Viewing Faults and Logs

This chapter includes the following sections:

Fault Summary

Viewing the Faults and Logs Summary

Procedure

	Command or Action	Purpose
Step 1	Server # **scope fault**	Enters fault command mode.
Step 2	Server # **show fault-entries**	Displays a log of all the faults.

Example

This example displays a summary of faults:

```
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 #
```

Cisco IMC Log

Viewing Cisco IMC Log

Procedure

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope log**	Enters log command mode.
Step 3	Server /chassis/log # **show entries detail**	Displays the CMC trace log details.

Example

This example displays the CMC trace log details:

```
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 #
```

Clearing Trace Logs

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **scope log**	Enters the log command mode.
Step 3	Server /chassis/log # **clear**	Clears the trace log.

Example

The following example clears the log of trace logs:

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

Server /chassis/log #
```

Configuring the Cisco IMC Log Threshold

You can specify the lowest level of messages that will be included in the syslog log.

Procedure

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope log**	Enters log command mode.
Step 3	Server /chassis/log # **set local-syslog-severity** *level*	The severity *level* can be one of the following, in decreasing order of severity: • emergency • alert • critical • error • warning • notice • informational • debug

	Command or Action	Purpose
		Note does not log any messages with a severity below the selected severity. For example, if you select **error**, then the log will contain all messages with the severity Emergency, Alert, Critical, or Error. It will not show Warning, Notice, Informational, or Debug messages.
Step 4	Server /chassis/log # **set remote-syslog-severity** *level*	The severity *level* can be one of the following, in decreasing order of severity: • emergency • alert • critical • error • warning • notice • informational • debug **Note** does not log any messages with a severity below the selected severity. For example, if you select **error**, then the log will contain all messages with the severity Emergency, Alert, Critical, or Error. It will not show Warning, Notice, Informational, or Debug messages.
Step 5	Server /chassis/log # **commit**	Commits the transaction to the system configuration.
Step 6	(Optional) Server /chassis/log # **show**	Displays the configured severity level.

Example

This example shows how to configure the logging of messages with a minimum severity of Debug for the local syslogs and error for the remote syslog:

```
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 #
```

Sending the Cisco IMC Log to a Remote Server

You can configure profiles for one or two remote syslog servers to receive system log entries.

Before you begin

- The remote syslog server must be configured to receive logs from a remote host.
- The remote syslog server must be configured to receive all types of logs, including authentication-related logs.
- The remote syslog server's firewall must be configured to allow syslog messages to reach the syslog server.

Procedure

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope log**	Enters log command mode.
Step 3	Server /chassis/log # **scope server** {**1** | **2**}	Selects one of the two remote syslog server profiles and enters the command mode for configuring the profile.
Step 4	Server /chassis/log/server # **set enabled** {**yes** | **no**}	Enables the sending of system log entries to this syslog server.
Step 5	Server /chassis/log/server # **commit**	Commits the transaction to the system configuration.
Step 6	Server /chassis/log/server # **exit**	Exits to the log command mode.
Step 7	Server /chassis/log/server # **showserver**	Exits to the log command mode.

Example

This example shows how to configure a remote syslog server profile and enable the sending of system log entries:

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** [**detail**]	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
-------------------- ------------- ----------------------------------------
[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--
```

Viewing the System Event Log for Servers

Procedure

	Command or Action	Purpose
Step 1	Server# **scope server** {*1* | *2* }	Enters the server mode for server 1 or 2.
Step 2	Server /server # **scope sel**	Enters the system event log (SEL) command mode.
Step 3	Server /server/sel # **show entries** [**detail**]	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 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"
```

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
```

Logging Controls

Configuring the Cisco IMC Log Threshold

You can specify the lowest level of messages that will be included in the syslog log.

Procedure

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope log**	Enters log command mode.
Step 3	Server /chassis/log # **set local-syslog-severity** *level*	The severity *level* can be one of the following, in decreasing order of severity: • emergency • alert

	Command or Action	Purpose
		• critical • error • warning • notice • informational • debug **Note** does not log any messages with a severity below the selected severity. For example, if you select **error**, then the log will contain all messages with the severity Emergency, Alert, Critical, or Error. It will not show Warning, Notice, Informational, or Debug messages.
Step 4	Server /chassis/log # **set remote-syslog-severity** *level*	The severity *level* can be one of the following, in decreasing order of severity: • emergency • alert • critical • error • warning • notice • informational • debug **Note** does not log any messages with a severity below the selected severity. For example, if you select **error**, then the log will contain all messages with the severity Emergency, Alert, Critical, or Error. It will not show Warning, Notice, Informational, or Debug messages.
Step 5	Server /chassis/log # **commit**	Commits the transaction to the system configuration.

	Command or Action	Purpose
Step 6	(Optional) Server /chassis/log # **show**	Displays the configured severity level.

Example

This example shows how to configure the logging of messages with a minimum severity of Debug for the local syslogs and error for the remote syslog:

```
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 #
```

Sending the Cisco IMC Log to a Remote Server

You can configure profiles for one or two remote syslog servers to receive system log entries.

Before you begin

- The remote syslog server must be configured to receive logs from a remote host.
- The remote syslog server must be configured to receive all types of logs, including authentication-related logs.
- The remote syslog server's firewall must be configured to allow syslog messages to reach the syslog server.

Procedure

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope log**	Enters log command mode.
Step 3	Server /chassis/log # **scope server** {**1** | **2**}	Selects one of the two remote syslog server profiles and enters the command mode for configuring the profile.
Step 4	Server /chassis/log/server # **set enabled** {**yes** | **no**}	Enables the sending of system log entries to this syslog server.
Step 5	Server /chassis/log/server # **commit**	Commits the transaction to the system configuration.
Step 6	Server /chassis/log/server # **exit**	Exits to the log command mode.

	Command or Action	Purpose
Step 7	Server /chassis/log/server # **showserver**	Exits to the log command mode.

Example

This example shows how to configure a remote syslog server profile and enable the sending of system log entries:

Sending a Test Cisco IMC Log to a Remote Server

Before you begin

- The remote syslog server must be configured to receive logs from a remote host.
- The remote syslog server must be configured to receive all types of logs, including authentication-related logs.
- The remote syslog server's firewall must be configured to allow syslog messages to reach the syslog server.

Procedure

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope log**	Enters log command mode.
Step 3	Server /chassis/log # **send-test-syslog**	Sends a test log to the remote server.

Example

This example shows how send a test log to a remote server:

Uploading Remote Syslog Certificate

Before you begin

- You must log in as a user with admin privileges.
- The certificate file to be uploaded must reside on a locally accessible file system.
- The following certificate formats are supported:
  - .crt
  - .cer

- .pem

Beginning with release 4.2(2a), you can upload a remote syslog certificate to Cisco UCS C-series servers. You can upload the certificate to one or two Cisco UCS C-series servers.

Procedure

Step 1 Server # **scope cimc**

Enters Cisco IMC command mode.

Step 2 Server /cimc # **scope log**

Enters Cisco IMC log command mode.

Step 3 Server /cimc/log # **scope server{1|2}**

Selects one of the two remote syslog server profiles and enters the command mode for uploading the remote syslog certificate and enabling secure remote syslog on the selected server.

Step 4 Server /cimc/log/server # **upload-certificate** *remote-protocol server_address path certificate_filename*

Specify the protocol to connect to the remote server. It can be of the following types:

- TFTP
- FTP
- SFTP
- SCP
- HTTP

Note If you enter the protocol as FTP, SCP or SFTP, you will be prompted to enter your username and password.

Along with the remote protocol, enter the filepath from where you want to upload the remote syslog certificate. After validating your remote server username and password, uploads the remote syslog certificate from the remote server.

Step 5 (Optional) Server /cimc/log/server # **paste-certificate**

This is an additional option to upload the remote syslog certificate.

At the prompt, paste the content of the certificate and press `CTRL+D`.

Step 6 Server /cimc/log/server # **setsecure-enabledyes**

Enables secure remote syslog on the server.

Step 7 Server /cimc/log/server # **commit**

Commits the transaction to the system configuration.

Example

- This example uploads a remote syslog certificate from a remote server and enables secure remote syslog on the selected server:

```
Server # scope cimc
Server /cimc # scope log
Server /cimc/log # scope server
Server /cimc/log/server # upload-certificate scp 10.10.10.10
/home/user-xyz/rem-sys-log-certif.cert
Server (RSA) key fingerprint is dd:b5:2b:07:ad:c0:30:b2:d5:6a:6a:78:80:85:93:b0
Do you wish to continue? [y/N]y
Username: user-xyz
Password:
Syslog Certificate uploaded successfully
Server /cimc/log/server # set secure-enabled yes
Server /cimc/log/server # commit
Server /cimc/log/server #
```

- This example uploads a remote syslog certificate using paste option:

```
Server # scope cimc
Server /cimc # scope log
Server /cimc/log # scope server
Server /cimc/log/server # paste-certificate
Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIFUDCCBDigAwIBAgIKYRF49gAAAAAAAjANBgkqhkiG9w0BAQUFADBLMRMwEQYK
CZImiZPyLGQBGRYDY29tMRMwEQYKCZImiZPyLGQBGRYDbmV3MR8wHQYDVQQDExZu
ZXctV0lOLU9WQlNBNElFU0NBLUNBMB4XDTE3MDczMDIxNTA1NVoXDTE5MDczMDIy
MDA1NVowSzETMBEGCgmSJomT8ixkARkWA2NvbTETMBEGCgmSJomT8ixkARkWA25l
dzEfMB0GA1UEAxMWbmV3LVdJTi1PVkJTQTRJRUJDQS1DQTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBALd8c+hhJddfUH6XKqBvllZVtIAiHfCx+l7z9o7F
bELOWu0LDVSC9pC1zpJ9wykr6VqUsVhZTkqQan23+84X4lYBsd92shQp9bri2gKj
MGntmnXE6qP3b6Trw94j6JVyWXKImYEda/SFtx722orLap8Sdliurue62JGNfq56
vxXBT1SNUHOmgOdfTOeNjVyeh51jceOCdKTppBij4wuq+jJfkndhW7KKE7ubmyRv
xpRSkiVaqNypf8jv7uG8Kwx1Q8jbCr0wG4nAbPndwhkyJpgyA5zuCdMRU2cN47om
u0VfMzJeVu+HuAif25BqKn4cjwHGOnrWKZcfHtnpKEbbmv0CAwEAAaOCAjQwggIw
MBAGCSsGAQQBgjcVAQQDAgEAMB0GA1UdDgQWBBR2+YJQuCmHKCkBkqVim0/kvfzB
bTAZBgkrBgEEAYI3FAIEDB4KAFMAdQBiAEMAQTAOBgNVHQ8BAf8EBAMCAYYwDwYD
VR0TAQH/BAUwAwEB/zAfBgNVHSMEGDAWgBRo6OQnLNNVa71VtllYAVRPmw8LQjCB
2AYDVR0fBIHQMIHNMIHKoIHHoIHEhoHBbGRhcDovLy9DTj1uZXctV0lOLU9WQlNB
NElFU0NBLUNBLENOPVdJTi1PVkJTQTRJRVNDQSxDTj1DRFAsQ049UHVibGljJTIw
S2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz1u
ZXcsREM9Y29tP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RD
bGFzcz1jUkxEaXN0cmlidXRpb25Qb2ludDCBxAYIKwYBBQUHAQEEgbcwgbQwgbEG
CCsGAQUFBzAChoGkbGRhcDovLy9DTj1uZXctV0lOLU9WQlNBNElFU0NBLUNBLENO
PUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1D
b25maWd1cmF0aW9uLERDPW5ldyxEQz1jb20/Y0FDZXJ0aWZpY2F0ZT9iYXNlP29i
amVjdENsYXNzPWNlcnRpZmljYXRpb25BdXRob3JpdHkwDQYJKoZIhvcNAQEFBQAD
ggEBAE8IWaRFEqrrwMHNaJunoomON2rdBWRNAMlJhKdIzi49J/9Yy9IlOGF+l0wR
Q5TeKFYIcWxBj5ltlYVWVdB+9YtTKsoEoq7/MeSg/c5KuprJhugqN3OU6zCqU4vq
rS1UHNnYkOJiSdOjkOdNeT9EG2YUqiDPr6CqIUcdU4+e36LdtQZW0TlIko+0z/be
bwIgtmxzkhlyDU711SuKmyz3uRrKq1CWhiIhSaOq4yYFQ0iw6TmFFKJGZ1KnjOrA
AwHhf8QvBBJhPMOwncWGL6DLFb7md21E2YBu+zcVPGLdXYm0Xgk8lXsE22bRJYJU
gyHqA2enmHAmJequlUFoSH9apKU=
-----END CERTIFICATE-----
Syslog Certificate pasted successfully.
Server /cimc/log/server #
```

- This example displays that the remote syslog certificate exists on the server and secure remote sylog is enabled on the server:

```
Server # scope cimc
Server /cimc # scope log
Server /cimc/log # scope server
Server /cimc/log/server # show detail
    Syslog Server 1:
    Syslog Server Address: 10.10.10.10
    Syslog Server Port: 514
    Enabled: yes
    Secure Enabled: yes
    Syslog Server protocol: udp
    Certificate Exists: yes
Server /cimc/log/server #
```

Deleting Remote Syslog Certificate

Before you begin

You must log in as a user with admin privileges.

Procedure

Step 1 Server # **scope cimc**

Enters Cisco IMC command mode.

Step 2 Server /cimc # **scope log**

Enters Cisco IMC log command mode.

Step 3 Server /cimc/log # **scope server{1|2}**

Selects one of the two remote syslog server profiles and enters the command mode for deleting the remote syslog certificate on the selected server.

Step 4 Server /cimc/log/server # **show detail**

Displays the server details and confirms that the remote syslog certificate exists on the selected server.

Step 5 Server /cimc/log/server # **delete-client-certificate**

Enter `y` at the confirmation prompt to delete the remote syslog certificate from the selected server.

Step 6 Server /cimc/log/server # **show detail**

Displays the server details and confirms that the remote syslog certificate is not available on the selected server.

Example

- This example displays that the remote syslog certificate exists on the server:

```
Server # scope cimc
Server /cimc # scope log
```

```
Server /cimc/log # scope server
Server /cimc/log/server # show detail
Server /cimc/log/server # commit
    Syslog Server 1:
    Syslog Server Address: 10.10.10.10
    Syslog Server Port: 514
    Enabled: yes
    Secure Enabled: yes
    Syslog Server protocol: udp
    Certificate Exists: yes
Server /cimc/log/server #
```

- This example deletes the remote syslog certificate on the server:

```
Server # scope cimc
Server /cimc # scope log
Server /cimc/log # scope server
Server /cimc/log/server # show detail
    Syslog Server 1:
    Syslog Server Address: 10.10.10.10
    Syslog Server Port: 514
    Enabled: yes
    Secure Enabled: yes
    Syslog Server protocol: udp
    Certificate Exists: yes
Server /cimc/log/server # delete-client-certificate
You are going to delete the Syslog Certificate.
Are you sure you want to proceed and delete the Syslog Certificate? [y|N]y
Syslog Certificate deleted successfully
Server /cimc/log/server #
```