Viewing Faults and Logs

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**]	(Optional) 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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope sel**	Enters the system event log (SEL) command mode.
Step 2	Server /sel # **show entries** [**details**]	(Optional) 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
-----------------------     -------------     ----------------------------------------
2023-06-30 21:17:53 UTC     Informational     "LED_BMC_ACT: Platform sensor, "
2023-06-30 21:17:53 UTC     Informational     "LED_BMC_ACT: Platform sensor, "
2023-06-30 21:17:52 UTC     Informational     "LED_SYS: Platform sensor, "
2023-06-30 21:17:52 UTC     Informational     "LED_SYS: Platform sensor, "
2023-06-30 21:17:51 UTC     Informational     "LED_HLTH_STATUS: Platform sensor, "
2023-06-30 21:17:51 UTC     Informational     "LED_HLTH_STATUS: Platform sensor, "
2023-06-30 21:17:50 UTC     Informational     "LED_PWR_BTN: Platform sensor, "
2023-06-30 21:17:50 UTC     Informational     "LED_PWR_BTN: Platform sensor, "
2023-06-30 21:17:50 UTC     Normal            "P1_PRESENT: Presence sensor, Device Removed
 / Device Absent was asserted"
2023-06-30 21:17:50 UTC     Normal            "BIOS_POST_CMPLT: Presence sensor, Device
Removed / Device Absent was asserted"
2023-06-30 21:17:50 UTC     Normal            "MINI_STORAGE_PRS: Presence sensor, Device
Removed / Device Absent was asserted"
2023-06-30 21:17:50 UTC     Normal            "MAIN_POWER_PRS: Presence sensor, Device
Inserted / Device Present was asserted"
2023-06-30 21:17:50 UTC    Normal           "HDD4_STATUS: Drive Slot sensor, Drive Presence
 was asserted"
sence was asserted" UTC     Normal            "HDD3_STATUS: Drive Slot sensor, Drive
Pre--More--
2023-06-30 21:17:50 UTC    Normal           "HDD2_STATUS: Drive Slot sensor, Drive Presence
 was asserted"
2023-06-30 21:17:50 UTC    Normal           "HDD1_STATUS: Drive Slot sensor, Drive Presence
 was asserted"
2023-06-30 21:17:50 UTC     Normal            "RISER3_PRESENT: Presence sensor, Device
Removed / Device Absent was asserted"
2023-06-30 21:17:50 UTC     Normal            "RISER2_PRESENT: Presence sensor, Device
Removed / Device Absent was asserted"
2023-06-30 21:17:50 UTC     Normal            "RISER1_PRESENT: Presence sensor, Device
Removed / Device Absent 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
```

Cisco IMC Log

Viewing the CIMC Log

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 # **show entries** [**detail**]	(Optional) 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:

Recovery-shell# `fs-check [p3| p4]`	Checks the file system of the specified partition and recover the corrupted file system.
Recovery-shell# `active image`	Shows the current active image that CIMC is running, which can be image 1 or image 2.

Recovery-shell# `active image [1 | 2]`	Changes the active image to 1 or 2. If the specified image is already active, a message is displayed. Otherwise,the specified image is made active. After you use the active image command, use the **reboot** command for the newly configured image to take effect.
Recovery-shell# `reboot`	Reboots the CIMC firmware.