Oracle® Integrated Lights Out Manager (ILOM) 3.0

Supplement for the Sun Datacenter InfiniBand Switch 648

Part No. 821-0896-11
May 2010, Revision A

Contents

Using This Documentation

This supplement provides detailed information regarding the installation, administration, and reference of the ILOM 3.0 firmware for the Sun Datacenter InfiniBand Switch 648 from Oracle®. This document is written for system administrators and authorized service providers who have experience with the ILOM firmware.

- "Related Documentation" on page xiii
- "Documentation, Support, and Training" on page xiv
- "Documentation Feedback" on page xv

Related Documentation

The documents listed as online are available at:

(http://docs.sun.com/app/docs/prod/ib.switch.648)

Application	Title	Part Number	Format	Location
Getting started	*Sun Datacenter InfiniBand Switch 648 Getting Started Guide*	820-7745	Printed PDF	Shipping kit Online
Last-minute information	*Sun Datacenter InfiniBand Switch 648 Product Notes*	820-7743	PDF	Online
Preparation and installation	*Sun Datacenter InfiniBand Switch 648 Installation Guide*	820-7738	PDF HTML	Online
Administration	*Sun Datacenter InfiniBand Switch 648 Administration Guide*	820-7739	PDF HTML	Online
Service	*Sun Datacenter InfiniBand Switch 648 Service Manual*	820-7740	PDF HTML	Online

Application	Title	Part Number	Format	Location
Command reference	*Sun Datacenter InfiniBand Switch 648 Command Reference*	820-7741	PDF HTML	Online
Compliance	*Sun Datacenter InfiniBand Switch 648 Safety and Compliance Guide*	820-7744	PDF	Online
ILOM information	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Supplement for the S*un Datacenter InfiniBand Switch 648	821-0896	PDF HTML	Online

The ILOM 3.0 documents listed as online are available at:

(http://docs.sun.com/app/docs/prod/int.lights.mgr30)

Application	Title	Part Number	Format	Location
Last-minute information	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Feature Updates and Release Notes*	820-7329	PDF HTML	Online
Getting started	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide*	820-5523	PDF HTML	Online
Overview	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*	820-6410	PDF HTML	Online
Administration from web interface	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Procedures Guide*	820-6411	PDF HTML	Online
Administration from CLI interface	*Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*	820-6412	PDF HTML	Online
Administration from SNMP and IPMI interface	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide*	820-6413	PDF HTML	Online

Documentation, Support, and Training

These web sites provide additional resources:

- Documentation (http://docs.sun.com)
- Support (http://www.sun.com/support)
- Training (http://www.sun.com/training)

Documentation Feedback

Submit comments about this document by clicking the Feedback[+] link at (http://docs.sun.com). Include the title and part number of your document with your feedback:

Oracle Integrated Lights Out Manager (ILOM) 3.0 Supplement for the Sun Datacenter InfiniBand Switch 648, part number 821-0896-11.

Understanding ILOM on the Switch

These topics provide an overview of ILOM and its implementation on the Sun Datacenter InfiniBand Switch 648.

Related Information

- "Administering ILOM (CLI)" on page 21
- "Administering ILOM (Web Interface)" on page 75
- "Administering ILOM (SNMP)" on page 113
- "Administering Hardware (IPMI)" on page 135
- "Understanding ILOM Commands" on page 139

ILOM Documentation

This document provides basic ILOM 3.0 information as it pertains to the Sun Datacenter InfiniBand Switch 648. More thorough ILOM 3.0 information is available online at this URL:

(http://docs.sun.com/app/docs/prod/int.lights.mgr30)

ILOM Overview

Integrated Lights Out Manager (ILOM) is a means of remotely managing a hardware device through a service processor (SP). For the Sun Datacenter InfiniBand Switch 648, the SP is the Pigeon Point Shelf Manager within the CMCs. It is often identified in screen output by the acronym, `ShMM` or `shmm1500`. ILOM enables monitoring and controlling of users, hardware, services, protocols, and configuration. In some aspects, ILOM is an alternative to switch-specific or CLIA commands.

ILOM has two primary interfaces, a command line and a web interface. The ILOM command-line interface uses 11 commands to affect the ILOM targets. The ILOM web interface enables point-and-click administration of the ILOM components and services. You access these interfaces using the default `ilom-admin` or `ilom-operator` user accounts. The `ilom-admin` account is for ILOM system administration. This account is fully privileged to add, delete, create, enable, disable, and so on, the ILOM targets, components, and services. The `ilom-operator` account is for users to monitor the many aspects of ILOM, but cannot affect change.

Additionally, the ILOM implementation supports industry-standard SNMP and IPMI interfaces.

When you upgrade the CMC firmware to version 1.0.2 or higher, ILOM 3.0 support is installed. An additional benefit of ILOM is that future CMC, H8, and I4 firmware upgrades are greatly simplified.

Related Information

- "Understanding ILOM Commands" on page 139
- "Web Interface Overview" on page 75
- "Access ILOM From the CLI" on page 22
- "Access ILOM From the Web Interface" on page 77
- "Upgrading the Switch Firmware Through ILOM (CLI)" on page 66

Supported Features

For the implementation of ILOM 3.0 on the CMC, the following features are supported:

- **Interfaces** – The following interfaces are supported:

    - **CLI** – Command-line interface. Succinct and human-readable administration interface.
    - **BI** – Browser interface or web interface. User-friendly administration interface.
    - **SNMP** – Simple Network Management Protocol. Advanced user interface for those experienced with SNMP.
    - **IPMI** – Interconnect Peripheral Management Interface. An interface between hardware devices.
- **Event and fault monitoring** – The following events are logged:
    - **ILOM events**
    - **SNMP alerts**
    - **IMPI PETs**
- **Firmware upgrade** – Chassis-level firmware upgrade, including CMC, fabric card H8 and I4, and line card H8 and I4 from a single repository file.
- **ILOM support** – The following features are supported for this implementation of ILOM:
    - **User management** – `ilom-admin`, `ilom-operator`, and user-created ILOM accounts.
    - **Network management** – IP address, netmask, gateway, and other parameters.
    - **Session monitoring** – Monitor active user sessions.
    - **Service management** – HTTP, HTTPS, SNMP, and others.
    - **Alert management** – Manage propagation of SNMP alerts and IPMI PETs.
    - **Event management** – Manage the local ILOM event log.
    - **Remote syslog** – Forward the Syslog to a remote server.
    - **Service Tag** – Support Sun's Service Tag program.
    - **Back Up and Restore ILOM configuration** – Save and restore the state of ILOM.
- **Launch OS shell from ILOM CLI** – Toggle between the ILOM CLI and the Linux OS.
- **Aggregate sensor** – Monitor switch health.
- **FRU ID** – FRU identification information display.

Related Information

- "Administering ILOM (CLI)" on page 21
- "Administering ILOM (Web Interface)" on page 75

Understanding ILOM Targets

These topics describe the ILOM targets and their properties.

Related Information

- "Understanding ILOM Commands" on page 139

ILOM Target Overview

ILOM targets represent all software and hardware components and services managed by ILOM. Targets are identified by a hierarchal path very similar to the directories and files of a file system. Each target has properties and commands that can affect it.

Target properties are of two types:

- **Read and write** – The value of these properties is displayed with the `show` command. The properties are changed with the `set` command. A typical read and write property would be an IP address.
- **Write only** – The value of these properties cannot be displayed with the `show` command. The value is typically displayed as `(Cannot show property)`. When you set the property value with the `set` command, it initiates a one-time action. For example, when the `commitpending` property is set to `true`, it copies the pending network properties into the standard network properties.

Target commands are specific to the permissions of the user that wants to affect the target. For example, the `ilom-admin` user can use the `show` or `set` command to affect an IP address property, but the `ilom-operator` user can only use the `show` command.

Related Information

- "ILOM Targets and Descriptions" on page 5

ILOM Targets and Descriptions

The following table lists the ILOM targets supported in the Sun Datacenter InfiniBand Switch 648 and provides a short description of the target.

ILOM Target	Description
/	Hierarchy root
/SYS	Sensors and FRU information
/SYS/CHASSIS_STATUS	Aggregate sensor
/SYS/ShM_CLI	Linux shells
/SP	Service processor
/SP/alertmgmt	Alert rule management
/SP/alertmgmt/rules	Alert rules
/SP/cli	Command-line interface
/SP/clients	Clients that connect to external services
/SP/clients/syslog	`syslogd` management
/SP/clients/syslog/1	`syslogd` remote logging management 1
/SP/clients/syslog/2	`syslogd` remote logging management 2
/SP/clock	Clock management
/SP/config	Configuration back up and restore settings
/SP/firmware	Firmware base target
/SP/logs	Log events
/SP/logs/event	Designations for event log
/SP/logs/event/list	Designations for event log
/SP/network	External network interface
/SP/services	Available services
/SP/services/http	HTTP service
/SP/services/https	HTTPS service

ILOM Target	Description
/SP/services/https/ssl	HTTPS SSL certificate settings
/SP/services/https/ssl/custom_cert	Custom SSL certificate settings
/SP/services/https/ssl/custom_key	Custom SSL private key settings
/SP/services/https/ssl/default_cert	Default SSL certificate settings
/SP/services/ipmi	Management of the IPMI service
/SP/services/servicetag	Service Tag configuration
/SP/services/snmp	SNMP agent service configuration
/SP/services/snmp/communities	SNMP communities
/SP/services/snmp/communities/private	SNMP community
/SP/services/snmp/communities/public	SNMP community
/SP/services/snmp/users	SNMP users
/SP/sessions	Session description
/SP/users	User description

Related Information

- "ILOM Target Overview" on page 4
- "ILOM System Targets and Properties" on page 7
- "ILOM General Targets and Properties" on page 7
- "ILOM Service Targets and Properties" on page 9
- "ILOM User and Session Targets and Properties" on page 11

ILOM System Targets and Properties

The following table lists the ILOM /SYS targets and their properties. Targets without properties are not listed.

Target and Path	Properties
/SYS	• type = Host System • ipmi_name = /SYS • product_name = Sun Datacenter Switch DCS 648 - Chassis • product_part_number = 511-1221-01 • product_serial_number = 0000002 • product_manufacturer = Sun Microsystems
/SYS/ShM_CLI	type = Container
/SYS/CHASSIS_STATUS	• type = OEM • ipmi_name = CHASSIS_STATUS • class = Discrete Sensor • value = State Deasserted • alarm_status = cleared

Related Information

- "ILOM Target Overview" on page 4
- "ILOM Targets and Descriptions" on page 5
- "ILOM General Targets and Properties" on page 7
- "ILOM Service Targets and Properties" on page 9
- "ILOM User and Session Targets and Properties" on page 11

ILOM General Targets and Properties

The following table lists general ILOM /SP targets and their properties. Targets without properties are not listed.

Note – Only the `/SP/alertmgmt/rules/1` target is listed, because there are 15 `rules` targets with identical default properties.

Target and Path	Properties
`/SP/alertmgmt/rules/1`	• `community_or_username = public` • `destination = 123.45.67.89` • `destination_port = 0` • `email_custom_sender = (none)` • `email_message_prefix = (none)` • `event_class_filter = (none)` • `event_type_filter = (none)` • `level = minor` • `snmp_version = 2c` • `testrule = (Cannot show property)` • `type = snmptrap`
`/SP/cli`	`timeout = 0`
`/SP/clients/syslog/1`	`address = 0.0.0.0`
`/SP/clients/syslog/2`	`address = 0.0.0.0`
`/SP/clock`	• `datetime = Thu Oct 15 02:54:28 2009` • `timezone = UTC` • `usentpserver = (none)`
`/SP/config`	• `dump_uri = (Cannot show property)` • `load_uri = (Cannot show property)` • `passphrase = none`
`/SP/firmware`	`load_uri = (Cannot show property)`

Target and Path	Properties
/SP/logs/event	clear = (Cannot show property)
/SP/network	• commitpending = (Cannot show property) • dhcp_server_ip = none • ipaddress = 123.45.67.89 • ipdiscovery = static • ipgateway = 123.45.67.1 • ipnetmask = 255.255.255.0 • macaddress = 00:AB:CD:EF:AB:CD • pendingipaddress = 123.45.67.89 • pendingipdiscovery = static • pendingipgateway = 123.45.67.1 • pendingipnetmask = 255.255.255.0 • state = enabled
/SP/network/test	ping = (Cannot show property)

Related Information

- "ILOM Target Overview" on page 4
- "ILOM Targets and Descriptions" on page 5
- "ILOM System Targets and Properties" on page 7
- "ILOM Service Targets and Properties" on page 9
- "ILOM User and Session Targets and Properties" on page 11

ILOM Service Targets and Properties

The following table lists the ILOM /SP/services targets and their properties. Targets without properties are not listed.

Target and Path	Properties
/SP/services/http	• port = 80 • secureredirect = enabled • servicestate = disabled
/SP/services/https	• port = 443 • servicestate = enabled
/SP/services/https/ssl	cert_status = Using Default (No custom certificate or private key loaded)

Target and Path	Properties
/SP/services/https/ssl/custom_cert	• clear_action = (Cannot show property) • issuer = (none) • load_uri = (Cannot show property) • subject = (none) • valid_from = (none) • valid_until = (none)
/SP/services/https/ssl/custom_key	• clear_action = (Cannot show property) • key_present = false • load_uri = (Cannot show property)
/SP/services/https/ssl/default_cert	• issuer = /C=US/ST=California/L=Santa Clara/O=Sun Microsystems, Inc./CN=sun-ilom • subject = /C=US/ST=California/L=Santa Clara/O=Sun Microsystems, Inc./CN=sun-ilom • valid_from = Apr 27 17:10:36 2005 GMT • valid_until = Apr 25 17:10:36 2015 GMT
/SP/services/ipmi	servicestate = enabled
/SP/services/servicetag	• passphrase = none • state = enabled
/SP/services/snmp	• engineid = (none) • port = 161 • servicestate = disabled • sets = disabled • v1 = disabled • v2c = disabled • v3 = enabled
/SP/services/snmp/communities/private	permission = rw
/SP/services/snmp/communities/public	permission = ro
/SP/services/snmp/mibs	dump_uri = (Cannot show property)
/SP/services/snmp/users/snmpuser	• authenticationpassword = (Cannot show property) • authenticationprotocol = MD5 • permission = ro • privacypassword = (Cannot show property) • privacyprotocol = none

Note – The /SP/services/snmp/users/snmpuser target was created so that its default properties could be displayed.

Related Information

- "ILOM Target Overview" on page 4
- "ILOM Targets and Descriptions" on page 5
- "ILOM System Targets and Properties" on page 7
- "ILOM General Targets and Properties" on page 7
- "ILOM User and Session Targets and Properties" on page 11

ILOM User and Session Targets and Properties

The following table lists the ILOM `/SP/users` targets and their properties. Targets without properties are not listed.

Note – The `/SP/sessions/1` target is included in this table because it is created when a user logs in.

Target and Path	Properties
`/SP/sessions/1`	• `username = ilom-admin` • `role = aucro` • `starttime = Thu Oct 15 02:36:11 2009` • `type = shell` • `mode = normal`
`/SP/users/ilom-admin`	• `role = aucro` • `password = *****`
`/SP/users/ilom-operator`	• `role = o` • `password = *****`

Related Information

- "ILOM Target Overview" on page 4
- "ILOM Targets and Descriptions" on page 5
- "ILOM System Targets and Properties" on page 7
- "ILOM General Targets and Properties" on page 7
- "ILOM Service Targets and Properties" on page 9

Installing the ILOM Firmware

When you upgrade the CMC firmware to version 1.0.2 or higher, ILOM 3.0 support is also installed. With ILOM support, upgrades of CMC, fabric card, fabric card filler, and line card firmware become a much simpler task. For instructions to upgrade firmware through ILOM, see "Upgrading the Switch Firmware Through ILOM (CLI)" on page 66.

If the CMC firmware has not been upgraded to ILOM support, the following topics assist you with upgrading the CMC firmware to version 1.0.2:

Related Information

- "Upgrading the Switch Firmware Through ILOM (CLI)" on page 66

Firmware Layout

The firmware inside of the CMC is divided into two primary sections:

- Persistent – This section of firmware is that being used. It is considered functional and not corrupt.
- Provisional – This section of firmware is that being updated. It is uncertain if it is functional or corrupt.

The CMC uses the persistent section for normal operations. When upgrading the firmware, the commands and routines in the persistent section are used to build their replacements in the provisional section. Once this is done, the provisional section is checked and verified, and then it becomes the persistent section. At this time, the older persistent section becomes the new provisional section. This way, a functional, uncorrupted version of the firmware is always available.

Within each section of the firmware, are three partitions:

- U-Boot – The core boot area.
- Linux kernel – The operating system for the CMC.
- Root file system – The file system used by the CMC.

To upgrade the firmware means to upgrade any one or all of these partitions.

Related Information

- "`rupgrade_tool` Application" on page 14
- "Download the ILOM Firmware" on page 15
- "Install the ILOM Firmware" on page 16

`rupgrade_tool` Application

The firmware in the switch is upgraded using the `rupgrade_tool` application. The format of the command line is:

`rupgrade_tool` *option [argument] [argument] .....*

The following table lists the options to the application.

Option	Description
`-h [--help]`	Prints help information.

`-s [--u=`*filename*`][--k=`*filename*`] [--r=`*filename*`][--proto=`*protocol*`] [--hook=`*script*`][-v][-d]`	Starts the upgrade.
	• `[--u=`*filename*`.bin]` – U-Boot firmware filename.
	• `[--k=`*filename*`.kernel]` – Linux kernel firmware filename.
	• `[--r=`*filename*`.rfs]` – `root` file system firmware filename.
	• `[--proto=`*protocol*`]` – Sets the protocol to use for upgrade. *protocol* can be in the form of:
	`no` – Firmware files are already in `/tmp`.
	`cp:`*path_to_files* – firmware files are already in a local directory
	`ftp:`*server_ip_address*`:`*path_to_files*`:`*username*`[:`*password*`]`
	`scp:`*server_ip_address*`:`*path_to_files*`:`*username*`[::`*port*`]`
	• `[--hook=`*script*`]` – Calls a script.
	• `[-v]` – Enables verbose output.
	• `[-d]` – Bypasses downloading the firmware file to the `/tmp` directory.

Option	Description
`-c [-v]`	Checks the upgrade. `[-v]` – Enables verbose output.
`-f [--hook=`*script*`] [-v]`	Completes the upgrade procedure. This command flips provisional to persistent and vice-versa. • `[--hook=`*script*`]` – Calls a script. • `[-v]` – Enables verbose output.
`-w [-f]`	Prints out the log of the upgrade, the `/var/upgrade/status` file. `[-f]` – Deletes the `/var/upgrade/status` file.
`-S [-v]`	Strobes the upgrade WDT and validates the sanity of the upgrade. `[-v]` – Enables verbose output.
`-u`	Undoes a successful upgrade session, reverting to the previous persistent section. Also invokes a reboot.

Related Information

- "Firmware Layout" on page 13
- "Download the ILOM Firmware" on page 15
- "Install the ILOM Firmware" on page 16

▼ Download the ILOM Firmware

1. **Open a web browser on a host that is on the same Ethernet network as the CMC that receives the firmware update.**
2. **Go to this URL:**

   `(www.sun.com/downloads)`

   The Sun Downloads page is displayed.
3. **Click the Downloads A-Z tab.**

   An alphabetical listing of downloads is displayed.
4. **Under S, click on the Sun Datacenter InfiniBand Switch 648 FW 1.0.2 (or higher) link.**

   The Sun Datacenter InfiniBand Switch 648 FW 1.0.2 page is displayed.
5. **Check the license agreement box and click Continue.**

   The page updates to list the available files.

6. **Download the required and optional files to your download directory.**

   The firmware is in the `SUN_DCS_648_1.0.2.tar.gz` file.

7. **In your download directory, unpack the `.gz` file:**

```
# gunzip SUN_DCS_648_1.0.2.tar.gz
#
```

8. **Untar the file:**

```
# tar xvf gunzip SUN_DCS_648_1.0.2.tar
```

   The extracted files are displayed. The firmware images have the following file name formats:

   - *U-Boot_filename*`.bin` – The U-Boot firmware image.
   - *Linux_filename*`.kernel` – The Linux kernel firmware image.
   - *RootFileSystem_filename*`.rfs` – The `root` file system firmware image.

9. **Read the README files for information about installing the firmware.**

10. **Install the ILOM firmware.**

    See "Install the ILOM Firmware" on page 16.

Related Information

- "Firmware Layout" on page 13
- "`rupgrade_tool` Application" on page 14
- "Install the ILOM Firmware" on page 16

▼ Install the ILOM Firmware

Note – If your switch is configured with only one CMC, that CMC is identified as CMC0 for this procedure. Additionally, this procedure brings the CMC offline until after the upgrade is completed.

1. **(Optional) Make a backup of any files on the CMCs that you want to keep.**

Caution – The firmware upgrade completely erases the CMC's file system.

2. **Log into CMC0 from the serial management port.**
   - If your switch is configured with only one CMC, go to Step 7.
   - If your switch is configured with two CMCs, continue to Step 3.
3. **Deactivate CMC0:**

```
# clia deactivate 10 0
Pigeon Point Shelf Manager Command Line Interpreter
  Command executed successfully
#
```

4. **Verify that CMC0 is inactive:**

```
# clia shmstatus
Pigeon Point Shelf Manager Command Line Interpreter
Host: "Inactive"
#
```

5. **Verify that `eth0` has a valid active state IP address:**

```
# ifconfig |grep -e 'eth0' -e 'inet'
eth0      Link encap:Ethernet  HWaddr 00:18:49:00:4F:B8
  inet addr:10.60.33.20  Bcast:10.60.33.255  Mask:255.255.255.0
.
.
.
#
```

   Only the first two lines of output are important.

6. **If invalid, set the active state IP address for CMC0:**

```
# ifconfig IP_address netmask 255.255.255.0
```

   where *IP_address* is in the form of xxx.xxx.xxx.xxx.

7. **Using the FTP protocol, copy the following extracted files from the host that received the `.tar` file to the `/tmp` directory of CMC0.**
   - `SUN_DCS_648_CMC__v1.1.4.kernel`
   - `SUN_DCS_648_CMC__v1.1.4.rfs`
   - `SUN_DCS_648_CMC__v1.1.4.u-boot.bin`

8. **Upgrade the firmware on CMC0 from the serial management port:**

```
# rm -R /etc/ssh
# cd /tmp
# rupgrade_tool -s -d --k=SUN_DCS_648_CMC__v1.1.4.kernel --r=
SUN_DCS_648_CMC__v1.1.4.rfs --u=SUN_DCS_648_CMC__v1.1.4.u-boot.bin --proto=no
--hook=erase
```

The firmware is upgraded and CMC0 reboots.

9. **Log into CMC0 from the serial management port.**

10. **Verify that the firmware has been upgraded:**

```
# mcmversion
M9CM version 1.1.4
Build time: Oct  6 2009 09:18:56
#
```

11. **Activate CMC0:**

```
# clia active 10 0
Pigeon Point Shelf Manager Command Line Interpreter
  Command issued via IPMB, status = 0 (0x0)
  Command executed successfully
#
```

12. **Set the active state IP address for CMC0:**

```
# clia setlanconfig 1 3 IP_address
```

where *IP_address* is in the form of *xxx.xxx.xxx.xxx*.

13. **Set the netmask for the CMC0:**

```
# clia setlanconfig 1 6 netmask
```

where *netmask* is the netmask. Typically, the netmask is `255.255.255.0`.

14. **Set the IP address for the CMC gateway:**

```
# clia setlanconfig 1 12 gateway_IP_address
```

where *gateway_IP_address* is in the form of *xxx.xxx.xxx.xxx*.

15. **If your switch has two CMCs, repeat** Step 2 **to** Step 14 **for CMC1.**

16. **After installing the CMC firmware with ILOM support, you can upgrade the fabric card, fabric card filler, and line card firmware using the ILOM interface.**

    See "Upgrading the Switch Firmware Through ILOM (CLI)" on page 66.

Related Information

- "Firmware Layout" on page 13
- "`rupgrade_tool` Application" on page 14
- "Download the ILOM Firmware" on page 15

Administering ILOM (CLI)

These topics describe how to administer ILOM from the command-line interface (CLI).

Related Information

CLI Overview

The ILOM CLI interface uses a set of commands that affect targets. The commands act like verbs and the targets are analogous to nouns. The command line is like a rudimentary sentence. For example, to *display* the *event log*, the command line is:

```
-> show /SP/logs/event/list
```

where:

- `show` is the command (or verb).
- `/SP/logs/event/list` is the target (or noun).

The following table lists the basic commands used in the ILOM CLI.

Command	Link to more information
`cd`	"`cd` Command" on page 140
`create`	"`create` Command" on page 141
`delete`	"`delete` Command" on page 142
`dump`	"`dump` Command" on page 143
`exit`	"`exit` Command (ILOM)" on page 144
`help`	"`help` Command (ILOM)" on page 145
`load`	"`load` Command" on page 146
`set`	"`set` Command" on page 147
`show`	"`show` Command" on page 148
`version`	"`version` Command (ILOM)" on page 149

More information about commands and targets are described in:

- "Understanding ILOM Commands" on page 139
- "Understanding ILOM Targets" on page 4

Related Information

- "Web Interface Overview" on page 75
- "SNMP Overview" on page 113
- "SNMP Commands" on page 114
- "`ipmitool` Overview" on page 135

▼ Access ILOM From the CLI

Note – You must configure the NET MGT port of the CMC in order to access the CLI. Refer to the *Sun Datacenter InfiniBand Switch 648 Installation Guide*, part number 820-7738, for information on how to configure the NET MGT port.

1. **Open a Telnet session and connect to the CMC by specifying the CMC's network address.**

   For example:

```
% telnet 123.45.67.89
Trying 123.45.67.89...
Connected to 123.45.67.89.
Escape character is '^]'.

shmm1500 login:
```

2. **Type `ilom-admin` for the login name followed by the `ilom-admin` password.**

```
shmm1500 login: ilom-admin
Password: password
->
```

Note – As shipped, the `ilom-admin` user password is `ilom-admin`. See "Change an ILOM User's Password and or Role (CLI)" on page 48 for instructions on how to change ILOM user passwords.

The ILOM shell prompt (`->`) is displayed.

Note – You can also log in as the `ilom-operator` user with the password `ilom-operator`. The `ilom-operator` user has only read permissions.

Related Information

- *Switch Installation*, accessing the CMC
- "Access ILOM From the Web Interface" on page 77
- "Monitoring ILOM Targets (CLI)" on page 25
- "Controlling ILOM Targets (CLI)" on page 41
- "Switching Between the ILOM Shell and the Linux Shell" on page 24

Switching Between the ILOM Shell and the Linux Shell

If you have accessed the CMC as the `root` user within the Linux shell, you can switch to the ILOM shell with the `spsh` command. Similarly, if you have accessed the ILOM shell as the `ilom-admin` user, you can switch to the Linux shell through the `/SYS/ShM_CLI` target.

Note – An ILOM user has the same permissions within the Linux shell.

These tasks enable you to switch back and forth between the ILOM shell and Linux shell.

- "Switch From the ILOM Shell to the Linux Shell" on page 24
- "Switch From the Linux Shell to the ILOM Shell" on page 25

Related Information

- "Access ILOM From the CLI" on page 22

▼ Switch From the ILOM Shell to the Linux Shell

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Switch to the Linux shell:**

```
-> show /SYS/ShM_CLI
NOTE: show on ShM_CLI  will launch Linux shell.
      Use exit command at Linux shell prompt to
      revert back to ILOM shell.
->
```

   You are now in the Linux shell.

   You can use the `exit` command to return to the ILOM shell.

Related Information

- "`show` Command" on page 148

- "Switch From the Linux Shell to the ILOM Shell" on page 25

▼ Switch From the Linux Shell to the ILOM Shell

1. **Access the CMC.**

   See the *Sun Datacenter InfiniBand Switch 648 Installation Guide*, part number 820-7738.

2. **Switch to the ILOM shell:**

```
# spsh
Sun(TM) Integrated Lights Out Manager
Version ILOM 3.0
Copyright 2009 Sun Microsystems, Inc. All rights reserved.
Use is subject to license terms.
->
```

   You are now in the ILOM shell.

   You can use the `exit` command to return to the Linux shell.

Related Information

- "Switch From the ILOM Shell to the Linux Shell" on page 24

Monitoring ILOM Targets (CLI)

These topics enable you to display the status of many ILOM targets.

- "Performing Daily Tasks (CLI)" on page 26
- "Checking the Status of Services (CLI)" on page 29
- "Verifying Other Aspects (CLI)" on page 34

Related Information

- "Access ILOM From the CLI" on page 22
- "Controlling ILOM Targets (CLI)" on page 41
- "Monitoring ILOM Targets (Web Interface)" on page 78
- "Understanding ILOM Targets" on page 4

Performing Daily Tasks (CLI)

These tasks help you see the status of ILOM targets that are continually changing.

- "Display the Date, Time, and Time Zone (CLI)" on page 26
- "Display the Aggregate Sensor State (CLI)" on page 27
- "Display the ILOM Sessions (CLI)" on page 27
- "Display the ILOM Event Log (CLI)" on page 28

Related Information

- "Performing Daily Tasks (Web Interface)" on page 79
- "Checking the Status of Services (CLI)" on page 29
- "Verifying Other Aspects (CLI)" on page 34

▼ Display the Date, Time, and Time Zone (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Display the date:**

```
-> show -d properties /SP/clock
 /SP/clock
  Properties:
      datetime = Fri Oct  9 03:12:02 2009
      timezone = UTC
      usentpserver = (none)
->
```

Note – The date and time are displayed as the `datetime` property. The is displayed underneath.

Related Information

- "`show` Command" on page 148
- "Display the Date, Time, and Time Zone (Web Interface)" on page 79
- "Display the Date and Time (SNMP)" on page 116
- "Display the Time Zone (SNMP)" on page 116
- "Set the Date, Time, and Time Zone (CLI)" on page 42

▼ Display the Aggregate Sensor State (CLI)

The aggregate sensor is the logical `and` summation of many binary sensor checks and provides the overall health of the switch. When all of the checks are `true`, the aggregate sensor's `value` property is set to `State Deasserted` and the `alarm_status` property is set to `cleared`. This situation means all sensors indicate that there are no faults.

When one of the binary sensor checks is `false`, a fault occurs, the `value` property becomes `State Asserted` and the `alarm_status` property is set to `major`. The switch is in an unhealthy state.

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Display the aggregate sensor state:**

```
-> show -d properties /SYS/CHASSIS_STATUS
 /SYS/CHASSIS_STATUS
  Properties:
      type = OEM
      ipmi_name = CHASSIS_STATUS
      class = Discrete Sensor
      value = State Deasserted
      alarm_status = cleared
->
```

Related Information

- "`show` Command" on page 148
- "Display the Aggregate Sensor State (Web Interface)" on page 80
- "Display the Aggregate Sensor State (SNMP)" on page 116
- "Display the Aggregate Sensor Status (SNMP)" on page 117
- "Display the Sensor State (IPMI)" on page 136
- "Display the Sensor Information (IPMI)" on page 137

▼ Display the ILOM Sessions (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Display the active ILOM sessions:**

```
-> show -d properties -l 2 /SP/sessions
 /SP/sessions
  Properties:
 /SP/sessions/23
      username = ilom-admin
      role = aucro
      starttime = Sat Oct 10 01:38:36 2009
      type = shell
      mode = normal
 /SP/sessions/24
  Properties:
      username = ilom-operator
      role = o
      starttime = Sat Oct 10 03:12:48 2009
      type = web
      mode = normal
->
```

Note – The `type` property indicates whether the user is using the CLI (`shell`) or web (`web`) interface.

Related Information

- "`show` Command" on page 148
- "Display the ILOM Sessions (Web Interface)" on page 80
- "Display ILOM Sessions (SNMP)" on page 117

▼ Display the ILOM Event Log (CLI)

The ILOM event message log contains ILOM events that happened to or were initiated by the management controller. For example, user login, sensor state change, configuring of `syslog` servers, etc. You can view these events using the ILOM `show` command for the `/SP/logs/event/list` target.

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Display the ILOM event log:**

```
-> show /SP/logs/event/list
/SP/logs/event/list
  Targets:
```

```
  Properties:
  Commands:
      cd
      show
ID      Date/Time                  Class      Type       Severity
------  -------------------------  --------   --------   --------
94      Fri Oct  9 01:15:13 2009   Audit      Log        minor
 root : Open Session : object = /session/type : value = shell : success
93      Fri Oct  9 01:13:51 2009   Audit      Log        minor
 test : Close Session : object = /session/type : value = www : success
92      Fri Oct  9 00:59:44 2009   Audit      Log        minor
.
.
.
->
```

Note – The output in the example is a portion of the full output.

Related Information

- "show Command" on page 148
- "Display the ILOM Event Log (Web Interface)" on page 81
- "Display the ILOM Event Log (SNMP)" on page 118
- "Display the System Event Log (IPMI)" on page 138
- "Display the Remote Log Hosts (CLI)" on page 38

Checking the Status of Services (CLI)

These topics enable you to display the status of the many services supported by ILOM.

- "Display the HTTP Service Status (CLI)" on page 30
- "Display the HTTPS Service Status (CLI)" on page 30
- "Display the SSL Certificates (CLI)" on page 31
- "Display the SNMP Service Status (CLI)" on page 32
- "Display the SNMP Service User Accounts (CLI)" on page 32
- "Display the SNMP Service Communities (CLI)" on page 33
- "Display the IPMI Service Status (CLI)" on page 34

Related Information

- "Checking the Status of Services (Web Interface)" on page 81
- "Performing Daily Tasks (CLI)" on page 26
- "Verifying Other Aspects (CLI)" on page 34

▼ Display the HTTP Service Status (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Display the HTTP status:**

```
-> show -d properties /SP/services/http
 /SP/services/http
  Properties:
      port = 80
      secureredirect = enabled
      servicestate = disabled
->
```

Related Information

- "`show` Command" on page 148
- "Display the HTTP Service Status (Web Interface)" on page 82
- "Display the HTTP Service Status (SNMP)" on page 119
- "Enable the HTTP Service (CLI)" on page 50
- "Disable the HTTP Service (CLI)" on page 50

▼ Display the HTTPS Service Status (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Display the HTTPS status:**

```
-> show -d properties /SP/services/https
 /SP/services/https
  Properties:
      port = 443
      servicestate = enabled
->
```

Related Information

- "show Command" on page 148
- "Display the HTTPS Service Status (Web Interface)" on page 82
- "Display the HTTPS Service Status (SNMP)" on page 119
- "Enable the HTTPS Service (CLI)" on page 51
- "Disable the HTTPS Service (CLI)" on page 53

▼ Display the SSL Certificates (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Display the SSL status:**

```
-> show -d properties /SP/services/https/ssl
 /SP/services/https/ssl
  Properties:
      cert_status = Using Default (No custom certificate or private key loaded)
->
```

3. **Display the properties of the** `default_cert` **certificate:**

```
-> show -d properties /SP/services/https/ssl/default_cert
 /SP/services/https/ssl/default_cert
  Properties:
      issuer = /C=US/ST=California/L=Santa Clara/O=Sun Microsystems, Inc./CN=
sun-ilom
      subject = /C=US/ST=California/L=Santa Clara/O=Sun Microsystems, Inc./CN=
sun-ilom
      valid_from = Apr 27 17:10:36 2005 GMT
      valid_until = Apr 25 17:10:36 2015 GMT
->
```

Related Information

- "show Command" on page 148
- "Display the SSL Certificates (Web Interface)" on page 83
- "Install a Custom SSL Certificate (CLI)" on page 52
- "Remove the Custom SSL Certificate (CLI)" on page 53

▼ Display the SNMP Service Status (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Display the SNMP status:**

```
-> show -d properties /SP/services/snmp
 /SP/services/snmp
 Properties:
 engineid = (none)
 port = 161
 servicestate = disabled
 sets = disabled
 v1 = disabled
 v2c = disabled
 v3 = enabled
->
```

Related Information

- "`show` Command" on page 148
- "Display the SNMP Service Status (Web Interface)" on page 83
- "Enable the SNMP Service (CLI)" on page 55
- "Disable the SNMP Service (CLI)" on page 61

▼ Display the SNMP Service User Accounts (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Display the SNMP users:**

```
-> show -d targets /SP/services/snmp/users
 /SP/services/snmp/users
  Targets:
      snmpuser
->
```

3. **Display the `snmpuser` user properties:**

```
-> show -d properties /SP/services/snmp/users/snmpuser
 /SP/services/snmp/users/snmpuser
  Properties:
```

```
      authenticationpassword = (Cannot show property)
      authenticationprotocol = MD5
      permission = ro
      privacypassword = (Cannot show property)
      privacyprotocol = none
->
```

Related Information

- "`show` Command" on page 148
- "Display the SNMP Service User Accounts (Web Interface)" on page 84
- "Add SNMP Service User Accounts (CLI)" on page 56
- "Delete SNMP Service User Accounts (CLI)" on page 58

▼ Display the SNMP Service Communities (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Display the SNMP communities:**

```
-> show -d targets /SP/services/snmp/communities
 /SP/services/snmp/communities
  Targets:
      private
      public
->
```

3. **Display the** `private` **community properties:**

```
-> show -d properties /SP/services/snmp/communities/private
 /SP/services/snmp/communities/private
  Properties:
      permission = rw
->
```

Related Information

- "`show` Command" on page 148
- "Display the SNMP Service Communities (Web Interface)" on page 84
- "Add SNMP Service Communities (CLI)" on page 59
- "Delete SNMP Service Communities (CLI)" on page 60

▼ Display the IPMI Service Status (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Display the IPMI status:**

```
-> show -d properties /SP/services/ipmi
 /SP/services/ipmi
  Properties:
      servicestate = enabled
->
```

Related Information

- "show Command" on page 148
- "Display the IPMI Service Status (Web Interface)" on page 85

Verifying Other Aspects (CLI)

These tasks display the status of other aspects of ILOM.

- "Get Help on an ILOM Command (CLI)" on page 35
- "Get Help on an ILOM Target Property (CLI)" on page 35
- "Display the Alert Properties (CLI)" on page 36
- "Display the ILOM User Accounts (CLI)" on page 37
- "Display the Remote Log Hosts (CLI)" on page 38
- "Display the Network Management Configuration (CLI)" on page 38
- "Display the ILOM CLI Session Timeout (CLI)" on page 39
- "Display Chassis FRU ID Information (CLI)" on page 39
- "Display the ILOM Firmware Version (CLI)" on page 40

Related Information

- "Verifying Other Aspects (Web Interface)" on page 85
- "Performing Daily Tasks (CLI)" on page 26
- "Checking the Status of Services (CLI)" on page 29

▼ Get Help on an ILOM Command (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Get help on a command:**

```
-> help -o verbose command
```

   where *command* is the ILOM command for which you need help.

   For example, to get help on the `exit` command:

```
-> help -o verbose exit
The exit command is used to terminate a session.
Usage: exit
Example:
  -> exit
  Connection to nyc-sp closed.
->
```

Related Information

- "`help` Command (ILOM)" on page 145
- "Get Help on an ILOM Target Property (CLI)" on page 35

▼ Get Help on an ILOM Target Property (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Get help on a target property:**

```
-> help target property
```

   where:

   - *target* is the target and path to act upon.
   - *property* is the property of the *target* for which you need help.

   For example, to get help about the `ilom-operator` user's `role` property:

```
-> help /SP/users/ilom-operator role
  Properties:
     role : Role of ilom-operator
```

```
      role : Possible values = Operator, Administrator, a, u, c, r, o, s
      role : User role required for set = u
->
```

Related Information

- "help Command (ILOM)" on page 145
- "Get Help on an ILOM Command (CLI)" on page 35

▼ Display the Alert Properties (CLI)

Alerts can provide advance notice of a system failure. The ILOM implementation in the management controller supports 15 alert rules, which configure alert properties. Supported alert types are SNMP trap and PET. The alert destination must have the relevant ILOM MIBs installed and must support SNMP traps or PETs.

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Display the alert properties:**

```
-> show -d properties /SP/alertmgmt/rules/alert
```

   where *alert* is the number of the alert to display.

   For example, to display the properties for alert 1:

```
-> show -d properties /SP/alertmgmt/rules/1
 /SP/alertmgmt/rules/1
  Properties:
      community_or_username = public
      destination = 0.0.0.0
      destination_port = 0
      email_custom_sender = (none)
      email_message_prefix = (none)
      event_class_filter = (none)
      event_type_filter = (none)
      level = disable
      snmp_version = 1
      testrule = (Cannot show property)
      type = snmptrap
->
```

Note – In the output, alert 1 is not configured to send any alerts.

Related Information

- "show Command" on page 148
- "Display the Alert Properties (Web Interface)" on page 85
- "Display the Alert Properties (SNMP)" on page 120
- "Enable Alerts to Send SNMP Traps (CLI)" on page 62
- "Enable Alerts to Send PET (CLI)" on page 63
- "Disable Alerts (CLI)" on page 64

▼ Display the ILOM User Accounts (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Display the ILOM user accounts:**

```
-> show -d targets /SP/users
 /SP/users
  Targets:
      ilom-admin
      ilom-operator
->
```

3. **Display the** `ilom-admin` **user's properties:**

```
-> Show -d properties /SP/users/ilom-admin
 /SP/users/ilom-admin
  Properties:
      role = aucro
      password = *****
->
```

Related Information

- "show Command" on page 148
- "Display the ILOM User Accounts (Web Interface)" on page 86
- "Display ILOM User Accounts (SNMP)" on page 121
- "Add an ILOM User Account (CLI)" on page 47
- "Delete an ILOM User Account (CLI)" on page 49

▼ Display the Remote Log Hosts (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Display the remote log hosts:**

```
-> show -d properties /SP/clients/syslog/number
```

   where *number* is the number of the host, either `1` or `2`.

   For example, to display the IP address of remote host 1:

```
-> show -d properties /SP/clients/syslog/1
 /SP/clients/syslog/1
  Properties:
      address = 0.0.0.0
->
```

Note – The address of `0.0.0.0` indicates that remote host 1 functionality is not configured.

Related Information

- "`show` Command" on page 148
- "Display the Remote Log Hosts (Web Interface)" on page 87
- "Display the Remote Log Hosts (SNMP)" on page 122
- "Set the Remote Log Hosts (CLI)" on page 43

▼ Display the Network Management Configuration (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Display the network management configuration:**

```
-> show -d properties /SP/network
 /SP/network
  Properties:
      commitpending = (Cannot show property)
      dhcp_server_ip = none
      ipaddress = 129.159.145.140
      ipdiscovery = static
```

```
      ipgateway = 129.159.145.5
      ipnetmask = 255.255.255.0
      macaddress = 00:18:49:00:86:72
      pendingipaddress = 129.159.145.140
      pendingipdiscovery = static
      pendingipgateway = 129.159.145.5
      pendingipnetmask = 255.255.255.0
      state = enabled
->
```

Related Information

- "show Command" on page 148
- "Display the Network Management Configuration (Web Interface)" on page 87
- "Display the Network Management Configuration (SNMP)" on page 123
- "Set the Network Management Parameters (CLI)" on page 45

▼ Display the ILOM CLI Session Timeout (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Display the CLI timeout:**

```
-> show -d properties /SP/cli
 /SP/cli
  Properties:
      timeout = 0
->
```

Related Information

- "show Command" on page 148
- "Display the ILOM CLI Session Timeout (Web Interface)" on page 87
- "Set the ILOM CLI Session Timeout (CLI)" on page 65

▼ Display Chassis FRU ID Information (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Display the chassis FRU information:**

```
-> show -d properties /SYS
 /SYS
  Properties:
      type = Host System
      ipmi_name = /SYS
      product_name =  Sun Datacenter Switch DCS 648 - Chassis
      product_part_number =  511-1221-01
      product_serial_number =  0000002
      product_manufacturer =  Sun Microsystems
```

Related Information

- "`show` Command" on page 148
- "Display Chassis FRU ID Information (Web Interface)" on page 88
- "Display the System Components (SNMP)" on page 123
- "Display the Additional System Component Information (SNMP)" on page 124

▼ Display the ILOM Firmware Version (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Display the ILOM firmware version:**

```
-> version
SP firmware 1.1.5
SP firmware build number: 44535
SP firmware date: Tue Jun 23 19:12:58 IST 2009
SP filesystem version: 0.1.22
->
```

Related Information

- "`version` Command (ILOM)" on page 149
- "Display the ILOM Firmware Version (Web Interface)" on page 88

Controlling ILOM Targets (CLI)

These topics enable you to change the behavior or configuration of many ILOM targets.

Related Information

Performing General Tasks on ILOM Targets (CLI)

You can perform these tasks periodically on a few ILOM targets.

Related Information

▼ Set the Date, Time, and Time Zone (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Set the date, time, and time zone:**

```
-> set /SP/clock datetime=MMDDhhmmYYYY timezone=timezone
```

   where:

   - *MMDDhhmmYYYY* is the month, date, hour, and minute as two digits, and the year as four digits.
   - *timezone* is the 3 or 4 alphanumeric string representing the time zone

   For example:

```
-> set /SP/clock datetime=100922352009 timezone=PDT
Set 'datetime' to '100922352009'
Set 'timezone' to 'PDT'
-> show -d properties /SP/clock
 /SP/clock
  Properties:
      datetime = Fri Oct  9 22:35:30 2009
      timezone = PDT
      usentpserver = (none)
->
```

Related Information

- "`set` Command" on page 147
- "Set the Date and Time (Web Interface)" on page 90
- "Set the Time Zone (Web Interface)" on page 90
- "Set the Date and Time (SNMP)" on page 126
- "Display the Date, Time, and Time Zone (CLI)" on page 26

▼ Clear the ILOM Event Log (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Clear the ILOM event log:**

```
-> set /SP/logs/event clear=true
Are you sure you want to clear /SP/logs/event (y/n)? y
Set 'clear' to 'true'
->
```

The ILOM event log is cleared.

Related Information

- "`set` Command" on page 147
- "Clear the ILOM Event Log (Web Interface)" on page 91
- "Clear the ILOM Event Log (SNMP)" on page 127
- "Display the ILOM Event Log (CLI)" on page 28

▼ Set the Remote Log Hosts (CLI)

The ILOM implementation in the management controller provides a protocol for transmitting ILOM events to a remote log host. The events transmitted are similar to those displayed in the local log.

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Set the remote log host IP address:**

```
-> set /SP/clients/syslog/number address=IP_address
```

where:

- *number* is `1` for the first log host and `2` for the second log host.
- *IP_address* is the IP address of the log host.

For example, to set the IP address of remote host 1 to 123.45.67.89:

```
-> set /SP/clients/syslog/1 address=123.45.67.89
Set 'address' to '123.45.67.89'
->
```

Note – Setting a remote log host IP address to 0.0.0.0 disables that functionality.

Related Information

- "`set` Command" on page 147
- "Set the Remote Log Hosts (Web Interface)" on page 91
- "Set the Remote Log Hosts (SNMP)" on page 127
- "Display the Remote Log Hosts (CLI)" on page 38

▼ Back Up the ILOM Configuration (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Back up the ILOM configuration:**

```
-> set /SP/config dump_uri=URI
```

   where *URI* is the uniform resource indicator.

   For example, to dump the configuration as the `my.config` file to the `/opt/dump` directory on a server with IP address 123.45.67.89 using the SCP protocol:

```
-> set /SP/config dump_uri=scp://root:changeme@123.45.67.89/opt/dump/my.config
Dump successful.
->
```

   The configuration is backed up as the `my.config` XML file.

Related Information

- "`set` Command" on page 147
- "Back Up the ILOM Configuration (Web Interface)" on page 92
- "Restore the ILOM Configuration (CLI)" on page 44

▼ Restore the ILOM Configuration (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Restore the ILOM configuration:**

```
-> set /SP/config load_uri=URI
```

where *URI* is the uniform resource indicator.

For example, to load the configuration as the `my.config` file from the `/opt/dump` directory on a server with IP address 123.45.67.89 using the SCP protocol:

```
-> set /SP/config load_uri=scp://root:changeme@123.45.67.89/opt/dump/my.config
Load successful.
->
```

The configuration is restored.

Related Information

- "`set` Command" on page 147
- "Restore the ILOM Configuration (Web Interface)" on page 93
- "Back Up the ILOM Configuration (CLI)" on page 44

▼ Set the Network Management Parameters (CLI)

This task enables you to configure the NET MGT interface.

Note – The following procedure makes changes that do not require a reset or reboot.

---

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Configure the network management parameters:**

```
-> set /SP/network property=value property=value ...
```

where:

- *property* is the parameter of the network to configure.
- *value* is the value of the *property* to configure.

The following properties are supported:

- `pendingipaddress` – The *value* is the IP address of the CMC to be configured.
- `pendingipdiscovery` – The *value* is the method of IP discovery to be configured, either `static` or `dhcp`.

- `pendingipgateway` – The *value* is the IP address of the gateway to be configured.
- `pendingipnetmask` – The *value* is the netmask to be configured.

Note – You can configure one, several, or all properties in one command line.

---

3. Commit to the changes:

```
-> set /SP/network commitpending=true
```

For example, to set the IP address of the CMC:

```
-> show /SP/network ipaddress
 /SP/network
  Properties:
      ipaddress = 123.45.67.89
-> set /SP/network pendingipaddress=123.45.67.90
Set 'pendingipaddress' to '123.45.67.90'
-> set /SP/network commitpending=true
Set 'commitpending' to 'true'
```

The IP address has changed to `123.45.67.90`.

Note – Changing some network management properties terminates the NET MGT connection to the CMC. You must re-establish the connection to continue administering the CMC. See "Access ILOM From the CLI" on page 22.

---

4. Access the ILOM CLI using the new IP address.

See "Access ILOM From the CLI" on page 22.

5. Display the new IP address:

```
-> show /SP/network ipaddress
 /SP/network
  Properties:
      ipaddress = 123.45.67.90
->
```

Related Information

- "`set` Command" on page 147
- "`show` Command" on page 148
- "Set the Network Management Parameters (Web Interface)" on page 93

- "Set the Network Management Parameters (SNMP)" on page 128
- "Display the Network Management Configuration (CLI)" on page 38

Performing ILOM User Tasks (CLI)

These tasks enable you to change and configure ILOM user targets.

- "Add an ILOM User Account (CLI)" on page 47
- "Change an ILOM User's Password and or Role (CLI)" on page 48
- "Delete an ILOM User Account (CLI)" on page 49

Related Information

- "Performing ILOM User Tasks (Web Interface)" on page 94
- "Performing General Tasks on ILOM Targets (CLI)" on page 41

▼ Add an ILOM User Account (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Add an ILOM user:**

```
-> create /SP/user/username
```

   where *username* is the name of the user's account.

   For example, to add a user named `testuser`:

```
-> create /SP/users/testuser
Creating user...
Enter new password: ********
Enter new password again: ********
Created /SP/users/testuser
->
```

   The ILOM user `testuser` is added.

Note – New users are assigned the role of `o` or `Read only` (operator) by default.

Related Information

- "`create` Command" on page 141
- "Add an ILOM User Account (Web Interface)" on page 94
- "Add an ILOM User Account (SNMP)" on page 130
- "Display the ILOM User Accounts (CLI)" on page 37
- "Delete an ILOM User Account (CLI)" on page 49

▼ Change an ILOM User's Password and or Role (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Change the ILOM user's configuration:**

```
-> set /SP/users/username password=password role=role
```

   where:

   - *username* is the user account name.
   - *password* is the new password.
   - *role* is the new role for the user.

   For the *role*, you can use the characters of the `aucros` string to enable the respective abilities:

   - `a` – Administrator
   - `u` – User management
   - `c` – Console
   - `r` – Reset and host control
   - `o` – Read only (operator)
   - `s` – Service

Note – You can change the user password and role independently.

For example, to change the password for the `ilom-operator` user:

```
-> set /SP/users/ilom-operator password=knockknock
Changing password for user /SP/users/ilom-operator...
Enter new password again: **********
New password was successfully set for user /SP/users/ilom-operator
->
```

The `ilom-operator` user's password is changed.

Related Information

- "`set` Command" on page 147
- "Change an ILOM User's Password and or Role (Web Interface)" on page 95

▼ Delete an ILOM User Account (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Delete the ILOM user:**

```
-> delete /SP/users/username
```

where *username* is the name of the user's account.

For example, to delete the `testuser` user:

```
-> delete /SP/users/testuser
Are you sure you want to delete /SP/users/testuser (y/n)? y
Deleted /SP/users/testuser
->
```

The ILOM user `testuser` is deleted.

Related Information

- "`delete` Command" on page 142
- "Delete an ILOM User Account (Web Interface)" on page 96
- "Delete an ILOM User Account (SNMP)" on page 131
- "Display the ILOM User Accounts (CLI)" on page 37

- "Add an ILOM User Account (CLI)" on page 47

Managing HTTP Services (CLI)

These tasks help you manage the ILOM HTTP service targets.

- "Enable the HTTP Service (CLI)" on page 50
- "Disable the HTTP Service (CLI)" on page 50

Related Information

- "Managing HTTP Services (Web Interface)" on page 96
- "Managing HTTPS Services (CLI)" on page 51
- "Managing SNMP Services (CLI)" on page 54

▼ Enable the HTTP Service (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Enable the HTTP service:**

```
-> set /SP/services/http servicestate=enabled
Set 'servicestate' to 'enabled'
->
```

   The HTTP service is enabled.

Related Information

- "`set` Command" on page 147
- "Enable the HTTP Service (Web Interface)" on page 97
- "Set the HTTP Service State (SNMP)" on page 132
- "Display the HTTP Service Status (CLI)" on page 30
- "Disable the HTTP Service (CLI)" on page 50

▼ Disable the HTTP Service (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Disable the HTTP service:**

```
-> set /SP/services/http servicestate=disabled
Set 'servicestate' to 'disabled'
->
```

The HTTP service is disabled.

Related Information

- "`set` Command" on page 147
- "Disable the HTTP Service (Web Interface)" on page 97
- "Set the HTTP Service State (SNMP)" on page 132
- "Display the HTTP Service Status (CLI)" on page 30
- "Enable the HTTP Service (CLI)" on page 50

Managing HTTPS Services (CLI)

These tasks help you manage the ILOM HTTPS service targets.

- "Enable the HTTPS Service (CLI)" on page 51
- "Install a Custom SSL Certificate (CLI)" on page 52
- "Remove the Custom SSL Certificate (CLI)" on page 53
- "Disable the HTTPS Service (CLI)" on page 53

Related Information

- "Managing HTTPS Services (Web Interface)" on page 98
- "Managing HTTP Services (CLI)" on page 50
- "Managing SNMP Services (CLI)" on page 54

▼ Enable the HTTPS Service (CLI)

Note – This procedure enables an HTTPS connection to the web interface. The HTTPS service is enabled by default.

---

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Enable secure redirection:**

```
-> set /SP/services/http secureredirect=enabled
Set 'secureredirect' to 'enabled'
->
```

3. **Enable the HTTPS service:**

```
-> set /SP/services/https servicestate=enabled
Set 'servicestate' to 'enabled'
->
```

The HTTPS service is enabled.

Related Information

- "`set` Command" on page 147
- "Enable the HTTPS Service (Web Interface)" on page 98
- "Display the HTTPS Service Status (CLI)" on page 30
- "Disable the HTTPS Service (CLI)" on page 53

▼ Install a Custom SSL Certificate (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Load the certificate:**

```
-> load -source URI /SP/services/https/ssl/custom_cert
```

where *URI* is the uniform resource indicator.

For example, to load a certificate `server.pem` from IP address 123.45.67.89 using the TFTP protocol:

```
-> load -source tftp://123.45.67.89/server.pem
/SP/services/https/ssl/custom_cert
Load successful.
->
```

The certificate is loaded.

Related Information

- "`load` Command" on page 146
- "Install a Custom SSL Certificate (Web Interface)" on page 99
- "Display the SSL Certificates (CLI)" on page 31
- "Remove the Custom SSL Certificate (CLI)" on page 53

▼ Remove the Custom SSL Certificate (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Remove the certificate:**

```
-> set /SP/services/https/ssl/custom_cert clear_action=true
Are you sure you want to reset /SP/services/https/ssl/customer_cert (y/n)? y
Performing reset on /SP/services/https/ssl/custom_cert
->
```

The certificate is removed.

Related Information

- "Remove the Custom SSL Certificate (Web Interface)" on page 99
- "Display the SSL Certificates (CLI)" on page 31
- "Install a Custom SSL Certificate (CLI)" on page 52

▼ Disable the HTTPS Service (CLI)

Note – This procedure disables the HTTPS connection to the web interface. To access the web interface, either the HTTP service or the HTTPS service must be enabled.

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Disable secure redirection:**

```
-> set /SP/services/http secureredirect=disabled
Set 'secureredirect' to 'disabled'
->
```

3. **Disable the HTTPS service:**

```
-> set /SP/services/https servicestate=disabled
Set 'servicestate' to 'disabled'
->
```

The HTTPS service is disabled.

Related Information

- "`set` Command" on page 147
- "Disable the HTTPS Service (Web Interface)" on page 100
- "Display the HTTPS Service Status (CLI)" on page 30
- "Enable the HTTPS Service (CLI)" on page 51

Managing SNMP Services (CLI)

These tasks help you manage the ILOM SNMP service targets.

- "Enable the SNMP Service (CLI)" on page 55
- "Configure the SNMP Service (CLI)" on page 55
- "Add SNMP Service User Accounts (CLI)" on page 56
- "Modify SNMP Service User Accounts (CLI)" on page 57
- "Delete SNMP Service User Accounts (CLI)" on page 58
- "Add SNMP Service Communities (CLI)" on page 59
- "Modify SNMP Service Communities (CLI)" on page 59
- "Delete SNMP Service Communities (CLI)" on page 60
- "Back Up SNMP Service MIBs (CLI)" on page 61
- "Disable the SNMP Service (CLI)" on page 61

Related Information

- "Managing SNMP Services (Web Interface)" on page 101
- "Managing HTTP Services (CLI)" on page 50
- "Managing HTTPS Services (CLI)" on page 51

▼ Enable the SNMP Service (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Enable the SNMP service:**

```
-> set /SP/services/snmp servicestate=enabled
Set 'servicestate' to 'enabled'
->
```

   The SNMP service is enabled.

Related Information

- "`set` Command" on page 147
- "Enable the SNMP Service (Web Interface)" on page 101
- "Display the SNMP Service Status (CLI)" on page 32
- "Disable the SNMP Service (CLI)" on page 61

▼ Configure the SNMP Service (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Configure the SNMP parameters:**

```
-> set /SP/services/snmp property=value property=value ...
```

   where:

   - *property* is the parameter of the network to configure.
   - *value* is the value of the *property* to configure

   The following properties are supported:

   - `port` – The *value* is the UDP port for SNMP.
   - `servicestate` – The *value* is either `enabled` or `disabled`.
   - `sets` – The *value* is either `enabled` or `disabled` for set requests.
   - `v1` – The *value* is either `enabled` or `disabled` for this protocol.
   - `v2c` – The *value* is either `enabled` or `disabled` for this protocol.
   - `v3` – The *value* is either `enabled` or `disabled` for this protocol.

Note – You can configure one to all properties in one command line.

For example, to enable `sets` and the `v2c` protocol:

```
-> set /SP/services/snmp sets=enabled v2c=enabled
Set 'sets' to 'enabled'
Set 'v2c' to 'enabled'
->
```

Related Information

- "`set` Command" on page 147
- "Configure the SNMP Service (Web Interface)" on page 102

▼ Add SNMP Service User Accounts (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Add a new SNMP user:**

```
-> create /SP/services/snmp/users/username authenticationpassword=password
```

where:

- *username* is the name of the SNMP user.
- *password* is the password used for authentication.

For example, to create a SNMP user with the name of `snmpuser` and the password of `changeme`:

```
-> create /SP/services/snmp/users/snmpuser authenticationpassword=changeme
Created /SP/services/snmp/users/snmpuser
->
```

Note – By default, new users are given read-only permissions and no privacy protocol.

3. **(Optional) Configure the user with a privacy protocol and password:**

```
-> set /SP/services/snmp/users/snmpuser privacyprotocol=DES privacypassword=
password authenticationpassword=password
```

For example, to configure the `snmpuser` with the DES protocol and privacy password of `changeme`:

```
-> set /SP/services/snmp/users/snmpuser privacyprotocol=DES privacypassword=
changeme authenticationpassword=changeme
Set 'privacyprotocol' to 'DES'
Set 'privacypassword' to 'changeme'
Set 'authenticationpassword' to 'changeme'
User /SP/services/snmp/users/snmpuser properties were updated successfully
->
```

The SNMP user `snmpuser` is configured.

Related Information

- "`load` Command" on page 146
- "`set` Command" on page 147
- "Add SNMP Service User Accounts (Web Interface)" on page 102
- "Display the SNMP Service User Accounts (CLI)" on page 32
- "Delete SNMP Service User Accounts (CLI)" on page 58

▼ Modify SNMP Service User Accounts (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Modify a SNMP user:**

```
-> set /SP/services/snmp/users/username property=value property=value ...
```

where:

- *username* is the name of the SNMP user to modify.
- *property* is the parameter of the SNMP user to configure.
- *value* is the value of the *property* to configure.

The following properties are supported:

- `authenticationpassword` – The *value* is the password used for authentication.
- `authenticationprotocol` – The *value* is the protocol used for authentication.
- `permission` – The *value* is permission granted to the SNMP user.
- `privacypassword` – The *value* is the password used for privacy.
- `privacyprotocol` – The *value* is the protocol used for privacy.

For example, to configure the `snmpuser` with read and write permissions:

```
-> set /SP/services/snmp/users/snmpuser permission=rw
Set 'permission' to 'rw'
User /SP/services/snmp/users/snmpuser properties were updated successfully
->
```

Related Information

- "`set` Command" on page 147
- "Modify SNMP Service User Accounts (Web Interface)" on page 103
- "Modify SNMP Service Communities (CLI)" on page 59

▼ Delete SNMP Service User Accounts (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Delete a SNMP user:**

```
-> delete /SP/services/snmp/users/username
```

   where *username* is the name of the SNMP user to be deleted.

   For example, to delete the `snmpuser`:

```
-> delete /SP/services/snmp/users/snmpuser
Are you sure you want to delete /SP/services/snmp/users/snmpuser (y/n)? y
Deleted /SP/services/snmp/users/snmpuser
->
```

   The SNMP user `snmpuser` is deleted.

Related Information

- "`delete` Command" on page 142
- "Delete SNMP Service User Accounts (Web Interface)" on page 104

- "Display the SNMP Service User Accounts (CLI)" on page 32
- "Add SNMP Service User Accounts (CLI)" on page 56

▼ Add SNMP Service Communities (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Add a SNMP community:**

```
-> create /SP/services/snmp/communities/community permission=rw
```

   where *community* is the name of the SNMP community to create.

   For example, to add the community `newcom`:

```
-> create /SP/services/snmp/communities/newcom permission=rw
Created /SP/services/snmp/communities/newcom
->
```

   The SNMP community `newcom` is added.

Related Information

- "`create` Command" on page 141
- "Add SNMP Service Communities (Web Interface)" on page 105
- "Display the SNMP Service Communities (CLI)" on page 33
- "Delete SNMP Service Communities (CLI)" on page 60

▼ Modify SNMP Service Communities (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Modify an SNMP community:**

```
-> set /SP/services/snmp/communities/community property=value property=
value ...
```

   where:

   - *community* is the name of the SNMP community to modify.
   - *property* is the parameter of the SNMP community to configure.

- *value* is the value of the *property* to configure.

The following property is supported:

- `permission` – The *value* is permission granted to the SNMP community.

For example, to configure the `newcom` community with read only permissions:

```
-> set /SP/services/snmp/users/snmpuser permission=ro
Set 'permission' to 'ro'
User /SP/services/snmp/users/snmpuser properties were updated successfully
->
```

Related Information

- "`set` Command" on page 147
- "Modify SNMP Service Communities (Web Interface)" on page 105
- "Modify SNMP Service User Accounts (CLI)" on page 57

▼ Delete SNMP Service Communities (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Delete a SNMP community:**

```
-> delete /SP/services/snmp/communities/community
```

where *community* is the name of the SNMP community to delete.

For example, to delete the `newcom` community:

```
-> delete /SP/services/snmp/communities/newcom
Are you sure you want to delete /SP/services/snmp/communities/newcom (y/n)? y
Deleted /SP/services/snmp/communities/newcom
->
```

The SNMP community `newcom` is deleted.

Related Information

- "`delete` Command" on page 142
- "Delete SNMP Service Communities (Web Interface)" on page 106
- "Display the SNMP Service Communities (CLI)" on page 33
- "Add SNMP Service Communities (CLI)" on page 59

▼ Back Up SNMP Service MIBs (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Back up the MIBs:**

```
-> dump -destination URI /SP/services/snmp/mibs
```

   where *URI* is the uniform resource indicator.

   For example, to dump the MIBs as the `ilom-mibs.zip` file to a server with IP address 123.45.67.89 using the FTP protocol:

```
-> dump -destination ftp://root:changeme@123.45.67.89/tftpboot/ilom-mibs.zip
/SP/services/snmp/mibs
Dump successful.
->
```

   The MIBs are dumped.

Related Information

- "`dump` Command" on page 143
- "Back Up SNMP Service MIBs (Web Interface)" on page 107

▼ Disable the SNMP Service (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Disable the service:**

```
-> set /SP/services/snmp servicestate=disabled
Set 'servicestate' to 'disabled'
->
```

   The SNMP service is disabled.

Related Information

- "`set` Command" on page 147
- "Disable the SNMP Service (Web Interface)" on page 107
- "Display the SNMP Service Status (CLI)" on page 32

- "Enable the SNMP Service (CLI)" on page 55

Managing Other Aspects (CLI)

These tasks help you manage other aspect of ILOM.

- "Enable Alerts to Send SNMP Traps (CLI)" on page 62
- "Enable Alerts to Send PET (CLI)" on page 63
- "Disable Alerts (CLI)" on page 64
- "Set the ILOM CLI Session Timeout (CLI)" on page 65

Related Information

- "Managing Other Aspects (Web Interface)" on page 108
- "Managing Other Aspects (SNMP)" on page 131
- "Performing General Tasks on ILOM Targets (CLI)" on page 41

▼ Enable Alerts to Send SNMP Traps (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Enable alerts to send SNMP traps:**

```
-> set /SP/alertmgmt/rules/alert/ destination=IP_address destination_port=162 level=
level snmp_version=version
```

   where:

   - *alert* is the number of the alert.
   - *IP_address* is the IP address of the host to receive the SNMP trap.
   - *level* is the level of the alert.
   - *version* is the version of SNMP trap.

   For example, to set alert 1 to send `v2c` SNMP traps on occurence of `minor` or higher severity events to the host at 123.45.67.89:

```
-> set /SP/alertmgmt/rules/1/ destination=123.45.67.89 destination_port=162
level=minor snmp_version=2c
Set 'destination' to '123.45.67.89'
Set 'destination_port' to '162'
```

```
Set 'level' to 'minor'
Set 'snmp_version' to '2c'
->
```

Note – The destination port of 162 is the default used.

The following is an example of a SNMP v2c trap of when the aggregate sensor is in the state of `Asserted`:

```
May 23 13:09:41 nsn-blr-12 snmptrapd[25375]: [ID 702911 daemon.warning]
123.45.67.90 [123.45.67.90]: Trap DISMAN-EVENT-MIB::sysUpTimeInstance =
Timeticks: (40228) 0:06:42.28, SNMPv2-MIB::snmpTrapOID.0 = OID:
SUN-HW-TRAP-MIB::sunHwTrapComponentError,
SUN-HW-TRAP-MIB::sunHwTrapSystemIdentifier.0 = STRING: 123.45.67.90,
SUN-HW-TRAP-MIB::sunHwTrapChassisId.0 = STRING: 0000002,
SUN-HW-TRAP-MIB::sunHwTrapProductName.0 = STRING: Sun Datacenter Switch DCS 648
- Chassis, SUN-HW-TRAP-MIB::sunHwTrapComponentName.0 = STRING:
/SYS/CHASSIS_STATUS, SUN-HW-TRAP-MIB::sunHwTrapAdditionalInfo.0 = STRING: State
Asserted, SUN-HW-TRAP-MIB::sunHwTrapAssocObjectId.0 = OID:
ENTITY-MIB::entPhysicalDescr.2
```

In the output, the trap source is the switch and the component raising the trap is `/SYS/CHASSIS_STATUS` or the aggregate sensor. The sensor is `State Asserted`.

Related Information

- "`set` Command" on page 147
- "Enable Alerts to Send SNMP Traps (Web Interface)" on page 108
- "Enable Alerts to Send SNMP Traps (SNMP)" on page 132
- "Display the Alert Properties (CLI)" on page 36
- "Disable Alerts (CLI)" on page 64

▼ Enable Alerts to Send PET (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Enable alerts to send PET:**

```
-> set /SP/alertmgmt/rules/alert/ destination=IP_address level=level type=ipmipet
```

where:

- *alert* is the number of the alert.
- *IP_address* is the IP address of the host to receive the PET trap.
- *level* is the level of the alert.

For example, to set alert 2 to send PET traps on occurrence of `minor` or higher severity events to the host at 123.45.67.89:

```
-> set /SP/alertmgmt/rules/2/ destination=123.45.67.89 level=minor type=ipmipet
Set 'destination' to '123.45.67.89'
Set 'level' to 'minor'
Set 'type' to 'ipmipet'
->
```

The following is an example of a PET trap of when the aggregate sensor is in the state of `Asserted`:

```
Jun 25 11:34:33 nsn-blr-12 snmptrapd[16055]: [ID 702911 daemon.warning]
123.45.67.90: Enterprise Specific Trap
(SUN-ILOM-PET-MIB::petTrapOEMStateAssertedAssert) Uptime: 144 days, 4:52:20.75,
SUN-ILOM-PET-MIB::petTrapData = Hex-STRING: FF 20 00 08 FF FF FF FF FF FF 34 86
00 49 18 00
Jun 25 11:34:33 nsn-blr-12 00 04 15 98 47 5B FF FF 20 20 02 20 01 00 00 01
Jun 25 11:34:33 nsn-blr-12 FF FF 00 00 00 00 00 19 00 00 00 2A 30 30 80 0F
Jun 25 11:34:33 nsn-blr-12 03 43 48 41 53 53 49 53 5F 53 54 41 54 55 53 00
Jun 25 11:34:33 nsn-blr-12 80 28 03 53 75 6E 20 44 61 74 61 63 65 6E 74 65
Jun 25 11:34:33 nsn-blr-12 72 20 53 77 69 74 63 68 20 44 43 53 20 36 34 38
Jun 25 11:34:33 nsn-blr-12 20 2D 20 43 68 61 73 73 69 73 00 C1 00 00
```

Related Information

- "`set` Command" on page 147
- "Enable Alerts to Send PET (Web Interface)" on page 109
- "Modify Alert SNMP Version (SNMP)" on page 133
- "Display the Alert Properties (CLI)" on page 36
- "Disable Alerts (CLI)" on page 64

▼ Disable Alerts (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Disable the alerts:**

```
-> set /SP/alertmgmt/rules/alert level=disable
```

where *alert* is the number of the alert to disable.

For example, to disable alert 1:

```
-> set /SP/alertmgmt/rules/1 level=disable
Set 'level' to 'disable'
->
```

The alert is disabled.

Related Information

- "set Command" on page 147
- "Disable Alerts (Web Interface)" on page 110
- "Disable Alerts (SNMP)" on page 134
- "Display the Alert Properties (CLI)" on page 36
- "Enable Alerts to Send SNMP Traps (CLI)" on page 62

▼ Set the ILOM CLI Session Timeout (CLI)

1. **Access the ILOM CLI.**

   See "Access ILOM From the CLI" on page 22.

2. **Set the ILOM CLI session timeout:**

```
-> set /SP/cli timeout=value
```

where *value* is the number of minutes for session timeout (1–1440).

For example, to set the timeout for 100 minutes:

```
-> set /SP/cli timeout=100
Set 'timeout' to '100'
->
```

The CLI session timeout is set.

Note – Setting a timeout *value* of 0 disables the timeout feature.

Related Information

- "`set` Command" on page 147
- "Set the ILOM CLI Session Timeout (Web Interface)" on page 110
- "Display the ILOM CLI Session Timeout (CLI)" on page 39

Upgrading the Switch Firmware Through ILOM (CLI)

One of the advantages of ILOM support on the CMCs is that all firmware upgrades, including upgrades for H8 and I4, have been simplified into a four-task process.

These topics enable you to upgrade the switch firmware through the ILOM CLI.

- "Firmware Overview" on page 66
- "Firmware Server" on page 67
- "`ibfw_server` Daemon" on page 67
- "`flint` Application" on page 67
- "Install the `flint` Application (CLI)" on page 67
- "Download the Switch Firmware Package (CLI)" on page 68
- "Set Component Firmware to Upgrade (CLI)" on page 69
- "Upgrade the Switch Firmware (CLI)" on page 71

Firmware Overview

The H8 is installed on every line card, fabric card, and fabric card filler as an interface between the IPMB bus and the component's hardware. The H8 chips have firmware that enables them to translate commands from the CMC to appropriate control signals, and interpret data from sensors into coherent values the CMC can understand.

The switch chips have firmware that instructs how to route links, set data rates, and configure signal parameters.

When you install a new line card, fabric card or fabric card filler, the H8 firmware and switch chip firmware might not be the same as for the other components. Additionally, a newer version of the firmware might become available.

Firmware Server

To upgrade the firmware through ILOM requires the configuration of a firmware server. The firmware server is a Linux host that is part of the InfiniBand fabric. It can be the Linux InfniBand host. The firmware server hosts the `ibfw_server` daemon and the `flint` application. The firmware server must also have an FTP client-server running.

`ibfw_server` Daemon

The `ibfw_server` firmware server daemon performs the I4 switch chip firmware upgrade within the InfiniBand fabric. You start the daemon on the firmware server before running the firmware configuration script.

`flint` Application

The Mellanox Firmware Tool (MFT) is a suite of applications used to administrate the I4 switch chips from a Linux host, which is part of the InfiniBand fabric. The `flint` application is part of the MFT and is used by the `ibfw_server` firmware server daemon to perform the switch chip firmware upgrade over the InfiniBand fabric. Because the switch chip firmware upgrade is performed in-band, the time required to upgrade the entire switch is greatly reduced.

Note – You must have the `flint` application installed into the `/usr/bin` directory to enable the switch chip firmware upgrade through ILOM. If the `flint` application is not installed in the Linux host, download and install it. See "Install the `flint` Application (CLI)" on page 67.

▼ Install the `flint` Application (CLI)

Note – You must have the `flint` application installed into the `/usr/bin` directory to enable the switch chip firmware upgrade through ILOM.

---

1. **On the Linux host that is part of the InfiniBand fabric, open a web browser to the following URL:**

   `(http://www.mellanox.com)`

2. **Click on the Downloads tab.**

3. **Click on the Firmware Tools link.**

   The Mellanox Firmware Tools (MFT) page is displayed.

4. **Click on the following links to download the respective Linux files.**
   - MFT_Linux_Release_Notes (PDF file)
   - MFT_User's Manual for Linux (PDF file)
   - MFT_SW for Linux (`.tgz` file)

5. **Read the user's manual for installation instructions.**

6. **Download the switch firmware package.**

   See "Download the Switch Firmware Package (CLI)" on page 68.

Related Information

- *Switch Installation*, installing the OFED InfiniBand software

▼ Download the Switch Firmware Package (CLI)

This procedure downloads the switch firmware and configures the firmware server.

1. **Open a web browser on a Linux host that is part of the InfiniBand fabric and will become the firmware server.**

2. **Go to this URL:**

   `(www.sun.com/downloads)`

   Oracle's Sun Downloads page is displayed.

3. **Click the Downloads A-Z tab.**

   An alphabetical listing of downloads is displayed.

4. **Under S, click on the Sun Datacenter InfiniBand Switch 648 FW 1.0.2 (or higher) link.**

   The Sun Datacenter InfiniBand Switch 648 FW 1.0.2 page is displayed.

5. **Check the license agreement box and click Continue.**

   The page updates to list the available files.

6. **Download the required and optional files to your download directory.**

   The firmware is in the `SUN_DCS_648_FW_v1.0.2.tar.gz` file.

7. **In your download directory, unpack the** `.gz` **file:**

```
$ gtar -zxvf SUN_DCS_648_FW_v1.0.2.tar.gz
```

   The extracted files are displayed.

8. **Unpack the** `SUN_DCS_648_ADDBLDRC2.tar.gz` **file:**

```
$ gtar -zxvf SUN_DCS_648_ADDBLDRC2.tar.gz
```

   The extracted files are displayed.

9. **Move the** `SUN_DCS_648_BINARY_1.0.2.pkg` **file to the transfer directory.**
10. **Become superuser.**
11. **Ensure that the** `portmapper` **application is running:**

```
# service portmap start
```

12. **Start the firmware server daemon:**

```
# ibfw_server
```

13. **Configure which firmware is to be updated.**

    See "Set Component Firmware to Upgrade (CLI)" on page 69.

Related Information

- "Download the ILOM Firmware" on page 15

▼ Set Component Firmware to Upgrade (CLI)

Note – For this procedure, the `setFWConfiguration.sh` script uses the word `update` interchangeably with the word `upgrade`.

---

1. **Access the Linux shell on the CMC.**

   See:

   - "Switch From the ILOM Shell to the Linux Shell" on page 24
   - *Sun Datacenter InfiniBand Switch 648 Installation Guide*, part number 820-7748.

2. **Run the firmware configuration script.**

```
# setFWConfiguration.sh
```

Respond to the script as you would to upgrade your switch

a. **Type the IP address of the firmware server, previously configured.**

For example:

```
Enter firmware server IP (): 123.45.67.89
```

b. **Type the name of the user that has access to the firmware files.**

For example:

```
Enter firmware server user (): root
```

c. **Type that user's password.**

For example:

```
Enter firmware server password: password
```

d. **Type** `none`, `all`, **or the specific line card slots (separated by commas) of the line cards you are upgrading.**

For example:

```
Enter line cards to update (none) [none/all/0,1,...,8]: all
```

e. **Type** `yes` **to upgrade the I4 switch chip firmware on the selected line cards or** `no` **to not upgrade them.**

For example:

```
Update FC I4 switches (yes) [yes/no]: yes
```

f. **Type** `none`, `all`, **or the specific fabric card slots (separated by commas) of the fabric cards you are upgrading.**

For example:

```
Enter fabric cards to update (2,5) [none/all/0,1,...,8]: all
```

g. **Type** `yes` **to upgrade the I4 switch chip firmware on the selected fabric cards or** `no` **to not upgrade them.**

For example:

```
Update LC I4 switches (yes) [yes/no]: yes
```

h. **Type** `yes` **to upgrade the Shelf Manager firmware or** `no` **to not upgrade it.**

For example:

```
Update ShMM (no) [yes/no]: no
```

The configuration file is created and the script ends.

3. **Validate the firmware upgrade configuration file.**

For example:

```
# getFWConfiguration.sh
Firmware server IP       : 123.45.67.89
Firmware server user     : root
Line cards to update     : all
Update LC I4 switches    : yes
Fabric cards to update   : all
Update FC I4 switches    : yes
Update ShMM              : no
#
```

4. **Upgrade the firmware.**

See "Upgrade the Switch Firmware (CLI)" on page 71.

▼ Upgrade the Switch Firmware (CLI)

When ILOM performs the firmware upgrade, it checks the following:

- All line cards configured for upgrade are in an active state and all links are up.
- All fabric cards configured for upgrade are in an active state and all links are up.
- All fabric card fillers configured for upgrade are in an active state.

Components that do not meet these criteria are not upgraded, and ILOM displays a warning indicating so.

1. **Access the ILOM CLI.**

See "Access ILOM From the CLI" on page 22.

2. **Upgrade the firmware:**

```
-> load -source URI/pkgname
```

where:

URI is the uniform resource indicator for the firmware server.

pkgname is the name of the firmware package in the transfer directory.

For example, using the FTP protocol:

```
-> load -source
ftp://root:password@123.45.67.89/transfer_directory/SUN_DCS_648_BINARY_1.0.2.pkg

Downloading firmware image. This will take approximately 2 minutes.
```

Respond to the upgrade.

a. **Read the note and respond appropriately.**

For example:

```
NOTE: Firmware upgrade will upgrade the chassis CMM firmware.
      It will also do H8 and I4 upgrade on all line cards
      and fabric cards of the chassis. For a fully loaded
      chassis, firmware upgrade takes couple of hours.

      ILOM will enter a special mode to load new firmware. No
      other tasks can be performed in ILOM until the firmware
      upgrade is complete and ILOM is reset.

Are you sure you want to load the specified file (y/n)? y
```

b. **Type** `y` **to preserve the existing ILOM configuration or** `n` **to have it removed.**

For example:

```
Preserve existing configuration (y/n)? y
```

c. **Type** `y` **to perform the firmware upgrade outside of the InfiniBand fabric should the upgrade within the InfiniBand fabric fail or** `n` **to just abort the firmware upgrade in that situation.**

For example:

```
Switch to outband update if inband update fails for I4 (y/n)? n
```

Note – An upgrade outside of the InfiniBand fabric can take many hours.

The firmware upgrade enviroment is set up and the following message is displayed:

```
Setting up environment for firmware upgrade. This will take approximately 2
minutes.

Starting FW upgrade
```

The firmware upgrade starts. During the process, you see messages of the progress. For example:

```
==========================
Performing operation: FC 2
==========================
FC 2: H8 is already at the given version.
FC 2: I4 0 is already at the given version.
FC 2: I4 1 is already at the given version.
```

When the firmware upgrade ends, a summary is displayed. For example:

```
===========================
Summary of Firmware update
===========================
LC status (1,8:full): FW UPDATE - FAILED
H8 succeeded on cards          :  none
H8 already up-to-date on cards :  none
H8 failed on cards             :  none
I4 succeeded on cards          :  none
I4 already up-to-date on cards :  none
I4 failed on cards             :  none
Cards in "Not Present" state   :  1
Cards not in "Ready" state     :  8
FC/FCF status (2:full): FW UPDATE - SUCCESS
H8 succeeded on cards          :  none
H8 already up-to-date on cards :  2
H8 failed on cards             :  none
I4 succeeded on cards          :  none
I4 already up-to-date on cards :  2(I4 - 0,1)
I4 failed on cards             :  none
Cards in "Not Present" state   :  none
Cards not in "Ready" state     :  none

Firmware update is complete.
```

Related Information

- "Upgrade the Switch Firmware (Web Interface)" on page 111

Administering ILOM (Web Interface)

These topics describe how to administer ILOM from the command-line interface.

Related Information

Web Interface Overview

The ILOM web interface uses a model of hierarchical tabbed pages that you select by clicking on the tab name. Once a page is displayed, you can provide information, set parameters, or access other subtabs. For some pages, initiating a task might spawn an additional window, which accepts further parameters. Clicking Save or Close closes the window.

The web interface enables you to accomplish most of the same tasks that are possible using the ILOM CLI. With the web interface, you do not need to use a command to specify a target or property. Therefore, the web interface is more user-friendly.

Note – The web interface does not support the CMC's Linux shell. You must access the CMC using the methods described in "Access ILOM From the CLI" on page 22 to enable ILOM shell - Linux shell toggling.

The following illustration displays the initial ILOM web interface page.

The following table lists the tabs and subtabs the ILOM web interface.

Tab	Subtabs	Description
System Information	Versions	Displays version of ILOM firmware.
	Session Time-Out	Sets inactivity time-out for auto-logout.
	Components	Displays component status.
System Monitoring	Sensor Readings	Displays sensor values.
	Event Logs	Displays event log.

Tab	Subtabs	Description
Configuration	System Management Access	subtabs for: • Web Server – Configures web server behavior and ports. • SSL Certificate – Displays certificate information. • SNMP – Manages SNMP users, communities, and access. • IPMI – Toggles the state of the IPMI service. • CLI – Sets inactivity time-out for auto-logout.
	Alert Management	Configures alerts.
	Network	Sets and enables basic network parameters. Has ping test.
	Clock	Sets date, time, and time server parameters.
	Timezone	Sets timezone.
	Syslog	Configures Syslog redirection to IP address.
User Management	User Accounts	Configures user accounts and enables single sign-on.
	Active Sessions	Displays active sessions.
Maintenance	Firmware Upgrade	Enables firmware upgrade.
	Back up/Restore	Configures system back up and restore.

Related Information

- "ILOM Targets and Descriptions" on page 5
- "CLI Overview" on page 21
- "SNMP Overview" on page 113
- "SNMP Commands" on page 114
- "`ipmitool` Overview" on page 135

▼ Access ILOM From the Web Interface

Note – You must configure the NET MGT port of the CMC in order to access the web interface. Refer to the *Sun Datacenter InfiniBand Switch 648 Installation Guide*, part number 820-7738, for information on how to configure the NET MGT port.

1. **Open a web browser and connect to the ILOM web interface by specifying the CMC's network address in the URL.**

   The ILOM login page is displayed.

Note – If the login page is not displayed or a 404 error is displayed, verify that the web interface is enabled. See "Enable the HTTP Service (CLI)" on page 50 and "Enable the HTTPS Service (CLI)" on page 51 to enable the web interface from the CLI.

---

2. **Type `ilom-admin` in to the User Name field and the `ilom-admin` password into the Password field.**

Note – As shipped, the `ilom-admin` user password is `ilom-admin`. See "Change an ILOM User's Password and or Role (Web Interface)" on page 95 for instructions on how to change ILOM user passwords.

---

3. **Click Submit.**

   The ILOM web interface is displayed.

Note – You can also log in as the `ilom-operator` user with the password `ilom-operator`. The `ilom-operator` user has only read permissions.

Related Information

- "Access ILOM From the CLI" on page 22
- "Web Interface Overview" on page 75
- "Monitoring ILOM Targets (Web Interface)" on page 78
- "Controlling ILOM Targets (Web Interface)" on page 89

Monitoring ILOM Targets (Web Interface)

These topics enable you to display the status of many ILOM targets.

- "Performing Daily Tasks (Web Interface)" on page 79
- "Checking the Status of Services (Web Interface)" on page 81
- "Verifying Other Aspects (Web Interface)" on page 85

Related Information

- "Access ILOM From the Web Interface" on page 77
- "Monitoring ILOM Targets (CLI)" on page 25
- "Controlling ILOM Targets (Web Interface)" on page 89

Performing Daily Tasks (Web Interface)

These tasks help you see the status of ILOM targets that are continually changing.

- "Display the Date, Time, and Time Zone (Web Interface)" on page 79
- "Display the Aggregate Sensor State (Web Interface)" on page 80
- "Display the ILOM Sessions (Web Interface)" on page 80
- "Display the ILOM Event Log (Web Interface)" on page 81

Related Information

- "Performing Daily Tasks (Web Interface)" on page 79
- "Checking the Status of Services (Web Interface)" on page 81
- "Verifying Other Aspects (Web Interface)" on page 85

▼ Display the Date, Time, and Time Zone (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

2. **Click the Configuration tab.**

3. **Click the Timezone subtab.**

   The Timezone Settings window opens.

   The current date, time and time zone are displayed in the Datetime field.

Related Information

- "Display the Date, Time, and Time Zone (CLI)" on page 26
- "Display the Date and Time (SNMP)" on page 116
- "Display the Time Zone (SNMP)" on page 116
- "Set the Date and Time (Web Interface)" on page 90
- "Set the Time Zone (Web Interface)" on page 90

▼ Display the Aggregate Sensor State (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

2. **Click the System Monitoring tab.**

3. **Click the Sensor Readings subtab.**

   The Sensor Readings window opens.

   In the Sensor Readings table, the sensor name, type and reading are displayed.

4. **Click the `/SYS/CHASSIS_STATUS` link in the table.**

   A new window opens and displays the sensor's properties and values. The property value of `State Deasserted` means no faults.

5. **Click Close.**

Related Information

- "Display the Aggregate Sensor State (CLI)" on page 27
- "Display the Aggregate Sensor State (SNMP)" on page 116
- "Display the Aggregate Sensor Status (SNMP)" on page 117
- "Display the Sensor State (IPMI)" on page 136
- "Display the Sensor Information (IPMI)" on page 137

▼ Display the ILOM Sessions (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

2. **Click the User Management tab.**

3. **Click the Active Sessions subtab.**

   The Active Sessions window opens.

   In the Active Sessions table, the session's user name, their role, the session start time, and the session type and mode are displayed.

Related Information

- "Display the ILOM Sessions (CLI)" on page 27
- "Display ILOM Sessions (SNMP)" on page 117

▼ Display the ILOM Event Log (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

2. **Click the System Monitoring tab.**

3. **Click the Event Logs subtab.**

   The event log is displayed.

   The Filter pull-down menu filters events by type.

Related Information

- "Display the ILOM Event Log (CLI)" on page 28
- "Display the ILOM Event Log (SNMP)" on page 118
- "Display the System Event Log (IPMI)" on page 138
- "Display the Remote Log Hosts (Web Interface)" on page 87

Checking the Status of Services (Web Interface)

These topics enable you to display the status of the many services supported by ILOM.

- "Display the HTTP Service Status (Web Interface)" on page 82
- "Display the HTTPS Service Status (Web Interface)" on page 82
- "Display the SSL Certificates (Web Interface)" on page 83
- "Display the SNMP Service Status (Web Interface)" on page 83
- "Display the SNMP Service User Accounts (Web Interface)" on page 84
- "Display the SNMP Service Communities (Web Interface)" on page 84
- "Display the IPMI Service Status (Web Interface)" on page 85

Related Information

- "Checking the Status of Services (CLI)" on page 29
- "Performing Daily Tasks (Web Interface)" on page 79
- "Verifying Other Aspects (Web Interface)" on page 85

▼ Display the HTTP Service Status (Web Interface)

1. **Access the ILOM web interface.**
   See "Access ILOM From the Web Interface" on page 77.
2. **Click the Configuration tab.**
3. **Click the Systems Management Access subtab.**
4. **Click the Web Server subtab.**
   The Web Server Settings window opens.
   The HTTP web server status and port are displayed.

Related Information

- "Display the HTTP Service Status (CLI)" on page 30
- "Display the HTTP Service Status (SNMP)" on page 119
- "Enable the HTTP Service (Web Interface)" on page 97
- "Disable the HTTP Service (Web Interface)" on page 97

▼ Display the HTTPS Service Status (Web Interface)

1. **Access the ILOM web interface.**
   See "Access ILOM From the Web Interface" on page 77.
2. **Click the Configuration tab.**
3. **Click the Systems Management Access subtab.**
4. **Click the Web Server subtab.**
   The Web Server Settings window opens.
   The HTTPS web server status and port are displayed.

Related Information

- "Display the HTTPS Service Status (CLI)" on page 30
- "Display the HTTPS Service Status (SNMP)" on page 119
- "Enable the HTTPS Service (Web Interface)" on page 98
- "Disable the HTTPS Service (Web Interface)" on page 100

▼ Display the SSL Certificates (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

2. **Click the Configuration tab.**

3. **Click the Systems Management Access subtab.**

4. **Click the SSL Certificate subtab.**

   The SSL Certificate Upload window opens.

   The certificate status and information about the default certificate, custom certificate, and custom private key are displayed.

Related Information

- "Display the SSL Certificates (CLI)" on page 31
- "Install a Custom SSL Certificate (Web Interface)" on page 99
- "Remove the Custom SSL Certificate (Web Interface)" on page 99

▼ Display the SNMP Service Status (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

2. **Click the Configuration tab.**

3. **Click the Systems Management Access subtab.**

4. **Click the SNMP subtab.**

   The SNMP Management window opens.

   Under Settings, the service status and operating parameters are displayed.

Related Information

- "Display the SNMP Service Status (CLI)" on page 32
- "Enable the SNMP Service (Web Interface)" on page 101
- "Disable the SNMP Service (Web Interface)" on page 107

▼ Display the SNMP Service User Accounts (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

2. **Click the Configuration tab.**

3. **Click the Systems Management Access subtab.**

4. **Click the SNMP subtab.**

   The SNMP Management window opens.

5. **Click the Users link.**

   The page scrolls to the SNMP Users table, where the configured SNMP users, their authentication protocol, permissions, and privacy protocol are displayed.

Related Information

- "Display the SNMP Service User Accounts (CLI)" on page 32
- "Add SNMP Service User Accounts (Web Interface)" on page 102
- "Delete SNMP Service User Accounts (Web Interface)" on page 104

▼ Display the SNMP Service Communities (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

2. **Click the Configuration tab.**

3. **Click the Systems Management Access subtab.**

4. **Click the SNMP subtab.**

   The SNMP Management window opens.

5. **Click the Communities link.**

   The page scrolls to the SNMP Communities table, where the configured SNMP communities and permissions are displayed.

Related Information

- "Display the SNMP Service Communities (CLI)" on page 33
- "Add SNMP Service Communities (Web Interface)" on page 105
- "Delete SNMP Service Communities (Web Interface)" on page 106

▼ Display the IPMI Service Status (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

2. **Click the Configuration tab.**

3. **Click the Systems Management Access subtab.**

4. **Click the IPMI subtab.**

   The IPMI Settings window opens.

   The status of the IPMI server is displayed.

Related Information

- "Display the IPMI Service Status (CLI)" on page 34

Verifying Other Aspects (Web Interface)

These topics enable you to display the status of other aspects of ILOM.

- "Display the Alert Properties (Web Interface)" on page 85
- "Display the ILOM User Accounts (Web Interface)" on page 86
- "Display the Remote Log Hosts (Web Interface)" on page 87
- "Display the Network Management Configuration (Web Interface)" on page 87
- "Display the ILOM CLI Session Timeout (Web Interface)" on page 87
- "Display Chassis FRU ID Information (Web Interface)" on page 88
- "Display the ILOM Firmware Version (Web Interface)" on page 88

Related Information

- "Verifying Other Aspects (CLI)" on page 34
- "Performing Daily Tasks (Web Interface)" on page 79
- "Checking the Status of Services (Web Interface)" on page 81

▼ Display the Alert Properties (Web Interface)

Alerts can provide advance notice of a system failure. The ILOM implementation in the management controller supports 15 alert rules, which configure alert properties. Supported alert types are SNMP trap and PET. The alert destination must have the relevant ILOM MIBs installed and must support SNMP traps or PETs.

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

2. **Click the Configuration tab.**

3. **Click the Alert Management subtab.**

   The Alert Settings window opens.

   In the Alerts table, the Alert ID, Level, Alert Type, and Destination Summary are displayed for each alert.

Related Information

- "Display the Alert Properties (CLI)" on page 36
- "Display the Alert Properties (SNMP)" on page 120
- "Enable Alerts to Send SNMP Traps (Web Interface)" on page 108
- "Enable Alerts to Send PET (Web Interface)" on page 109
- "Disable Alerts (Web Interface)" on page 110

▼ Display the ILOM User Accounts (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

2. **Click the User Management tab.**

3. **Click the User Accounts subtab.**

   The User Account Settings window opens.

4. **Click the Users link.**

   The page scrolls and the Users table is displayed.

   In the Users table, the user's name and role are displayed.

Related Information

- "Display the ILOM User Accounts (CLI)" on page 37
- "Display ILOM User Accounts (SNMP)" on page 121
- "Add an ILOM User Account (Web Interface)" on page 94
- "Delete an ILOM User Account (Web Interface)" on page 96

▼ Display the Remote Log Hosts (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

2. **Click the Configuration tab.**

3. **Click the Syslog subtab.**

   The Syslog window opens.

   The remote log host IP addresses are displayed.

Related Information

- "Display the Remote Log Hosts (CLI)" on page 38
- "Display the Remote Log Hosts (SNMP)" on page 122
- "Set the Remote Log Hosts (Web Interface)" on page 91

▼ Display the Network Management Configuration (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

2. **Click the Configuration tab.**

3. **Click the Network subtab.**

   The Network Settings window opens.

   The network status, MAC address, IP discovery mode, IP address, netmask and gateway are displayed.

Related Information

- "Display the Network Management Configuration (CLI)" on page 38
- "Display the Network Management Configuration (SNMP)" on page 123
- "Set the Network Management Parameters (Web Interface)" on page 93

▼ Display the ILOM CLI Session Timeout (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

2. **Click the Configuration tab.**

3. **Click the Systems Management Access subtab.**
4. **Click the CLI subtab.**

   The CLI Settings window opens.

   The CLI session timeout is displayed.

Related Information

- "Display the ILOM CLI Session Timeout (CLI)" on page 39
- "Set the ILOM CLI Session Timeout (Web Interface)" on page 110

▼ Display Chassis FRU ID Information (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.
2. **Click the System Information tab.**
3. **Click the Components subtab.**

   The Component Management window opens.

   In the Component Status table, the component name (target) and type are displayed.
4. **Click the `/SYS` link in the table.**

   A new window opens and displays the chassis' properties and values.
5. **Click Close.**

Related Information

- "Display Chassis FRU ID Information (CLI)" on page 39
- "Display the System Components (SNMP)" on page 123
- "Display the Additional System Component Information (SNMP)" on page 124

▼ Display the ILOM Firmware Version (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.
2. **Click the System Information tab.**

3. **Click the Versions subtab.**

   The Versions window opens.

   In the Version Information table, the ILOM firmware, build, date, and file system version information are displayed.

Related Information

- "Display the ILOM Firmware Version (CLI)" on page 40

Controlling ILOM Targets (Web Interface)

These topics enable you to change the behavior or configuration of many ILOM targets.

- "Performing General Tasks on ILOM Targets (Web Interface)" on page 89
- "Performing ILOM User Tasks (Web Interface)" on page 94
- "Managing HTTP Services (Web Interface)" on page 96
- "Managing HTTPS Services (Web Interface)" on page 98
- "Managing SNMP Services (Web Interface)" on page 101
- "Managing Other Aspects (Web Interface)" on page 108

Related Information

- "Access ILOM From the Web Interface" on page 77
- "Controlling ILOM Targets (CLI)" on page 41
- "Monitoring ILOM Targets (Web Interface)" on page 78
- "Understanding ILOM Targets" on page 4

Performing General Tasks on ILOM Targets (Web Interface)

You can perform these tasks periodically on a few ILOM targets.

- "Set the Date and Time (Web Interface)" on page 90
- "Set the Time Zone (Web Interface)" on page 90

- "Clear the ILOM Event Log (Web Interface)" on page 91
- "Set the Remote Log Hosts (Web Interface)" on page 91
- "Back Up the ILOM Configuration (Web Interface)" on page 92
- "Restore the ILOM Configuration (Web Interface)" on page 93
- "Set the Network Management Parameters (Web Interface)" on page 93

Related Information

- "Performing General Tasks on ILOM Targets (CLI)" on page 41
- "Performing ILOM User Tasks (Web Interface)" on page 94

▼ Set the Date and Time (Web Interface)

1. **Access the ILOM web interface.**
   See "Access ILOM From the Web Interface" on page 77.
2. **Click the Configuration tab.**
3. **Click the Clock subtab.**
   The Clock Settings window opens.
4. **Type the date into the Date field.**
5. **Select the time from the Time pull-down menus.**
6. **Click Save.**

Related Information

- "Set the Date, Time, and Time Zone (CLI)" on page 42
- "Set the Date and Time (SNMP)" on page 126
- "Display the Date, Time, and Time Zone (Web Interface)" on page 79

▼ Set the Time Zone (Web Interface)

1. **Access the ILOM web interface.**
   See "Access ILOM From the Web Interface" on page 77.
2. **Click the Configuration tab.**
3. **Click the Timezone subtab.**
   The Timezone Settings window opens.

4. **Select the time zone from the Timezone pull-down menu.**
5. **Click Save.**

Related Information

- "Set the Date, Time, and Time Zone (CLI)" on page 42
- "Display the Date, Time, and Time Zone (Web Interface)" on page 79

▼ Clear the ILOM Event Log (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.
2. **Click the System Monitoring tab.**
3. **Click the Event Logs subtab.**

   The Event Log window opens.
4. **In the Event Log table, click Clear Log.**

   A dialog box opens and asks you to confirm.
5. **Click OK.**

   The event log is cleared.

Related Information

- "Clear the ILOM Event Log (CLI)" on page 42
- "Clear the ILOM Event Log (SNMP)" on page 127
- "Display the ILOM Event Log (Web Interface)" on page 81

▼ Set the Remote Log Hosts (Web Interface)

The ILOM implementation in the management controller provides a protocol for transmitting ILOM events to a remote log host. The events transmitted are similar to those displayed in the local log.

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.
2. **Click the Configuration tab.**
3. **Click the Syslog subtab.**

   The Syslog window opens.

4. **Type the IP address or hostname of the remote log hosts into the respective fields.**
5. **Click Save.**

   The remote log hosts are set.

Note – Setting a remote log host IP address to 0.0.0.0 disables that functionality.

Related Information

- "Set the Remote Log Hosts (CLI)" on page 43
- "Set the Remote Log Hosts (SNMP)" on page 127
- "Display the Remote Log Hosts (Web Interface)" on page 87

▼ Back Up the ILOM Configuration (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.
2. **Click the Maintenance tab.**
3. **Click the Back up/Restore subtab.**

   The Configuration Back up/Restore window opens.
4. **Select Back up from the Operation pull-down menu.**
5. **Select the transfer protocol from the Transfer Method pull-down menu.**
6. **For the protocol selected, provide the host IP address, file and path, user name, and password into the respective fields.**
7. **If you want to back up the configuration with a passphrase, type the passphrase into the Passphrase and Confirm Passphrase fields.**
8. **Click Run.**

   A dialog box opens and asks you to confirm.
9. **Click OK.**

   The ILOM configuration is backed up in the specified file on the specified host using the specified protocol.

Related Information

- "Back Up the ILOM Configuration (CLI)" on page 44
- "Restore the ILOM Configuration (Web Interface)" on page 93

▼ Restore the ILOM Configuration (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

2. **Click the Maintenance tab.**

3. **Click the Back up/Restore subtab.**

   The Configuration Back up/Restore window opens.

4. **Select Restore from the Operation pull-down menu.**

5. **Select the transfer protocol from the Transfer Method pull-down menu.**

6. **For the protocol selected, provide the file, host IP address, file path, user name, and password into the respective fields.**

7. **If you used a passphrase with the backup, type the passphrase into the Passphrase and Confirm Passphrase fields.**

8. **Click Run.**

   A dialog box opens and asks you to confirm.

9. **Click OK.**

   The ILOM configuration is restored from the specified file on the specified host using the specified protocol.

Related Information

- "Restore the ILOM Configuration (CLI)" on page 44
- "Back Up the ILOM Configuration (Web Interface)" on page 92

▼ Set the Network Management Parameters (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

2. **Click the Configuration tab.**

3. **Click the Network subtab.**

   The Network Settings window opens.

4. **Type the IP Address, Netmask, and Gateway into their respective fields.**

5. **Click Save.**

Note – Changing some network management properties terminates the NET MGT connection to the CMC (web interface). You must re-establish the connection to continue administering the CMC. See "Access ILOM From the Web Interface" on page 77.

Related Information

- "Set the Network Management Parameters (CLI)" on page 45
- "Set the Network Management Parameters (SNMP)" on page 128
- "Display the Network Management Configuration (Web Interface)" on page 87

Performing ILOM User Tasks (Web Interface)

These topics enable you to change and configure ILOM user targets.

- "Add an ILOM User Account (Web Interface)" on page 94
- "Change an ILOM User's Password and or Role (Web Interface)" on page 95
- "Delete an ILOM User Account (Web Interface)" on page 96

Related Information

- "Performing ILOM User Tasks (CLI)" on page 47
- "Performing General Tasks on ILOM Targets (Web Interface)" on page 89

▼ Add an ILOM User Account (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

2. **Click the User Management tab.**
3. **Click the User Accounts subtab.**

   The User Accounts Settings window opens.

4. **Click the Users link.**

   The page scrolls to the Users table.

5. **In the Users table, click Add.**

   A new window opens.

6. **In the window, type the name of the new user account in the User Name field.**

7. **Select the abilities of the new user from the Roles pull-down menu.**

   If a check box is not grayed-out, you can add that ability to the selected role.

8. **Type the password into the Password fields.**

9. **Click Save.**

   The new user account is created and the window closes.

Related Information

- "Add an ILOM User Account (CLI)" on page 47
- "Add an ILOM User Account (SNMP)" on page 130
- "Display the ILOM User Accounts (Web Interface)" on page 86
- "Delete an ILOM User Account (Web Interface)" on page 96

▼ Change an ILOM User's Password and or Role (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

2. **Click the User Management tab.**

3. **Click the User Accounts subtab.**

   The User Accounts Settings window opens.

4. **Click the Users link.**

   The page scrolls to the Users table.

5. **In the Users table, select the user whose password and role you want to change and click Edit.**

   A new window opens.

6. **In the window, type the new password for the user and or select the new abilities of the user from the Roles pull-down menu.**

   If a check box is not grayed-out, you can add that ability to the selected role.

7. **Click Save.**

   The new settings are saved and the window closes.

Related Information

- "Change an ILOM User's Password and or Role (CLI)" on page 48

▼ Delete an ILOM User Account (Web Interface)

1. **Access the ILOM web interface.**
   See "Access ILOM From the Web Interface" on page 77.
2. **Click the User Management tab.**
3. **Click the User Accounts subtab.**
   The User Accounts Settings window opens.
4. **Click the Users link.**
   The page scrolls to the Users table.
5. **In the Users table, select the user to delete and click Delete.**
   A dialog box opens and asks for confirmation.
6. **Click OK.**
   The user account is deleted.

Related Information

- "Delete an ILOM User Account (CLI)" on page 49
- "Delete an ILOM User Account (SNMP)" on page 131
- "Display the ILOM User Accounts (Web Interface)" on page 86
- "Add an ILOM User Account (Web Interface)" on page 94

Managing HTTP Services (Web Interface)

These tasks help you manage the ILOM HTTP service targets.

- "Enable the HTTP Service (Web Interface)" on page 97
- "Disable the HTTP Service (Web Interface)" on page 97

Related Information

- "Managing HTTP Services (CLI)" on page 50
- "Managing HTTPS Services (Web Interface)" on page 98
- "Managing SNMP Services (Web Interface)" on page 101

▼ Enable the HTTP Service (Web Interface)

Note – Performing this task on an already active HTTP server effectively resets the server.

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

2. **Click the Configuration tab.**
3. **Click the System Management Access subtab.**
4. **Click the Web Server subtab.**

   The Web Server Settings window opens.

5. **Select either Enabled or Redirect HTTP Connection to HTTPS from the HTTP Web server pull-down menu.**
6. **Type the web server port number into the HTTP Port field.**
7. **Click Save.**

Related Information

- "Enable the HTTP Service (CLI)" on page 50
- "Set the HTTP Service State (SNMP)" on page 132
- "Display the HTTP Service Status (Web Interface)" on page 82
- "Disable the HTTP Service (Web Interface)" on page 97

▼ Disable the HTTP Service (Web Interface)

Note – Performing this task on an already active HTTPS server effectively resets the server.

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

2. **Click the Configuration tab.**
3. **Click the System Management Access subtab.**
4. **Click the Web Server subtab.**

   The Web Server Settings window opens.

5. **Select Disabled from the HTTP web server pull-down menu.**
6. **Click Save.**

Related Information

- "Disable the HTTP Service (CLI)" on page 50
- "Set the HTTP Service State (SNMP)" on page 132
- "Display the HTTP Service Status (Web Interface)" on page 82
- "Enable the HTTP Service (Web Interface)" on page 97

Managing HTTPS Services (Web Interface)

These tasks help you manage the ILOM HTTPS service targets.

- "Enable the HTTPS Service (Web Interface)" on page 98
- "Install a Custom SSL Certificate (Web Interface)" on page 99
- "Remove the Custom SSL Certificate (Web Interface)" on page 99
- "Disable the HTTPS Service (Web Interface)" on page 100

Related Information

- "Managing HTTPS Services (CLI)" on page 51
- "Managing HTTP Services (Web Interface)" on page 96
- "Managing SNMP Services (Web Interface)" on page 101

▼ Enable the HTTPS Service (Web Interface)

Note – Performing this task on an already active HTTPS server effectively resets the server.

---

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.
2. **Click the Configuration tab.**
3. **Click the System Management Access subtab.**
4. **Click the Web Server subtab.**

   The Web Server Settings window opens.

5. **Check the Enabled box for the HTTPS web server.**
6. **Type the web server port into the HTTPS Port field.**
7. **Click Save.**

Related Information

- "Enable the HTTPS Service (CLI)" on page 51
- "Display the HTTPS Service Status (Web Interface)" on page 82
- "Disable the HTTPS Service (Web Interface)" on page 100

▼ Install a Custom SSL Certificate (Web Interface)

1. **Access the ILOM web interface.**
   See "Access ILOM From the Web Interface" on page 77.
2. **Click the Configuration tab.**
3. **Click the System Management Access subtab.**
4. **Click the SSL Certificate subtab.**
   The SSL Certificate Upload window opens.
5. **Under Custom Certificate, click Load.**
   The Custom Certificate Upload window opens.
6. **Select the transfer protocol from the Transfer Method pull-down menu.**
7. **For the protocol selected, provide the file, host IP address, file path, user name, and password into the respective fields.**
8. **Click Load.**
   The custom certificate is loaded and the window closes.

Related Information

- "Install a Custom SSL Certificate (CLI)" on page 52
- "Display the SSL Certificates (Web Interface)" on page 83
- "Remove the Custom SSL Certificate (Web Interface)" on page 99

▼ Remove the Custom SSL Certificate (Web Interface)

1. **Access the ILOM web interface.**
   See "Access ILOM From the Web Interface" on page 77.

2. **Click the Configuration tab.**
3. **Click the System Management Access subtab.**
4. **Click the SSL Certificate subtab.**

   The SSL Certificate Upload window opens.
5. **Under Custom Certificate, click Remove.**

   A dialog box opens and asks for you to confirm.
6. **Click OK.**

   The custom SSL certificate is removed.

Related Information

- "Remove the Custom SSL Certificate (CLI)" on page 53
- "Display the SSL Certificates (Web Interface)" on page 83
- "Install a Custom SSL Certificate (Web Interface)" on page 99

▼ Disable the HTTPS Service (Web Interface)

Note – Performing this task on an already active HTTPS server effectively resets the server.

---

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.
2. **Click the Configuration tab.**
3. **Click the System Management Access subtab.**
4. **Click the Web Server subtab.**

   The Web Server Settings window opens.
5. **Uncheck the Enabled box for the HTTPS web server.**
6. **Click Save.**

Related Information

- "Disable the HTTPS Service (CLI)" on page 53
- "Display the HTTPS Service Status (Web Interface)" on page 82
- "Enable the HTTPS Service (Web Interface)" on page 98

Managing SNMP Services (Web Interface)

These tasks help you manage the ILOM SNMP service targets.

Related Information

- "Managing SNMP Services (CLI)" on page 54
- "Managing HTTP Services (Web Interface)" on page 96
- "Managing HTTPS Services (Web Interface)" on page 98

▼ Enable the SNMP Service (Web Interface)

1. **Access the ILOM web interface.**
   See "Access ILOM From the Web Interface" on page 77.
2. **Click the Configuration tab.**
3. **Click the System Management Access subtab.**
4. **Click the SNMP subtab.**
   The SNMP Management window opens.
5. **Under Settings, check the Enabled box for State.**
6. **Click Save.**
   The SNMP server is enabled.

Related Information

- "Enable the SNMP Service (CLI)" on page 55
- "Display the SNMP Service Status (Web Interface)" on page 83

- "Disable the SNMP Service (Web Interface)" on page 107

▼ Configure the SNMP Service (Web Interface)

1. **Access the ILOM web interface.**
   See "Access ILOM From the Web Interface" on page 77.
2. **Click the Configuration tab.**
3. **Click the System Management Access subtab.**
4. **Click the SNMP subtab.**
   The SNMP Management window opens.
5. **Type the port number into the Port field.**
6. **Check the Enabled box for Set Requests to enable set requests.**
7. **Check the boxes for the protocols you want to enable.**
8. **Click Save.**

Related Information

- "Configure the SNMP Service (CLI)" on page 55

▼ Add SNMP Service User Accounts (Web Interface)

1. **Access the ILOM web interface.**
   See "Access ILOM From the Web Interface" on page 77.
2. **Click the Configuration tab.**
3. **Click the System Management Access subtab.**
4. **Click the SNMP subtab.**
   The SNMP Management window opens.
5. **Click the Users link.**
   The page scrolls to the SNMP Users table.
6. **In the SNMP Users table, click Add.**
   A new window opens.
7. **Type the user name into the User Name field.**

8. **Select the authentication protocol from the Authentication Protocol pull-down menu.**
9. **Type the authentication password into the Authentication Password field.**
10. **Type the password again into the Confirm Password field.**
11. **Select the user permissions from the Permission pull-down menu.**
12. **(Optional) Select the privacy protocol from the Privacy Protocol pull down menu.**
13. **If required, type the privacy password into the Privacy Password field.**
14. **Type the password again into the Confirm Password field.**
15. **Click Save.**

    The user is created and the window closes.

Related Information

- "Add SNMP Service User Accounts (CLI)" on page 56
- "Display the SNMP Service User Accounts (Web Interface)" on page 84
- "Delete SNMP Service User Accounts (Web Interface)" on page 104

▼ Modify SNMP Service User Accounts (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.
2. **Click the Configuration tab.**
3. **Click the System Management Access subtab.**
4. **Click the SNMP subtab.**

   The SNMP Management window opens.
5. **Click the Users link.**

   The page scrolls to the SNMP Users table.
6. **In the SNMP Users table, select the user to modify and click Edit.**

   A new window opens.
7. **Select the authentication protocol from the Authentication Protocol pull-down menu.**
8. **Type the authentication password into the Authentication Password field.**

9. **Type the password again into the Confirm Password field.**
10. **Select the user permissions from the Permission pull-down menu.**
11. **(Optional) Select the privacy protocol from the Privacy Protocol pull down menu.**
12. **If required, type the privacy password into the Privacy Password field.**
13. **Type the password again into the Confirm Password field.**
14. **Click Save.**

    The user is modified and the window closes.

Related Information

- "Modify SNMP Service User Accounts (CLI)" on page 57
- "Modify SNMP Service Communities (Web Interface)" on page 105

▼ Delete SNMP Service User Accounts (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.
2. **Click the Configuration tab.**
3. **Click the System Management Access subtab.**
4. **Click the SNMP subtab.**

   The SNMP Management window opens.
5. **Click the Users link.**

   The page scrolls to the SNMP Users table.
6. **Select the user to delete and click Delete.**

   A dialog box opens and asks you to confirm.
7. **Click OK.**

   The user is deleted.

Related Information

- "Delete SNMP Service User Accounts (CLI)" on page 58
- "Display the SNMP Service User Accounts (Web Interface)" on page 84
- "Add SNMP Service User Accounts (Web Interface)" on page 102

▼ Add SNMP Service Communities (Web Interface)

1. **Access the ILOM web interface.**
   See "Access ILOM From the Web Interface" on page 77.
2. **Click the Configuration tab.**
3. **Click the System Management Access subtab.**
4. **Click the SNMP subtab.**
   The SNMP Management window opens.
5. **Click the Communities link.**
   The page scrolls to the SNMP Communities table.
6. **In the SNMP Communities table, click Add.**
   A new window opens.
7. **Type the community name into the Community Name field.**
8. **Select the permissions from the Permission pull-down menu.**
9. **Click Save.**
   The community is created and the window closes.

Related Information

- "Add SNMP Service Communities (CLI)" on page 59
- "Display the SNMP Service Communities (Web Interface)" on page 84
- "Delete SNMP Service Communities (Web Interface)" on page 106

▼ Modify SNMP Service Communities (Web Interface)

1. **Access the ILOM web interface.**
   See "Access ILOM From the Web Interface" on page 77.
2. **Click the Configuration tab.**
3. **Click the System Management Access subtab.**
4. **Click the SNMP subtab.**
   The SNMP Management window opens.
5. **Click the Communities link.**
   The page scrolls to the SNMP Communities table.

6. **In the SNMP Communities table, select the community to modify and click Edit.**

   A new window opens.

7. **Select the permissions from the Permission pull-down menu.**

8. **Click Save.**

   The community is created and the window closes.

Related Information

- "Modify SNMP Service Communities (CLI)" on page 59
- "Modify SNMP Service User Accounts (Web Interface)" on page 103

▼ Delete SNMP Service Communities (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

2. **Click the Configuration tab.**

3. **Click the System Management Access subtab.**

4. **Click the SNMP subtab.**

   The SNMP Management window opens.

5. **Click the Communities link.**

   The page scrolls to the SNMP Communities table.

6. **Select the community to delete and click Delete.**

   A dialog box opens and asks you to confirm.

7. **Click OK.**

   The community is deleted.

Related Information

- "Delete SNMP Service Communities (CLI)" on page 60
- "Display the SNMP Service Communities (Web Interface)" on page 84
- "Add SNMP Service Communities (Web Interface)" on page 105

▼ Back Up SNMP Service MIBs (Web Interface)

This procedure creates a compressed file, `ilom-mibs.zip`, which contains the following MIBs:

- `ENTITY-MIB.mib`
- `SUN-HW-CTRL-MIB.mib`
- `SUN-HW-TRAP-MIB.mib`
- `SUN-ILOM-CONTROL-MIB.mib`
- `SUN-PLATFORM-MIB.mib`

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

2. **Click the Configuration tab.**
3. **Click the System Management Access subtab.**
4. **Click the SNMP subtab.**

   The SNMP Management window opens.

5. **Click the MIBs link.**

   The page scrolls to MIBs.

6. **Click Download.**

   Depending upon how your web browser is configured, you might either open the file, or save the file.

Related Information

- "Back Up SNMP Service MIBs (CLI)" on page 61

▼ Disable the SNMP Service (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

2. **Click the Configuration tab.**
3. **Click the System Management Access subtab.**
4. **Click the SNMP subtab.**

   The SNMP Management window opens.

5. **Under Settings, uncheck the Enabled box for State.**

6. **Click Save.**

   The SNMP server is disabled.

Related Information

- "Disable the SNMP Service (CLI)" on page 61
- "Display the SNMP Service Status (Web Interface)" on page 83
- "Enable the SNMP Service (Web Interface)" on page 101

Managing Other Aspects (Web Interface)

These tasks help you manage other aspects of ILOM.

- "Enable Alerts to Send SNMP Traps (Web Interface)" on page 108
- "Enable Alerts to Send PET (Web Interface)" on page 109
- "Disable Alerts (Web Interface)" on page 110
- "Set the ILOM CLI Session Timeout (Web Interface)" on page 110

Related Information

- "Managing Other Aspects (CLI)" on page 62
- "Managing Other Aspects (SNMP)" on page 131
- "Performing General Tasks on ILOM Targets (Web Interface)" on page 89

▼ Enable Alerts to Send SNMP Traps (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

2. **Click the Configuration tab.**
3. **Click the Alert Management subtab.**

   The Alert Settings window opens.

4. **In the Alerts table, select the alert to enable and click Edit.**

   A new window opens.

5. **Select the alert level from the Level pull-down menu.**
6. **Select the SNMP Trap alert type from the Type pull-down menu.**
7. **Type the SNMP trap destination address or host name into the Address field.**

8. **Select the SNMP version from the SNMP Version pull-down menu.**
9. **Type the SNMP community name into the Community Name field.**
10. **Click Save.**

    The alert is enabled.

Related Information

- "Enable Alerts to Send SNMP Traps (CLI)" on page 62
- "Enable Alerts to Send SNMP Traps (SNMP)" on page 132
- "Display the Alert Properties (Web Interface)" on page 85
- "Disable Alerts (Web Interface)" on page 110

▼ Enable Alerts to Send PET (Web Interface)

1. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.
2. **Click the Configuration tab.**
3. **Click the Alert Management subtab.**

   The Alert Settings window opens.
4. **In the Alerts table, select the alert to modify and click Edit.**

   A new window opens.
5. **Select the alert level from the Level pull-down menu.**
6. **Select the IPMI PET alert type from the Type pull-down menu.**
7. **Type the IPMI PET destination IP address into the IP Address field.**
8. **Click Save.**

   The alert is enabled.

Related Information

- "Enable Alerts to Send PET (CLI)" on page 63
- "Modify Alert SNMP Version (SNMP)" on page 133
- "Display the Alert Properties (Web Interface)" on page 85
- "Disable Alerts (Web Interface)" on page 110

▼ Disable Alerts (Web Interface)

1. **Access the ILOM web interface.**
   See "Access ILOM From the Web Interface" on page 77.
2. **Click the Configuration tab.**
3. **Click the Alert Management subtab.**
   The Alert Settings window opens.
4. **In the Alerts table, select the alert to disable and click Edit.**
   A new window opens.
5. **Select the Disable level from the Level pull-down menu.**
6. **Click Save.**
   The alert is disabled.

Related Information

- "Disable Alerts (CLI)" on page 64
- "Disable Alerts (SNMP)" on page 134
- "Display the Alert Properties (Web Interface)" on page 85
- "Enable Alerts to Send SNMP Traps (Web Interface)" on page 108

▼ Set the ILOM CLI Session Timeout (Web Interface)

1. **Access the ILOM web interface.**
   See "Access ILOM From the Web Interface" on page 77.
2. **Click the Configuration tab.**
3. **Click the System Management Access subtab.**
4. **Click the CLI subtab.**
   The CLI Settings window opens.
5. **Check the Enabled box for Session timeout and type the number of minutes into the Minutes field.**
6. **Click Save.**

Related Information

- "Set the ILOM CLI Session Timeout (CLI)" on page 65
- "Display the ILOM CLI Session Timeout (Web Interface)" on page 87

Upgrading the Switch Firmware Through ILOM (Web Interface)

One of the advantages of ILOM support on the CMCs is that all firmware upgrades, including upgrades for H8 and I4, have been simplified into a four-task process.

These topics enable you to upgrade the switch firmware through the ILOM CLI.

Related Information

- "Upgrading the Switch Firmware Through ILOM (CLI)" on page 66

▼ Upgrade the Switch Firmware (Web Interface)

1. **Install the `flint` application.**

   See "Install the `flint` Application (CLI)" on page 67.

2. **Download the Switch Firmware Package.**

   See "Download the Switch Firmware Package (CLI)" on page 68.

3. **Set the component firmware to upgrade.**

   See "Set Component Firmware to Upgrade (CLI)" on page 69.

4. **Access the ILOM web interface.**

   See "Access ILOM From the Web Interface" on page 77.

5. **Click the Maintenance tab.**

6. **Click the Firmware Upgrade subtab.**

   The Firmware Upgrade window opens.

7. **Click Enter Upgrade Mode.**

   A dialog box opens and asks you to confirm.

8. **Click OK.**

   A secondFirmware Upgrade window opens.

9. **Click Specify URL.**

   Type the URL of the location of the firmware package on the firmware server.

10. **Click Upload.**

    The firmware package is uploaded to the shelf manager.

    ILOM verifies the firmware package integrity and a new window displays the current firmware version and the version of the firmware package. Addtionally, two check boxes are displayed:

    - If the ILOM configuration should be preserved during upgrade, click the appropriate box
    - If an outside the InfiniBand fabric method of upgrade should be used if the within the InfiniBand fabric upgrade fails, click the appropriate box.

Note – An upgrade outside of the InfiniBand fabric can take many hours.

---

11. **Click Start Upgrade.**

    A dialog box opens and asks you to confirm.

12. **Click OK.**

    The firmware is upgraded.

    When the firmware upgrade ends, a summary is displayed.

13. **Click OK.**

    A final status report is displayed.

14. **Click Reconnect.**

Note – If the shelf manager firmware was upgraded, the shelf manager reboots. You must log in again to access the shelf manager

---

Related Information

- "Upgrade the Switch Firmware (CLI)" on page 71

Administering ILOM (SNMP)

These topics describe how to administer ILOM through the Simple Network Management Protocol (SNMP).

Related Information

- "Understanding ILOM on the Switch" on page 1
- "Administering ILOM (CLI)" on page 21
- "Administering ILOM (Web Interface)" on page 75
- "Administering Hardware (IPMI)" on page 135
- "Understanding ILOM Commands" on page 139

SNMP Overview

The ILOM implementation on the management controller within the switch can communicate the state of and enable remote management of ILOM through the Simple Network Management Protocol (SNMP).

An SNMP client is required to interface with the ILOM SNMP agent on the management controller. The SNMP client must have the ILOM MIBs installed. These MIBs are included in the `SUN_DCS_648_ADDBLDRC2.tar.gz` file, which is part of the ILOM firmware package that you downloaded. See "Installing the ILOM Firmware" on page 13.

For more information about and use of SNMP with ILOM, refer to the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Guide*, 820-6413, available online at:

(http://docs.sun.com/app/docs/prod/int.lights.mgr30)

Related Information

- "SNMP Commands" on page 114
- "Monitoring ILOM Targets (SNMP)" on page 115
- "Controlling ILOM Targets (SNMP)" on page 125
- "CLI Overview" on page 21
- "Web Interface Overview" on page 75
- "`ipmitool` Overview" on page 135

SNMP Commands

You can use several SNMP commands to perform tasks:

- `snmpget` – Returns the value of an SNMP variable.
- `snmpset` – Sets the value of an SNMP variable.
- `snmpwalk` – Returns values for multiple SNMP variables.

These commands assume that the `v2c` and sets properties are enabled in the ILOM SNMP service and that the SNMP community `public` has `rw` permission. Commands are provided in this format:

`$` *command* `-v2c -c public` *mc_IP MIB_name*`::`*parameter*

where:

- *command* is one of the commands previously discussed.
- *mc_IP* is the IP address of the management controller.
- *MIB_name* is the name of the MIB. For example:
  - `SUN-ILOM-CONTROL-MIB`
  - `ENTITY-MIB`
  - `SUN-PLATFORM-MIB`
- *parameter* is the aspect of ILOM that is to be acted upon.

Note – Type the management controller IP address in place of the characters "*mc_IP*".

Related Information

- “Monitoring ILOM Targets (SNMP)” on page 115
- “Controlling ILOM Targets (SNMP)” on page 125
- “Understanding ILOM Commands” on page 139

Monitoring ILOM Targets (SNMP)

These topics enable you to display the status of many ILOM targets.

- “Performing Daily Tasks (SNMP)” on page 115
- “Checking the Status of Services (SNMP)” on page 119
- “Verifying Other Aspects (SNMP)” on page 120

Related Information

- “Monitoring ILOM Targets (CLI)” on page 25
- “Monitoring ILOM Targets (Web Interface)” on page 78
- “Controlling ILOM Targets (SNMP)” on page 125

Performing Daily Tasks (SNMP)

These tasks help you see the status of ILOM targets that are continually changing.

- “Display the Date and Time (SNMP)” on page 116
- “Display the Time Zone (SNMP)” on page 116
- “Display the Aggregate Sensor State (SNMP)” on page 116
- “Display the Aggregate Sensor Status (SNMP)” on page 117
- “Display ILOM Sessions (SNMP)” on page 117
- “Display the ILOM Event Log (SNMP)” on page 118

Related Information

- “Checking the Status of Services (SNMP)” on page 119
- “Verifying Other Aspects (SNMP)” on page 120

▼ Display the Date and Time (SNMP)

- **From the SNMP client, type:**

```
$ snmpget -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlDateAndTime.0
SUN-ILOM-CONTROL-MIB::ilomCtrlDateAndTime.0 = STRING: 2010-1-20,12:19:19.0
$
```

Related Information

- "Display the Date, Time, and Time Zone (CLI)" on page 26
- "Display the Date, Time, and Time Zone (Web Interface)" on page 79
- "Display the Time Zone (SNMP)" on page 116

▼ Display the Time Zone (SNMP)

- **From the SNMP client, type:**

```
$ snmpget -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlTimezone.0
SUN-ILOM-CONTROL-MIB::ilomCtrlTimezone.0 = STRING: PST (US/Pacific)
$
```

Related Information

- "Display the Date, Time, and Time Zone (CLI)" on page 26
- "Display the Date, Time, and Time Zone (Web Interface)" on page 79
- "Display the Date and Time (SNMP)" on page 116

▼ Display the Aggregate Sensor State (SNMP)

- **From the SNMP client, type:**

```
$ snmpwalk -v2c -c public mc_IP SUN-PLATFORM-MIB::sunPlatDiscreteSensorTable
SUN-PLATFORM-MIB::sunPlatDiscreteSensorCurrent.3 = INTEGER: 1
$
```

In the output, `INTEGER: 1` means the sensor is in `Deasserted` state. `INTEGER: 2` means the sensor is in `Asserted` state.

Related Information

- "Display the Aggregate Sensor State (CLI)" on page 27
- "Display the Aggregate Sensor State (Web Interface)" on page 80

- "Display the Sensor State (IPMI)" on page 136
- "Display the Sensor Entities (SNMP)" on page 125
- "Display the Aggregate Sensor Status (SNMP)" on page 117

▼ Display the Aggregate Sensor Status (SNMP)

- **From the SNMP client, type:**

```
$ snmpwalk -v2c -c public mc_IP SUN-PLATFORM-MIB::sunPlatEquipmentAlarmStatus.3
SUN-PLATFORM-MIB::sunPlatEquipmentAlarmStatus.3 = INTEGER: cleared(7)
$
```

In the output, `INTEGER: cleared` means the sensor is clear. `INTEGER: major` means the sensor is in an alarm state.

Related Information

- "Display the Aggregate Sensor State (SNMP)" on page 116
- "Display the Sensor Entities (SNMP)" on page 125

▼ Display ILOM Sessions (SNMP)

- **From the SNMP client, type:**

```
$ snmpwalk -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlSessions
SUN-ILOM-CONTROL-MIB::ilomCtrlSessionsUsername.154 = STRING: root
SUN-ILOM-CONTROL-MIB::ilomCtrlSessionsUsername.155 = STRING: root
SUN-ILOM-CONTROL-MIB::ilomCtrlSessionsConnectionType.154 = INTEGER: shell(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlSessionsConnectionType.155 = INTEGER: other(3)
SUN-ILOM-CONTROL-MIB::ilomCtrlSessionsLoginTime.154 = STRING:
2009-5-15,13:44:31.0
SUN-ILOM-CONTROL-MIB::ilomCtrlSessionsLoginTime.155 = STRING:
2009-5-15,13:44:38.0
$
```

The output displays two users. Both users are the `root` user and one is using the CLI interface.

Related Information

- "Display the ILOM Sessions (CLI)" on page 27
- "Display the ILOM Sessions (Web Interface)" on page 80
- "Display ILOM User Accounts (SNMP)" on page 121

▼ Display the ILOM Event Log (SNMP)

The event log displays:

- type
- timestamp
- class
- severity
- description

- **From the SNMP client, type:**

```
$ snmpwalk -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogTable
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogType.1 = INTEGER: log(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogType.2 = INTEGER: log(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogType.3 = INTEGER: log(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogTimestamp.1 = STRING:
2009-5-14,10:10:52.0
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogTimestamp.2 = STRING:
2009-5-14,10:40:7.0
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogTimestamp.3 = STRING:
2009-5-15,13:15:0.0
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogClass.1 = INTEGER: audit(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogClass.2 = INTEGER: audit(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogClass.3 = INTEGER: audit(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogSeverity.1 = INTEGER: minor(4)
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogSeverity.2 = INTEGER: minor(4)
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogSeverity.3 = INTEGER: minor(4)
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogClass.3 = INTEGER: audit(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogClass.4 = INTEGER: audit(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogClass.5 = INTEGER: audit(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogSeverity.1 = INTEGER: minor(4)
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogSeverity.2 = INTEGER: minor(4)
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogSeverity.3 = INTEGER: minor(4)
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogDescription.1 = STRING: root : Open
Session : object = /session/type : value = shell : success
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogDescription.2 = STRING: root : Close
Session : object = /session/type : value = shell : success
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogDescription.3 = STRING: public : Set :
object = /clock/datetime : value = 051513152009.00 : success
$
```

Related Information

- "Display the ILOM Event Log (CLI)" on page 28
- "Display the ILOM Event Log (Web Interface)" on page 81
- "Display the System Event Log (IPMI)" on page 138

- "Clear the ILOM Event Log (SNMP)" on page 127
- "Set the Remote Log Hosts (SNMP)" on page 127

Checking the Status of Services (SNMP)

These topics enable you to display the status of the many services supported by ILOM.

- "Display the HTTP Service Status (SNMP)" on page 119
- "Display the HTTPS Service Status (SNMP)" on page 119

Related Information

- "Performing Daily Tasks (SNMP)" on page 115
- "Verifying Other Aspects (SNMP)" on page 120

▼ Display the HTTP Service Status (SNMP)

- **From the SNMP client, type:**

```
$ snmpwalk -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlHttp
SUN-ILOM-CONTROL-MIB::ilomCtrlHttpEnabled.0 = INTEGER: false(2)
SUN-ILOM-CONTROL-MIB::ilomCtrlHttpPortNumber.0 = INTEGER: 80
SUN-ILOM-CONTROL-MIB::ilomCtrlHttpSecureRedirect.0 = INTEGER: true(1)
$
```

Related Information

- "Display the HTTP Service Status (CLI)" on page 30
- "Display the HTTP Service Status (Web Interface)" on page 82
- "Display the HTTPS Service Status (SNMP)" on page 119
- "Set the HTTP Service State (SNMP)" on page 132

▼ Display the HTTPS Service Status (SNMP)

- **From the SNMP client, type:**

```
$ snmpwalk -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlHttps
SUN-ILOM-CONTROL-MIB::ilomCtrlHttpsEnabled.0 = INTEGER: true(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlHttpsPortNumber.0 = INTEGER: 443
$
```

Related Information

- "Display the HTTPS Service Status (CLI)" on page 30
- "Display the HTTPS Service Status (Web Interface)" on page 82
- "Display the HTTP Service Status (SNMP)" on page 119

Verifying Other Aspects (SNMP)

These tasks display the status of other aspects of ILOM.

- "Display the Alert Properties (SNMP)" on page 120
- "Display ILOM User Accounts (SNMP)" on page 121
- "Display the Remote Log Hosts (SNMP)" on page 122
- "Display the Network Management Configuration (SNMP)" on page 123
- "Display the System Components (SNMP)" on page 123
- "Display the Additional System Component Information (SNMP)" on page 124
- "Display the Sensor Entities (SNMP)" on page 125

Related Information

- "Performing Daily Tasks (SNMP)" on page 115
- "Checking the Status of Services (SNMP)" on page 119

▼ Display the Alert Properties (SNMP)

Alerts can provide advance notice of a system failure. The ILOM implementation in the management controller supports 15 alert rules, which configure alert properties. Supported alert types are SNMP trap and PET. The alert destination must have the relevant ILOM MIBs installed and must support SNMP traps or PETs.

- **From the SNMP client, type:**

```
$ snmpwalk -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlAlerts
SUN-ILOM-CONTROL-MIB::ilomCtrlAlerts
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSeverity.1 = INTEGER: major(3)
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSeverity.2 = INTEGER: critical(2)
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSeverity.3 = INTEGER: disable(1)
.
.
.
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSeverity.14 = INTEGER: disable(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSeverity.15 = INTEGER: disable(1)
```

```
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertType.1 = INTEGER: snmptrap(2)
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertType.2 = INTEGER: snmptrap(2)
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertType.3 = INTEGER: snmptrap(2)
.
.
.
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertType.14 = INTEGER: snmptrap(2)
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertType.15 = INTEGER: snmptrap(2)
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertDestinationIP.2 = IpAddress: 10.60.33.40
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertDestinationIP.3 = IpAddress: 0.0.0.0
.
.
.
$
```

Note – The output seen in the example is a portion of the full output and might be different for your environment.

Related Information

- "Display the Alert Properties (CLI)" on page 36
- "Display the Alert Properties (Web Interface)" on page 85
- "Enable Alerts to Send SNMP Traps (SNMP)" on page 132
- "Modify Alert SNMP Version (SNMP)" on page 133
- "Disable Alerts (SNMP)" on page 134

▼ Display ILOM User Accounts (SNMP)

- **From the SNMP client, type:**

```
$ snmpwalk -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserTable
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserPassword."root" = STRING: "(Not
Viewable)"
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserPassword."user1" = STRING: "(Not
Viewable)"
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserPassword."user2" = STRING: "(Not
Viewable)"
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserRoles."root" = STRING: "aucro"
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserRoles."user1" = STRING: "aucros"
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserRoles."user2" = STRING: "o"
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserRowStatus."root" = INTEGER: active(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserRowStatus."user1" = INTEGER: active(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserRowStatus."user2" = INTEGER: active(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserCLIMode."root" = INTEGER: default(1)
```

```
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserCLIMode."user1" = INTEGER: default(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserCLIMode."user2" = INTEGER: default(1)
$
```

Note – The output identifies three users. Of them, users `root` and `user1` have an administrative role.

Related Information

- "Display the ILOM User Accounts (CLI)" on page 37
- "Display the ILOM User Accounts (Web Interface)" on page 86
- "Add an ILOM User Account (SNMP)" on page 130
- "Delete an ILOM User Account (SNMP)" on page 131

▼ Display the Remote Log Hosts (SNMP)

- **From the SNMP client, type:**

```
$ snmpget -v2c -c public mc_IP
SUN-ILOM-CONTROL-MIB::ilomCtrlRemoteSyslogDestnumber.0
```

wher *number* is the number of the remote log host. For example:

```
$ snmpget -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlRemoteSyslogDest1.0
SUN-ILOM-CONTROL-MIB::ilomCtrlRemoteSyslogDest1.0 = IpAddress: 123.45.67.89
$
```

Related Information

- "Display the Remote Log Hosts (CLI)" on page 38
- "Display the Remote Log Hosts (Web Interface)" on page 87
- "Set the Remote Log Hosts (SNMP)" on page 127

▼ Display the Network Management Configuration (SNMP)

- **From the SNMP client, type:**

```
$ snmpwalk -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlNetwork
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkMacAddress."SP/network" = STRING:
46:46:41:39:00:FF
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkIpDiscovery."SP/network" = INTEGER:
static(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkIpAddress."SP/network" = IpAddress:
123.45.67.89
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkIpGateway."SP/network" = IpAddress:
123.45.67.5
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkIpNetmask."SP/network" = IpAddress:
255.255.255.0
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkPendingIpDiscovery."SP/network" =
INTEGER: static(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkPendingIpAddress."SP/network" =
IpAddress: 123.45.67.89
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkPendingIpGateway."SP/network" =
IpAddress: 123.45.67.5
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkPendingIpNetmask."SP/network" =
IpAddress: 255.255.255.0
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkCommitPending."SP/network" = INTEGER:
false(2)
$
```

Related Information

- "Display the Network Management Configuration (CLI)" on page 38
- "Display the Network Management Configuration (Web Interface)" on page 87
- "Set the Network Management Parameters (SNMP)" on page 128

▼ Display the System Components (SNMP)

The ENTITY-MIB and SUN-PLATFORM-MIB MIBs are used to view system components.

1. **From the SNMP client, display the physical entities:**

```
$ snmpwalk -v2c -c public mc_IP ENTITY-MIB::entPhysicalName
ENTITY-MIB::entPhysicalName.1 = STRING: /SYS
ENTITY-MIB::entPhysicalName.2 = STRING: /SYS/ShM_CLI
ENTITY-MIB::entPhysicalName.3 = STRING: /SYS/CHASSIS_STATUS
$
```

The output contains three entities.

2. **Display the physical entity descriptions:**

```
$ snmpwalk -v2c -c public mc_IP ENTITY-MIB::entPhysicalDescr
ENTITY-MIB::entPhysicalDescr.1 = STRING:  Sun Datacenter Switch DCS 648 -
Chassis
ENTITY-MIB::entPhysicalDescr.2 = STRING: Container
ENTITY-MIB::entPhysicalDescr.3 = STRING: Fault Sensor
$
```

The output contains descriptions for the three entities.

3. **Display the physical entity classes:**

```
$ snmpwalk -v2c -c public mc_IP ENTITY-MIB::entPhysicalClass
ENTITY-MIB::entPhysicalClass.1 = INTEGER: chassis(3)
ENTITY-MIB::entPhysicalClass.2 = INTEGER: other(1)
ENTITY-MIB::entPhysicalClass.3 = INTEGER: sensor(8)
$
```

The output contains the classes for the three entities.

Related Information

- "Display the Additional System Component Information (SNMP)" on page 124

▼ Display the Additional System Component Information (SNMP)

- **From the SNMP client, type:**

```
$ snmpwalk -v2c -c public mc_IP SUN-PLATFORM-MIB::sunPlatEquipmentTable
SUN-PLATFORM-MIB::sunPlatEquipmentAdministrativeState.1 = INTEGER: unlocked(2)
SUN-PLATFORM-MIB::sunPlatEquipmentAdministrativeState.2 = INTEGER: unlocked(2)
SUN-PLATFORM-MIB::sunPlatEquipmentOperationalState.1 = INTEGER: enabled(2)
SUN-PLATFORM-MIB::sunPlatEquipmentOperationalState.2 = INTEGER: enabled(2)
```

```
SUN-PLATFORM-MIB::sunPlatEquipmentAlarmStatus.1 = INTEGER: indeterminate(4)
SUN-PLATFORM-MIB::sunPlatEquipmentAlarmStatus.2 = INTEGER: cleared(7)
SUN-PLATFORM-MIB::sunPlatEquipmentUnknownStatus.1 = INTEGER: false(2)
SUN-PLATFORM-MIB::sunPlatEquipmentUnknownStatus.2 = INTEGER: false(2)
SUN-PLATFORM-MIB::sunPlatEquipmentLocationName.1 = STRING: unknown
SUN-PLATFORM-MIB::sunPlatEquipmentLocationName.2 = STRING: /SYS
$
```

Note – The output is ordered for the two entities.

Related Information

- "Display the System Components (SNMP)" on page 123

▼ Display the Sensor Entities (SNMP)

There is currently one discrete OEM sensor, the aggregate sensor.

- **From the SNMP client, type:**

```
$ snmpwalk -v2c -c public mc_IP SUN-PLATFORM-MIB::sunPlatSensorTable
SUN-PLATFORM-MIB::sunPlatSensorClass.2 = INTEGER: discrete(3)
SUN-PLATFORM-MIB::sunPlatSensorType.2 = INTEGER: other(1)
SUN-PLATFORM-MIB::sunPlatSensorLatency.2 = Gauge32: 0 milliseconds
$
```

Related Information

- "Display the Aggregate Sensor State (SNMP)" on page 116
- "Display the Aggregate Sensor Status (SNMP)" on page 117

Controlling ILOM Targets (SNMP)

These topics enable you to change the behavior or configuration of many ILOM targets.

- "Performing General Tasks on ILOM Targets (SNMP)" on page 126
- "Performing ILOM User Tasks (SNMP)" on page 129
- "Managing Other Aspects (SNMP)" on page 131

Related Information

- "Controlling ILOM Targets (CLI)" on page 41
- "Controlling ILOM Targets (Web Interface)" on page 89
- "Monitoring ILOM Targets (SNMP)" on page 115

Performing General Tasks on ILOM Targets (SNMP)

You can perform these tasks periodically on a few ILOM targets.

- "Set the Date and Time (SNMP)" on page 126
- "Clear the ILOM Event Log (SNMP)" on page 127
- "Set the Remote Log Hosts (SNMP)" on page 127
- "Set the Network Management Parameters (SNMP)" on page 128

Related Information

- "Performing ILOM User Tasks (SNMP)" on page 129
- "Managing Other Aspects (SNMP)" on page 131

▼ Set the Date and Time (SNMP)

- **From the SNMP client, type:**

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlDateAndTime.0 s
"YYYY-MM-DD,hh:mm:ss.0"
```

where *YYYY-MM-DD,hh:mm:ss* is the year as four digits, and the month, date, hour, minute, and seconds as two digits.

For example:

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlDateAndTime.0 s
"2010-1-28,13:24:31.0"
SUN-ILOM-CONTROL-MIB::ilomCtrlDateAndTime.0 = STRING: 2010-1-28,13:24:31.0
$
```

Related Information

- "Set the Date, Time, and Time Zone (CLI)" on page 42
- "Set the Date and Time (Web Interface)" on page 90

- "Display the Date and Time (SNMP)" on page 116

▼ Clear the ILOM Event Log (SNMP)

- **From the SNMP client, type:**

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogClear.0 i 1
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogClear.0 = INTEGER: true(1)
$
```

Related Information

- "Clear the ILOM Event Log (CLI)" on page 42
- "Clear the ILOM Event Log (Web Interface)" on page 91
- "Display the ILOM Event Log (SNMP)" on page 118
- "Set the Remote Log Hosts (SNMP)" on page 127

▼ Set the Remote Log Hosts (SNMP)

The ILOM implementation in the management controller provides a protocol for transmitting ILOM events to a remote log host. The events transmitted are similar to those displayed in the local log.

- **From the SNMP client, type:**

```
$ snmpset -v2c -c public mc_IP
SUN-ILOM-CONTROL-MIB::ilomCtrlRemoteSyslogDestnumber.0 a "IP_address"
```

where:

- *number* is the number of the remote log host.
- *IP_address* is the IP address of the remote log host.

For example, to set the IP address of remote log host 2:

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlRemoteSyslogDest2.0
a "123.45.67.90"
SUN-ILOM-CONTROL-MIB::ilomCtrlRemoteSyslogDest2.0 = IpAddress: 123.45.67.90
$
```

Note – Setting a remote log host IP address to 0.0.0.0 disables that functionality.

Related Information

- "Display the Remote Log Hosts (SNMP)" on page 122

▼ Set the Network Management Parameters (SNMP)

1. **From the SNMP client, set the network parameter:**

```
$ snmpset -v2c -c public mc_IP
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkPendingIpparameter.\"SP/network\" a "value"
```

where:

- *parameter* is the network parameter to configure:
  - `Discovery` – The IP address discovery method, `static` or `dhcp`.
  - `Address` – The IP address of the managment controller, should static discovery be configured.
  - `Gateway` – The IP address of the subnet gateway.
  - `Netmask` – The netmask for the subnet.
- *value* is the value of the parameter

For example, to set the network netmask:

```
$ snmpset -v2c -c public mc_IP
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkPendingIpNetmask.\"SP/network\" a
"255.255.0.0"
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkPendingIpNetmask."SP/network" = IpAddress:
255.255.0.0
$
```

2. **Commit the pending netmask:**

```
$ snmpset -v2c -c public mc_IP
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkCommitPending.\"SP/network\" i 1
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkCommitPending."SP/network" = INTEGER:
true(1)
$
```

3. **Verify the netmask:**

```
$ snmpwalk -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlNetwork
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkMacAddress."SP/network" = STRING:
46:46:41:39:00:FF
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkIpDiscovery."SP/network" = INTEGER:
static(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkIpAddress."SP/network" = IpAddress:
123.45.67.89
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkIpGateway."SP/network" = IpAddress:
123.45.67.5
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkIpNetmask."SP/network" = IpAddress:
255.255.0.0
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkPendingIpDiscovery."SP/network" =
INTEGER: static(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkPendingIpAddress."SP/network" =
IpAddress: 123.45.67.89
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkPendingIpGateway."SP/network" =
IpAddress: 123.45.67.5
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkPendingIpNetmask."SP/network" =
IpAddress: 255.255.0.0
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkCommitPending."SP/network" = INTEGER:
false(2)
$
```

Related Information

- "Set the Network Management Parameters (CLI)" on page 45
- "Set the Network Management Parameters (Web Interface)" on page 93
- "Display the Network Management Configuration (SNMP)" on page 123

Performing ILOM User Tasks (SNMP)

These tasks enable you to add and delete ILOM users.

- "Add an ILOM User Account (SNMP)" on page 130
- "Delete an ILOM User Account (SNMP)" on page 131

Related Information

- "Performing General Tasks on ILOM Targets (SNMP)" on page 126
- "Managing Other Aspects (SNMP)" on page 131

▼ Add an ILOM User Account (SNMP)

1. From the SNMP client, create an ILOM user:

```
$ snmpset -v2c -c public mc_IP
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserRowStatus.\"username\" = 5
```

where *username* is the user name. For example, to create a user called `newuser`:

```
$ snmpset -v2c -c public mc_IP
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserRowStatus.\"newuser\" = 5
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserRoles.\"newuser\" = "o"
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserPassword.\"newuser\" = "changeme"
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserRowStatus."newuser" = INTEGER:
createAndWait(5)
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserRoles."newuser" = STRING: "o"
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserPassword."newuser" = STRING: "changeme"
$
```

Note – When typing the command of this step, do not press the Return or Enter key until after typing `"changeme"` .

2. Activate the user:

```
$ snmpset -v2c -c public mc_IP
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserRowStatus.\"newuser\" = 1
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserRowStatus."newuser" = INTEGER:
active(1)
$
```

Related Information

- "Add an ILOM User Account (CLI)" on page 47
- "Add an ILOM User Account (Web Interface)" on page 94
- "Delete an ILOM User Account (SNMP)" on page 131
- "Display ILOM User Accounts (SNMP)" on page 121

▼ Delete an ILOM User Account (SNMP)

- **From the SNMP client, type:**

```
$ snmpset -v2c -c public mc_IP
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserRowStatus.\"username\" = 6
```

where *username* is the user name. For example, to delete `newuser`:

```
$ snmpset -v2c -c public mc_IP
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserRowStatus.\"newuser\" = 6
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserRowStatus."newuser" = INTEGER:
destroy(6)
$
```

Related Information

- "Delete an ILOM User Account (CLI)" on page 49
- "Delete an ILOM User Account (Web Interface)" on page 96
- "Add an ILOM User Account (SNMP)" on page 130
- "Display ILOM User Accounts (SNMP)" on page 121

Managing Other Aspects (SNMP)

These tasks help you manage the ILOM services.

- "Set the HTTP Service State (SNMP)" on page 132
- "Enable Alerts to Send SNMP Traps (SNMP)" on page 132
- "Modify Alert SNMP Version (SNMP)" on page 133
- "Disable Alerts (SNMP)" on page 134

Related Information

- "Managing Other Aspects (CLI)" on page 62
- "Managing Other Aspects (Web Interface)" on page 108
- "Performing General Tasks on ILOM Targets (SNMP)" on page 126

▼ Set the HTTP Service State (SNMP)

- **From the SNMP client, type:**

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlHttpEnabled.0 i state
```

where *state* is either `1` for enabled or `2` for disabled. For example, to enable the HTTP service:

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlHttpEnabled.0 i 1
SUN-ILOM-CONTROL-MIB::ilomCtrlHttpEnabled.0 = INTEGER: true(1)
$
```

Related Information

- "Enable the HTTP Service (CLI)" on page 50
- "Disable the HTTP Service (CLI)" on page 50
- "Enable the HTTP Service (Web Interface)" on page 97
- "Disable the HTTP Service (Web Interface)" on page 97
- "Display the HTTP Service Status (SNMP)" on page 119

▼ Enable Alerts to Send SNMP Traps (SNMP)

- **From the SNMP client, type:**

```
$ snmpset -v2c -c public mc_IP
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertDestinationIP.number = "IP_address"
```

where:

- *number* is the number of the alert.
- *IP_address* is the IP address of the host to receive the trap.

For example, to enable alert 2 to send traps to the host at IP address 123.45.67.90:

```
$ snmpset -v2c -c public mc_IP
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertDestinationIP.2 = "123.45.67.90"
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertDestinationPort.2 = 162
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSeverity.2 = 4
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertDestinationIP.2 = IpAddress: 123.45.67.90
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertDestinationPort.2 = INTEGER: 162
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSeverity.2 = INTEGER: minor(4)
$
```

Related Information

- "Enable Alerts to Send SNMP Traps (CLI)" on page 62
- "Enable Alerts to Send SNMP Traps (Web Interface)" on page 108
- "Disable Alerts (SNMP)" on page 134
- "Modify Alert SNMP Version (SNMP)" on page 133

▼ Modify Alert SNMP Version (SNMP)

- **From the SNMP client, type:**

```
$ snmpset -v2c -c public mc_IP
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSNMPVersion.number = 2
```

where *number* is the number of the alert. For example, to modify alert 2:

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSNMPVersion.2
= 2
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSNMPVersion.2 = INTEGER: v2c(2)
$
```

Note – All alert configuration parameters can be modified using SNMP. Refer to the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Guide*, 820-6413, for more information.

Related Information

- "Enable Alerts to Send PET (CLI)" on page 63
- "Enable Alerts to Send PET (Web Interface)" on page 109
- "Enable Alerts to Send SNMP Traps (SNMP)" on page 132
- "Disable Alerts (SNMP)" on page 134

▼ Disable Alerts (SNMP)

- **From the SNMP client, type:**

```
$ snmpset -v2c -c public mc_IP
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSeverity.number = 1
```

where *number* is the number of the alert. For example, to disable alert 2:

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSeverity.2 = 1
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSeverity.2 = INTEGER: disable(1)
$
```

Related Information

- "Disable Alerts (CLI)" on page 64
- "Disable Alerts (Web Interface)" on page 110
- "Enable Alerts to Send SNMP Traps (SNMP)" on page 132
- "Modify Alert SNMP Version (SNMP)" on page 133

Administering Hardware (IPMI)

These topics describe how to administer the hardware of Oracle's Sun Datacenter InfiniBand Switch 648 using the `ipmitool` utility.

Related Information

- "Understanding ILOM on the Switch" on page 1
- "Administering ILOM (CLI)" on page 21
- "Administering ILOM (Web Interface)" on page 75
- "Administering ILOM (SNMP)" on page 113
- "Understanding ILOM Commands" on page 139

`ipmitool` Overview

The ILOM implementation on the management controller within the switch provides an IPMI server, which can communicate the state of the switch hardware through the Intelligent Platform Management Interface.

An IPMI client is required to interface with the ILOM IPMI stack on the management controller. You must have administrator priviledges to interface with the stack.

The `ipmitool` utility is the IPMI client used in these topics and has the following format:

```
$ ipmitool -v -H mc_IP -U user command option
```

where:

- *mc_IP* is the IP address of the management controller.

- *user* is the user with administrative privileges. For example, `ilom-admin`.
- *command* is the command to be run on the managment controller.
- *option* is an optional argument or parameter to the *command*.

Note – After typing the `ipmitool` command line, you must type the password of the user for the utility to continue. For the `ilom-admin` user, the default password is `ilom-admin`.

For more information about and use of IPMI with ILOM, refer to the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Guide*, 820-6413, available online at:

`(http://docs.sun.com/app/docs/prod/int.lights.mgr30)`

Related Information

- "CLI Overview" on page 21
- "Web Interface Overview" on page 75
- "SNMP Overview" on page 113
- "SNMP Commands" on page 114

▼ Display the Sensor State (IPMI)

- **From the IPMI client, type:**

```
$ ipmitool -v -I lan -H mc_IP -U ilom-admin sensor
Password: password
Sensor ID              : CHASSIS_STATUS (0x1)
 Entity ID             : 7.0
 Sensor Type (Discrete): OEM reserved #c0
 States Asserted       : Digital State
                        [State Asserted]
$
```

In the output, the string `CHASSIS_STATUS (0x1)` identifies the sensor as the aggregate sensor and the string `[State Asserted]` indicates that the sensor is in an `Asserted` state.

Related Information

- "Display the Aggregate Sensor State (CLI)" on page 27
- "Display the Aggregate Sensor State (Web Interface)" on page 80
- "Display the Aggregate Sensor State (SNMP)" on page 116
- "Display the Sensor Information (IPMI)" on page 137

▼ Display the Sensor Information (IPMI)

- **From the IPMI client, type:**

```
$ ipmitool -v -I lan -H mc_IP -U ilom-admin sdr
Password: password
Sensor ID              : CHASSIS_STATUS (0x1)
 Entity ID             : 7.0 (System Board)
 Sensor Type (Discrete): OEM reserved #c0
 States Asserted       : Digital State
                       [State Asserted]
 Assertions Enabled    : Digital State
                       [State Deasserted]
                       [State Asserted]
$
```

In the output, the string `CHASSIS_STATUS (0x1)` identifies the aggregate sensor and indicates that it is an `OEM reserved` sensor. The `Assertions Enabled` property indicates the binary state of the aggregate sensor, either `State Deasserted` or `State Asserted`. The `States Asserted` property indicates that the sensor is in the `Asserted` state.

Related Information

- "Display the Sensor State (IPMI)" on page 136

▼ Display the System Event Log (IPMI)

- **From the IPMI client, type:**

```
$ ipmitool -v -I lan -H mc_IP -U ilom-admin sel list number
```

where *number* is the number of records to display. For example:

```
$ ipmitool -v -I lan -H mc_IP -U ilom-admin sel list 2
Password: password
SEL Record ID          : 0001
 Record Type           : 02
 Timestamp             : 01/19/2010 21:57:05
 Generator ID          : 0020
 EvM Revision          : 04
 Sensor Type           : OEM
 Sensor Number         : 01
 Event Type            : Generic Discrete
 Event Direction       : Assertion Event
 Event Data            : 00ffff
 Description           : State Deasserted

SEL Record ID          : 0002
 Record Type           : 02
 Timestamp             : 01/20/2010 03:17:11
 Generator ID          : 0020
 EvM Revision          : 04
 Sensor Type           : OEM
 Sensor Number         : 01
 Event Type            : Generic Discrete
 Event Direction       : Assertion Event
 Event Data            : 01ffff
 Description           : State Asserted
$
```

In the output, the events were both for sensor 1, the aggregate sensor. The events describe the sensor going from `State Deasserted` to `State Asserted`.

Related Information

- "Display the ILOM Event Log (CLI)" on page 28
- "Display the ILOM Event Log (Web Interface)" on page 81
- "Display the ILOM Event Log (SNMP)" on page 118

Understanding ILOM Commands

Only the `ilom-admin` user of the ILOM shell can run all of the ILOM commands. The format of the ILOM commands is typically as follows:

`->` *command* `[`*argument*`]` `[`*argument*`]` `...`

where:

- *command* is the command being issued.
- *argument* is any option or variable for that command.

Command Syntax	Links
`cd [-default][`*target*`]`	"`cd` Command" on page 140
`create [`*target*`][`*property=value property=value* `...]`	"`create` Command" on page 141
`delete [-script][`*target*`]`	"`delete` Command" on page 142
`dump [-destination` *URI*`][`*target*`]`	"`dump` Command" on page 143
`exit`	"`exit` Command (ILOM)" on page 144
`help [-o terse|verbose][`*command*`|legal|targets|`*target*`|` *target property*`]`	"`help` Command (ILOM)" on page 145
`load [-o verbose][-script]-source` *URI*`[`*target*`]`	"`load` Command" on page 146
`set [`*target*`]`*property=value*`[`*property=value*`...]`	"`set` Command" on page 147
`show [-d targets|properties|commands|all][-l 1|2|3...255|all][-o table][`*target*`][`*property property*`...]`	"`show` Command" on page 148
`version`	"`version` Command (ILOM)" on page 149

Related Information

- *Switch Reference*
- "Understanding ILOM on the Switch" on page 1
- "Administering ILOM (CLI)" on page 21
- "Administering ILOM (Web Interface)" on page 75

- "Administering ILOM (SNMP)" on page 113
- "Administering Hardware (IPMI)" on page 135

cd Command

Changes and displays the current target.

Syntax

`cd [-default][`*target*`]`

where *target* is the target and path to act upon.

Description

This ILOM command changes the ILOM attention to the specified *target*. This command is similar to the change directory (`cd`) command of many operating systems.The `-default` option returns the attention to the default target.

Example

The following example shows how to change to the `/SP/logs/event/list` target with the `cd` command.

```
-> cd /SP/logs/event/list
/SP/logs/event/list

-> show
  /SP/logs/event/list
     Targets:
     Properties:
     Commands:
         cd
         how
 s
ID      Date/Time                  Class      Type       Severity
------  -------------------------  ---------  ---------  ---------
75      Wed Oct  7 20:12:31 2009   Audit      Log        minor
```

```
 root : Open Session : object = /session/type : value = shell : success
74     Wed Oct  7 20:12:28 2009  Audit     Log       minor
 root : Close Session : object = /session/type : value = shell : success
73     Wed Oct  7 20:11:21 2009  Audit     Log       minor
 root : Open Session : object = /session/type : value = shell : success
.
.
.
->
```

Note – The output in the example is a portion of the full output.

`create` Command

Creates a target.

Syntax

`create [`*target*`][`*property* `=` *value* *property* `=` *value* `...]`

where:

- *target* is the target and path to create or act upon.
- *property* is the property of the target to create.
- *value* is the value of the property created.

Description

This ILOM command creates the specified target with the specified properties. Your user must have administrator (a) privileges to use this command.

Example

The following example shows how to create a `/SP/users/test` user target with the `create` command.

```
-> create /SP/users/test
Creating user...
Enter new password: password
Enter new password again: password
Created /SP/users/test
->
```

Related Information

- "`delete` Command" on page 142

`delete` Command

Deletes a target.

Syntax

`delete [-script][`*target*`]`

where *target* is the target and path to act upon.

Description

This ILOM command deletes the *target* and all subordinate targets. If no *target* is specified, the current target is affected. Your user must have administrator (`a`) privileges to use this command. The `-script` option skips confirmation of the target deletion and proceeds as if `y` was specified.

Example

The following example shows how to delete the `/SYS/users/test` target with the `delete` command.

```
-> delete /SP/users/test
Are you sure you want to delete /SP/users/test (y/n)? y
Deleted /SP/users/test.
->
```

Related Information

- "`create` Command" on page 141

`dump` Command

Dumps target information to a remote location.

Syntax

`dump [-destination` *URI*`][`*target*`]`

where:

- *URI* is the uniform resource indicator.
- *target* is the target and path to act upon.

Description

This ILOM command transfers *target* information to a remote location specified by the *URI*. If no *target* is specified, the current target is affected. Your user must have administrator (`a`) privileges to use this command. The `-destination` option specifies the location. If the `-destination` option is not used, then the information is transferred to `stdout`.

Example

The following example shows how to transfer the `/SP/services/snmp/mibs` target information to the `ilom-mibs.zip` file on the host with IP address 123.45.67.89 using the FTP protocol with the `dump` command.

```
-> dump -destination ftp://root:changeme@123.45.67.89/tftpboot/ilom-mibs.zip
/SP/services/snmp/mibs
->
```

Related Information

- "`load` Command" on page 146

`exit` Command (ILOM)

Terminates the ILOM session.

Syntax

```
exit
```

Description

This ILOM command exits the ILOM shell and either:

- Returns the `root` user to the Linux `root` user prompt of the Shelf Manager.
- Logs off the `ilom-admin` user or `ilom-operator` user from the CMC.

Example

The following example shows how to exit the ILOM session using the `exit` command.

```
-> exit
#
```

Related Information

- *Switch Reference*, `exit` command

`help` Command (ILOM)

Provides help with ILOM commands.

Syntax

`help [-o terse|verbose][`*command*`|legal|targets|`*target*`|`*target property*`]`

where:

- *command* is the ILOM command for which you are seeking help.
- *target* is the target for which you are seeking help.
- *property* is the property of the target for which you are seeking help.

Description

This ILOM command gives information and assistance about commands and targets. The `-o` option enables either terse or verbose output. The `help targets` command displays a basic list of targets. The `help legal` command displays the legal notice.

Example

The following example shows how to display verbose help about the `exit` command with the `help` command.

```
-> help -o verbose exit
The exit command is used to terminate a session.
Usage: exit
Example:
  -> exit
  Connection to nyc-sp closed.
->
```

Related Information

- *Switch Reference*, `help` command

`load` Command

Transfers a file from a remote location to update a target.

Syntax

`load [-o verbose][-script]-source` *URI*`[`*target*`]`

where:

- *URI* is the uniform resource indicator.
- *target* is the target and path to act upon.

Description

This ILOM command transfers information in a file from a remote location specified by the *URI* to update a *target*. If no *target* is specified, the current target is affected. Your user must have administrator (`a`) privileges to use this command.

Options

The following table describes the options to the `load` command and their purposes:

Option	Purpose
`-o`	Enables verbose output.
`-script`	Skips confirmation of the action and proceeds as if `yes` was specified.

Example

The following example shows how to load a custom certificate file, `server.pem`, to the `/SP/services/https/ssl/custom_cert` target from the host at IP address 123.45.67.89 using the TFTP protocol with the `load` command.

```
-> load -source tftp://123.45.67.89/server.pem
/SP/services/https/ssl/custom_cert
Load successful.
->
```

Related Information

- "`dump` Command" on page 143

`set` Command

Sets a property.

Syntax

`set [`*target*`]`*property*`=`*value*`[`*property*`=`*value*`...]`

where:

- *target* is the target and path to act upon.
- *property* is the property of the target to change.
- *value* is what to set the property to.

Description

This ILOM command sets the *property* of a *target*. If no *target* is specified, the current target is affected. Your user must have administrator (`a`) privileges to use this command.

Example

The following example shows how to change the role of the `/SP/users/test` user to administrator with the `set` command.

```
-> set /SP/users/test role=a
Set 'role' to 'a'
->
```

Related Information

- "`show` Command" on page 148

`show` Command

Display information about targets, properties and commands.

Syntax

`show [-d targets|properties|commands|all]|[-l 1|2|3...255|all][-o table][`*target*`][`*property property*`...]`

where:

- *target* is the target and path to act upon.
- *property* is the property of the target to show.

Description

This ILOM command displays information about targets, their properties, and associated commands. If no *target* is specified, information about the current target is displayed.

Options

The following table describes the options to the `show` command and their purposes:

Option	Purpose
`-d`	Specifies what information to display. • `targets` – The subtargets of the target. • `properties` – The properties of the target. • `commands` – The supported commands of the target. • `all` – The subtargets, properties, and supported commands of the target.
`-l`	Specifies the relative level in the target hierarchy to which the action applies.
`-o`	Enables output in tabular form.

Example

The following example shows how to display the ILOM user accounts with the `show` command.

```
-> show -d targets /SP/users
  /SP/users
     Targets:
         root
         ilom-admin
         ilom-operator
         for_Check
         test
->
```

Related Information

- "`set` Command" on page 147

`version` Command (ILOM)

Displays version information.

Syntax

```
version
```

Description

This ILOM command displays the version information within the Shelf Manager.

Example

The following example shows how to display the version information with the `version` command.

```
-> version
SP firmware 1.1.8
SP firmware build number: 44535
SP firmware date: Tue Jun 23 19:12:58 IST 2009
SP filesystem version: 0.1.22
->
```

Related Information

- *Switch Reference*, `version` command

Index

D

E

F

H

I

L

M

N

O

P

R

S

T

U

V

W