36 BMC:kernel:-     "
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:402: Controller-4 Initiating I2c recovery
 sequence. "
1970 Jan 4 18:55:36 BMC:IPMI:480     last message repeated 22 times
1970 Jan 4 18:55:28 BMC:IPMI:480     "  mcddI2CDrv.c:850:PI2CWriteRead: ioctl to driver
failed to read Bus[f4].Dev[5e]! ErrorStatus[77] "
1970 Jan 4 18:55:33 BMC:IPMI:486     last message repeated 17 times
1970 Jan 4 18:55:28 BMC:IPMI:486     "  mcddI2CDrv.c:850:PI2CWriteRead: ioctl to driver
failed to read Bus[f4].Dev[b0]! ErrorStatus[77] "
1970 Jan 4 18:55:31 BMC:IPMI:486     last message repeated 17 times
1970 Jan 4 18:55:26 BMC:IPMI:486     "  mcddI2CDrv.c:850:PI2CWriteRead: ioctl to driver
failed to read Bus[f4].Dev[b2]! ErrorStatus[77] "
1970 Jan 4 18:55:26 BMC:kernel:-
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:306:I2c Controller-4 DAT is stuck-low,
 issuing One Clock Pulse.
1970 Jan 4 18:55:26 BMC:kernel:-
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:301:I2c Controller-4 Loop:[8].
--More--
```

Clearing the CIMC Log

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **scope log**
3. Server /cimc/log # **clear**

DETAILED STEPS

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

Example

This example clears the log of CIMC events:

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

Configuring the CIMC Log Threshold

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

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **scope log**
3. Server /cimc/log # **set local-syslog-severity** *level*
4. Server /cimc/log # **commit**
5. (Optional) Server /cimc/log # **show local-syslog-severity**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope log**	Enters CIMC 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

	Command or Action	Purpose
		• informational • debug **Note** The CIMC does not log any messages with a severity below the selected severity. For example, if you select **error**, then the CIMC 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.
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 CIMC Log to a Remote Server

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope log**	Enters CIMC log command mode.
Step 3	Server /cimc/log # **scope server** {**1** | **2**}	Selects one of two remote syslog server profiles and enters the command mode for configuring the profile.
Step 4	Server /cimc/log/server # **set server-ip** *ip-address*	Specifies the remote syslog server IP address.
Step 5	Server /cimc/log/server # **set enabled** {**yes** | **no**}	Enables the sending of CIMC log entries to this syslog server.
Step 6	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 CIMC log entries:

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # scope server 2
Server /cimc/log/server # set server-ip 192.0.2.34
Server /cimc/log/server *# set enabled yes
Server /cimc/log/server *# commit
Server /cimc/log/server #
```