



## ログの表示

この章は、次の内容で構成されています。

- CIMC ログ, 1 ページ
- System Event Log, 5 ページ

## CIMC ログ

### CIMC ログの表示

#### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope cimc</b>	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # <b>scope log</b>	CIMC ログ コマンド モードを開始します。
ステップ 3	Server /cimc/log # <b>show entries [detail]</b>	CIMC イベントをタイムスタンプ、イベントを記録したソフトウェア モジュール、およびイベントの説明とともに表示します。

次に、CIMC イベントのログを表示する例を示します。

```
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].
```

## CIMC ログのクリア

```

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--

```

## CIMC ログのクリア

## 手順

	コマンドまたはアクション	目的
ステップ1	Server# <b>scope cimc</b>	CIMC コマンド モードを開始します。
ステップ2	Server /cimc # <b>scope log</b>	CIMC ログ コマンド モードを開始します。
ステップ3	Server /cimc/log # <b>clear</b>	CIMC ログをクリアします。

次に、CIMC イベントのログをクリアする例を示します。

```

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

```

## CIMC ログしきい値の設定

CIMC ログに含まれるメッセージの最低レベルを指定できます。

## 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope cimc</b>	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # <b>scope log</b>	CIMC ログ コマンド モードを開始します。
ステップ 3	Server /cimc/log # <b>set local-syslog-severity level</b>	重大度の <i>level</i> には、次のいずれかを指定できます。順に重大度が下がります。 <ul style="list-style-type: none"> <li>• emergency</li> <li>• alert</li> <li>• critical</li> <li>• error</li> <li>• warning</li> <li>• notice</li> <li>• informational</li> <li>• debug</li> </ul> (注) CIMC では、選択した重大度よりも低い重大度のメッセージはログに記録されません。たとえば、 <b>error</b> を選択した場合、CIMC ログには重大度が Emergency、Alert、Critical、または Error のすべてのメッセージが含まれます。Warning、Notice、Informational、または Debug のメッセージは表示されません。
ステップ 4	Server /cimc/log # <b>commit</b>	トランザクションをシステムの設定にコミットします。
ステップ 5	Server /cimc/log # <b>show local-syslog-severity</b>	(任意) 設定された重大度レベルを表示します。

次に、最小重大度を警告として、メッセージのロギングを設定する例を示します。

```
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 #
```

## リモートサーバへの CIMC ログの送信

1台または2台のリモートsyslogサーバが CIMC ログエントリを受信するように、プロファイルを設定できます。

### 手順

	コマンドまたはアクション	目的
ステップ1	Server# <b>scope cimc</b>	CIMC コマンドモードを開始します。
ステップ2	Server /cimc # <b>scope log</b>	CIMC ログコマンドモードを開始します。
ステップ3	Server /cimc/log # <b>scope server {1   2}</b>	2つのリモートsyslogサーバプロファイルのうち1つを選択し、プロファイルを設定するコマンドモードを開始します。
ステップ4	Server /cimc/log/server # <b>set server-ip ip-address</b>	リモートsyslogサーバのIPアドレスを指定します。
ステップ5	Server /cimc/log/server # <b>set enabled {yes   no}</b>	このsyslogサーバへのCIMC ログエントリの送信をイネーブルにします。
ステップ6	Server /cimc/log/server # <b>commit</b>	トランザクションをシステムの設定にコミットします。

次に、リモートsyslogサーバプロファイルを設定し、CIMC ログエントリの送信をイネーブルにする例を示します。

```
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 #
```

# System Event Log

## システムイベントログの表示

### 手順

	コマンドまたはアクション	目的
ステップ1	Server# <b>scope sel</b>	システムイベントログ (SEL) コマンドモードを開始します。
ステップ2	Server /sel # <b>show entries [detail]</b>	システムイベントについて、タイムスタンプ、イベントの重大度、およびイベントの説明を表示します。 <b>detail</b> キーワードを指定すると、表形式ではなくリスト形式で情報が表示されます。

次に、システムイベントログを表示する例を示します。

```
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--
```

## システムイベントログのクリア

### 手順

	コマンドまたはアクション	目的
ステップ1	Server# <b>scope sel</b>	システムイベントログコマンドモードを開始します。
ステップ2	Server /sel # <b>clear</b>	処理の確認を求めるプロンプトが表示されます。プロンプトにyと入力すると、システムイベントログはクリアされます。

次に、システムイベントログをクリアする例を示します。

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