障害およびログの表示

この章は、次の項で構成されています。

障害のサマリー

障害およびログのサマリーの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope fault**	障害コマンド モードを開始します。
ステップ 2	Server # **show fault-entries**	すべての障害のログを表示します。

例

次に、障害のサマリーの例を示します。

```
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 #
```

障害履歴

障害履歴の表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope fault**	障害コマンド モードを開始します。
ステップ 2	Server # **show fault-history**	障害の履歴を表示します。

例

次に、障害の履歴を表示する例を示します。

```
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 ログ

Cisco IMC 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 # **scope chassis**	シャーシ コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	Server /chassis # **scope log**	ログ コマンド モードを開始します。
ステップ 3	Server /chassis/log # **show entries detail**	CMC トレース ログの詳細を表示します。

例

この例では、CMC トレース ログの詳細が表示されます。

```
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 #
```

トレース ログの消去

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope log**	ログ コマンド モードを開始します。
ステップ 3	Server /chassis/log # **clear**	トレース ログを消去します。

例

次の例では、トレース ログのログを消去します。

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

Server /chassis/log #
```

Cisco IMC ログしきい値の設定

syslog 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 # **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope log**	ログ コマンド モードを開始します。
ステップ 3	Server /chassis/log # **set local-syslog-severity** *level*	重大度の *level* 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。 • emergency • alert • critical • error • warning • notice • informational • debug

	コマンドまたはアクション	目的
		（注） Cisco IMC 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、**error** を選択した場合、Cisco IMC 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 /chassis/log # **set remote-syslog-severity** *level*	重大度の *level* 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。 • emergency • alert • critical • error • warning • notice • informational • debug （注） Cisco IMC 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、**error** を選択した場合、Cisco IMC 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 5	Server /chassis/log # **commit**	トランザクションをシステムの設定にコミットします。

	コマンドまたはアクション	目的
ステップ 6	（任意） Server /chassis/log # **show**	設定された重大度レベルを表示します。

例

この例では、ローカル syslog のデバッグの最低重大度とリモートの syslog のエラーを示すメッセージのロギングを設定する方法を示します。

```
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 #
```

リモート サーバへの Cisco IMC ログの送信

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

始める前に

- リモート syslog サーバが、リモート ホストからログを受信するように設定されている必要があります。
- リモート syslog サーバが、認証関連のログを含め、すべてのタイプのログを受信するように設定されている必要があります。
- リモート syslog サーバのファイアウォールが、syslog メッセージが syslog サーバに到達するように設定されている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope log**	ログ コマンド モードを開始します。
ステップ 3	Server /chassis/log # **scope server** {**1** |**2**}	2 台のリモート syslog サーバ プロファイルのいずれかを選択し、プロファイルを設定するコマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	Server /chassis/log # **set server-ip** *ipv4* または *ipv6* アドレスまたはドメイン名	リモート syslog サーバのアドレスを指定します。 （注） リモート サーバのアドレスとして IPv4 アドレスまたは IPv6 アドレス、あるいはメイン名を設定できます。
ステップ 5	Server /chassis/log/server # **set server-port** ポート番号	リモート syslog サーバの宛先ポート番号を設定します。
ステップ 6	Server /chassis/log/server # **set enabled** {**yes** | **no**}	この syslog サーバへのシステム ログ エントリを有効にします。
ステップ 7	Server /chassis/log/server # **commit**	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 8	Server /chassis/log/server # **exit**	ログコマンドモードを終了します。
ステップ 9	Server /chassis/log/server # **showserver**	ログコマンドモードを終了します。

例

次に、リモート syslog サーバ プロファイルを設定し、システム ログ エントリの送信を有効にする例を示します。

システム イベント ログ

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# **scope sel**	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 # **show entries** [**detail**]	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。 **detail** 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。

例

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--
```

サーバのシステム 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 # **scope server** {*1* |*2* }	サーバ 1 または 2 のサーバ モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	Server /server # **scope sel**	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 3	Server /server/sel # **show entries** [**detail**]	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。 **detail** 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。

例

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 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"
```

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# **scope sel**	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 # **clear**	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。

例

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
```

ロギング制御

Cisco IMC ログしきい値の設定

syslog 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 # **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope log**	ログ コマンド モードを開始します。
ステップ 3	Server /chassis/log # **set local-syslog-severity** *level*	重大度の *level* 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。 • emergency • alert • critical

	コマンドまたはアクション	目的
		• error • warning • notice • informational • debug （注） Cisco IMC 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、**error** を選択した場合、Cisco IMC 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 /chassis/log # **set remote-syslog-severity** *level*	重大度の *level* 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。 • emergency • alert • critical • error • warning • notice • informational • debug

	コマンドまたはアクション	目的
		（注） Cisco IMC 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、**error** を選択した場合、Cisco IMC 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 5	Server /chassis/log # **commit**	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 6	（任意） Server /chassis/log # **show**	設定された重大度レベルを表示します。

例

この例では、ローカル syslog のデバッグの最低重大度とリモートの syslog のエラーを示すメッセージのロギングを設定する方法を示します。

```
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 #
```

リモート サーバへの Cisco IMC ログの送信

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

始める前に

- リモート syslog サーバが、リモート ホストからログを受信するように設定されている必要があります。
- リモート syslog サーバが、認証関連のログを含め、すべてのタイプのログを受信するように設定されている必要があります。

- リモート syslog サーバのファイアウォールが、syslog メッセージが syslog サーバに到達するように設定されている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope log**	ログ コマンド モードを開始します。
ステップ 3	Server /chassis/log # **scope server** {**1** |**2**}	2 台のリモート syslog サーバ プロファイルのいずれかを選択し、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 /chassis/log # **set server-ip** *ipv4* または *ipv6* アドレスまたはドメイン名	リモート syslog サーバのアドレスを指定します。 （注） リモート サーバのアドレスとして IPv4 アドレスまたは IPv6 アドレス、あるいはメイン名を設定できます。
ステップ 5	Server /chassis/log/server # **set server-port** ポート番号	リモート syslog サーバの宛先ポート番号を設定します。
ステップ 6	Server /chassis/log/server # **set enabled** {**yes** |**no**}	この syslog サーバへのシステム ログ エントリを有効にします。
ステップ 7	Server /chassis/log/server # **commit**	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 8	Server /chassis/log/server # **exit**	ログコマンドモードを終了します。
ステップ 9	Server /chassis/log/server # **showserver**	ログコマンドモードを終了します。

例

次に、リモート syslog サーバ プロファイルを設定し、システム ログ エントリの送信を有効にする例を示します。

リモート サーバへのテスト Cisco IMC ログの送信

始める前に

- リモート syslog サーバが、リモート ホストからログを受信するように設定されている必要があります。
- リモート syslog サーバが、認証関連のログを含め、すべてのタイプのログを受信するように設定されている必要があります。
- リモート syslog サーバのファイアウォールが、syslog メッセージが syslog サーバに到達するように設定されている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope log**	ログ コマンド モードを開始します。
ステップ 3	Server /chassis/log # **send-test-syslog**	テスト ログをリモート サーバに送信します。

例

この例では、テスト ログをリモート サーバに送信する方法の例を示します。