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      Description
------------------------ ------------ -----------------
Sun Jun 27 04:00:52 2013  info         Storage Local disk 12 missing
Sat Jun 26 05:00:22 2013  warning      Power Supply redundancy is lost

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 cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope log**	Cisco IMC ログ 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 3	Server /cimc/log # **show entries** [**detail**]	Cisco IMC 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。

例

次に、Cisco IMC 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                 Severity      Source           Description

------------------- ------------ --------------- ---------------------------------------

2012 Jan 30 05:20:45 Informational BMC:ciscoNET:961 " rpc_aim_callback_function_1_svc()
 - result == SUCCESS, callbackData size: 600 "
2012 Jan 30 05:20:45 Informational BMC:ciscoNET:961 rpc_aim_callback_function_1_svc() -
 returned from pFunctionCallback result:0
2012 Jan 30 05:20:45 Informational BMC:ciscoNET:961 " rpc_aim_callback_function_1_svc()
 - szFunctionName:netGetCurrentIfConfig nSize:0 nMaxSize: 600 "
--More--

Server /cimc/log # show entries detail
Trace Log:
    Time: 2012 Jan 30 05:20:45
    Severity: Informational
    Source: BMC:ciscoNET:961
    Description: " rpc_aim_callback_function_1_svc() - result == SUCCESS, callbackData
size: 600 "
    Order: 0
Trace Log:
    Time: 2012 Jan 30 05:20:45
    Severity: Informational
    Source: BMC:ciscoNET:961
    Description: rpc_aim_callback_function_1_svc() - returned from pFunctionCallback
result:0
    Order: 1
Trace Log:
    Time: 2012 Jan 30 05:20:45
    Severity: Informational
    Source: BMC:ciscoNET:961
   Description: " rpc_aim_callback_function_1_svc() - szFunctionName:netGetCurrentIfConfig
 nSize:0 nMaxSize: 600 "
    Order: 2
--More--

Server /cimc/log #
```

Cisco IMC 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 cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope log**	Cisco IMC ログ コマンド モードを開始します。
ステップ 3	Server /cimc/log # **clear**	Cisco IMC ログをクリアします。

例

次に、Cisco IMC 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
```

Cisco IMC ログしきい値の設定

Cisco IMC 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 cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope log**	Cisco IMC ログ コマンド モードを開始します。
ステップ 3	Server /cimc/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

	コマンドまたはアクション	目的
		• 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 /cimc/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 5	（任意） Server /cimc/log # **show local-syslog-severity**	設定された重大度レベルを表示します。

例

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 Cisco IMC ログの送信

Cisco IMC 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 cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope log**	Cisco IMC ログ コマンド モードを開始します。
ステップ 3	（任意） Server /cimc/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、リモートでログに記録されません。たとえば、**error** を選択した場合、リモート syslog サーバは重大度が Emergency、Alert、Critical、または Error のすべての Cisco IMC ログ メッセージを受信します。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 # **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

	コマンドまたはアクション	目的
		を設定するコマンド モードを開始します。
ステップ 5	Server /cimc/log/server # **set server-ip** *ipv4 or ipv6 address or domain name*	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 6	Server /cimc/log/server # **set server-port** *port number*	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 7	Server /cimc/log/server # **set enabled** {**yes** | **no**}	この syslog サーバへの Cisco IMC ログ エントリの送信を有効にします。
ステップ 8	Server /cimc/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。

例

次に、リモート syslog サーバ プロファイルを設定し、重大度レベル Warning 以上の Cisco IMC ログ エントリの送信を有効にする例を示します。

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # set remote-syslog-severity warning
Server /cimc/log *# scope server 1
Server /cimc/log/server *# set server-ip www.abc.com
Server /cimc/log/server *# set server-port 514
Server /cimc/log/server *# set enabled yes
Server /cimc/log/server *# commit
Server /cimc/log/server # exit
Server /cimc/log # show server
Syslog Server 1:
    Syslog Server Address: www.abc.com
    Syslog Server Port: 514
    Enabled: yes

Server /cimc/log # show remote-syslog-severity
    Remote Syslog Severity: warning

Server /cimc/log #
```

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 cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope log**	Cisco IMC ログ コマンド モードを開始します。
ステップ 3	Server /cimc/log # **send-test-syslog**	テスト Cisco IMC ログを設定したリモート サーバに送信します。

例

次に、テスト Cisco IMC の syslog を設定したリモート サーバに送信する例を示します。

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # send-test-syslog

Syslog Test message will be sent to configured Syslog destinations.
If no Syslog destinations configured, this command will be silently ignored.
Syslog Test message has been requested.

Server /cimc/log #
```

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--
```

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
```