Configuring Platform Event Filters

This chapter includes the following sections:

Platform Event Filters

A platform event filter (PEF) can trigger an action and generate an alert when a critical hardware-related event occurs. For each PEF, you can choose the action to be taken (or take no action) when a platform event occurs. You can also choose to generate and send an alert when a platform event occurs. Alerts are sent as an SNMP trap, so you must configure an SNMP trap destination before the alerts can be sent.

You can globally enable or disable the generation of platform event alerts. When disabled, alerts are not sent even if PEFs are configured to send them.

Enabling Platform Event Alerts

Procedure

	Command or Action	Purpose
Step 1	Server# **scope fault**	Enters the fault command mode.
Step 2	Server /fault # **set platform-event-enabled yes**	Enables platform event alerts.

	Command or Action	Purpose
Step 3	Server /fault # **commit**	Commits the transaction to the system configuration.
Step 4	Server /fault # **show** [**detail**]	(Optional) Displays the platform event alert configuration.

The following example enables platform event alerts:

```
Server# scope fault
Server /fault # set platform-event-enabled yes
Server /fault *# commit
Server /fault # show
SNMP Community String Platform Event Enabled
--------------------- ----------------------
public                yes

Server /fault #
```

Disabling Platform Event Alerts

Procedure

	Command or Action	Purpose
Step 1	Server# **scope fault**	Enters the fault command mode.
Step 2	Server /fault # **set platform-event-enabled no**	Disables platform event alerts.
Step 3	Server /fault # **commit**	Commits the transaction to the system configuration.
Step 4	Server /fault # **show** [**detail**]	(Optional) Displays the platform event alert configuration.

The following example disables platform event alerts:

```
Server# scope fault
Server /fault # set platform-event-enabled no
Server /fault *# commit
Server /fault # show
SNMP Community String Platform Event Enabled
--------------------- ----------------------
public                no

Server /fault #
```

Configuring Platform Event Filters

You can configure actions and alerts for the following platform event filters:

ID	Platform Event Filter
1	Temperature Critical Assert Filter
2	Temperature Warning Assert Filter
3	Voltage Critical Assert Filter
4	Current Assert Filter
5	Fan Critical Assert Filter
6	Processor Assert Filter
7	Power Supply Critical Assert Filter
8	Power Supply Warning Assert Filter
9	Power Supply Redundancy Lost Filter
10	Discrete Power Supply Assert Filter
11	Memory Assert Filter
12	Drive Slot Assert Filter

Procedure

	Command or Action	Purpose
Step 1	Server# **scope fault**	Enters the fault command mode.
Step 2	Server /fault # **scope pef** *id*	Enters the platform event filter command mode for the specified event. See the Platform Event Filter table for event ID numbers.
Step 3	Server /fault/pef # **set action** {**none** | **reboot** | **power-cycle** | **power-off**}	Selects the desired system action when this event occurs. The action can be one of the following: • **none** —No system action is taken. • **reboot** —The server is rebooted. • **power-cycle** —The server is power cycled. • **power-off** —The server is powered off.
Step 4	Server /fault/pef # **set send-alert** {**yes** | **no**}	Enables or disables the sending of a platform event alert for this event.

	Command or Action	Purpose
		Note For an alert to be sent, the filter trap settings must be configured properly and platform event alerts must be enabled.
Step 5	Server /fault/pef # **commit**	Commits the transaction to the system configuration.

This example configures the platform event alert for an event:

```
Server# scope fault
Server /fault # scope pef 13
Server /fault/pef # set action reboot
Server /fault/pef *# set send-alert yes
Server /fault/pef *# commit
Server /fault/pef # show
Platform Event Filter Event                      Action      Send Alert
-------------------- --------------------------- ----------- ------------------
13                   Memory Assert Filter        reboot      yes

Server /fault/pef #
```

What to Do Next

If you configure any PEFs to send an alert, complete the following tasks:

- Enable platform event alerts
- Configure SNMP trap settings

Configuring SNMP Trap Settings

Before You Begin

- You must log in with admin privileges to perform this task.
- SNMP must be enabled and saved before trap settings can be configured.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope snmp**	Enters the SNMP command mode.
Step 2	Server /snmp # **set trap-community-str** *string*	Enter the name of the SNMP community to which trap information should be sent.
Step 3	Server /snmp # **set trap-ver** {**1** | **2** | **3**}	Specify the desired SNMP version of the trap message. **Note** SNMPv3 traps will be delivered only to locations where the SNMPv3 user and key values are configured correctly.

	Command or Action	Purpose
Step 4	Server /snmp # **set inform-type** {**trap** | **inform**}	Specifies whether SNMP notification messages are sent as simple traps or as inform requests requiring acknowledgment by the receiver.
Step 5	Server /snmp # **scope trap-destination** *number*	Enters the SNMP trap destination command mode for the specified destination. Four SNMP trap destinations are available. The destination *number* is an integer between 1 and 4.
Step 6	Server /snmp/trap-destination # **set enabled** {**yes** | **no**}	Enables or disables the SNMP trap destination.
Step 7	Server /snmp/trap-destination # **set addr** *ip-address*	Specifies the destination IP address to which SNMP trap information is sent.
Step 8	Server /snmp/trap-destination # **commit**	Commits the transaction to the system configuration.

This example configures general SNMP trap settings and trap destination number 1 and commits the transaction:

```
Server# scope snmp
Server /snmp # set trap-community-str public
Server /snmp # set trap-ver 3
Server /snmp # set inform-type inform
Server /snmp *# scope trap-destination 1
Server /snmp/trap-destination *# set enabled yes
Server /snmp/trap-destination *# set addr 192.0.20.41
Server /snmp/trap-destination *# commit
Server /snmp/trap-destination # show
Trap Destination IP Address       Enabled
---------------- ---------------- --------
1                192.0.20.41      yes

Server /snmp/trap-destination #
```

Sending a Test SNMP Trap Message

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope snmp**	Enters the SNMP command mode.
Step 2	Server /snmp # **scope trap-destination** *number*	Enters the SNMP trap destination command mode for the specified destination. Four SNMP trap destinations are available. The destination *number* is an integer between 1 and 4.

	Command or Action	Purpose
Step 3	Server /snmp/trap-destination # **sendSNMPtrap**	Sends an SNMPv1 test trap to the configured SNMP trap destination. **Note** The trap must be configured and enabled in order to send a test message.

This example sends a test message to SNMP trap destination 1:

```
Server# scope snmp
Server /snmp # scope trap-destination 1
Server /snmp/trap-destination # sendSNMPtrap
SNMP Test Trap sent to Destination:1
Server /snmp/trap-destination #
```

Interpreting Platform Event Traps

A CIMC platform event alert sent as an SNMP trap contains an enterprise object identifier (OID) in the form `1.3.6.1.4.1.3183.1.1.0.event`. The first ten fields of the OID represent the following information: `iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).wired_for_management(3183).PET(1).version(1).version(0)`, indicating an IPMI platform event trap (PET) version 1.0 message. The last field is an event number, indicating the specific condition or alert being notified.

Platform Event Trap Descriptions

The following table provides a description of the event being notified in a platform event trap message, based on the event number in the trap OID.

Event Number [Note 1]		Platform Event Description
0	0h	Test Trap
65799	010107h	Temperature Warning
65801	010109h	Temperature Critical
131330	020102h	Under Voltage, Critical
131337	020109h	Voltage Critical
196871	030107h	Current Warning
262402	040102h	Fan Critical
459776	070400h	Processor related (IOH-Thermalert/Caterr sensor) – predictive failure deasserted
459777	070401h	Processor related (IOH-Thermalert/Caterr sensor) – predictive failure asserted
460032	070500h	Processor Power Warning – limit not exceeded
460033	070501h	Processor Power Warning – limit exceeded

Event Number [Note 1]		Platform Event Description
524533	0800F5h	Power Supply Critical
524551	080107h	Power Supply Warning
525313	080401h	Discrete Power Supply Warning
527105	080B01h	Power Supply Redundancy Lost
527106	080B02h	Power Supply Redundancy Restored
552704	086F00h	Power Supply Inserted
552705	086F01h	Power Supply Failure
552707	086F03h	Power Supply AC Lost
786433	0C0001h	Correctable ECC Memory Errors, Release 1.3(1) and later releases, filter set to accept all reading types [Note 4]
786439	0C0007h	DDR3_INFO sensor LED - RED bit asserted (Probable ECC error on a DIMM), Generic Sensor [Notes 2,3]
786689	0C0101h	Correctable ECC Memory Errors, Release 1.3(1) and later releases
818945	0C7F01h	Correctable ECC Memory Errors, Release 1.2(x) and earlier releases
818951	0C7F07h	DDR3_INFO sensor LED - RED bit asserted (Probable ECC error on a DIMM), 1.2(x) and earlier releases [Note 3]
851968	0D0000h	HDD sensor indicates no fault, Generic Sensor [Note 2]
851972	0D0004h	HDD sensor indicates a fault, Generic Sensor [Note 2]
854016	0D0800h	HDD Absent, Generic Sensor [Note 2]
854017	0D0801h	HDD Present, Generic Sensor [Note 2]
880384	0D6F00h	HDD Present, no fault indicated
880385	0D6F01h	HDD Fault
880512	0D6F80h	HDD Not Present
880513	0D6F81h	HDD is deasserted but not in a fault state
884480	0D7F00h	Drive Slot LED Off
884481	0D7F01h	Drive Slot LED On
884482	0D7F02h	Drive Slot LED fast blink
884483	0D7F03h	Drive Slot LED slow blink
884484	0D7F04h	Drive Slot LED green
884485	0D7F05h	Drive Slot LED amber
884486	0D7F01h	Drive Slot LED blue
884487	0D7F01h	Drive Slot LED read

Event Number [Note 1]		Platform Event Description
884488	0D7F08h	Drive Slot Online
884489	0D7F09h	Drive Slot Degraded
Note 1: Basic information about the event number format can be found in the *IPMI Platform Event Trap Format Specification v1.0* at this URL: ftp://download.intel.com/design/servers/ipmi/pet100.pdf.		
Note 2: Some platforms and releases use generic sensor implementations, while some use Cisco proprietary sensor implementations.		
Note 3: In Release 1.3(1) and later releases, the ECC sensor no longer activates the LED.		
Note 4: When the event filter is set to accept all reading types, bits 15:8 of the hex event number are masked to 0. For example, event number 786689 (0C0101h) becomes 786433 (0C0001h).		