

Oracle Integrated Lights Out Manager (ILOM) 3.0

Supplement for the Sun Network QDR InfiniBand
Gateway Switch Firmware Version 2.0



Part No.: E26709-01
November 2011, Revision A

Copyright © 2011, Oracle and /or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related software documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and /or its affiliates. Other names may be trademarks of their respective owners.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through X/Open Company, Ltd.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Copyright © 2011, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

U.S. GOVERNMENT RIGHTS. Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. UNIX est une marque déposée concédée sous licence par X/Open Company, Ltd.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation.



Adobe PostScript

Contents

Using This Documentation xvii

Understanding Oracle ILOM on the Gateway 1

Oracle ILOM Overview 1

Supported Features 2

Understanding Oracle ILOM Targets 4

 Oracle ILOM Target Overview 4

 Oracle ILOM Targets and Descriptions 5

 Oracle ILOM General System Targets and Properties 9

 Oracle ILOM Fan Targets and Properties 11

 Oracle ILOM Indicator Targets and Properties 12

 Oracle ILOM Power Supply Targets and Properties 13

 Oracle ILOM Temperature Targets and Properties 15

 Oracle ILOM Voltage Targets and Properties 17

 Oracle ILOM General Targets and Properties 22

 Oracle ILOM Service Targets and Properties 25

 Oracle ILOM User and Session Targets and Properties 27

Administering Oracle ILOM (CLI) 29

CLI Overview 29

Accessing Oracle ILOM From the CLI 30

 ▼ Access the Oracle ILOM Shell From the CLI (NET MGT Port) 30

▼ Access the Oracle ILOM Shell From the CLI (USB Management Port)	31
Switching Between the Oracle ILOM Shell and the Linux Shell	32
/SYS/Switch_Diag, /SYS/Gateway_Mgmt, and /SYS/Fabric_Mgmt Linux Shells	33
▼ Switch From the Oracle ILOM Shell to the Linux Shell	36
▼ Switch From the Linux Shell to the Oracle ILOM Shell	38
Monitoring Oracle ILOM Targets (CLI)	39
Performing Daily Tasks (CLI)	39
▼ Display the Date (CLI)	40
▼ Display Gateway Status LEDs States (CLI)	40
▼ Display the Aggregate Sensors State (CLI)	41
Aggregate Sensor States	42
▼ Display Power Supply Status (CLI)	43
▼ Display Board-Level Voltages (CLI)	44
Board Level Voltages	46
▼ Display Internal Temperatures (CLI)	47
Internal Temperature Sensors	48
▼ Display Fan Status (CLI)	48
▼ Display the Oracle ILOM Sessions (CLI)	50
▼ Display the Oracle ILOM Event Log (CLI)	51
Checking the Status of Services (CLI)	52
▼ Display the HTTP Service Status (CLI)	52
▼ Display the HTTPS Service Status (CLI)	53
▼ Display the SSL Certificates (CLI)	53
▼ Display the SNMP Service Status (CLI)	54
▼ Display the SNMP User Accounts (CLI)	54
▼ Display the SNMP Service Communities (CLI)	55
▼ Display the IPMI Service Status (CLI)	56

- ▼ Display the DNS Client Status (CLI) 56
- ▼ Display the SMTP Client Status (CLI) 57
- ▼ Display the NTP Servers (CLI) 57

Verifying Other Aspects With Oracle ILOM (CLI) 58

- ▼ Get Help on an Oracle ILOM Command (CLI) 59
- ▼ Get Help on an Oracle ILOM Target Property (CLI) 60
- ▼ Display the Alert Properties (CLI) 60
- ▼ Display the Oracle ILOM User Accounts (CLI) 61
- ▼ Display the Remote Log Hosts (CLI) 62
- ▼ Display the Network Management Configuration (CLI) 63
- ▼ Display the CLI Session Timeout (CLI) 64
- ▼ Display Gateway FRU ID (CLI) 64
- ▼ Display Power Supply FRU ID (CLI) 65
- ▼ Display the Firmware Version (CLI) 66
- ▼ Display System Identification Properties (CLI) 66

Controlling Oracle ILOM Targets (CLI) 67

Performing General Tasks on Oracle ILOM Targets (CLI) 67

- ▼ Restart the Management Controller (CLI) 68
- ▼ Set the Date and Time (CLI) 69
- ▼ Enable the Locator LED (CLI) 70
- ▼ Disable the Locator LED (CLI) 71
- ▼ Clear the Oracle ILOM Event Log (CLI) 71
- ▼ Set the Remote Log Hosts (CLI) 72
- ▼ Configure the DNS Client (CLI) 73
- ▼ Configure the SMTP Client (CLI) 74
- ▼ Back Up the Configuration (CLI) 75

Gateway Configuration Information Backed Up 76

- ▼ Restore the Configuration (CLI) 76

▼ Create a Snapshot of the Gateway State (CLI)	77
Snapshot Dataset Information (CLI)	79
▼ Set the Network Management Parameters (CLI)	80
▼ Set the System Identification Properties (CLI)	82
Performing Oracle ILOM User Tasks (CLI)	83
▼ Add an Oracle ILOM User Account (CLI)	84
▼ Change an Oracle ILOM User's Password and or Role (CLI)	84
▼ Delete an Oracle ILOM User Account (CLI)	85
Managing HTTP Services (CLI)	86
▼ Enable the HTTP Service (CLI)	86
▼ Disable the HTTP Service (CLI)	87
Managing HTTPS Services (CLI)	88
▼ Enable the HTTPS Service (CLI)	88
▼ Install a Custom SSL Certificate (CLI)	89
▼ Remove the Custom SSL Certificate (CLI)	89
▼ Disable the HTTPS Service (CLI)	90
Managing SNMP Services (CLI)	91
▼ Enable the SNMP Service (CLI)	91
▼ Configure the SNMP Service (CLI)	92
▼ Add SNMP Service User Accounts (CLI)	93
▼ Modify SNMP Service User Accounts (CLI)	94
▼ Delete SNMP Service User Accounts (CLI)	95
▼ Add SNMP Service Communities (CLI)	95
▼ Modify SNMP Service Communities (CLI)	96
▼ Delete SNMP Service Communities (CLI)	96
▼ Download SNMP Service MIBs (CLI)	97
▼ Disable the SNMP Service (CLI)	98
Managing IPMI Services (CLI)	98

▼	Enable the IPMI Service (CLI)	99
▼	Disable the IPMI Service (CLI)	99
	Managing Other Aspects With Oracle ILOM (CLI)	100
▼	Enable Alerts to Send SNMP Traps (CLI)	100
▼	Enable Alerts to Send PETs (CLI)	102
▼	Enable Alerts to Send Email Alerts (CLI)	103
▼	Disable Alerts (CLI)	104
▼	Set the Oracle ILOM CLI Session Timeout (CLI)	105
	Upgrading the Gateway Firmware Through Oracle ILOM (CLI)	105
	Firmware Overview	106
▼	Verify Firmware Integrity (CLI)	106
▼	Acquire the Gateway Firmware Package (CLI)	107
▼	Upgrade the Gateway Firmware (CLI)	109
	Administering Oracle ILOM (Web)	115
	Web Interface Overview	115
▼	Access Oracle ILOM From the Web Interface	118
	Monitoring Oracle ILOM Targets (Web)	119
	Performing Daily Tasks (Web)	119
▼	Display the Date (Web)	120
▼	Display the Gateway Status LEDs States (Web)	120
▼	Display the Aggregate Sensors State (Web)	120
▼	Display Power Supply Status (Web)	121
▼	Display Board-Level Voltages (Web)	122
▼	Display Internal Temperatures (Web)	122
▼	Display Fan Status (Web)	123
▼	Display the Oracle ILOM Sessions (Web)	123
▼	Display the Oracle ILOM Event Log (Web)	124
	Checking the Status of Services (Web)	124

▼ Display the HTTP Service Status (Web)	125
▼ Display the HTTPS Service Status (Web)	125
▼ Display the SSL Certificates (Web)	125
▼ Display the SNMP Service Status (Web)	126
▼ Display the SNMP Service User Accounts (Web)	126
▼ Display the SNMP Service Communities (Web)	127
▼ Display the IPMI Service Status (Web)	127
▼ Display the DNS Client Status (Web)	127
▼ Display the SMTP Client Status (Web)	128
▼ Display the Network Time Protocol Servers (Web)	128
Verifying Other Aspects With Oracle ILOM (Web)	129
▼ Display the Alert Properties (Web)	129
▼ Display the Oracle ILOM User Accounts (Web)	130
▼ Display the Remote Log Hosts (Web)	130
▼ Display the Network Management Configuration (Web)	131
▼ Display the CLI Session Timeout (Web)	131
▼ Display System Component FRU ID (Web)	132
▼ Display the Firmware Version (Web)	132
▼ Display the Oracle ILOM Version (Web)	133
▼ Display System Identification Properties (Web)	133
Controlling Oracle ILOM Targets (Web)	134
Performing General Tasks on Oracle ILOM Targets (Web)	134
▼ Restart the Management Controller (Web)	135
▼ Set the Date and Time (Web)	136
▼ Set the Time Zone (Web)	136
▼ Enable the Locator LED (Web)	137
▼ Disable the Locator LED (Web)	137
▼ Clear the Oracle ILOM Event Log (Web)	138

▼ Set the Remote Log Hosts (Web)	138
▼ Configure the DNS Client (Web)	139
▼ Configure the SMTP Client (Web)	140
▼ Back Up the Configuration (Web)	141
▼ Restore the Configuration (Web)	142
▼ Create a Snapshot of the Gateway State (Web)	142
Snapshot Dataset Information (Web)	143
▼ Set the Network Management Parameters (Web)	144
▼ Set the System Identification Properties (Web)	145
Performing Oracle ILOM User Tasks (Web)	145
▼ Add an Oracle ILOM User Account (Web)	145
▼ Change an Oracle ILOM User's Password and or Role (Web)	146
▼ Delete an Oracle ILOM User Account (Web)	147
Managing HTTP Services (Web)	147
▼ Enable the HTTP Service (Web)	148
▼ Disable the HTTP Service (Web)	148
Managing HTTPS Services (Web)	149
▼ Enable the HTTPS Service (Web)	149
▼ Install a Custom SSL Certificate (Web)	150
▼ Remove the Custom SSL Certificate (Web)	151
▼ Disable the HTTPS Service (Web)	151
Managing SNMP Services (Web)	152
▼ Enable the SNMP Service (Web)	152
▼ Configure the SNMP Service (Web)	153
▼ Add SNMP Service User Accounts (Web)	153
▼ Modify SNMP Service User Accounts (Web)	154
▼ Delete SNMP Service User Accounts (Web)	155
▼ Add SNMP Service Communities (Web)	156

- ▼ Modify SNMP Service Communities (Web) 156
- ▼ Delete SNMP Service Communities (Web) 157
- ▼ Download SNMP Service MIBs (Web) 158
- ▼ Disable the SNMP Service (Web) 158

Managing IPMI Services (Web) 159

- ▼ Enable the IPMI Service (Web) 159
- ▼ Disable the IPMI Service (Web) 160

Managing Other Aspects With Oracle ILOM (Web) 160

- ▼ Enable Alerts to Send SNMP Traps (Web) 161
- ▼ Enable Alerts to Send PETs (Web) 161
- ▼ Enable Alerts to Send Email Alerts (Web) 162
- ▼ Disable Alerts (Web) 163
- ▼ Set the CLI Session Timeout (Web) 164
- ▼ Upgrade the Gateway Firmware (Web) 164

Using the Fabric Monitor 169

- ▼ Access the Fabric Monitor 169

Fabric Monitor Features 170

Accessing the Rear Panel Diagram 172

Rear Panel Diagram Overview 172

InfiniBand Connector Status Window 173

Gateway Connector Status Window 176

BridgeX Port Status Window 178

Accessing Status Pane Information 180

System Info Tab 181

Sensor Info Tab 182

IB Performance Tab 183

IB Port Map Tab 185

Subnet Manager Tab 186

Control Panel Function	187
Monitoring Parameters and Status	188
Chassis Parameters and Status	189
InfiniBand Connector Parameters and Status	191
Gateway Connector Parameters and Status	194
I4 to Gateway Interface Parameters and Status	195
I4 Switch Chip Port Parameters and Status	196
Administering Oracle ILOM (SNMP)	199
SNMP Overview	199
Understanding SNMP Commands	200
SNMP Commands	200
V1 and V2c Protocol Command Format	201
V3 Protocol Command Format	202
Monitoring Oracle ILOM Targets (SNMP)	203
Performing Daily Tasks (SNMP)	204
▼ Display the Date and Time (SNMP)	204
▼ Display the Time Zone (SNMP)	205
▼ Display the Aggregate Sensors State (SNMP)	205
▼ Display Power Supply Status (SNMP)	206
▼ Display Board-Level Voltages (SNMP)	208
▼ Display Internal Temperatures (SNMP)	212
▼ Display Fan Status (SNMP)	215
▼ Display the Sensor Alarm State (SNMP)	219
▼ Display the Entity Numbers	220
▼ Display Oracle ILOM Sessions (SNMP)	222
▼ Display the Oracle ILOM Event Log (SNMP)	223
Checking the Status of Services (SNMP)	225
▼ Display the HTTP Service Status (SNMP)	225

▼ Display the HTTPS Service Status (SNMP)	226
▼ Display the DNS Client Status (SNMP)	226
▼ Display the SMTP Client Status (SNMP)	227
▼ Display the NTP State (SNMP)	227
▼ Display the NTP Servers (SNMP)	228
Verifying Other Aspects With Oracle ILOM (SNMP)	228
▼ Display the Alert Properties (SNMP)	229
▼ Display Oracle ILOM User Accounts (SNMP)	230
▼ Display the Remote Log Hosts (SNMP)	231
▼ Display the Network Management Configuration (SNMP)	231
▼ Display Gateway FRU ID (SNMP)	232
▼ Display Power Supply FRU ID (SNMP)	234
▼ Display the System Components (SNMP)	236
▼ Display the Additional System Component Information (SNMP)	238
▼ Display the Firmware Version (SNMP)	239
▼ Display System Identification Properties (SNMP)	239
Controlling Oracle ILOM Targets (SNMP)	240
Performing General Tasks (SNMP)	240
▼ Set the Date and Time (SNMP)	241
▼ Set the Time Zone (SNMP)	241
▼ Set the Network Time Protocol State (SNMP)	242
▼ Set the Network Time Protocol Servers (SNMP)	242
▼ Clear the Oracle ILOM Event Log (SNMP)	243
▼ Set the Remote Log Hosts (SNMP)	243
▼ Configure the DNS Client (SNMP)	244
▼ Configure the SMTP Client (SNMP)	245
▼ Set the Network Parameters (SNMP)	246
▼ Set the System Identification Properties (SNMP)	248

Performing User Tasks (SNMP) 248

- ▼ Add an Oracle ILOM User Account (SNMP) 249
- ▼ Delete an Oracle ILOM User Account (SNMP) 250

Managing Other Aspects With Oracle ILOM (SNMP) 250

- ▼ Set the HTTP Service State (SNMP) 251
- ▼ Set the HTTPS Service State (SNMP) 251
- ▼ Enable Alerts to Send SNMP Traps (SNMP) 252
- ▼ Enable Alerts to Send PETs (SNMP) 253
- ▼ Enable Alerts to Send Email Alerts (SNMP) 254
- ▼ Modify Alert SNMP Version (SNMP) 255
- ▼ Disable Alerts (SNMP) 256

Administering Hardware (IPMI) 257

`ipmitool` Overview 257

- ▼ Display the Sensor States (IPMI) 258
- ▼ Display the Sensor Information (IPMI) 259
- ▼ Display the System Event Log (IPMI) 261
- ▼ Display FRU ID Information (IPMI) 262
- ▼ Display Gateway Status LED States (IPMI) 263
- ▼ Enable the Locator LED (IPMI) 264
- ▼ Disable the Locator LED (IPMI) 264

Understanding Oracle ILOM Commands 265

`cd` Command 266

Syntax 266

Description 266

Example 266

`create` Command 267

Syntax 267

Description	268
Example	268
delete Command	268
Syntax	268
Description	269
Example	269
dump Command	269
Syntax	269
Description	270
Example	270
exit Command (ILOM)	270
Syntax	270
Description	270
Example	271
help Command (ILOM)	271
Syntax	271
Description	271
Example	272
load Command	272
Syntax	272
Description	272
Options	273
Example	273
reset Command	273
Syntax	273
Description	274
Example	274
set Command	274

Syntax	274
Description	275
Example	275
show Command	275
Syntax	275
Description	276
Options	276
Example	276
version Command (ILOM)	277
Syntax	277
Description	277
Example	277
Index	279

Using This Documentation

This supplement provides detailed information regarding the installation, administration, and reference of Oracle Integrated Lights Out Manager (ILOM) 3.0 firmware for the Sun Network QDR Infiniband Gateway Switch from Oracle. This document is written for system administrators and authorized service providers who have experience with the Oracle ILOM firmware.

- “Product Notes” on page xvii
- “Related Documentation” on page xviii
- “Feedback” on page xviii
- “Support and Accessibility” on page xviii

Product Notes

For late-breaking information and known issues about this product, refer to the product notes at:

<http://www.oracle.com/pls/topic/lookup?ctx=E26699-01>

Related Documentation

Documentation	Links
All Oracle products	http://www.oracle.com/documentation
Sun Network QDR InfiniBand Gateway Switch	http://www.oracle.com/pls/topic/lookup?ctx=E26699-01
Oracle Solaris OS and other systems software	http://www.oracle.com/technetwork/indexes/documentation/index.html#sys_sw
Oracle Integrated Lights Out Manager (ILOM) 3.0	http://www.oracle.com/pls/topic/lookup?ctx=E19860-01

Feedback

Provide feedback on this documentation at:

<http://www.oracle.com/goto/docfeedback>

Support and Accessibility

Description	Links
Access electronic support through My Oracle Support	http://support.oracle.com For hearing impaired: http://www.oracle.com/accessibility/support.html
Learn about Oracle's commitment to accessibility	http://www.oracle.com/us/corporate/accessibility/index.html

Understanding Oracle ILOM on the Gateway

These topics provide an overview of Oracle ILOM and its implementation on the gateway.

- [“Oracle ILOM Overview” on page 1](#)
- [“Supported Features” on page 2](#)
- [“Understanding Oracle ILOM Targets” on page 4](#)

Related Information

- [“Administering Oracle ILOM \(CLI\)” on page 29](#)
- [“Administering Oracle ILOM \(Web\)” on page 115](#)
- [“Using the Fabric Monitor” on page 169](#)
- [“Administering Oracle ILOM \(SNMP\)” on page 199](#)
- [“Administering Hardware \(IPMI\)” on page 257](#)
- [“Understanding Oracle ILOM Commands” on page 265](#)

Oracle ILOM Overview

This document provides basic Oracle ILOM 3.0 information as it pertains to the gateway. See [“Related Documentation” on page xviii](#).

Oracle ILOM is a means of remotely managing a hardware device through a SP. For the gateway, the SP is the Komtron management controller within the gateway. Oracle ILOM enables monitoring and controlling of users, hardware, services, protocols, and configuration. You can use Oracle ILOM to perform tasks that could otherwise be accomplished with the hardware commands.

Oracle ILOM has two primary interfaces, a command line and a web interface. The Oracle ILOM web interface enables point-and-click administration of the Oracle ILOM components and services. You access these interfaces using the default `ilom-admin` or `ilom-operator` user accounts. The `ilom-admin` account is for Oracle ILOM system administration. This account is fully privileged to add, delete, create, enable, disable, and so on, the Oracle ILOM targets, components, and services. The `ilom-operator` account is for users to only monitor the many aspects of Oracle ILOM.

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

When you upgrade the management controller firmware to version 1.1.2 or higher, Oracle ILOM 3.0 support is installed. An additional benefit of Oracle ILOM is that future management controller and I4 firmware upgrades are greatly simplified.

Related Information

- [“Understanding Oracle ILOM Commands” on page 265](#)
- [“Web Interface Overview” on page 115](#)
- [“Accessing Oracle ILOM From the CLI” on page 30](#)
- [“Access Oracle ILOM From the Web Interface” on page 118](#)
- [“Upgrading the Gateway Firmware Through Oracle ILOM \(CLI\)” on page 105](#)

Supported Features

For the implementation of Oracle ILOM 3.0 on the management controller, these features are supported:

- **Interfaces** – These interfaces are supported:
 - **CLI** – Succinct and human-readable administration interface.
 - **BI** – Browser interface or web interface. User-friendly administration interface.
 - **SNMP** – Advanced user interface for those experienced with SNMP.
 - **IPMI** – An interface between hardware devices.
- **Event and fault monitoring** – These events are logged:
 - **Oracle ILOM events**
 - **Gateway-specific events** – Non-Oracle ILOM events are also logged into the Oracle ILOM event log.

- **Firmware upgrade** – I4 switch chip, BridgeX, and management controller firmware upgrade from a single repository file.
- **Fabric Monitor** – Browser interface to monitor gateway configuration, status, and activity.
- **Oracle ILOM support** – These features are supported for this implementation of Oracle ILOM:
 - **User management** – `ilom-admin`, `ilom-operator`, and user-created Oracle 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, IPMI PETs, and Email alerts.
 - **DNS** – Domain name services are provided.
 - **SMTP management** – Configure SMTP client setting to support email alerts.
 - **Snapshot feature** – Take a *snapshot* of the state of Oracle ILOM.
 - **Event management** – Manage the local Oracle ILOM event log.
 - **Remote syslog** – Forward the Syslog to a remote server.
 - **Service Tag** – Support for the Service Tag program.
 - **Back up and restore Oracle ILOM configuration** – Save and restore the state of Oracle ILOM.
 - **Modification of back up and restore** – Gateway-specific configuration information can be selectively backed up or restored.
 - **NTP management** – Automatically set time with NTP servers.
 - **Timezone management** – Configure the correct timezone for the management controller.
- **Start OS shell from Oracle ILOM CLI** – Toggle between the Oracle ILOM CLI and the Linux OS.
- **Sensors**
 - **Aggregate sensor** – Reports general health of gateway, power redundancy, cooling redundancy status, etc.
 - **Fan sensors** – Return the speed of the fans.
 - **Power supply sensors** – Report the state of the power supplies.
 - **Voltage sensors** – Return the various voltages on the main board.
 - **Temperature sensors** – Report the temperatures within the gateway.
- **Indicators**
- **FRU ID** – FRU identification information display.

Related Information

- [“Administering Oracle ILOM \(CLI\)” on page 29](#)
 - [“Administering Oracle ILOM \(Web\)” on page 115](#)
-

Understanding Oracle ILOM Targets

These topics describe the Oracle ILOM targets and their properties.

- [“Oracle ILOM Target Overview” on page 4](#)
- [“Oracle ILOM Targets and Descriptions” on page 5](#)
- [“Oracle ILOM General System Targets and Properties” on page 9](#)
- [“Oracle ILOM Fan Targets and Properties” on page 11](#)
- [“Oracle ILOM Indicator Targets and Properties” on page 12](#)
- [“Oracle ILOM Power Supply Targets and Properties” on page 13](#)
- [“Oracle ILOM Temperature Targets and Properties” on page 15](#)
- [“Oracle ILOM Voltage Targets and Properties” on page 17](#)
- [“Oracle ILOM General Targets and Properties” on page 22](#)
- [“Oracle ILOM Service Targets and Properties” on page 25](#)
- [“Oracle ILOM User and Session Targets and Properties” on page 27](#)

Related Information

- [“Understanding Oracle ILOM Commands” on page 265](#)

Oracle ILOM Target Overview

Oracle ILOM targets represent all software and hardware components and services managed by Oracle ILOM. Targets are identified by a hierarchical 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** – Display the value of these properties with the `show` command. Change the properties with the `set` command. A typical read and write property would be an IP address.

- **Write only** – You cannot display the value of these properties 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

- [“show Command” on page 275](#)
- [“set Command” on page 274](#)
- [“Oracle ILOM Targets and Descriptions” on page 5](#)
- [“Oracle ILOM General System Targets and Properties” on page 9](#)
- [“Oracle ILOM Fan Targets and Properties” on page 11](#)
- [“Oracle ILOM Indicator Targets and Properties” on page 12](#)
- [“Oracle ILOM Power Supply Targets and Properties” on page 13](#)
- [“Oracle ILOM Temperature Targets and Properties” on page 15](#)
- [“Oracle ILOM Voltage Targets and Properties” on page 17](#)
- [“Oracle ILOM General Targets and Properties” on page 22](#)
- [“Oracle ILOM Service Targets and Properties” on page 25](#)
- [“Oracle ILOM User and Session Targets and Properties” on page 27](#)

Oracle ILOM Targets and Descriptions

This table lists the Oracle ILOM targets supported in the gateway and provides a short description of the target.

Oracle ILOM Target	Description
/	Hierarchy root
/SYS	Sensors and FRU information
/SYS/CABLE_ATTN	Aggregate sensor – Overall connector hardware state
/SYS/CABLE_CONN_STAT	Aggregate sensor – Change in cable connectivity state
/SYS/CHASSIS_STATUS	Aggregate sensor – Overall chassis state

Oracle ILOM Target	Description
/SYS/COOLING_ATTN	Aggregate sensor – Overall cooling state
/SYS/COOLING_REDUN	Aggregate sensor – Cooling redundancy state
/SYS/Fabric_Mgmt	Fabric management Linux shell (ilom-admin user)
/SYS/FANx	Fan <i>x</i> information
/SYS/FANx/PRSNT	Presence of fan <i>x</i>
/SYS/FANx/TACH	Speed of fan <i>x</i>
/SYS/Gateway_Mgmt	Gateway management Linux shell (ilom-admin user)
/SYS/I_ATTENTION	State of Attention LED
/SYS/I_LOCATOR	State of Locator LED
/SYS/I_POWER	State of Power LED
/SYS/IBDEV_ATTN	Aggregate sensor – Overall I4 switch chip state
/SYS/MB	Motherboard information
/SYS/MB/BOOT_I4A	Status of I4 switch chip boot
/SYS/MB/T_B0	Temperature of BridgeX chip 0
/SYS/MB/T_B1	Temperature of BridgeX chip 1
/SYS/MB/T_BACK	Temperature at rear of chassis
/SYS/MB/T_FRONT	Temperature at front of chassis
/SYS/MB/T_I4A	Temperature of the I4 switch chip
/SYS/MB/T_SP	Temperature of the management controller
/SYS/MB/V_1.0V	Voltage of the main 1.0V source
/SYS/MB/V_1.0VOK	State of the main 1.0V source
/SYS/MB/V_1.2VStby	Voltage of the standby 1.2V source
/SYS/MB/V_1.8V	Voltage of the main 1.8V source
/SYS/MB/V_1.8VOK	State of the main 1.8V source
/SYS/MB/V_2.5V	Voltage of the main 2.5V source
/SYS/MB/V_2.5VOK	State of the main 2.5V source
/SYS/MB/V_3.3VMain	Voltage of the main 3.3V source
/SYS/MB/V_3.3VMainOK	State of the main 3.3V source
/SYS/MB/V_3.3VStby	Voltage of the standby 3.3V source
/SYS/MB/V_5V	Voltage of the main 5V source
/SYS/MB/V_5VOK	State of the main 5V source

Oracle ILOM Target	Description
/SYS/MB/V_12V	Voltage of the main 12V source
/SYS/MB/V_BAT	Voltage of the battery
/SYS/MB/V_BX1.2V	Voltage of the BridgeX main 1.2V source
/SYS/MB/V_BX1.2VOK	State of the BridgeX main 1.2V source
/SYS/MB/V_ECB	State of the Electronic Circuit Breaker
/SYS/MB/V_I41.2V	Voltage of the I4 switch chip
/SYS/MB/V_I41.2VOK	State of the I4 switch chip 1.2V source
/SYS/MB/V_V1P2ANG	1.2V source for analog power pins
/SYS/MB/V_V1P2DIG	1.2V source for digital power pins
/SYS/Platform_CLII	Comprehensive Linux shell
/SYS/POWER_ATTN	Aggregate sensor – Overall power state
/SYS/POWER_REDUN	Aggregate sensor – Power redundancy state
/SYS/PSUx	Power supply <i>x</i> information
/SYS/PSUx/PRSNT	Presence of power supply <i>x</i>
/SYS/PSUx/ALERT	State of power supply <i>x</i>
/SYS/PSUx/AC_PRESENT	Presence of AC input power for power supply <i>x</i>
/SYS/TEMP_ATTN	Aggregate sensor – Overall temperature state
/SYS/Switch_Diag	Diagnostic Linux shell (ilom-operator and ilom-admin users)
/SP	Management controller or Host
/SP/alertmgmt	Alert rule management
/SP/alertmgmt/rules	Alert rules
/SP/cli	CLI
/SP/clients	Clients that connect to external services
/SP/clients/dns	DNS client configuration
/SP/clients/ntp	NTP configuration
/SP/clients/ntp/server	NTP server configuration
/SP/clients/smtp	SMTP email client configuration
/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

Oracle ILOM Target	Description
/SP/config	Configuration back up and restore settings
/SP/diag/snapshot	State of gateway snapshot
/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
/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

- [“Oracle ILOM Target Overview” on page 4](#)
- [“Oracle ILOM General System Targets and Properties” on page 9](#)
- [“Oracle ILOM Fan Targets and Properties” on page 11](#)
- [“Oracle ILOM Indicator Targets and Properties” on page 12](#)
- [“Oracle ILOM Power Supply Targets and Properties” on page 13](#)
- [“Oracle ILOM Temperature Targets and Properties” on page 15](#)
- [“Oracle ILOM Voltage Targets and Properties” on page 17](#)
- [“Oracle ILOM General Targets and Properties” on page 22](#)

- “Oracle ILOM Service Targets and Properties” on page 25
- “Oracle ILOM User and Session Targets and Properties” on page 27

Oracle ILOM General System Targets and Properties

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

Target and Path	Properties
/SYS	<ul style="list-style-type: none"> • type = Host System • ipmi_name = SYS • product_name = Sun Datacenter InfiniBand Switch GW • product_part_number = 5111402 • product_serial_number = 0110SJC-1099XY9992 • product_manufacturer = Sun Microsystems
/SYS/CABLE_ATTN	<ul style="list-style-type: none"> • type = OEM • ipmi_name = CABLE_ATTN • class = Discrete Sensor • value = State Deasserted • alarm_status = cleared
/SYS/CABLE_CONN_STAT	<ul style="list-style-type: none"> • type = OEM • ipmi_name = CABLE_CONN_STAT • class = Discrete Sensor • value = State Deasserted • alarm_status = cleared
/SYS/CHASSIS_STATUS	<ul style="list-style-type: none"> • type = OEM • ipmi_name = CHASSIS_STATUS • class = Discrete Sensor • value = State Deasserted • alarm_status = cleared
/SYS/COOLING_ATTN	<ul style="list-style-type: none"> • type = OEM • ipmi_name = COOLING_ATTN • class = Discrete Sensor • value = State Deasserted • alarm_status = cleared

Target and Path	Properties
/SYS/COOLING_REDUN	<ul style="list-style-type: none"> • type = OEM • ipmi_name = COOLING_REDUN • class = Discrete Sensor • value = State Deasserted • alarm_status = cleared
/SYS/IBDEV_ATTN	<ul style="list-style-type: none"> • type = OEM • ipmi_name = IBDEV_ATTN • class = Discrete Sensor • value = State Deasserted • alarm_status = cleared
/SYS/MB	<ul style="list-style-type: none"> • type = Motherboard • ipmi_name = MB • product_name = Sun Datacenter InfiniBand Switch GW • product_part_number = 5111402 • product_serial_number = 0110SJC-1099XY9992 • product_manufacturer = Sun Microsystems • fru_name = Chassis and Motherboard • fru_description = Chassis and Motherboard • fru_extra_1 = ComEx: manufacturing_date - 2010.01.26 • fru_extra_2 = ComEx: serial_number - NCD4J0289 • fru_extra_3 = ComEx: hardware_rev - 0x6, firmware_rev - 0x102 • fru_extra_4 = ComEx: bios_version - NOW1R112 , bios_date - 04/24/2009
/SYS/MB/BOOT_I4A	<ul style="list-style-type: none"> • type = OEM • ipmi_name = MB/BOOT_I4A • class = Discrete Sensor • value = State Deasserted • alarm_status = cleared

Target and Path	Properties
/SYS/POWER_ATTN	<ul style="list-style-type: none"> • type = OEM • ipmi_name = POWER_ATTN • class = Discrete Sensor • value = State Deasserted • alarm_status = cleared
/SYS/POWER_REDUN	<ul style="list-style-type: none"> • type = OEM • ipmi_name = POWER_REDUN • class = Discrete Sensor • value = State Deasserted • alarm_status = cleared
/SYS/TEMP_ATTN	<ul style="list-style-type: none"> • type = OEM • ipmi_name = TEMP_ATTN • class = Discrete Sensor • value = State Deasserted • alarm_status = cleared

Related Information

- [“Oracle ILOM Target Overview” on page 4](#)
- [“Oracle ILOM Targets and Descriptions” on page 5](#)
- [“Oracle ILOM Fan Targets and Properties” on page 11](#)
- [“Oracle ILOM Indicator Targets and Properties” on page 12](#)
- [“Oracle ILOM Power Supply Targets and Properties” on page 13](#)
- [“Oracle ILOM Temperature Targets and Properties” on page 15](#)
- [“Oracle ILOM Voltage Targets and Properties” on page 17](#)
- [“Oracle ILOM General Targets and Properties” on page 22](#)
- [“Oracle ILOM Service Targets and Properties” on page 25](#)
- [“Oracle ILOM User and Session Targets and Properties” on page 27](#)

Oracle ILOM Fan Targets and Properties

This table lists the Oracle ILOM /SYS/FANx targets and their properties. Targets without properties are not listed.

Note – The /SYS/FANx target is only available for currently present fans.

Target and Path	Properties
/SYS/FANx	<ul style="list-style-type: none"> • type = Rear Fan
/SYS/FANx/PRSNT	<ul style="list-style-type: none"> • type = Entity Presence • ipmi_name = FAN1/PRSNT • class = Discrete Sensor • value = Present • alarm_status = cleared
/SYS/FANx/TACH	<ul style="list-style-type: none"> • type = Fan • ipmi_name = FAN1/TACH • class = Threshold Sensor • value = 12208.000 RPM • upper_critical_threshold = 26705.000 RPM • lower_noncritical_threshold = 6322.000 RPM • alarm_status = cleared

Related Information

- [“Oracle ILOM Target Overview” on page 4](#)
- [“Oracle ILOM Targets and Descriptions” on page 5](#)
- [“Oracle ILOM General System Targets and Properties” on page 9](#)
- [“Oracle ILOM Indicator Targets and Properties” on page 12](#)
- [“Oracle ILOM Power Supply Targets and Properties” on page 13](#)
- [“Oracle ILOM Temperature Targets and Properties” on page 15](#)
- [“Oracle ILOM Voltage Targets and Properties” on page 17](#)
- [“Oracle ILOM General Targets and Properties” on page 22](#)
- [“Oracle ILOM Service Targets and Properties” on page 25](#)
- [“Oracle ILOM User and Session Targets and Properties” on page 27](#)

Oracle ILOM Indicator Targets and Properties

This table lists the Oracle ILOM `/SYS/I_indicator` indicator targets and their properties. Targets without properties are not listed.

Target and Path	Properties
/SYS/I_ATTENTION	<ul style="list-style-type: none"> • type = Indicator • ipmi_name = I_ATTENTION • value = Off
/SYS/I_LOCATOR	<ul style="list-style-type: none"> • type = Indicator • ipmi_name = I_LOCATOR • value = Off
/SYS/I_POWER	<ul style="list-style-type: none"> • type = Indicator • ipmi_name = I_POWER • value = On

Related Information

- [“Oracle ILOM Target Overview” on page 4](#)
- [“Oracle ILOM Targets and Descriptions” on page 5](#)
- [“Oracle ILOM General System Targets and Properties” on page 9](#)
- [“Oracle ILOM Fan Targets and Properties” on page 11](#)
- [“Oracle ILOM Power Supply Targets and Properties” on page 13](#)
- [“Oracle ILOM Temperature Targets and Properties” on page 15](#)
- [“Oracle ILOM Voltage Targets and Properties” on page 17](#)
- [“Oracle ILOM General Targets and Properties” on page 22](#)
- [“Oracle ILOM Service Targets and Properties” on page 25](#)
- [“Oracle ILOM User and Session Targets and Properties” on page 27](#)

Oracle ILOM Power Supply Targets and Properties

This table lists the Oracle ILOM /SYS/PSUX targets and their properties. Targets without properties are not listed.

Note – The /SYS/PSUX target is only available for currently present power supplies.

Target and Path	Properties
/SYS/PSUx	<ul style="list-style-type: none"> • type = Power Supply • ipmi_name = PSU0 • fru_name = A236 • fru_description = Power Supply • fru_manufacturer = Delta Energy Systems • fru_version = 01 • fru_part_number = 3002234 • fru_serial_number = 006541 • fru_extra_1 = sun_spec_part_number - 885-1390-01 • fru_extra_2 = ipmi_serial_number - 1841DET-0915B26541 • fru_extra_3 = ipmi_part_number - 300-2234-01
/SYS/PSUx/PRSNT	<ul style="list-style-type: none"> • type = Entity Presence • ipmi_name = PSU0/PRSNT • class = Discrete Sensor • value = Present • alarm_status = cleared
/SYS/PSUx/ALERT	<ul style="list-style-type: none"> • type = OEM • ipmi_name = PSU0/ALERT • class = Discrete Sensor • value = State Deasserted • alarm_status = cleared
/SYS/PSUx/AC_PRESENT	<ul style="list-style-type: none"> • type = OEM • ipmi_name = PSU0/AC_PRESENT • class = Discrete Sensor • value = State Deasserted • alarm_status = cleared

Related Information

- [“Oracle ILOM Target Overview” on page 4](#)
- [“Oracle ILOM Targets and Descriptions” on page 5](#)
- [“Oracle ILOM General System Targets and Properties” on page 9](#)
- [“Oracle ILOM Fan Targets and Properties” on page 11](#)
- [“Oracle ILOM Indicator Targets and Properties” on page 12](#)
- [“Oracle ILOM Temperature Targets and Properties” on page 15](#)
- [“Oracle ILOM Voltage Targets and Properties” on page 17](#)
- [“Oracle ILOM General Targets and Properties” on page 22](#)

- [“Oracle ILOM Service Targets and Properties” on page 25](#)
- [“Oracle ILOM User and Session Targets and Properties” on page 27](#)

Oracle ILOM Temperature Targets and Properties

This table lists the Oracle ILOM /SYS/MB temperature parameter targets and their properties. Targets without properties are not listed.

Target and Path	Properties
/SYS/MB/T_B0	<ul style="list-style-type: none"> • type = Temperature • ipmi_name = MB/T_B0 • class = Threshold Sensor • value = 49.000 degree C • upper_nonrecov_threshold = 70.000 degree C • upper_critical_threshold = 70.000 degree C • alarm_status = cleared
/SYS/MB/T_B1	<ul style="list-style-type: none"> • type = Temperature • ipmi_name = MB/T_B1 • class = Threshold Sensor • value = 54.000 degree C • upper_nonrecov_threshold = 70.000 degree C • upper_critical_threshold = 70.000 degree C • alarm_status = cleared
/SYS/MB/T_BACK	<ul style="list-style-type: none"> • type = Temperature • ipmi_name = MB/T_BACK • class = Threshold Sensor • value = 27.000 degree C • upper_nonrecov_threshold = 80.000 degree C • upper_critical_threshold = 70.000 degree C • alarm_status = cleared

Target and Path	Properties
/SYS/MB/T_FRONT	<ul style="list-style-type: none"> • type = Temperature • ipmi_name = MB/T_FRONT • class = Threshold Sensor • value = 28.000 degree C • upper_nonrecov_threshold = 80.000 degree C • upper_critical_threshold = 70.000 degree C • alarm_status = cleared
/SYS/MB/T_I4A	<ul style="list-style-type: none"> • type = Temperature • ipmi_name = MB/T_I4A • class = Threshold Sensor • value = 45.000 degree C • upper_nonrecov_threshold = 100.000 degree C • upper_critical_threshold = 70.000 degree C • alarm_status = cleared
/SYS/MB/T_SP	<ul style="list-style-type: none"> • type = Temperature • ipmi_name = MB/T_SP • class = Threshold Sensor • value = 41.000 degree C • upper_nonrecov_threshold = 70.000 degree C • upper_critical_threshold = 60.000 degree C • alarm_status = cleared

Related Information

- [“Oracle ILOM Target Overview” on page 4](#)
- [“Oracle ILOM Targets and Descriptions” on page 5](#)
- [“Oracle ILOM General System Targets and Properties” on page 9](#)
- [“Oracle ILOM Fan Targets and Properties” on page 11](#)
- [“Oracle ILOM Indicator Targets and Properties” on page 12](#)
- [“Oracle ILOM Power Supply Targets and Properties” on page 13](#)
- [“Oracle ILOM Voltage Targets and Properties” on page 17](#)
- [“Oracle ILOM General Targets and Properties” on page 22](#)
- [“Oracle ILOM Service Targets and Properties” on page 25](#)
- [“Oracle ILOM User and Session Targets and Properties” on page 27](#)

Oracle ILOM Voltage Targets and Properties

This table lists the Oracle ILOM /SYS/MB voltage parameter and state targets, and their properties. Targets without properties are not listed.

Target and Path	Properties
/SYS/MB/V_1.0V	<ul style="list-style-type: none">• type = Voltage• ipmi_name = MB/V_1.0V• class = Threshold Sensor• value = 1.006 Volts• upper_nonrecov_threshold = 1.252 Volts• upper_critical_threshold = 1.205 Volts• upper_noncritical_threshold = 1.158 Volts• lower_noncritical_threshold = 0.877 Volts• lower_critical_threshold = 0.819 Volts• lower_nonrecov_threshold = 0.749 Volts• alarm_status = cleared
/SYS/MB/V_1.2VStby	<ul style="list-style-type: none">• type = Voltage• ipmi_name = MB/V_1.2VStby• class = Threshold Sensor• value = 1.203 Volts• upper_nonrecov_threshold = 1.494 Volts• upper_critical_threshold = 1.436 Volts• upper_noncritical_threshold = 1.387 Volts• lower_noncritical_threshold = 1.048 Volts• lower_critical_threshold = 0.999 Volts• lower_nonrecov_threshold = 0.892 Volts• alarm_status = cleared
/SYS/MB/V_1.8V	<ul style="list-style-type: none">• type = Voltage• ipmi_name = MB/V_1.8V• class = Threshold Sensor• value = 1.785 Volts• upper_nonrecov_threshold = 1.979 Volts• upper_critical_threshold = 1.940 Volts• upper_noncritical_threshold = 1.891 Volts• lower_noncritical_threshold = 1.697 Volts• lower_critical_threshold = 1.639 Volts• lower_nonrecov_threshold = 1.591 Volts• alarm_status = cleared

Target and Path	Properties
/SYS/MB/V_2.5V	<ul style="list-style-type: none"> • type = Voltage • ipmi_name = MB/V_2.5V • class = Threshold Sensor • value = 2.480 Volts • upper_nonrecov_threshold = 2.878 Volts • upper_critical_threshold = 2.679 Volts • upper_noncritical_threshold = 2.586 Volts • lower_noncritical_threshold = 2.387 Volts • lower_critical_threshold = 2.282 Volts • lower_nonrecov_threshold = 2.083 Volts • alarm_status = cleared
/SYS/MB/V_3.3VMain	<ul style="list-style-type: none"> • type = Voltage • ipmi_name = MB/V_3.3VMain • class = Threshold Sensor • value = 3.283 Volts • upper_nonrecov_threshold = 3.540 Volts • upper_critical_threshold = 3.454 Volts • upper_noncritical_threshold = 3.403 Volts • lower_noncritical_threshold = 3.112 Volts • lower_critical_threshold = 3.061 Volts • lower_nonrecov_threshold = 2.958 Volts • alarm_status = cleared
/SYS/MB/V_3.3VStby	<ul style="list-style-type: none"> • type = Voltage • ipmi_name = MB/V_3.3VStby • class = Threshold Sensor • value = 3.420 Volts • upper_nonrecov_threshold = 3.540 Volts • upper_critical_threshold = 3.454 Volts • upper_noncritical_threshold = 3.403 Volts • lower_noncritical_threshold = 3.112 Volts • lower_critical_threshold = 3.061 Volts • lower_nonrecov_threshold = 2.958 Volts • alarm_status = warning

Target and Path	Properties
/SYS/MB/V_5V	<ul style="list-style-type: none"> • type = Voltage • ipmi_name = MB/V_5V • class = Threshold Sensor • value = 5.018 Volts • upper_nonrecov_threshold = 5.902 Volts • upper_critical_threshold = 5.694 Volts • upper_noncritical_threshold = 5.486 Volts • lower_noncritical_threshold = 4.498 Volts • lower_critical_threshold = 4.290 Volts • lower_nonrecov_threshold = 4.108 Volts • alarm_status = cleared
/SYS/MB/V_12V	<ul style="list-style-type: none"> • type = Voltage • ipmi_name = MB/V_12V • class = Threshold Sensor • value = 11.966 Volts • upper_nonrecov_threshold = 12.710 Volts • upper_critical_threshold = 12.524 Volts • upper_noncritical_threshold = 12.338 Volts • lower_noncritical_threshold = 11.346 Volts • lower_critical_threshold = 11.160 Volts • lower_nonrecov_threshold = 10.974 Volts • alarm_status = cleared
/SYS/MB/V_BAT	<ul style="list-style-type: none"> • type = Voltage • ipmi_name = MB/V_BAT • class = Threshold Sensor • value = 3.120 Volts • upper_critical_threshold = 3.494 Volts • lower_noncritical_threshold = 2.746 Volts • lower_critical_threshold = 2.621 Volts • alarm_status = cleared

Target and Path	Properties
/SYS/MB/V_BX1.2V	<ul style="list-style-type: none"> • type = Voltage • ipmi_name = MB/V_BX1.2V • class = Threshold Sensor • value = 1.193 Volts • upper_nonrecov_threshold = 1.498 Volts • upper_critical_threshold = 1.462 Volts • upper_noncritical_threshold = 1.392 Volts • lower_noncritical_threshold = 1.041 Volts • lower_critical_threshold = 0.994 Volts • lower_nonrecov_threshold = 0.901 Volts • alarm_status = cleared
/SYS/MB/V_I41.2V	<ul style="list-style-type: none"> • type = Voltage • ipmi_name = MB/V_I41.2V • class = Threshold Sensor • value = 1.217 Volts • upper_nonrecov_threshold = 1.498 Volts • upper_critical_threshold = 1.462 Volts • upper_noncritical_threshold = 1.392 Volts • lower_noncritical_threshold = 1.041 Volts • lower_critical_threshold = 0.994 Volts • lower_nonrecov_threshold = 0.901 Volts • alarm_status = cleared
/SYS/MB/V_V1P2ANG	<ul style="list-style-type: none"> • type = Voltage • ipmi_name = MB/V_V1P2ANG • class = Threshold Sensor • value = 1.182 Volts • upper_nonrecov_threshold = 1.498 Volts • upper_critical_threshold = 1.462 Volts • upper_noncritical_threshold = 1.392 Volts • lower_noncritical_threshold = 1.135 Volts • lower_critical_threshold = 1.123 Volts • lower_nonrecov_threshold = 0.901 Volts • alarm_status = cleared

Target and Path	Properties
/SYS/MB/V_V1P2DIG	<ul style="list-style-type: none"> • type = Voltage • ipmi_name = MB/V_V1P2DIG • class = Threshold Sensor • value = 1.182 Volts • upper_nonrecov_threshold = 1.498 Volts • upper_critical_threshold = 1.462 Volts • upper_noncritical_threshold = 1.392 Volts • lower_noncritical_threshold = 1.135 Volts • lower_critical_threshold = 1.123 Volts • lower_nonrecov_threshold = 0.901 Volts • alarm_status = cleared
/SYS/MB/V_1.0VOK	<ul style="list-style-type: none"> • type = OEM • ipmi_name = MB/V_1.0VOK • class = Discrete Sensor • value = State Deasserted • alarm_status = cleared
/SYS/MB/V_1.8VOK	<ul style="list-style-type: none"> • type = OEM • ipmi_name = MB/V_1.8VOK • class = Discrete Sensor • value = State Deasserted • alarm_status = cleared
/SYS/MB/V_2.5VOK	<ul style="list-style-type: none"> • type = OEM • ipmi_name = MB/V_2.5VOK • class = Discrete Sensor • value = State Deasserted • alarm_status = cleared
/SYS/MB/V_3.3VMain OK	<ul style="list-style-type: none"> • type = OEM • ipmi_name = MB/V_3.3VMainOK • class = Discrete Sensor • value = State Deasserted • alarm_status = cleared
/SYS/MB/V_5VOK	<ul style="list-style-type: none"> • type = OEM • ipmi_name = MB/V_5VOK • class = Discrete Sensor • value = State Deasserted • alarm_status = cleared

Target and Path	Properties
/SYS/MB/V_BX1.2VOK	<ul style="list-style-type: none"> • type = OEM • ipmi_name = MB/V_BX1.2VOK • class = Discrete Sensor • value = State Deasserted • alarm_status = cleared
/SYS/MB/V_ECB	<ul style="list-style-type: none"> • type = OEM • ipmi_name = MB/V_ECB • class = Discrete Sensor • value = State Deasserted • alarm_status = cleared
/SYS/MB/V_I41.2VOK	<ul style="list-style-type: none"> • type = OEM • ipmi_name = MB/V_I41.2VOK • class = Discrete Sensor • value = State Deasserted • alarm_status = cleared

Related Information

- [“Oracle ILOM Target Overview” on page 4](#)
- [“Oracle ILOM Targets and Descriptions” on page 5](#)
- [“Oracle ILOM General System Targets and Properties” on page 9](#)
- [“Oracle ILOM Fan Targets and Properties” on page 11](#)
- [“Oracle ILOM Indicator Targets and Properties” on page 12](#)
- [“Oracle ILOM Power Supply Targets and Properties” on page 13](#)
- [“Oracle ILOM Temperature Targets and Properties” on page 15](#)
- [“Oracle ILOM General Targets and Properties” on page 22](#)
- [“Oracle ILOM Service Targets and Properties” on page 25](#)
- [“Oracle ILOM User and Session Targets and Properties” on page 27](#)

Oracle ILOM General Targets and Properties

This table lists general Oracle 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	<ul style="list-style-type: none"> • hostname = us-gw-1 • system_contact = (none) • system_description = Sun Datacenter InfiniBand Switch GW, ILOM v2.0.5-1, r47111 • system_identifier = (none) • system_location = (none)
/SP/alertmgmt/rules/1	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • timeout = 0
/SP/clients/dns	<ul style="list-style-type: none"> • auto_dns = enabled • nameserver = (none) • retries = 1 • searchpath = (none) • timeout = 5
/SP/clients/ntp/server/1	<ul style="list-style-type: none"> • address = 0.0.0.0
/SP/clients/ntp/server/2	<ul style="list-style-type: none"> • address = 0.0.0.0
/SP/clients/smtp	<ul style="list-style-type: none"> • address = 0.0.0.0 • custom_sender = (none) • port = 25 • send_test_email_to = (Cannot show property) • state = disabled
/SP/clients/syslog/1	<ul style="list-style-type: none"> • address = 0.0.0.0
/SP/clients/syslog/2	<ul style="list-style-type: none"> • address = 0.0.0.0
/SP/clock	<ul style="list-style-type: none"> • datetime = Thu Oct 15 02:54:28 2009 • timezone = UTC • usentpserver = disabled

Target and Path	Properties
/SP/config	<ul style="list-style-type: none"> • dump_uri = (Cannot show property) • load_uri = (Cannot show property) • passphrase = none
/SP/diag/snapshot	<ul style="list-style-type: none"> • dataset = normal • dump_uri = (Cannot show property) • encrypt_output = false • result = (none)
/SP/logs/event	<ul style="list-style-type: none"> • clear = (Cannot show property)
/SP/network	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • ping = (Cannot show property)

Related Information

- [“Oracle ILOM Target Overview” on page 4](#)
- [“Oracle ILOM Targets and Descriptions” on page 5](#)
- [“Oracle ILOM General System Targets and Properties” on page 9](#)
- [“Oracle ILOM Fan Targets and Properties” on page 11](#)
- [“Oracle ILOM Indicator Targets and Properties” on page 12](#)
- [“Oracle ILOM Power Supply Targets and Properties” on page 13](#)
- [“Oracle ILOM Temperature Targets and Properties” on page 15](#)
- [“Oracle ILOM Voltage Targets and Properties” on page 17](#)
- [“Oracle ILOM Service Targets and Properties” on page 25](#)
- [“Oracle ILOM User and Session Targets and Properties” on page 27](#)

Oracle ILOM Service Targets and Properties

This table lists the Oracle ILOM `/SP/services` targets and their properties. Targets without properties are not listed.

Note – The `/SP/services/snmp/users/snmpuser` target was created for this table so that the default SNMP user properties could be displayed.

Target and Path	Properties
<code>/SP/services/http</code>	<ul style="list-style-type: none">• <code>port</code> = 80• <code>secureredirect</code> = enabled• <code>servicestate</code> = disabled
<code>/SP/services/https</code>	<ul style="list-style-type: none">• <code>port</code> = 443• <code>servicestate</code> = enabled
<code>/SP/services/https/ssl</code>	<ul style="list-style-type: none">• <code>cert_status</code> = Using Default (No custom certificate or private key loaded)
<code>/SP/services/https/ssl/custom_cert</code>	<ul style="list-style-type: none">• <code>clear_action</code> = (Cannot show property)• <code>issuer</code> = (none)• <code>load_uri</code> = (Cannot show property)• <code>subject</code> = (none)• <code>valid_from</code> = (none)• <code>valid_until</code> = (none)
<code>/SP/services/https/ssl/custom_key</code>	<ul style="list-style-type: none">• <code>clear_action</code> = (Cannot show property)• <code>key_present</code> = false• <code>load_uri</code> = (Cannot show property)
<code>/SP/services/https/ssl/default_cert</code>	<ul style="list-style-type: none">• <code>issuer</code> = /C=US/ST=California/L=Santa Clara/O=Sun Microsystems, Inc./CN=sun-ilom• <code>subject</code> = /C=US/ST=California/L=Santa Clara/O=Sun Microsystems, Inc./CN=sun-ilom• <code>valid_from</code> = Apr 27 17:10:36 2005 GMT• <code>valid_until</code> = Apr 25 17:10:36 2015 GMT
<code>/SP/services/ipmi</code>	<ul style="list-style-type: none">• <code>servicestate</code> = enabled
<code>/SP/services/servicetag</code>	<ul style="list-style-type: none">• <code>passphrase</code> = none• <code>state</code> = enabled

Target and Path	Properties
/SP/services/snmp	<ul style="list-style-type: none"> • engineid = (none) • port = 161 • servicestate = enabled • sets = disabled • v1 = disabled • v2c = disabled • v3 = enabled
/SP/services/snmp/communities/private	<ul style="list-style-type: none"> • permission = rw
/SP/services/snmp/communities/public	<ul style="list-style-type: none"> • permission = ro
/SP/services/snmp/mibs	<ul style="list-style-type: none"> • dump_uri = (Cannot show property)
/SP/services/snmp/users/snmpuser	<ul style="list-style-type: none"> • authenticationpassword = (Cannot show property) • authenticationprotocol = MD5 • permission = ro • privacypassword = (Cannot show property) • privacyprotocol = none

Related Information

- [“Oracle ILOM Target Overview” on page 4](#)
- [“Oracle ILOM Targets and Descriptions” on page 5](#)
- [“Oracle ILOM General System Targets and Properties” on page 9](#)
- [“Oracle ILOM Fan Targets and Properties” on page 11](#)
- [“Oracle ILOM Indicator Targets and Properties” on page 12](#)
- [“Oracle ILOM Power Supply Targets and Properties” on page 13](#)
- [“Oracle ILOM Temperature Targets and Properties” on page 15](#)
- [“Oracle ILOM Voltage Targets and Properties” on page 17](#)
- [“Oracle ILOM General Targets and Properties” on page 22](#)
- [“Oracle ILOM User and Session Targets and Properties” on page 27](#)

Oracle ILOM User and Session Targets and Properties

This table lists the Oracle 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
<code>/SP/sessions/1</code>	<ul style="list-style-type: none">• <code>username = ilom-admin</code>• <code>role = aucro</code>• <code>starttime = Thu Oct 15 02:36:11 2009</code>• <code>type = shell</code>• <code>mode = normal</code>
<code>/SP/users/ilom-admin</code>	<ul style="list-style-type: none">• <code>role = aucro</code>• <code>password = *****</code>
<code>/SP/users/ilom-operator</code>	<ul style="list-style-type: none">• <code>role = o</code>• <code>password = *****</code>

Related Information

- [“Oracle ILOM Target Overview” on page 4](#)
- [“Oracle ILOM Targets and Descriptions” on page 5](#)
- [“Oracle ILOM General System Targets and Properties” on page 9](#)
- [“Oracle ILOM Fan Targets and Properties” on page 11](#)
- [“Oracle ILOM Indicator Targets and Properties” on page 12](#)
- [“Oracle ILOM Power Supply Targets and Properties” on page 13](#)
- [“Oracle ILOM Temperature Targets and Properties” on page 15](#)
- [“Oracle ILOM Voltage Targets and Properties” on page 17](#)
- [“Oracle ILOM General Targets and Properties” on page 22](#)
- [“Oracle ILOM Service Targets and Properties” on page 25](#)

Administering Oracle ILOM (CLI)

These topics describe how to administer Oracle ILOM from the CLI.

- [“CLI Overview” on page 29](#)
- [“Accessing Oracle ILOM From the CLI” on page 30](#)
- [“Switching Between the Oracle ILOM Shell and the Linux Shell” on page 32](#)
- [“Monitoring Oracle ILOM Targets \(CLI\)” on page 39](#)
- [“Controlling Oracle ILOM Targets \(CLI\)” on page 67](#)
- [“Upgrading the Gateway Firmware Through Oracle ILOM \(CLI\)” on page 105](#)

Related Information

- [“Administering Oracle ILOM \(Web\)” on page 115](#)
- [“Using the Fabric Monitor” on page 169](#)
- [“Administering Oracle ILOM \(SNMP\)” on page 199](#)
- [“Administering Hardware \(IPMI\)” on page 257](#)
- [“Understanding Oracle ILOM Commands” on page 265](#)

CLI Overview

The Oracle 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).

For a list of the basic commands in the Oracle ILOM CLI, see [“Understanding Oracle ILOM Commands”](#) on page 265.

Related Information

- [“Understanding Oracle ILOM Targets”](#) on page 4
- [“Access Oracle ILOM From the Web Interface”](#) on page 118
- [“Switching Between the Oracle ILOM Shell and the Linux Shell”](#) on page 32
- [“Monitoring Oracle ILOM Targets \(CLI\)”](#) on page 39
- [“Controlling Oracle ILOM Targets \(CLI\)”](#) on page 67

Accessing Oracle ILOM From the CLI

You use the same method to access the Oracle ILOM shell as you would the management controller. Specifying the user name determines the shell (Linux or Oracle ILOM) that is presented.

- [“Access the Oracle ILOM Shell From the CLI \(NET MGT Port\)”](#) on page 30
- [“Access the Oracle ILOM Shell From the CLI \(USB Management Port\)”](#) on page 31

Related Information

- *Gateway Installation*, accessing the management controller
- [“Access Oracle ILOM From the Web Interface”](#) on page 118
- [“Monitoring Oracle ILOM Targets \(CLI\)”](#) on page 39
- [“Controlling Oracle ILOM Targets \(CLI\)”](#) on page 67
- [“Switching Between the Oracle ILOM Shell and the Linux Shell”](#) on page 32

▼ Access the Oracle ILOM Shell From the CLI (NET MGT Port)

1. **If you have not already done so, configure the DHCP server with the MAC address and new host name of the management controller inside of the gateway.**

The MAC address is printed on the customer information (yellow) sheet on the outside of the gateway shipping carton and on the pull-out tab on the left side front of the gateway, adjacent to power supply 0.

2. Open an SSH session and connect to the management controller by specifying the controller's host name.

For example:

```
% ssh -l ilom-admin nm2name
ilom-admin@nm2name's password: password
->
```

where *nm2name* is the host name of the management controller. Initially, the password is *ilom-admin*.

Note – You can change the *password* at a later time. See [“Change an Oracle ILOM User’s Password and or Role \(CLI\)” on page 84](#) for instructions on how to change Oracle ILOM user passwords.

The Oracle 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

- [“Access the Oracle ILOM Shell From the CLI \(USB Management Port\)” on page 31](#)

▼ Access the Oracle ILOM Shell From the CLI (USB Management Port)

1. If you have not already done so, connect a USB-to-serial adapter to the USB port of the gateway.
2. Connect a serial terminal, terminal server, or workstation with a TIP connection to the USB-to-serial adapter.

Configure the terminal or terminal emulator with these settings:

- 115200 baud
- 8 bits
- No parity
- 1 Stop bit
- No handshaking

3. Press the Return or Enter key on the serial device several times to synchronize the connection.

You might see text similar to this.

```
...
CentOS release 5.2 (Final)
Kernel 2.6.27.13-nm2 on an i686

nm2name login:
```

where *nm2name* is the host name of the management controller.

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

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

```
nm2name login: ilom-admin
Password: password
->
```

Note – As shipped, the `ilom-admin` user password is `ilom-admin`. See [“Change an Oracle ILOM User’s Password and or Role \(CLI\)” on page 84](#) for instructions on how to change Oracle ILOM user passwords.

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

Related Information

- [“Access the Oracle ILOM Shell From the CLI \(NET MGT Port\)” on page 30](#)

Switching Between the Oracle ILOM Shell and the Linux Shell

If you accessed the management controller as the `root` user within the Linux shell, you can switch to the Oracle ILOM shell with the `spsh` command. Similarly, if you accessed the management controller as an Oracle ILOM user within the Oracle ILOM shell, you can switch to the Linux shell through the `/SYS/Switch_Diag`, `/SYS/Gateway_Mgmt`, or `/SYS/Fabric_Mgmt` target.

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

- [“/SYS/Switch_Diag, /SYS/Gateway_Mgmt, and /SYS/Fabric_Mgmt Linux Shells” on page 33](#)
- [“Switch From the Oracle ILOM Shell to the Linux Shell” on page 36](#)
- [“Switch From the Linux Shell to the Oracle ILOM Shell” on page 38](#)

Related Information

- [“Accessing Oracle ILOM From the CLI” on page 30](#)

/SYS/Switch_Diag, /SYS/Gateway_Mgmt, and /SYS/Fabric_Mgmt Linux Shells

The preferred method of accessing the Linux shell is through the /SYS/Switch_Diag, /SYS/Gateway_Mgmt, and /SYS/Fabric_Mgmt Linux shell targets of the Oracle ILOM CLI interface.

Using the show command on the /SYS/Switch_Diag target opens a restricted Linux shell that enables the ilom-admin user, ilom-operator user, and users with similar permissions, to run diagnostic commands.

Using the show command on the /SYS/Gateway_Mgmt target opens a different restricted Linux shell that enables the ilom-admin user, and users with similar permissions, to run both diagnostic and gateway management commands.

Using the show command on the /SYS/Fabric_Mgmt target opens still an other restricted Linux shell that enables the ilom-admin user, and users with similar permissions, to run diagnostic, gateway, and fabric management commands.

Note – The ilom-operator user cannot access the Linux shell from either the /SYS/Gateway_Mgmt or /SYS/Fabric_Mgmt target.

This table lists the Linux shell commands and their availability from the respective Linux shell targets. Typing the help all command from within the restricted shells lists the commands available to that shell.

Note – Linux shell commands that are not listed are unavailable from the /SYS/Switch_Diag, /SYS/Gateway_Mgmt, or /SYS/Fabric_Mgmt targets.

Command	/SYS/Switch_Diag	/SYS/Gateway_Mgmt	/SYS/Fabric_Mgmt
addlagport		Available	Available
allowhostconfig		Available	Available
checkboot	Available	Available	Available
checkpower	Available	Available	Available
checktopomax			Available
checkvoltages	Available	Available	Available
connector	Available	Available	Available
createlag		Available	Available
createvlan		Available	Available
createvnic		Available	Available
dcsport	Available	Available	Available
deletelag		Available	Available
deletevlan		Available	Available
deletevnic		Available	Available
dellagport		Available	Available
disablecablelog			Available
disablegwport		Available	Available
disablelagmode		Available	Available
disablelinklog			Available
disablesm			Available
disableswitchport			Available
disablevnic		Available	Available
disallowhostconfig		Available	Available
enablecablelog			Available
enablegwport		Available	Available
enablelagmode		Available	Available
enablelinklog			Available
enablesm			Available
enableswitchport			Available
enablevnic		Available	Available

Command	/SYS/Switch_Diag	/SYS/Gateway_Mgmt	/SYS/Fabric_Mgmt
env_test	Available	Available	Available
exit	Available	Available	Available
fdconfig			Available
fwverify	Available	Available	Available
generatetopology			Available
getfanspeed	Available	Available	Available
getmaster	Available	Available	Available
getportcounters	Available	Available	Available
getportstatus	Available	Available	Available
help	Available	Available	Available
ibdiagnet			Available
ibhosts	Available	Available	Available
ibnetstatus	Available	Available	Available
ibnodes	Available	Available	Available
ibportstate	Available	Available	Available
ibroute	Available	Available	Available
ibrouters	Available	Available	Available
ibstat	Available	Available	Available
ibswitches	Available	Available	Available
ibtracert	Available	Available	Available
listlinkup	Available	Available	Available
matchtopology			Available
perfquery	Available	Available	Available
saquery			Available
setcontrolledhandover			Available
setdefaultgwdiscpkey		Available	Available
setgwethport		Available	Available
setgwinstance		Available	Available
setgws1		Available	Available
setgwsystemname		Available	Available
setmsmlocationmonitor			Available

Command	/SYS/Switch_Diag	/SYS/Gateway_Mgmt	/SYS/Fabric_Mgmt
setsmmkey			Available
setsmpriority			Available
setsubnetprefix			Available
showfruinfo	Available	Available	Available
showgwconfig		Available	Available
showgwports		Available	Available
showlag		Available	Available
showpsufu	Available	Available	Available
showsmlog	Available	Available	Available
showtemps	Available	Available	Available
showtopology	Available	Available	Available
showunhealthy	Available	Available	Available
showvlan		Available	Available
showvnics		Available	Available
smconfigtest			Available
smnodes			Available
smpartition			Available
smpquery	Available	Available	Available
version	Available	Available	Available

Related Information

- [“show Command” on page 275](#)
- [“Switch From the Oracle ILOM Shell to the Linux Shell” on page 36](#)
- [“Switch From the Linux Shell to the Oracle ILOM Shell” on page 38](#)

▼ Switch From the Oracle ILOM Shell to the Linux Shell

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30.](#)

2. Switch to the Linux shell.

```
-> show /SYS/Switch_Diag
```

NOTE: show on Switch_Diag will launch a restricted Linux shell.
User can execute switch diagnosis and IB monitoring commands in the shell. To view the list of commands, use "help" at rsh prompt.

Use exit command at rsh prompt to revert back to ILOM shell.

```
Diag@hostname->
```

Or.

```
-> show /SYS/Gateway_Mgmt
```

NOTE: show on Gateway_Mgmt will launch a restricted Linux shell.
User can execute switch diagnosis, Ethernet Gateway resource administration and configuration commands and IB monitoring commands in the shell. To view the list of commands, use "help" at rsh prompt.

Use exit command at rsh prompt to revert back to ILOM shell.

```
GWMan@hostname->
```

Or.

```
-> show /SYS/Fabric_Mgmt
```

NOTE: show on Fabric_Mgmt will launch a restricted Linux shell.
User can execute switch diagnosis, SM Configuration and IB monitoring commands in the shell. To view the list of commands, use "help" at rsh prompt.

Use exit command at rsh prompt to revert back to ILOM shell.

```
FabMan@hostname->
```

where *hostname* is the host name of the management controller.

You are now in the Linux shell.

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

If you try to switch to the /SYS/Gateway_Mgmt or /SYS/Fabric_Mgmt Linux

shell as the ilom-operator user, this message is displayed.

```
-> show /SYS/Gateway_Mgmt  
show: User role does not allow this action to be performed  
->
```

Related Information

- [“show Command” on page 275](#)
- [“exit Command \(ILOM\)” on page 270](#)
- [“/SYS/Switch_Diag, /SYS/Gateway_Mgmt, and /SYS/Fabric_Mgmt Linux Shells” on page 33](#)
- [“Switch From the Linux Shell to the Oracle ILOM Shell” on page 38](#)

▼ Switch From the Linux Shell to the Oracle ILOM Shell

1. Access the management controller.

See *Gateway Administration*, accessing the management controller.

2. Switch to the Oracle ILOM shell.

```
# spsb  
Oracle(R) Integrated Lights Out Manager  
Version ILOM 3.0 r47111  
Copyright (c) 2010, Oracle and/or its affiliates. All rights reserved.  
->
```

You are now in the Oracle ILOM shell.

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

Related Information

- [“exit Command \(ILOM\)” on page 270](#)
- [“/SYS/Switch_Diag, /SYS/Gateway_Mgmt, and /SYS/Fabric_Mgmt Linux Shells” on page 33](#)
- [“Switch From the Oracle ILOM Shell to the Linux Shell” on page 36](#)

Monitoring Oracle ILOM Targets (CLI)

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

- [“Performing Daily Tasks \(CLI\)” on page 39](#)
- [“Checking the Status of Services \(CLI\)” on page 52](#)
- [“Verifying Other Aspects With Oracle ILOM \(CLI\)” on page 58](#)

Related Information

- [“Accessing Oracle ILOM From the CLI” on page 30](#)
- [“Controlling Oracle ILOM Targets \(CLI\)” on page 67](#)
- [“Monitoring Oracle ILOM Targets \(Web\)” on page 119](#)
- [“Upgrading the Gateway Firmware Through Oracle ILOM \(CLI\)” on page 105](#)
- [“Understanding Oracle ILOM Targets” on page 4](#)

Performing Daily Tasks (CLI)

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

- [“Display the Date \(CLI\)” on page 40](#)
- [“Display Gateway Status LEDs States \(CLI\)” on page 40](#)
- [“Display the Aggregate Sensors State \(CLI\)” on page 41](#)
- [“Aggregate Sensor States” on page 42](#)
- [“Display Power Supply Status \(CLI\)” on page 43](#)
- [“Display Board-Level Voltages \(CLI\)” on page 44](#)
- [“Board Level Voltages” on page 46](#)
- [“Display Internal Temperatures \(CLI\)” on page 47](#)
- [“Internal Temperature Sensors” on page 48](#)
- [“Display Fan Status \(CLI\)” on page 48](#)
- [“Display the Oracle ILOM Sessions \(CLI\)” on page 50](#)
- [“Display the Oracle ILOM Event Log \(CLI\)” on page 51](#)

Related Information

- [“Performing Daily Tasks \(Web\)” on page 119](#)

- [“Checking the Status of Services \(CLI\)” on page 52](#)
- [“Verifying Other Aspects With Oracle ILOM \(CLI\)” on page 58](#)

▼ Display the Date (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Display the date.

```
-> show /SP/clock datetime timezone
```

For example:

```
-> show /SP/clock datetime timezone
/SP/clock
Properties:
  datetime = Sat Oct 22 07:57:19 2011
  timezone = CEST (Europe/Oslo)
->
```

Related Information

- [“show Command” on page 275](#)
- [“Display the Date \(Web\)” on page 120](#)
- [“Display the Date and Time \(SNMP\)” on page 204](#)

▼ Display Gateway Status LEDs States (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Display the status of the Power LED.

```
-> show /SYS/I_POWER value
/SYS/I_POWER
Properties:
  value = On
->
```

3. Display the status of the Attention LED.

```
-> show /SYS/I_ATTENTION value  
/SYS/I_ATTENTION  
Properties:  
    value = Off  
->
```

4. Display the status of the Locator LED.

```
-> show /SYS/I_LOCATOR value  
/SYS/I_LOCATOR  
Properties:  
    value = Off  
->
```

Related Information

- [“show Command” on page 275](#)
- [“Display the Gateway Status LEDs States \(Web\)” on page 120](#)
- [“Display Gateway Status LED States \(IPMI\)” on page 263](#)
- [“Enable the Locator LED \(CLI\)” on page 70](#)
- [“Disable the Locator LED \(CLI\)” on page 71](#)

▼ Display the Aggregate Sensors State (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Display the aggregate sensor state.

```
-> show aggregate_sensor_target value alarm_status
```

where *aggregate_sensor_target* is from the table in “Aggregate Sensor States” on page 42.

For example, to display the overall gateway state:

```
-> show /SYS/CHASSIS_STATUS value alarm_status
/SYS/CHASSIS_STATUS
Properties:
  value = State Deasserted
  alarm_status = cleared
->
```

The value = State Deasserted and alarm_status = cleared means there are no faults.

Related Information

- “show Command” on page 275
- “Display the Aggregate Sensors State (Web)” on page 120
- “Display the Aggregate Sensors State (SNMP)” on page 205
- “Display the Sensor States (IPMI)” on page 258
- “Aggregate Sensor States” on page 42

Aggregate Sensor States

Nine aggregate sensors provide an overall status of particular aspects of the gateway. Each aggregate sensor is the logical and summation of many binary sensor checks.

When all of the checks are true, the respective aggregate sensor’s value property is set to State Deasserted, and the alarm_status property is set to cleared. This situation means all binary 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. That aspect of the gateway is in an unhealthy state.

Aspect	Aggregate Sensor Target
Overall connector hardware state	/SYS/CABLE_ATTN
Change in cable connectivity state	/SYS/CABLE_CONN_STAT

Aspect	Aggregate Sensor Target
Overall gateway state	/SYS/CHASSIS_STATUS
Overall cooling state	/SYS/COOLING_ATTN
Cooling redundancy state	/SYS/COOLING_REDUN
Overall I4 switch chip state	/SYS/IBDEV_ATTN
Overall power state	/SYS/POWER_ATTN
Power redundancy state	/SYS/POWER_REDUN
Overall temperature state	/SYS/TEMP_ATTN

Related Information

- [“Display the Aggregate Sensors State \(CLI\)” on page 41](#)
- [“Display the Aggregate Sensors State \(Web\)” on page 120](#)
- [“Display the Entity Numbers” on page 220](#)

▼ Display Power Supply Status (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Check for the presence of the power supply.

```
-> show /SYS/PSUx/PRSNT value
```

where x is either 0 (left power supply) or 1 (right power supply). For example:

```
-> show /SYS/PSU0/PRSNT value
/SYS/PSU0/PRSNT
Properties:
    value = Present
->
```

Note – The /SYS/PSU x target is available only for currently installed power supplies.

3. Check for the presence of input power.

```
-> show /SYS/PSUX/AC_PRESENT value alarm_status
/SYS/PSU0/AC_PRESENT
Properties:
    value = State Deasserted
    alarm_status = cleared
->
```

The value = State Deasserted and alarm_status = cleared means that there is no error, and input power is present.

4. Check for an alert.

```
-> show /SYS/PSUX/ALERT value alarm_status
/SYS/PSU0/ALERT
Properties:
    value = State Deasserted
    alarm_status = cleared
->
```

The value = State Deasserted and alarm_status = cleared means that there is no alert.

Related Information

- [“show Command” on page 275](#)
- [“Display Power Supply Status \(Web\)” on page 121](#)
- [“Display Power Supply Status \(SNMP\)” on page 206](#)

▼ Display Board-Level Voltages (CLI)

There are sensor targets that enable you to display the voltage levels and alarm states on the motherboard.

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Display the board-level voltage data.

```
-> show voltage_sensor_target value
```

where *voltage_sensor_target* is from the table in “Board Level Voltages” on page 46.
For example, to display the voltage of the main 1.8V source:

```
-> show /SYS/MB/V_1.8V value  
/SYS/MB/V_1.8V  
Properties:  
    value = 1.785 Volts  
->
```

3. For more sensor information, type.

```
-> show -d properties voltage_sensor_target
```

where *voltage_sensor_target* is from the table in “Board Level Voltages” on page 46.
For example, to display the properties of the main 1.8V source:

```
-> show -d properties /SYS/MB/V_1.8V  
/SYS/MB/V_1.8V  
Properties:  
    type = Voltage  
    ipmi_name = MB/V_1.8V  
    class = Threshold Sensor  
    value = 1.785 Volts  
    upper_nonrecov_threshold = 1.979 Volts  
    upper_critical_threshold = 1.940 Volts  
    upper_noncritical_threshold = 1.891 Volts  
    lower_noncritical_threshold = 1.697 Volts  
    lower_critical_threshold = 1.639 Volts  
    lower_nonrecov_threshold = 1.591 Volts  
    alarm_status = cleared  
->
```

Related Information

- “show Command” on page 275
- “Display Board-Level Voltages (Web)” on page 122
- “Display Board-Level Voltages (SNMP)” on page 208
- “Board Level Voltages” on page 46

Board Level Voltages

This table lists board voltages and their respective sensor targets, which enable you to check the voltage levels and alarm states.

Board Level Voltage	Voltage Sensor Target
Voltage of the main 1.0V source	/SYS/MB/V_1.0V
State of the main 1.0V source	/SYS/MB/V_1.0VOK
Voltage of the standby 1.2V source	/SYS/MB/V_1.2VStby
Voltage of the main 1.8V source	/SYS/MB/V_1.8V
State of the main 1.8V source	/SYS/MB/V_1.8VOK
Voltage of the main 2.5V source	/SYS/MB/V_2.5V
State of the main 2.5V source	/SYS/MB/V_2.5VOK
Voltage of the main 3.3V source	/SYS/MB/V_3.3VMain
State of the main 3.3V source	/SYS/MB/V_3.3VMainOK
Voltage of the standby 3.3V source	/SYS/MB/V_3.3VStby
Voltage of the main 5V source	/SYS/MB/V_5V
State of the main 5V source	/SYS/MB/V_5VOK
Voltage of the main 12V source	/SYS/MB/V_12V
Voltage of the battery	/SYS/MB/V_BAT
Voltage of the BridgeX main 1.2V source	/SYS/MB/V_BX1.2V
State of the BridgeX main 1.2V source	/SYS/MB/V_BX1.2VOK
State of the ECB	/SYS/MB/V_ECB
Voltage of the I4 switch chip	/SYS/MB/V_I41.2V
State of the I4 switch chip 1.2V source	/SYS/MB/V_I41.2VOK
Voltage of the 1.2V source for analog power pins.	/SYS/MB/V_V1P2ANG
Voltage of the 1.2V source for digital power pins.	/SYS/MB/V_V1P2DIG

Related Information

- [“Display Board-Level Voltages \(CLI\)” on page 44](#)
- [“Display Board-Level Voltages \(Web\)” on page 122](#)
- [“Display the Entity Numbers” on page 220](#)

▼ Display Internal Temperatures (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Display the internal temperatures.

```
-> show temperature_sensor_target value
```

where *temperature_sensor_target* is from the table in [“Internal Temperature Sensors” on page 48](#).

For example, to display the temperature at the front of the gateway:

```
-> show /SYS/MB/T_FRONT value  
/SYS/MB/T_FRONT  
Properties:  
    value = 27.000 degree C  
->
```

3. For more sensor information, type.

```
-> show -d properties temperature_sensor_target
```

where *temperature_sensor_target* is from the table in [“Internal Temperature Sensors” on page 48](#).

For example, to display the properties of the front temperature sensor:

```
-> show -d properties /SYS/MB/T_FRONT  
/SYS/MB/T_FRONT  
Properties:  
    type = Temperature  
    ipmi_name = MB/T_FRONT  
    class = Threshold Sensor  
    value = 33.000 degree C  
    upper_nonrecov_threshold = 80.000 degree C  
    upper_critical_threshold = 70.000 degree C  
    upper_noncritical_threshold = N/A  
    lower_noncritical_threshold = N/A  
    lower_critical_threshold = N/A  
    lower_nonrecov_threshold = N/A  
    alarm_status = cleared  
->
```

Related Information

- [“show Command” on page 275](#)
- [“Display Internal Temperatures \(Web\)” on page 122](#)
- [“Display Internal Temperatures \(SNMP\)” on page 212](#)
- [“Internal Temperature Sensors” on page 48](#)

Internal Temperature Sensors

This table provides the temperature sensor locations and their respective sensor targets.

Temperature Location	Temperature Sensor Target
Temperature of BridgeX chip 0	/SYS/MB/T_B0
Temperature of BridgeX chip 1	/SYS/MB/T_B1
Temperature at front of gateway	/SYS/MB/T_FRONT
Temperature of the I4 switch chip	/SYS/MB/T_I4A
Temperature of the management controller	/SYS/MB/T_SP
Temperature at rear of gateway	/SYS/MB/T_BACK

Related Information

- [“Display Internal Temperatures \(CLI\)” on page 47](#)
- [“Display Internal Temperatures \(Web\)” on page 122](#)
- [“Display the Entity Numbers” on page 220](#)

▼ Display Fan Status (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Check for the presence of the fan module.

```
-> show /SYS/FANx/PRSNT value
```

where *x* is either 0 (far left) to 4 (far right). For example:

```
-> show /SYS/FAN1/PRSNT value  
/SYS/FAN1/PRSNT  
Properties:  
    value = Present  
->
```

Note – The /SYS/FAN*x* target is available only for currently installed fans.

3. Display the fan speed.

```
-> show /SYS/FAN1/TACH value  
/SYS/FAN1/TACH  
Properties:  
    value = 12208.000 RPM  
->
```

4. For more sensor information, type.

```
-> show -d properties /SYS/FAN1/TACH  
/SYS/FAN1/TACH  
Properties:  
    type = Fan  
    ipmi_name = FAN1/TACH  
    class = Threshold Sensor  
    value = 12208.000 RPM  
    upper_nonrecov_threshold = N/A  
    upper_critical_threshold = 26705.000 RPM  
    upper_noncritical_threshold = N/A  
    lower_noncritical_threshold = 6322.000 RPM  
    lower_critical_threshold = N/A  
    lower_nonrecov_threshold = N/A  
    alarm_status = cleared  
->
```

Related Information

- [“show Command” on page 275](#)
- [“Display Fan Status \(Web\)” on page 123](#)

- [“Display Fan Status \(SNMP\)” on page 215](#)

▼ Display the Oracle ILOM Sessions (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Display the active Oracle ILOM sessions.

```
-> show -d properties -l 2 /SP/sessions
```

For example:

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

```
-> 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
->
```

Related Information

- [“show Command” on page 275](#)
- [“Display the Oracle ILOM Sessions \(Web\)” on page 123](#)
- [“Display Oracle ILOM Sessions \(SNMP\)” on page 222](#)

▼ Display the Oracle ILOM Event Log (CLI)

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

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Display the Oracle ILOM event log.

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

For example:

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

```
-> 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
.
.
.
->
```

Related Information

- [“show Command” on page 275](#)
- [“Display the Oracle ILOM Event Log \(Web\)” on page 124](#)
- [“Display the Oracle ILOM Event Log \(SNMP\)” on page 223](#)
- [“Display the System Event Log \(IPMI\)” on page 261](#)

Checking the Status of Services (CLI)

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

- [“Display the HTTP Service Status \(CLI\)” on page 52](#)
- [“Display the HTTPS Service Status \(CLI\)” on page 53](#)
- [“Display the SSL Certificates \(CLI\)” on page 53](#)
- [“Display the SNMP Service Status \(CLI\)” on page 54](#)
- [“Display the SNMP User Accounts \(CLI\)” on page 54](#)
- [“Display the SNMP Service Communities \(CLI\)” on page 55](#)
- [“Display the IPMI Service Status \(CLI\)” on page 56](#)
- [“Display the DNS Client Status \(CLI\)” on page 56](#)
- [“Display the SMTP Client Status \(CLI\)” on page 57](#)
- [“Display the NTP Servers \(CLI\)” on page 57](#)

Related Information

- [“Checking the Status of Services \(Web\)” on page 124](#)
- [“Performing Daily Tasks \(CLI\)” on page 39](#)
- [“Verifying Other Aspects With Oracle ILOM \(CLI\)” on page 58](#)

▼ Display the HTTP Service Status (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Display the HTTP status.

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

Related Information

- [“show Command” on page 275](#)
- [“Display the HTTP Service Status \(Web\)” on page 125](#)
- [“Display the HTTP Service Status \(SNMP\)” on page 225](#)

▼ Display the HTTPS Service Status (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

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 275](#)
- [“Display the HTTPS Service Status \(Web\)” on page 125](#)
- [“Display the HTTPS Service Status \(SNMP\)” on page 226](#)

▼ Display the SSL Certificates (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

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 275](#)
- [“Display the SSL Certificates \(Web\)” on page 125](#)

▼ Display the SNMP Service Status (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Display the SNMP status.

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

Related Information

- [“show Command” on page 275](#)
- [“Display the SNMP Service Status \(Web\)” on page 126](#)

▼ Display the SNMP User Accounts (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Display the SNMP users.

```
-> show -d targets /SP/services/snmp/users
```

For example:

```
-> 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 275](#)
- [“Display the SNMP Service User Accounts \(Web\)” on page 126](#)

▼ Display the SNMP Service Communities (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

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 275](#)
- [“Display the SNMP Service Communities \(Web\)” on page 127](#)

▼ Display the IPMI Service Status (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Display the IPMI status.

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

Related Information

- [“show Command” on page 275](#)
- [“Display the IPMI Service Status \(Web\)” on page 127](#)
- [“Enable the IPMI Service \(CLI\)” on page 99](#)
- [“Disable the IPMI Service \(CLI\)” on page 99](#)

▼ Display the DNS Client Status (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Display the DNS status.

```
-> show -d properties /SP/clients/dns
/SP/clients/dns
Properties:
    auto_dns = enabled
    nameserver = 10.172.157.73, 10.172.157.74
    retries = 1
    searchpath = no.oracle.com
    timeout = 5
->
```

Related Information

- [“show Command” on page 275](#)
- [“Display the DNS Client Status \(Web\)” on page 127](#)
- [“Display the DNS Client Status \(SNMP\)” on page 226](#)
- [“Configure the DNS Client \(CLI\)” on page 73](#)

▼ Display the SMTP Client Status (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Display the SMTP client status.

Note – This example shows that the SMTP client is not enabled

```
-> show -d properties /SP/clients/smtp
/SP/clients/smtp
Properties:
  address = 0.0.0.0
  custom_sender = (none)
  port = 25
  send_test_email_to = (Cannot show property)
  state = disabled
->
```

Related Information

- [“show Command” on page 275](#)
- [“Display the SMTP Client Status \(Web\)” on page 128](#)
- [“Display the SMTP Client Status \(SNMP\)” on page 227](#)
- [“Configure the SMTP Client \(CLI\)” on page 74](#)

▼ Display the NTP Servers (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Display the IP addresses of the NTP servers.

```
-> show /SP/clients/ntp/server/1 address
/SP/clients/ntp/server/1
Properties:
address = 123.45.67.89

-> show /SP/clients/ntp/server/2 address
/SP/clients/ntp/server/2
Properties:
address = 0.0.0.0

->
```

In the output, the IP address of NTP server 1 is 123.45.67.89. The IP address of 0.0.0.0 for NTP server 2 means the server is not configured.

3. Display the NTP server status.

```
-> show /SP/clock usentpserver
/SP/clock
Properties:
usentpserver = disabled

->
```

The value of the `usentpserver` property determines if the management controller synchronizes time with the configured NTP servers. The value is either enabled or disabled.

Related Information

- [“show Command” on page 275](#)
- [“Display the Network Time Protocol Servers \(Web\)” on page 128](#)
- [“Display the NTP State \(SNMP\)” on page 227](#)
- [“Display the NTP Servers \(SNMP\)” on page 228](#)
- [“Set the Date and Time \(CLI\)” on page 69](#)

Verifying Other Aspects With Oracle ILOM (CLI)

These tasks display the status of aspects of Oracle ILOM not included in [“Performing Daily Tasks \(CLI\)” on page 39](#) or [“Checking the Status of Services \(CLI\)” on page 52](#).

- [“Get Help on an Oracle ILOM Command \(CLI\)” on page 59](#)
- [“Get Help on an Oracle ILOM Target Property \(CLI\)” on page 60](#)
- [“Display the Alert Properties \(CLI\)” on page 60](#)

- “Display the Oracle ILOM User Accounts (CLI)” on page 61
- “Display the Remote Log Hosts (CLI)” on page 62
- “Display the Network Management Configuration (CLI)” on page 63
- “Display the CLI Session Timeout (CLI)” on page 64
- “Display Gateway FRU ID (CLI)” on page 64
- “Display Power Supply FRU ID (CLI)” on page 65
- “Display the Firmware Version (CLI)” on page 66
- “Display System Identification Properties (CLI)” on page 66

Related Information

- “Verifying Other Aspects With Oracle ILOM (Web)” on page 129
- “Performing Daily Tasks (CLI)” on page 39
- “Checking the Status of Services (CLI)” on page 52

▼ Get Help on an Oracle ILOM Command (CLI)

1. Access the Oracle ILOM CLI.

See “Accessing Oracle ILOM From the CLI” on page 30.

2. Get help on a command.

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

where *command* is the Oracle 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 271
- “Get Help on an Oracle ILOM Target Property (CLI)” on page 60

▼ Get Help on an Oracle ILOM Target Property (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

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 271](#)
- [“Get Help on an Oracle ILOM Command \(CLI\)” on page 59](#)

▼ Display the Alert Properties (CLI)

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

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

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 275](#)
- [“Display the Alert Properties \(Web\)” on page 129](#)
- [“Display the Alert Properties \(SNMP\)” on page 229](#)
- [“Enable Alerts to Send SNMP Traps \(CLI\)” on page 100](#)
- [“Enable Alerts to Send PETs \(CLI\)” on page 102](#)
- [“Enable Alerts to Send Email Alerts \(CLI\)” on page 103](#)
- [“Disable Alerts \(CLI\)” on page 104](#)

▼ Display the Oracle ILOM User Accounts (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Display the Oracle ILOM user accounts.

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

3. Display the ilom-admin user's role.

```
-> show /SP/users/ilom-admin role
/SP/users/ilom-admin
Properties:
    role = aucro
->
```

Related Information

- [“show Command” on page 275](#)
- [“Display the Oracle ILOM User Accounts \(Web\)” on page 130](#)
- [“Display Oracle ILOM User Accounts \(SNMP\)” on page 230](#)

▼ Display the Remote Log Hosts (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Display the remote log hosts.

```
-> show /SP/clients/syslog/number address
```

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

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

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

Note – The address of 0.0.0.0 or (none) indicates that remote host 1 functionality is not configured.

Related Information

- [“show Command” on page 275](#)
- [“Display the Remote Log Hosts \(Web\)” on page 130](#)
- [“Display the Remote Log Hosts \(SNMP\)” on page 231](#)
- [“Set the Remote Log Hosts \(CLI\)” on page 72](#)

▼ Display the Network Management Configuration (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Display the network management configuration.

```
-> show -d properties /SP/network
```

For example:

```
-> show -d properties /SP/network
/SP/network
Properties:
  commitpending = (Cannot show property)
  dhcp_server_ip = 10.12.235.35
  ipaddress = 10.12.235.70
  ipdiscovery = dhcp
  ipgateway = 10.12.235.254
  ipnetmask = 255.255.255.0
  macaddress = 00:E0:4B:28:00:8E
  pendingipaddress = 10.12.235.70
  pendingipdiscovery = dhcp
  pendingipgateway = 10.12.235.254
  pendingipnetmask = 255.255.255.0
  state = enabled
->
```

Related Information

- [“show Command” on page 275](#)
- [“Display the Network Management Configuration \(Web\)” on page 131](#)
- [“Display the Network Management Configuration \(SNMP\)” on page 231](#)

▼ Display the CLI Session Timeout (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI”](#) on page 30.

2. Display the CLI session timeout.

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

Related Information

- [“show Command”](#) on page 275
- [“Display the CLI Session Timeout \(Web\)”](#) on page 131
- [“Set the Oracle ILOM CLI Session Timeout \(CLI\)”](#) on page 105

▼ Display Gateway FRU ID (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI”](#) on page 30.

2. Display the gateway FRU information.

```
-> show -d properties /SYS/MB
/SYS/MB
  Properties:
    type = Motherboard
    ipmi_name = MB
    product_name = Sun Datacenter InfiniBand Switch GW
    product_part_number = 5111402
    product_serial_number = 0110SJC-1099XY9992
    product_manufacturer = Sun Microsystems
    fru_name = Chassis and Motherboard
    fru_description = Chassis and Motherboard
    fru_extra_1 = ComEx: manufacturing_date - 2009.02.20
    fru_extra_2 = ComEx: serial_number - NCD3R0527
    fru_extra_3 = ComEx: hardware_rev - 0x100, firmware_rev - 0x102
    fru_extra_4 = ComEx: bios_version - NOW1R112
    , bios_date - 04/24/2009
->
```

Related Information

- [“show Command” on page 275](#)
- [“Display System Component FRU ID \(Web\)” on page 132](#)
- [“Display Gateway FRU ID \(SNMP\)” on page 232](#)
- [“Display FRU ID Information \(IPMI\)” on page 262](#)

▼ Display Power Supply FRU ID (CLI)

Note – You can only display FRU ID information for currently present power supplies.

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Display the power supply FRU information.

```
-> show -d properties /SYS/PSUslot
```

where *slot* is the slot of the power supply (0 or 1).

In the output, the FRU information is listed under Properties.

For example, for power supply 0:

```
-> show -d properties /SYS/PSU0
/SYS
Properties:
  type = Power Supply
  ipmi_name = PSU0
  fru_name = A247
  fru_description = Power Supply
  fru_manufacturer = Delta Energy Systems
  fru_version = 02
  fru_part_number = 3002233
  fru_serial_number = 001180
  fru_extra_1 = sun_spec_part_number - 885-1389-02
  fru_extra_2 = ipmi_serial_number - 1841DET-1008B51180
  fru_extra_3 = ipmi_part_number - 300-2233-02
->
```

Related Information

- [“show Command” on page 275](#)
- [“Display System Component FRU ID \(Web\)” on page 132](#)

- [“Display Power Supply FRU ID \(SNMP\)” on page 234](#)
- [“Display FRU ID Information \(IPMI\)” on page 262](#)

▼ Display the Firmware Version (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Display the firmware version.

```
-> version
```

For example:

```
-> version
SP firmware 2.0.5-1
SP firmware build number: 47111
SP firmware date: Sun Oct 16 14:03:22 IST 2011
SP filesystem version: 0.1.22
->
```

Related Information

- [“version Command \(ILOM\)” on page 277](#)
- [“Display the Oracle ILOM Version \(Web\)” on page 133](#)
- [“Display the Firmware Version \(SNMP\)” on page 239](#)

▼ Display System Identification Properties (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Display the identification properties.

```
-> show -d properties /SP
/SP/cli
Properties:
  hostname = us-gw-1
  system_contact = (none)
  system_description = Sun Datacenter InfiniBand Switch GW, ILOM v2.0.5-1,
r47111
```

```
system_identifier = (none)
system_location = (none)
->
```

Related Information

- [“Display System Identification Properties \(Web\)” on page 133](#)
- [“Display System Identification Properties \(SNMP\)” on page 239](#)
- [“Set the System Identification Properties \(CLI\)” on page 82](#)

Controlling Oracle ILOM Targets (CLI)

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

- [“Performing General Tasks on Oracle ILOM Targets \(CLI\)” on page 67](#)
- [“Performing Oracle ILOM User Tasks \(CLI\)” on page 83](#)
- [“Managing HTTP Services \(CLI\)” on page 86](#)
- [“Managing HTTPS Services \(CLI\)” on page 88](#)
- [“Managing SNMP Services \(CLI\)” on page 91](#)
- [“Managing IPMI Services \(CLI\)” on page 98](#)
- [“Managing Other Aspects With Oracle ILOM \(CLI\)” on page 100](#)

Related Information

- [“Accessing Oracle ILOM From the CLI” on page 30](#)
- [“Controlling Oracle ILOM Targets \(Web\)” on page 134](#)
- [“Monitoring Oracle ILOM Targets \(CLI\)” on page 39](#)
- [“Upgrading the Gateway Firmware Through Oracle ILOM \(CLI\)” on page 105](#)
- [“Understanding Oracle ILOM Targets” on page 4](#)

Performing General Tasks on Oracle ILOM Targets (CLI)

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

- [“Restart the Management Controller \(CLI\)” on page 68](#)

- “Set the Date and Time (CLI)” on page 69
- “Enable the Locator LED (CLI)” on page 70
- “Disable the Locator LED (CLI)” on page 71
- “Clear the Oracle ILOM Event Log (CLI)” on page 71
- “Set the Remote Log Hosts (CLI)” on page 72
- “Configure the DNS Client (CLI)” on page 73
- “Configure the SMTP Client (CLI)” on page 74
- “Back Up the Configuration (CLI)” on page 75
- “Gateway Configuration Information Backed Up” on page 76
- “Restore the Configuration (CLI)” on page 76
- “Create a Snapshot of the Gateway State (CLI)” on page 77
- “Snapshot Dataset Information (CLI)” on page 79
- “Set the Network Management Parameters (CLI)” on page 80
- “Set the System Identification Properties (CLI)” on page 82

Related Information

- “Performing General Tasks on Oracle ILOM Targets (Web)” on page 134
- “Performing Oracle ILOM User Tasks (CLI)” on page 83

▼ Restart the Management Controller (CLI)

Note – Restarting the management controller severs any management console link to the management controller. You must reaccess the management controller to regain administrative control.

1. Access the Oracle ILOM CLI.

See “Accessing Oracle ILOM From the CLI” on page 30.

2. Reset the management controller.

```
-> reset /SP
Are you sure you want to reset /SP (y/n)? y
->
```

The management controller is reset and you must reaccess the management controller to regain administrative control.

Related Information

- [“reset Command” on page 273](#)
- [Gateway Administration](#), restarting the management controller
- [“Restart the Management Controller \(Web\)” on page 135](#)

▼ Set the Date and Time (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Set the date and time.

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

where *MMDDhhmmYYYY* is the month, date, hour, and minute as two digits, and the year as four digits.

For example:

```
-> set /SP/clock datetime=100922352009  
Set 'datetime' to '100922352009'  
-> show /SP/clock datetime  
/SP/clock  
Properties:  
    datetime = Fri Oct  9 22:35:30 2009  
->
```

3. Set the time zone.

```
-> set /SP/clock timezone=XXX
```

where *XXX* is the identifier of the time zone.

For example:

```
-> set /SP/clock timezone=CET  
Set 'timezone' to 'CET'  
-> show /SP/clock timezone  
/SP/clock  
Properties:  
    timezone = CET  
->
```

4. (Optional) If you want to use a time server, follow these steps:

a. Set the IP addresses of the time servers.

```
-> set /SP/clients/ntp/server/number address=IP_address
```

where:

- *number* is 1 for the first time server and 2 for the second time server.
- *IP_address* is the IP address of the time server.

For example, to use the time servers with addresses 123.45.67.89 and 123.45.67.88:

```
-> set /SP/clients/ntp/server/1 address=123.45.67.89
Set 'address' to '123.45.67.89'
-> set /SP/clients/ntp/server/2 address=123.45.67.88
Set 'address' to '123.45.67.88'
->
```

b. Start using the time servers.

```
-> set /SP/clock usentpserver=enabled
Set 'usentpserver' to 'enabled'
->
```

The management controller is configured to use the time servers.

Related Information

- [“set Command” on page 274](#)
- [“Set the Date and Time \(Web\)” on page 136](#)
- [“Set the Date and Time \(SNMP\)” on page 241](#)

▼ Enable the Locator LED (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Enable the Locator LED.

```
-> set /SYS/I_LOCATOR value=on
Set 'value' to 'on'
->
```

The Locator LED flashes.

Related Information

- [“set Command” on page 274](#)
- [“Enable the Locator LED \(Web\)” on page 137](#)
- [“Enable the Locator LED \(IPMI\)” on page 264](#)
- [“Disable the Locator LED \(CLI\)” on page 71](#)
- [“Display Gateway Status LEDs States \(CLI\)” on page 40](#)

▼ Disable the Locator LED (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Disable the Locator LED.

```
-> set /SYS/I_LOCATOR value=off
Set 'value' to 'off'
->
```

The Locator LED is unlit.

Related Information

- [“set Command” on page 274](#)
- [“Disable the Locator LED \(Web\)” on page 137](#)
- [“Disable the Locator LED \(IPMI\)” on page 264](#)
- [“Enable the Locator LED \(CLI\)” on page 70](#)
- [“Display Gateway Status LEDs States \(CLI\)” on page 40](#)

▼ Clear the Oracle ILOM Event Log (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Clear the Oracle 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 Oracle ILOM event log is cleared.

Related Information

- [“set Command” on page 274](#)
- [“Clear the Oracle ILOM Event Log \(Web\)” on page 138](#)
- [“Clear the Oracle ILOM Event Log \(SNMP\)” on page 243](#)
- [“Display the Oracle ILOM Event Log \(CLI\)” on page 51](#)
- [“Set the Remote Log Hosts \(CLI\)” on page 72](#)

▼ Set the Remote Log Hosts (CLI)

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

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

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 274](#)
- [“Set the Remote Log Hosts \(Web\)” on page 138](#)
- [“Set the Remote Log Hosts \(SNMP\)” on page 243](#)
- [“Display the Remote Log Hosts \(CLI\)” on page 62](#)

▼ Configure the DNS Client (CLI)

To enable name services within the management controller, Oracle ILOM must be configured as a DNS client.

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI”](#) on page 30.

2. Configure the client with the DNS server information.

```
-> set /SP/clients/dns auto_dns=state nameserver=IP_addresses searchpath='domains'
```

where:

- *state* is whether to retrieve DNS settings from the DHCP server. A value of *enabled* means from the DHCP server. A value of *disabled* means local settings.
- *IP_addresses* are a comma delimited list of up to three IP addresses of name servers in search order.
- *domains* are a comma delimited list of up to six domains or search suffixes in search order.

For example, to configure for local settings for the DNS client:

```
-> set /SP/clients/dns auto_dns=disabled nameserver=123.45.67.89,123.45.67.90
searchpath='india.sun.com,norway.sun.com'
Set 'auto_dns' to 'disabled'
Set 'nameserver' to '123.45.67.89,123.45.67.90'
Set 'searchpath' to 'india.sun.com,norway.sun.com'
->
```

Note – The number of retries and timeout are configurable. The default values of 1 and 5, respectively, provide for optimal performance.

Related Information

- [“set Command”](#) on page 274
- [“Configure the DNS Client \(Web\)”](#) on page 139
- [“Configure the DNS Client \(SNMP\)”](#) on page 244
- [“Display the DNS Client Status \(CLI\)”](#) on page 56

▼ Configure the SMTP Client (CLI)

To enable email alerts, Oracle ILOM must be configured as an SMTP client.

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Configure the client with the SMTP server information.

```
-> set /SP/clients/smtp address=IP_address custom_sender=email state=state
```

where:

- *IP_address* is the IP address of the SMTP server.
- *email* is the sender, as seen in the From: field. For example:
ilom-gwl@*hostname*, where *hostname* is the host name of the management controller.
- *state* is either enabled or disabled.

For example:

```
-> set /SP/clients/smtp address=123.45.67.89 custom_sender=ilom-gwl@hostname
state=enabled
Set 'address' to '123.45.67.89'
Set 'custom_sender' to 'ilom-gwl@hostname'
Set 'state' to 'enabled'
->
```

3. (Optional) Send a test email to verify SMTP client settings:

a. Type.

```
-> set /SP/clients/smtp send_test_email_to=email_to
```

where *email_to* is the destination email address.

b. Verify the email was received.

Related Information

- [“set Command” on page 274](#)
- [“Configure the SMTP Client \(Web\)” on page 140](#)
- [“Configure the SMTP Client \(SNMP\)” on page 245](#)
- [“Display the SMTP Client Status \(CLI\)” on page 57](#)

▼ Back Up the Configuration (CLI)

Note – You must use a passphrase to back up sensitive information, such as passwords.

Note – See [“Gateway Configuration Information Backed Up”](#) on page 76 for what gateway configuration information is backed up.

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI”](#) on page 30.

2. Set the passphrase for the backup.

```
-> set /SP/config passphrase=phrase
```

where *phrase* is an alphanumeric string. For example:

```
-> set /SP/config passphrase=user1234
Set 'passphrase' to 'user1234'
->
```

3. Back up the 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 274
- [“Gateway Configuration Information Backed Up”](#) on page 76
- [“Back Up the Configuration \(Web\)”](#) on page 141
- [“Restore the Configuration \(CLI\)”](#) on page 76

Gateway Configuration Information Backed Up

When you back up the configuration with a passphrase, this gateway-specific information is saved into an `.xml` file:

- DCS configuration
- User Subnet Manager configuration
- Environment daemon configuration
- List of disabled ports
- Boot monitor configuration
- BridgeX Manager settings
- BridgeX Manager LAG settings
- BridgeX Manager VNIC settings

Related Information

- [“Back Up the Configuration \(CLI\)” on page 75](#)
- [“Back Up the Configuration \(Web\)” on page 141](#)

▼ Restore the Configuration (CLI)

Note – You must use the correct passphrase when restoring the configuration that was backed up with a passphrase.

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Set the passphrase for the restore.

```
-> set /SP/config passphrase=phrase
```

where *phrase* is an alphanumeric string. For example

```
-> set /SP/config passphrase=user1234
Set 'passphrase' to 'user1234'
->
```

3. Restore the 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 274](#)
- [“Restore the Configuration \(Web\)” on page 142](#)
- [“Back Up the Configuration \(CLI\)” on page 75](#)
- [“Gateway Configuration Information Backed Up” on page 76](#)

▼ Create a Snapshot of the Gateway State (CLI)

The snapshot utility collects log files, executes various commands and collects their output, and sends the data collected to a user-defined location. The dataset property of the `/SP/diag/snapshot` target defines the data that is collected. See [“Snapshot Dataset Information \(CLI\)” on page 79](#).

The snapshot describes the state of the gateway at a particular moment in time. You can use this information for fault diagnosis. The snapshot utility requires administrator privileges.

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Create a snapshot of the gateway state.

```
-> set /SP/diag/snapshot dataset=value dump_uri=URI
```

where:

- *value* is the type of dataset, as described in the table in [“Snapshot Dataset Information \(CLI\)” on page 79](#).

- *URI* is the uniform resource indicator (FTP and SFTP supported)

For example, to take a snapshot of the normal dataset and transfer the snapshot using the FTP protocol to the /tftpboot/normal directory of the host with IP address 123.45.67.89 as the root user:

```
-> set /SP/diag/snapshot dataset=normal dump_uri=
ftp://root:changeme@123.45.67.89//tftpboot/normal
Set 'dataset' to 'normal'
Set 'dump_uri' to 'ftp://root:changeme@123.45.67.89//tftpboot/normal'
->
```

The snapshot process takes several minutes to complete.

3. (Optional) Check the progress of the snapshot process.

```
-> show /SP/diag/snapshot result
/SP/diag/snapshot
Properties:
    result = Running
->
```

This example shows the progress of the snapshot process, after it has finished:

```
-> show /SP/diag/snapshot result
/SP/diag/snapshot
Properties:
    result = Collecting data into
ftp://root:****@123.45.67.89//tftpboot/normal/magnum_123.45.67.89_2011-01-07T
14-43-15.zip
Snapshot Complete
Done.
->
```

Related Information

- [“set Command” on page 274](#)
- [“show Command” on page 275](#)
- [“Snapshot Dataset Information \(CLI\)” on page 79](#)
- [“Create a Snapshot of the Gateway State \(Web\)” on page 142](#)

Snapshot Dataset Information (CLI)

The dataset property of the `/SP/diag/snapshot` target determines what data is included in the snapshot. This table provides a listing of the dataset values and the data that is included in the snapshot.

Dataset Value	Description
<code>normal</code>	Contains Oracle ILOM data, basic operating system data, and gateway configuration data.
<code>normal-logonly</code>	Contains only log entries that pertain to Oracle ILOM data, basic operating system data, and gateway hardware data.
<code>fruid</code>	Contains normal dataset information, with additional FRUID data.
<code>fruid-logonly</code>	Contains only log entries that pertain to Oracle ILOM data, basic operating system data, gateway hardware data, and additional FRUID data.
<code>full</code>	Contains normal dataset information, with additional FRUID data and diagnostic data.
<code>full-logonly</code>	Contains only log entries that pertain to Oracle ILOM data, basic operating system data, gateway hardware data, additional FRUID data, and diagnostic data.

The snapshot is stored as a `.zip` file with a filename of this format:

hostname_IP_address_year-month-dayThour-minute-second.zip

for example:

`magnum_123.45.67.89_2011-01-07T14-43-15.zip`

Note – The `normal`, `fruid`, and `full` datasets of the snapshot utility are currently equivalent and contain the same data in the snapshot.

Related Information

- [“Create a Snapshot of the Gateway State \(CLI\)” on page 77](#)

▼ Set the Network Management Parameters (CLI)

This task enables you to configure the NET MGT interface.

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

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

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.

These properties are supported:

- `pendingipaddress` – The *value* is the IP address of the management controller 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 the changes.

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

For example, to set the IP address of the management controller:

```
-> 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 management controller. You must re-establish the connection to continue administering the management controller. See [“Accessing Oracle ILOM From the CLI” on page 30](#).

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

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

5. Display the new IP address.

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

Related Information

- [“set Command” on page 274](#)
- [“show Command” on page 275](#)
- [“Set the Network Management Parameters \(Web\)” on page 144](#)
- [“Set the Network Parameters \(SNMP\)” on page 246](#)

▼ Set the System Identification Properties (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI”](#) on page 30.

2. Set the host name property.

```
-> set /SP hostname=string
```

For example:

```
-> set /SP hostname=us-gw-1
Set 'hostname' to 'us-gw-1'
->
```

3. Set the system contact property.

```
-> set /SP system_contact=string
```

For example:

```
-> set /SP system_contact='sysadmin'
Set 'system_contact' to 'sysadmin'
->
```

4. Set the system identifier property.

```
-> set /SP system_identifier=string
```

For example:

```
-> set /SP system_identifier='data center'
Set 'system_identifier' to 'data center'
->
```

5. Set the system location property.

```
-> set /SP system_location=string
```

For example:

```
-> set /SP system_location='3rd floor'  
Set 'system_location' to '3rd floor'  
->
```

6. Display the identification properties.

```
-> show -d properties /SP  
/SP/cli  
Properties:  
  hostname = us-gw-1  
  system_contact = sysadmin  
  system_description = Sun Datacenter InfiniBand Switch GW, ILOM v2.0.5-1,  
r47111  
  system_identifier = data center  
  system_location = 3rd floor  
->
```

Related Information

- [“Set the System Identification Properties \(Web\)” on page 145](#)
- [“Set the System Identification Properties \(SNMP\)” on page 248](#)
- [“Display System Identification Properties \(CLI\)” on page 66](#)

Performing Oracle ILOM User Tasks (CLI)

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

- [“Add an Oracle ILOM User Account \(CLI\)” on page 84](#)
- [“Change an Oracle ILOM User’s Password and or Role \(CLI\)” on page 84](#)
- [“Delete an Oracle ILOM User Account \(CLI\)” on page 85](#)

Related Information

- [“Performing Oracle ILOM User Tasks \(Web\)” on page 145](#)
- [“Performing General Tasks on Oracle ILOM Targets \(CLI\)” on page 67](#)

▼ Add an Oracle ILOM User Account (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI”](#) on page 30.

2. Add an Oracle 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  
->
```

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

The Oracle ILOM user testuser is added.

Related Information

- [“create Command”](#) on page 267
- [“Add an Oracle ILOM User Account \(Web\)”](#) on page 145
- [“Add an Oracle ILOM User Account \(SNMP\)”](#) on page 249
- [“Delete an Oracle ILOM User Account \(CLI\)”](#) on page 85

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

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI”](#) on page 30.

2. Change the Oracle 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.



Caution – With this procedure, it is also possible for the ilom-admin user to reset the root user password, should it be lost or forgotten. The ilom-admin user must use the USB management port to reset the root user password. See [“Access the Oracle ILOM Shell From the CLI \(USB Management Port\)”](#) on page 31.

Related Information

- [“set Command”](#) on page 274
- [“Change an Oracle ILOM User's Password and or Role \(Web\)”](#) on page 146

▼ Delete an Oracle ILOM User Account (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI”](#) on page 30.

2. Delete the Oracle 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 Oracle ILOM user testuser is deleted.

Related Information

- [“delete Command” on page 268](#)
- [“Delete an Oracle ILOM User Account \(Web\)” on page 147](#)
- [“Delete an Oracle ILOM User Account \(SNMP\)” on page 250](#)
- [“Add an Oracle ILOM User Account \(CLI\)” on page 84](#)

Managing HTTP Services (CLI)

These tasks help you manage the Oracle ILOM HTTP service targets.

- [“Enable the HTTP Service \(CLI\)” on page 86](#)
- [“Disable the HTTP Service \(CLI\)” on page 87](#)

Related Information

- [“Managing HTTP Services \(Web\)” on page 147](#)
- [“Managing HTTPS Services \(CLI\)” on page 88](#)
- [“Managing SNMP Services \(CLI\)” on page 91](#)
- [“Managing IPMI Services \(CLI\)” on page 98](#)

▼ Enable the HTTP Service (CLI)

Note – The HTTP service is disabled and the HTTPS service is enabled by default.

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI”](#) on page 30.

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 274
- [“Enable the HTTP Service \(Web\)”](#) on page 148
- [“Set the HTTP Service State \(SNMP\)”](#) on page 251
- [“Disable the HTTP Service \(CLI\)”](#) on page 87

▼ Disable the HTTP Service (CLI)

Note – The HTTP service is disabled by default.

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI”](#) on page 30.

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 274
- [“Disable the HTTP Service \(Web\)”](#) on page 148
- [“Set the HTTP Service State \(SNMP\)”](#) on page 251
- [“Enable the HTTP Service \(CLI\)”](#) on page 86

Managing HTTPS Services (CLI)

These tasks help you manage the Oracle ILOM HTTPS service targets.

- [“Enable the HTTPS Service \(CLI\)” on page 88](#)
- [“Install a Custom SSL Certificate \(CLI\)” on page 89](#)
- [“Remove the Custom SSL Certificate \(CLI\)” on page 89](#)
- [“Disable the HTTPS Service \(CLI\)” on page 90](#)

Related Information

- [“Managing HTTPS Services \(Web\)” on page 149](#)
- [“Managing HTTP Services \(CLI\)” on page 86](#)
- [“Managing SNMP Services \(CLI\)” on page 91](#)
- [“Managing IPMI Services \(CLI\)” on page 98](#)

▼ 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 Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Enable secure redirection.

```
-> set /SP/services/http securerredirect=enabled
Set 'securerredirect' 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 274](#)

- “Enable the HTTPS Service (Web)” on page 149
- “Set the HTTPS Service State (SNMP)” on page 251
- “Disable the HTTPS Service (CLI)” on page 90

▼ Install a Custom SSL Certificate (CLI)

1. Access the Oracle ILOM CLI.

See “Accessing Oracle ILOM From the CLI” on page 30.

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 named `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 272
- “Install a Custom SSL Certificate (Web)” on page 150
- “Remove the Custom SSL Certificate (CLI)” on page 89

▼ Remove the Custom SSL Certificate (CLI)

1. Access the Oracle ILOM CLI.

See “Accessing Oracle ILOM From the CLI” on page 30.

2. Remove the certificate.

```
-> reset /SP/services/https/ssl/custom_cert
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

- [“reset Command” on page 273](#)
- [“Remove the Custom SSL Certificate \(Web\)” on page 151](#)
- [“Install a Custom SSL Certificate \(CLI\)” on page 89](#)

▼ 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 Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Disable secure redirection.

```
-> set /SP/services/http securereredirect=disabled
Set 'securereredirect' 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 274](#)
- [“Disable the HTTPS Service \(Web\)” on page 151](#)
- [“Set the HTTPS Service State \(SNMP\)” on page 251](#)

- [“Enable the HTTPS Service \(CLI\)” on page 88](#)

Managing SNMP Services (CLI)

These tasks help you manage the Oracle ILOM SNMP service targets.

- [“Enable the SNMP Service \(CLI\)” on page 91](#)
- [“Configure the SNMP Service \(CLI\)” on page 92](#)
- [“Add SNMP Service User Accounts \(CLI\)” on page 93](#)
- [“Modify SNMP Service User Accounts \(CLI\)” on page 94](#)
- [“Delete SNMP Service User Accounts \(CLI\)” on page 95](#)
- [“Add SNMP Service Communities \(CLI\)” on page 95](#)
- [“Modify SNMP Service Communities \(CLI\)” on page 96](#)
- [“Delete SNMP Service Communities \(CLI\)” on page 96](#)
- [“Download SNMP Service MIBs \(CLI\)” on page 97](#)
- [“Disable the SNMP Service \(CLI\)” on page 98](#)

Related Information

- [“Managing SNMP Services \(Web\)” on page 152](#)
- [“Managing HTTP Services \(CLI\)” on page 86](#)
- [“Managing HTTPS Services \(CLI\)” on page 88](#)
- [“Managing IPMI Services \(CLI\)” on page 98](#)

▼ Enable the SNMP Service (CLI)

Note – The SNMP service is enabled by default.

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

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 274](#)
- [“Enable the SNMP Service \(Web\)” on page 152](#)
- [“Disable the SNMP Service \(CLI\)” on page 98](#)

▼ Configure the SNMP Service (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Configure the SNMP parameters.

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

where:

- *property* is the parameter of the SNMP service to configure.
- *value* is the value of the *property* to configure

These 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 274](#)
- [“Configure the SNMP Service \(Web\)” on page 153](#)

▼ Add SNMP Service User Accounts (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

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 an 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 272](#)

- [“set Command” on page 274](#)
- [“Add SNMP Service User Accounts \(Web\)” on page 153](#)
- [“Delete SNMP Service User Accounts \(CLI\)” on page 95](#)

▼ Modify SNMP Service User Accounts (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Modify an 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.

These 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 274](#)
- [“Modify SNMP Service User Accounts \(Web\)” on page 154](#)

▼ Delete SNMP Service User Accounts (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Delete an 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 268](#)
- [“Delete SNMP Service User Accounts \(Web\)” on page 155](#)
- [“Add SNMP Service User Accounts \(CLI\)” on page 93](#)

▼ Add SNMP Service Communities (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Add an 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 267](#)
- [“Add SNMP Service Communities \(Web\)” on page 156](#)
- [“Delete SNMP Service Communities \(CLI\)” on page 96](#)

▼ Modify SNMP Service Communities (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

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.

This 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/communities/newcom permission=ro
Set 'permission' to 'ro'
->
```

Related Information

- [“set Command” on page 274](#)
- [“Modify SNMP Service Communities \(Web\)” on page 156](#)

▼ Delete SNMP Service Communities (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Delete an 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 268](#)
- [“Delete SNMP Service Communities \(Web\)” on page 157](#)
- [“Add SNMP Service Communities \(CLI\)” on page 95](#)

▼ Download SNMP Service MIBs (CLI)

This procedure creates a compressed file, `ilom-mibs.zip`, that contains these MIBs:

- ENTITY-MIB.mib
- SUN-HW-TRAP-MIB.mib
- SUN-ILOM-CONTROL-MIB.mib
- SUN-PLATFORM-MIB.mib
- SUN-FABRIC-MIB.mib
- SUN-DCS-IB-MIB.txt

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Download 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 downloaded.

Related Information

- [“dump Command” on page 269](#)
- [“Download SNMP Service MIBs \(Web\)” on page 158](#)

▼ Disable the SNMP Service (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

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 274](#)
- [“Disable the SNMP Service \(Web\)” on page 158](#)
- [“Enable the SNMP Service \(CLI\)” on page 91](#)

Managing IPMI Services (CLI)

These tasks help you manage the Oracle ILOM IPMI service target.

- “Enable the IPMI Service (CLI)” on page 99
- “Disable the IPMI Service (CLI)” on page 99

Related Information

- “Managing IPMI Services (Web)” on page 159
- “Managing HTTP Services (CLI)” on page 86
- “Managing HTTPS Services (CLI)” on page 88
- “Managing SNMP Services (CLI)” on page 91

▼ Enable the IPMI Service (CLI)

Note – The IPMI service is enabled by default.

1. Access the Oracle ILOM CLI.

See “Accessing Oracle ILOM From the CLI” on page 30.

2. Enable the IPMI service.

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

The IPMI service is enabled.

Related Information

- “set Command” on page 274
- “Enable the IPMI Service (Web)” on page 159
- “Disable the IPMI Service (CLI)” on page 99
- “Display the IPMI Service Status (CLI)” on page 56

▼ Disable the IPMI Service (CLI)

1. Access the Oracle ILOM CLI.

See “Accessing Oracle ILOM From the CLI” on page 30.

2. Disable the service.

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

The IPMI service is disabled.

Related Information

- [“set Command” on page 274](#)
- [“Disable the IPMI Service \(Web\)” on page 160](#)
- [“Enable the IPMI Service \(CLI\)” on page 99](#)
- [“Display the IPMI Service Status \(CLI\)” on page 56](#)

Managing Other Aspects With Oracle ILOM (CLI)

These tasks help you manage other aspect of ILOM.

- [“Enable Alerts to Send SNMP Traps \(CLI\)” on page 100](#)
- [“Enable Alerts to Send PETs \(CLI\)” on page 102](#)
- [“Enable Alerts to Send Email Alerts \(CLI\)” on page 103](#)
- [“Disable Alerts \(CLI\)” on page 104](#)
- [“Set the Oracle ILOM CLI Session Timeout \(CLI\)” on page 105](#)

Related Information

- [“Managing Other Aspects With Oracle ILOM \(Web\)” on page 160](#)
- [“Managing Other Aspects With Oracle ILOM \(SNMP\)” on page 250](#)
- [“Performing General Tasks on Oracle ILOM Targets \(CLI\)” on page 67](#)

▼ Enable Alerts to Send SNMP Traps (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

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 occurrence 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.

This is an example of an SNMP v2c trap of when the aggregate sensor is in the state of Asserted:

```
Sep 12 13:12:38 mnm-blr-2 snmptrapd[1514]: [ID 702911 daemon.warning]
123.45.67.90 [123.45.67.90]: Trap
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (4472) 0:00:44.72,
SNMPv2-MIB::snmpTrapOID.0 = OID:
SNMPv2-SMI::enterprises.42.2.175.103.2.0.43,
SNMPv2-SMI::enterprises.42.2.175.103.2.1.1.0 = STRING: "123.45.67.90",
SNMPv2-SMI::enterprises.42.2.175.103.2.1.14.0 = STRING: "00000002",
SNMPv2-SMI::enterprises.42.2.175.103.2.1.15.0 = STRING: "Sun
Datacenter InfiniBand Switch GW", SNMPv2-SMI::enterprises.42.2.175.103.2.1.2.0
= STRING: "/SYS/CHASSIS_STATUS",
SNMPv2-SMI::enterprises.42.2.175.103.2.1.9.0 = STRING: "State Asserted",
SNMPv2-SMI::enterprises.42.2.175.103.2.1.10.0 = OID:
SNMPv2-SMI::mib-2.47.1.1.1.1.2.3
```

In the output, the trap source is the gateway 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 274
- “Enable Alerts to Send SNMP Traps (Web)” on page 161
- “Enable Alerts to Send SNMP Traps (SNMP)” on page 252
- “Enable Alerts to Send PETs (CLI)” on page 102
- “Enable Alerts to Send Email Alerts (CLI)” on page 103
- “Display the Alert Properties (CLI)” on page 60
- “Disable Alerts (CLI)” on page 104

▼ Enable Alerts to Send PETs (CLI)

1. Access the Oracle ILOM CLI.

See “Accessing Oracle ILOM From the CLI” on page 30.

2. Enable alerts to send PETs.

```
-> 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'
->
```

This is an example of a PET trap of when the aggregate sensor is in the state of Asserted:

```
Sep 12 13:12:38 mnm-blr-2 snmptrapd[1514]: [ID 702911 daemon.warning]
123.45.67.90: Enterprise Specific Trap (12583681) Uptime: 117 days, 8:00:20.80,
SNMPv2-SMI::enterprises.3183.1.1.1 = Hex-STRING: FF 20 00 08 FF FF FF FF FF FF
8E 00 28 4B E0 00
Sep 12 13:12:38 mnm-blr-2 02 00 A0 EB C1 07 FF FF 20 20 02 20 01 00 00 01
Sep 12 13:12:38 mnm-blr-2 FF FF 00 00 00 00 00 00 19 2A 00 00 00 30 30 80 0F
Sep 12 13:12:38 mnm-blr-2 03 43 48 41 53 53 49 53 5F 53 54 41 54 55 53 00
```

```
Sep 12 13:12:38 mnm-blr-2 80 26 03 53 75 6E 54 4D 20 44 61 74 61 63 65 6E
Sep 12 13:12:38 mnm-blr-2 74 65 72 20 49 6E 66 69 6E 69 42 61 6E 64 20 53
Sep 12 13:12:38 mnm-blr-2 77 69 74 63 68 20 33 36 00 C1 00 00 00 00
```

Related Information

- [“set Command” on page 274](#)
- [“Enable Alerts to Send PETs \(Web\)” on page 161](#)
- [“Enable Alerts to Send PETs \(SNMP\)” on page 253](#)
- [“Enable Alerts to Send SNMP Traps \(CLI\)” on page 100](#)
- [“Enable Alerts to Send Email Alerts \(CLI\)” on page 103](#)
- [“Display the Alert Properties \(CLI\)” on page 60](#)
- [“Disable Alerts \(CLI\)” on page 104](#)

▼ Enable Alerts to Send Email Alerts (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Enable alerts to send emails.

```
-> set /SP/alertmgmt/rules/alert destination=email_to type=email
email_custom_sender=email_from level=level
```

where:

- *alert* is the number of the alert.
- *email_to* is the email address to receive the alert.
- *email_from* is the sender, as seen in the From: field. For example:
ilom-gwl-hostname, where *hostname* is the host name of the management controller.
- *level* is the level of the alert.

For example, to set alert 1 to send an email to `user@headsup.com` whenever a major or higher severity event happens:

```
-> set /SP/alertmgmt/rules/1 destination=user@headsup.com type=email
email_custom_sender=ilom-gwl-magnum level=major
Set 'destination' to 'user@headsup.com'
Set 'type' to 'email'
Set 'email_custom_sender' to 'ilom-gwl-magnum'
Set 'level' to 'major'
->
```

Related Information

- [“set Command” on page 274](#)
- [“Enable Alerts to Send Email Alerts \(Web\)” on page 162](#)
- [“Enable Alerts to Send Email Alerts \(SNMP\)” on page 254](#)
- [“Enable Alerts to Send SNMP Traps \(CLI\)” on page 100](#)
- [“Enable Alerts to Send PETs \(CLI\)” on page 102](#)
- [“Display the Alert Properties \(CLI\)” on page 60](#)
- [“Disable Alerts \(CLI\)” on page 104](#)

▼ Disable Alerts (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

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 274](#)
- [“Disable Alerts \(Web\)” on page 163](#)
- [“Disable Alerts \(SNMP\)” on page 256](#)
- [“Display the Alert Properties \(CLI\)” on page 60](#)
- [“Enable Alerts to Send SNMP Traps \(CLI\)” on page 100](#)
- [“Enable Alerts to Send PETs \(CLI\)” on page 102](#)
- [“Enable Alerts to Send Email Alerts \(CLI\)” on page 103](#)

▼ Set the Oracle ILOM CLI Session Timeout (CLI)

1. Access the Oracle ILOM CLI.

See [“Accessing Oracle ILOM From the CLI” on page 30](#).

2. Set the Oracle 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'
->
```

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

The CLI session timeout is set.

Related Information

- [“set Command” on page 274](#)
- [“Set the CLI Session Timeout \(Web\)” on page 164](#)

Upgrading the Gateway Firmware Through Oracle ILOM (CLI)

One of the advantages of Oracle ILOM support on the management controller is that all firmware upgrades and downgrades have been simplified into a two-task process.

These topics enable you to either upgrade or downgrade the gateway firmware through the Oracle ILOM CLI.

- [“Firmware Overview” on page 106](#)
- [“Verify Firmware Integrity \(CLI\)” on page 106](#)
- [“Acquire the Gateway Firmware Package \(CLI\)” on page 107](#)
- [“Upgrade the Gateway Firmware \(CLI\)” on page 109](#)

Related Information

- [“Upgrade the Gateway Firmware \(Web\)” on page 164](#)
- [“Monitoring Oracle ILOM Targets \(CLI\)” on page 39](#)
- [“Controlling Oracle ILOM Targets \(CLI\)” on page 67](#)

Firmware Overview

The management controller has firmware that represents the following:

- Basic I/O system for initial startup of the controller.
- Linux operating system that enables the management controller to function as a service processor and host for the gateway.
- File system that contains the many hardware commands, InfiniBand commands, Subnet Manager, and other applications for the administration of the gateway and InfiniBand fabric.

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

When improvements to the operation of the gateway are made or features are added, these enhancements are delivered through a firmware upgrade.

Related Information

- [“Verify Firmware Integrity \(CLI\)” on page 106](#)
- [“Acquire the Gateway Firmware Package \(CLI\)” on page 107](#)
- [“Upgrade the Gateway Firmware \(CLI\)” on page 109](#)

▼ Verify Firmware Integrity (CLI)

Over time, you might become concerned that the filesystem of the management controller is corrupted, or inappropriate `.rpm` packages have been installed. The `fwverify` command can help troubleshoot these problems for you.

The `fwverify` command checks for correct version numbers of present packages, if any required packages are missing, and the integrity of installed files. More information about the `fwverify` command is provided in the *Gateway Reference*, `fwverify` command.

- On the management controller, verify the firmware integrity.

```
# fwverify
Checking all present packages:
..... OK
Checking if any packages are missing:
..... OK
Verifying installed files:
..... FAILED
* Package nm2gw-phs-2.0.5-1.i386:
S.5....T /etc/init.d/dcs
#
```

In this example, within the nm2gw-phs-2.0.5-1.i386 RPM package, the /etc/init.d/dcs file size differs, the MD5 sum differs, and the time differs.

Related Information

- *Gateway Reference*, fwverify command
- [“Firmware Overview” on page 106](#)
- [“Acquire the Gateway Firmware Package \(CLI\)” on page 107](#)
- [“Upgrade the Gateway Firmware \(CLI\)” on page 109](#)

▼ Acquire the Gateway Firmware Package (CLI)

Note – See the *Gateway Product Notes* for the most up-to-date method of acquiring the firmware. If no information is provided there, use these instructions.

Note – The version numbers in this procedure are represented as *x.y*, *x.y.z*, and *x.y.z.w*. For example, for the 2.0.5-1 version of the firmware, *x*=2, *y*=0, *z*=5, and *w*=1. See the *Gateway Product Notes* for the most current version numbers.

1. Open a web browser on a host that is on the same Ethernet network as the management controller to receive the firmware update.
2. Go to this URL.

<http://support.oracle.com>

Oracle’s My Oracle Support page is displayed.

Note – This web page requires Flash support.

3. Sign in if you already have an account.

The dashboard page is displayed.

Note – If you do not have an account, you must register.

4. Click the Patches & Updates tab.

The Patches and Downloads page is displayed.

5. In the Patch Search for Oracle....window, click the Advanced Search tab.

The Patch Search for Oracle... window updates.

6. In the Product drop-down menu, select Sun Network QDR Infiniband Gateway Switch.

7. In the Release drop-down menu, select Sun Network QDR Infiniband Gateway Switch *x.y.z*.

Where *x.y.z* is the version number of the firmware package to be acquired. For example, 2.0.5.

8. Click Search.

The Patch Search window expands with the search results.

9. In the Patch Name column, click the respective patch number link.

For example, 13374046. The Patch Search window reformats.

10. Click the *filename.zip* link to initiate the download.

For example, p13374046_205-1_Generic.zip.

11. Indicate where the file should be saved.

The file is downloaded and saved.

12. In your receiving directory, decompress the *filename.zip* file.

The firmware is in the SUN_DCS_gw_*x.y.z*.tar.gz file.

The readme file contains the latest information about the firmware release.

13. Unpack the .gz file.

```
$ gtar -zxvf SUN_DCS_gw_x.y.z.tar.gz
```

The extracted files are displayed.

14. Move the gateway firmware package (*filename.pkg*) to a directory on a host that is accessible by Oracle ILOM.

15. Upgrade the gateway firmware.

See “Upgrade the Gateway Firmware (CLI)” on page 109 or “Upgrade the Gateway Firmware (Web)” on page 164.

Related Information

- “Firmware Overview” on page 106
- “Verify Firmware Integrity (CLI)” on page 106
- “Upgrade the Gateway Firmware (CLI)” on page 109

▼ Upgrade the Gateway Firmware (CLI)

Note – If you are going to downgrade the firmware to a version earlier than 2.0, you must remove user partitions and depopulate the Subnet Manager nodes list. See *Gateway Administration*, removing partitions for firmware downgrade.

1. Open an SSH session as user `root` and connect to the management controller by specifying the controller’s host name.

For example:

```
% ssh -l root gateway_name
root@gateway_name's password: password
#
```

where *gateway_name* is the host name of the management controller. Initially, the *password* is *changeme*.

2. If the Subnet Manager is running on the management controller, disable it with the `disableesm` command.

```
# disableesm
Stopping partitiond daemon.                [ OK ]
Stopping IB Subnet Manager..                [ OK ]
#
```

3. Verify that there is at least 150 MB available in the /tmp directory.

```
# df -h /tmp
Filesystem                Size      Used Avail Use% Mounted on
tmpfs                     250M      240K  249M   1% /tmp
#
```

In this example, there are 249 MB available. If not enough space is available, you must delete files from the /tmp directory.

4. Verify that there is at least 1 MB available in the /config directory.

```
# df -h /config
Filesystem                Size      Used Avail Use% Mounted on
/dev/hda2                 16M       3.6M   11M   25% /config
#
```

In this example, there are 11 MB available. If not enough space is available, you must delete files from the /config directory.

5. Verify that there is at least 1 MB available in the /var/log directory.

```
# df -h /var/log
Filesystem                Size      Used Avail Use% Mounted on
/dev/hda3                 16M       3.6M   11M   25% /var/log
#
```

In this example, there are 11 MB available. If not enough space is available, you must delete files from the /var/log directory.

6. Verify that there is at least 150 MB free memory available.

```
# free -m
              total        used        free      shared    buffers     cached
Mem:           498          104          393           0          12          47
-/+ buffers/cache:           45          453
Swap:           0           0           0
#
```

In the -/+ buffers/cache: row of the free column, there should be at least 150 MB free memory. In this example, there are 453 MB available. If not enough memory is available, you must exit non-essential applications that are running.

7. Start the Oracle ILOM shell.

```
# spsh
Oracle(R) Integrated Lights Out Manager
Version ILOM 3.0 r47111
Copyright (c) 2010, Oracle and/or its affiliates. All rights reserved.
->
```

You are now in the Oracle ILOM shell.

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

8. Begin the upgrade process.

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

where:

- *URI* is the uniform resource indicator for the host where the gateway firmware package is located. The FTP and HTTP protocols are supported.
- *pkgname* is the name of the firmware package in the transfer directory.

For example, using the FTP protocol:

```
-> load -source
ftp://root:changeme@123.45.67.99//tmp/sundcs_gw_repository_2.0.5_1.pkg
Downloading firmware image. This will take a few minutes.
```

Note – If you are upgrading from firmware version 2.0.X, you can use the `-force` option to disable version number checking, and force the upgrade.

The firmware is downloaded. The upgrade begins. A caution is displayed and you are asked to commit to the upgrade.

```
NOTE: Firmware upgrade will upgrade firmware on SUN DCS gw Kontron module,
I4 and BridgeX. Upgrade takes few minutes to complete.
```

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

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

9. Answer y to the prompt to commit to the upgrade.

The upgrade begins.

```
Setting up environment for firmware upgrade. This will take few minutes.
Starting SUN DCS gw FW update

=====
Performing operation: I4 A
=====
I4 A: I4 is already at the given version.

=====
Performing operation: BX A
=====
BX fw upgrade from 8.3.3166(INI:4) to 8.4.2740(INI:5):
Upgrade started...
Upgrade completed.
INFO: BX fw upgrade from 8.3.3166(INI:4) to 8.4.2740(INI:5) succeeded

=====
Performing operation: BX B
=====
BX fw upgrade from 8.3.3166(INI:4) to 8.4.2740(INI:5):
Upgrade started...
Upgrade completed.
INFO: BX fw upgrade from 8.3.3166(INI:4) to 8.4.2740(INI:5) succeeded

=====
Summary of Firmware update
=====
I4 status : FW UPDATE - SUCCESS
I4 update succeeded on : none
I4 already up-to-date on : A
I4 update failed on : none
BX status : FW UPDATE - SUCCESS
BX update succeeded on : A, B
BX already up-to-date on : none
BX update failed on : none

=====
Performing operation: SUN DCS gw firmware update
=====
SUN DCS gw Kontron module fw upgrade from 1.3.2-1 to 2.0.5-1:
Please reboot the system to enable firmware update of Kontron module. The
download of the Kontron firmware image happens during reboot.

After system reboot, Kontron FW update progress can be monitored in browser using
URL [http://GWsystem] OR at OS
```

```
command line prompt by using command [telnet GWsystem 1234] where GWsystem is
the hostname or IP address of SUN DCS GW.
```

```
Firmware update is complete.
->
```

10. Exit the Oracle ILOM CLI shell.

```
-> exit
exit
#
```

11. Reboot the gateway to enable the new firmware.

See *Gateway Administration*, restarting the entire gateway.

Note – The restart process takes between 4 to 5 minutes to complete.

You can monitor the update progress through:

- web browser – `http://gateway_name`
- CLI – `telnet gateway_name 1234`

where *gateway_name* is the host name or IP address of the management controller.

Note – The Oracle ILOM stack requires at least 2 minutes to become operational after a reboot.

The next time you login to the gateway, this message is displayed:

```
FW upgrade completed successfully on Mon Oct 17 18:36:14 IST 2011.
Please run the "fwverify" CLI command to verify the new image.
This message will be cleared on next reboot.
```

12. If the Subnet Manager was previously disabled, log in as the `root` user and enable the Subnet Manager.

```
% ssh -l root gateway_name
root@gateway_name's password: password
# enablesm
Starting IB Subnet Manager.                [ OK ]
Starting partitiond daemon.                [ OK ]
#
```

13. Verify the firmware version.

```
# version
SUN DCS gw version: 2.0.5-1
Build time: Nov 25 2011 12:56:05
FPGA version: 0x33
SP board info:
Manufacturing Date: 2009.06.23
Serial Number: "NCD3R0527"
Hardware Revision: 0x0006
Firmware Revision: 0x0102
BIOS version: NOW1R112
BIOS date: 04/24/2009
#
```

In the first line of the output is `SUN DCS gw version x.y.z-w`, where *x.y.z-w* is the version of the firmware upgraded (or downgraded). For example, 2.0.5-1.

14. Verify the firmware integrity.

See [“Verify Firmware Integrity \(CLI\)”](#) on page 106.

Related Information

- [“Upgrade the Gateway Firmware \(Web\)”](#) on page 164

Administering Oracle ILOM (Web)

These topics describe how to administer Oracle ILOM from the web interface.

- [“Web Interface Overview” on page 115](#)
- [“Access Oracle ILOM From the Web Interface” on page 118](#)
- [“Monitoring Oracle ILOM Targets \(Web\)” on page 119](#)
- [“Controlling Oracle ILOM Targets \(Web\)” on page 134](#)
- [“Upgrade the Gateway Firmware \(Web\)” on page 164](#)

Related Information

- [“Administering Oracle ILOM \(CLI\)” on page 29](#)
- [“Using the Fabric Monitor” on page 169](#)
- [“Administering Oracle ILOM \(SNMP\)” on page 199](#)
- [“Administering Hardware \(IPMI\)” on page 257](#)
- [“Understanding Oracle ILOM Commands” on page 265](#)

Web Interface Overview

The Oracle 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.

Note – The Oracle ILOM web interface is only supported with the Internet Explorer and Mozilla Firefox web browsers.

The web interface enables you to accomplish most of the same tasks that are possible using the Oracle 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 management controller’s Linux shell. You must access the management controller using the methods described in [“Accessing Oracle ILOM From the CLI” on page 30](#) to enable Oracle ILOM shell - Linux shell toggling.

This illustration displays the initial Oracle ILOM web interface page.



This table lists the tabs and subtabs in the Oracle ILOM web interface.

Tab	Subtabs	Description
System Information	SUN DCS GW Firmware Versions	Displays version information of the gateway firmware.
	ILOM Versions	Displays Oracle ILOM version information.
	Session Time-Out	Sets inactivity timeout for autologout.
	Components	Displays component status.
	Identification Information	Displays gateway identification information.
System Monitoring	Sensor Readings	Displays sensor values.
	Indicators	Displays gateway status LED state.

Tab	Subtabs	Description
Configuration	Event Logs	Displays event log.
	System Management Access	Subtabs for: <ul style="list-style-type: none"> • 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 timeout for autologout.
	Alert Management	Configures alerts.
	Network	Sets and enables basic network parameters. Has ping test.
	DNS	Sets DNS client parameters.
	Clock	Sets date, time, and time server parameters.
	Timezone	Sets time zone.
	Syslog	Configures Syslog redirection to IP address.
	SMTP Client	Configures SMTP client for email alerts. Has email test.
User Management	User Accounts	Configures user accounts.
	Active Sessions	Displays active sessions.
Maintenance	Firmware Upgrade	Enables firmware upgrade.
	Back Up/Restore	Configures system back up and restore.
	Reset SP	Resets the management controller.
	Snapshot	Configures and takes a snapshot of the gateway state.
Switch/Fabric Monitoring Tools	SUN DCS GW Monitor	Enables the Fabric Monitor interactive GUI.

Related Information

- [“Oracle ILOM Targets and Descriptions” on page 5](#)

▼ Access Oracle ILOM From the Web Interface

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

The Oracle 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 86](#) and [“Enable the HTTPS Service \(CLI\)” on page 88](#) to enable the web interface from the CLI.

2. **Type `ilom-admin` into 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 Oracle ILOM User's Password and or Role \(Web\)” on page 146](#) for instructions on how to change Oracle ILOM user passwords.

3. **Click Submit.**

The Oracle 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

- [“Accessing Oracle ILOM From the CLI” on page 30](#)
- [“Web Interface Overview” on page 115](#)
- [“Monitoring Oracle ILOM Targets \(Web\)” on page 119](#)
- [“Controlling Oracle ILOM Targets \(Web\)” on page 134](#)

Monitoring Oracle ILOM Targets (Web)

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

- [“Performing Daily Tasks \(Web\)” on page 119](#)
- [“Checking the Status of Services \(Web\)” on page 124](#)
- [“Verifying Other Aspects With Oracle ILOM \(Web\)” on page 129](#)

Related Information

- [“Access Oracle ILOM From the Web Interface” on page 118](#)
- [“Monitoring Oracle ILOM Targets \(CLI\)” on page 39](#)
- [“Controlling Oracle ILOM Targets \(Web\)” on page 134](#)

Performing Daily Tasks (Web)

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

- [“Display the Date \(Web\)” on page 120](#)
- [“Display the Gateway Status LEDs States \(Web\)” on page 120](#)
- [“Display the Aggregate Sensors State \(Web\)” on page 120](#)
- [“Display Power Supply Status \(Web\)” on page 121](#)
- [“Display Board-Level Voltages \(Web\)” on page 122](#)
- [“Display Internal Temperatures \(Web\)” on page 122](#)
- [“Display Fan Status \(Web\)” on page 123](#)
- [“Display the Oracle ILOM Sessions \(Web\)” on page 123](#)
- [“Display the Oracle ILOM Event Log \(Web\)” on page 124](#)

Related Information

- [“Performing Daily Tasks \(Web\)” on page 119](#)
- [“Checking the Status of Services \(Web\)” on page 124](#)
- [“Verifying Other Aspects With Oracle ILOM \(Web\)” on page 129](#)

▼ Display the Date (Web)

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

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

2. **Click the Configuration tab.**

3. **Click the Clock subtab.**

The Clock Settings window opens.

The current date and time is displayed in the Date and Time fields respectively.

Related Information

- [“Display the Date \(CLI\)”](#) on page 40
- [“Display the Date and Time \(SNMP\)”](#) on page 204

▼ Display the Gateway Status LEDs States (Web)

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

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

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

3. **Click the Indicators subtab.**

The Indicators window opens.

In the Indicators table, the indicator target and status are displayed.

Related Information

- [“Display Gateway Status LEDs States \(CLI\)”](#) on page 40
- [“Display Gateway Status LED States \(IPMI\)”](#) on page 263
- [“Enable the Locator LED \(Web\)”](#) on page 137
- [“Disable the Locator LED \(Web\)”](#) on page 137

▼ Display the Aggregate Sensors State (Web)

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

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

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 (aggregate sensor target), type, and reading are displayed. Use the table in [“Aggregate Sensor States” on page 42](#) to determine the aggregate sensor target for the respective sensor.

4. Click an aggregate sensor’s target 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

- [“Aggregate Sensor States” on page 42](#)
- [“Display the Aggregate Sensors State \(CLI\)” on page 41](#)
- [“Display the Aggregate Sensors State \(SNMP\)” on page 205](#)
- [“Display the Sensor Alarm State \(SNMP\)” on page 219](#)
- [“Display the Sensor States \(IPMI\)” on page 258](#)

▼ Display Power Supply Status (Web)

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface” on page 118](#).

2. Click the System Monitoring tab.

3. Click the Sensor Readings subtab.

The Sensor Readings window opens.

4. Click the next page arrow.

The Sensor Readings table is updated.

5. Look for /SYS/PSU in the Sensor Readings table.

A Reading value of State Deasserted means no faults.

Related Information

- [“Display Power Supply Status \(CLI\)” on page 43](#)
- [“Display Power Supply Status \(SNMP\)” on page 206](#)

▼ Display Board-Level Voltages (Web)

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

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

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

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

The Sensor Readings window opens.

4. **Select Type: Voltage from the All Sensors drop-down menu.**

The voltage sensor target, type, and reading are displayed. Use the table in [“Board Level Voltages”](#) on page 46 to determine the voltage sensor target for the respective voltage sensor.

5. **Click a voltage sensor’s target link in the table.**

A new window opens and displays the voltage sensor’s properties and values.

6. **Click Close.**

Related Information

- [“Board Level Voltages”](#) on page 46
- [“Display Board-Level Voltages \(CLI\)”](#) on page 44
- [“Display Board-Level Voltages \(SNMP\)”](#) on page 208

▼ Display Internal Temperatures (Web)

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

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

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

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

The Sensor Readings window opens.

4. **Select Type: Temperature from the All Sensors drop-down menu.**

The temperature sensor target, type, and reading are displayed. Use the table in [“Internal Temperature Sensors”](#) on page 48 to determine the temperature sensor target for the respective temperature sensor.

5. **Click a temperature sensor’s target link in the table.**

A new window opens and displays the temperature sensor’s properties and values.

6. **Click Close.**

Related Information

- [“Internal Temperature Sensors” on page 48](#)
- [“Display Internal Temperatures \(CLI\)” on page 47](#)
- [“Display Internal Temperatures \(SNMP\)” on page 212](#)

▼ Display Fan Status (Web)

1. **Access the Oracle ILOM web interface.**
See [“Access Oracle ILOM From the Web Interface” on page 118](#).
2. **Click the System Monitoring tab.**
3. **Click the Sensor Readings subtab.**
The Sensor Readings window opens.
4. **Select Type: Fan from the All Sensors drop-down menu.**
The fan speed sensor target, type, and reading are displayed.
5. **Click a fan speed sensor’s target link in the table.**
A new window opens and displays the fan speed sensor’s properties and values.
6. **Click Close.**

Related Information

- [“Display Fan Status \(CLI\)” on page 48](#)
- [“Display Fan Status \(SNMP\)” on page 215](#)

▼ Display the Oracle ILOM Sessions (Web)

1. **Access the Oracle ILOM web interface.**
See [“Access Oracle ILOM From the Web Interface” on page 118](#).
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, the user’s role, the session start time, and the session type and mode are displayed.

Related Information

- [“Display the Oracle ILOM Sessions \(CLI\)” on page 50](#)
- [“Display Oracle ILOM Sessions \(SNMP\)” on page 222](#)

▼ Display the Oracle ILOM Event Log (Web)

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

2. Click the System Monitoring tab.

3. Click the Event Logs subtab.

The event log is displayed.

The Filter drop-down menu filters events by type.

Related Information

- [“Display the Oracle ILOM Event Log \(CLI\)”](#) on page 51
- [“Display the Oracle ILOM Event Log \(SNMP\)”](#) on page 223
- [“Display the System Event Log \(IPMI\)”](#) on page 261
- [“Clear the Oracle ILOM Event Log \(Web\)”](#) on page 138

Checking the Status of Services (Web)

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

- [“Display the HTTP Service Status \(Web\)”](#) on page 125
- [“Display the HTTPS Service Status \(Web\)”](#) on page 125
- [“Display the SSL Certificates \(Web\)”](#) on page 125
- [“Display the SNMP Service Status \(Web\)”](#) on page 126
- [“Display the SNMP Service User Accounts \(Web\)”](#) on page 126
- [“Display the SNMP Service Communities \(Web\)”](#) on page 127
- [“Display the IPMI Service Status \(Web\)”](#) on page 127
- [“Display the DNS Client Status \(Web\)”](#) on page 127
- [“Display the SMTP Client Status \(Web\)”](#) on page 128
- [“Display the Network Time Protocol Servers \(Web\)”](#) on page 128

Related Information

- [“Checking the Status of Services \(CLI\)”](#) on page 52
- [“Performing Daily Tasks \(Web\)”](#) on page 119
- [“Verifying Other Aspects With Oracle ILOM \(Web\)”](#) on page 129

▼ Display the HTTP Service Status (Web)

1. **Access the Oracle ILOM web interface.**
See [“Access Oracle ILOM From the Web Interface”](#) on page 118.
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 52
- [“Display the HTTP Service Status \(SNMP\)”](#) on page 225

▼ Display the HTTPS Service Status (Web)

1. **Access the Oracle ILOM web interface.**
See [“Access Oracle ILOM From the Web Interface”](#) on page 118.
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 53
- [“Display the HTTP Service Status \(SNMP\)”](#) on page 225

▼ Display the SSL Certificates (Web)

1. **Access the Oracle ILOM web interface.**
See [“Access Oracle ILOM From the Web Interface”](#) on page 118.
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 53](#)

▼ Display the SNMP Service Status (Web)

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface” on page 118](#).

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 54](#)

▼ Display the SNMP Service User Accounts (Web)

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface” on page 118](#).

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 protocols, permissions, and privacy protocols are displayed.

Related Information

- [“Display the SNMP User Accounts \(CLI\)” on page 54](#)

▼ Display the SNMP Service Communities (Web)

1. **Access the Oracle ILOM web interface.**
See [“Access Oracle ILOM From the Web Interface”](#) on page 118.
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 55

▼ Display the IPMI Service Status (Web)

1. **Access the Oracle ILOM web interface.**
See [“Access Oracle ILOM From the Web Interface”](#) on page 118.
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 56

▼ Display the DNS Client Status (Web)

1. **Access the Oracle ILOM web interface.**
See [“Access Oracle ILOM From the Web Interface”](#) on page 118.
2. **Click the Configuration tab.**

3. Click the DNS subtab.

The DNS Configuration window opens.

The DNS client configuration settings are displayed.

Note – If Auto DNS via DHCP is enabled, then the Name Server and Search Path fields are greyed-out.

Related Information

- [“Display the DNS Client Status \(CLI\)” on page 56](#)
- [“Display the DNS Client Status \(SNMP\)” on page 226](#)
- [“Configure the DNS Client \(Web\)” on page 139](#)

▼ Display the SMTP Client Status (Web)

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface” on page 118](#).

2. Click the Configuration tab.

3. Click the SMTP Client subtab.

The SMTP Client Settings window opens.

The status of the SMTP client is displayed.

Related Information

- [“Display the SMTP Client Status \(CLI\)” on page 57](#)
- [“Display the SMTP Client Status \(SNMP\)” on page 227](#)
- [“Configure the SMTP Client \(Web\)” on page 140](#)

▼ Display the Network Time Protocol Servers (Web)

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface” on page 118](#).

2. Click the Configuration tab.

3. Click the Clock subtab.

The Clock Settings window opens.

The Network Time Protocol status and server IP addresses are displayed.

Related Information

- [“Display the NTP Servers \(CLI\)” on page 57](#)
- [“Display the NTP State \(SNMP\)” on page 227](#)
- [“Display the NTP Servers \(SNMP\)” on page 228](#)
- [“Set the Date and Time \(Web\)” on page 136](#)

Verifying Other Aspects With Oracle ILOM (Web)

These topics enable you to display the status of aspects of Oracle ILOM not included in [“Performing Daily Tasks \(Web\)” on page 119](#) or [“Checking the Status of Services \(Web\)” on page 124](#).

- [“Display the Alert Properties \(Web\)” on page 129](#)
- [“Display the Oracle ILOM User Accounts \(Web\)” on page 130](#)
- [“Display the Remote Log Hosts \(Web\)” on page 130](#)
- [“Display the Network Management Configuration \(Web\)” on page 131](#)
- [“Display the CLI Session Timeout \(Web\)” on page 131](#)
- [“Display System Component FRU ID \(Web\)” on page 132](#)
- [“Display the Firmware Version \(Web\)” on page 132](#)
- [“Display the Oracle ILOM Version \(Web\)” on page 133](#)
- [“Display System Identification Properties \(Web\)” on page 133](#)

Related Information

- [“Verifying Other Aspects With Oracle ILOM \(CLI\)” on page 58](#)
- [“Performing Daily Tasks \(Web\)” on page 119](#)
- [“Checking the Status of Services \(Web\)” on page 124](#)

▼ Display the Alert Properties (Web)

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

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface” on page 118](#).

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 60](#)
- [“Display the Alert Properties \(SNMP\)” on page 229](#)
- [“Enable Alerts to Send SNMP Traps \(Web\)” on page 161](#)
- [“Enable Alerts to Send PETs \(Web\)” on page 161](#)
- [“Enable Alerts to Send Email Alerts \(Web\)” on page 162](#)
- [“Disable Alerts \(Web\)” on page 163](#)

▼ Display the Oracle ILOM User Accounts (Web)

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface” on page 118](#).

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 Oracle ILOM User Accounts \(CLI\)” on page 61](#)
- [“Display Oracle ILOM User Accounts \(SNMP\)” on page 230](#)

▼ Display the Remote Log Hosts (Web)

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface” on page 118](#).

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 62](#)
- [“Display the Remote Log Hosts \(SNMP\)” on page 231](#)
- [“Set the Remote Log Hosts \(Web\)” on page 138](#)

▼ Display the Network Management Configuration (Web)

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface” on page 118](#).

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 63](#)
- [“Display the Network Management Configuration \(SNMP\)” on page 231](#)

▼ Display the CLI Session Timeout (Web)

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface” on page 118](#).

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 CLI Session Timeout \(CLI\)” on page 64](#)
- [“Set the CLI Session Timeout \(Web\)” on page 164](#)

▼ Display System Component FRU ID (Web)

Note – You can only display FRU ID information for currently present fans and power supplies.

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

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

2. **Click the System Information tab.**

3. **Click the Components subtab.**

The Components Management window opens.

In the Component Status table, the component names (targets) and type are listed.

4. **Click a component name (target) link in the table.**

A new window opens and displays the component’s properties and values.

5. **Click Close.**

Related Information

- [“Display Gateway FRU ID \(CLI\)”](#) on page 64
- [“Display Power Supply FRU ID \(CLI\)”](#) on page 65
- [“Display Gateway FRU ID \(SNMP\)”](#) on page 232
- [“Display Power Supply FRU ID \(SNMP\)”](#) on page 234
- [“Display FRU ID Information \(IPMI\)”](#) on page 262

▼ Display the Firmware Version (Web)

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

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

2. **Click the System Information tab.**

3. **Click the SUN DCS GW Firmware Versions subtab.**

The SUN DCS GW Firmware Versions window opens.

In the GW Firmware Version Information table, the firmware version, buildtime, last upgrade date, and update status are displayed.

Related Information

- [“Display the Firmware Version \(CLI\)”](#) on page 66
- [“Display the Firmware Version \(SNMP\)”](#) on page 239

- [“Display the Oracle ILOM Version \(Web\)” on page 133](#)

▼ Display the Oracle ILOM Version (Web)

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

See [“Access Oracle ILOM From the Web Interface” on page 118](#).

2. **Click the System Information tab.**

3. **Click the ILOM Versions subtab.**

The Versions window opens.

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

Related Information

- [“Display the Firmware Version \(CLI\)” on page 66](#)
- [“Display the Firmware Version \(SNMP\)” on page 239](#)
- [“Display the Firmware Version \(Web\)” on page 132](#)

▼ Display System Identification Properties (Web)

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

See [“Access Oracle ILOM From the Web Interface” on page 118](#).

2. **Click the System Information tab.**

3. **Click the Identification Information subtab.**

The Identification Information window opens.

The host name, system identifier, system contact, system location, and system description are displayed.

Related Information

- [“Display System Identification Properties \(CLI\)” on page 66](#)
- [“Display System Identification Properties \(SNMP\)” on page 239](#)
- [“Set the System Identification Properties \(Web\)” on page 145](#)

Controlling Oracle ILOM Targets (Web)

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

- [“Performing General Tasks on Oracle ILOM Targets \(Web\)” on page 134](#)
- [“Performing Oracle ILOM User Tasks \(Web\)” on page 145](#)
- [“Managing HTTP Services \(Web\)” on page 147](#)
- [“Managing HTTPS Services \(Web\)” on page 149](#)
- [“Managing SNMP Services \(Web\)” on page 152](#)
- [“Managing IPMI Services \(Web\)” on page 159](#)
- [“Managing Other Aspects With Oracle ILOM \(Web\)” on page 160](#)

Related Information

- [“Access Oracle ILOM From the Web Interface” on page 118](#)
- [“Controlling Oracle ILOM Targets \(CLI\)” on page 67](#)
- [“Monitoring Oracle ILOM Targets \(Web\)” on page 119](#)
- [“Understanding Oracle ILOM Targets” on page 4](#)

Performing General Tasks on Oracle ILOM Targets (Web)

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

- [“Restart the Management Controller \(Web\)” on page 135](#)
- [“Set the Date and Time \(Web\)” on page 136](#)
- [“Set the Time Zone \(Web\)” on page 136](#)
- [“Enable the Locator LED \(Web\)” on page 137](#)
- [“Disable the Locator LED \(Web\)” on page 137](#)
- [“Clear the Oracle ILOM Event Log \(Web\)” on page 138](#)
- [“Set the Remote Log Hosts \(Web\)” on page 138](#)
- [“Configure the DNS Client \(Web\)” on page 139](#)
- [“Configure the SMTP Client \(Web\)” on page 140](#)
- [“Back Up the Configuration \(Web\)” on page 141](#)
- [“Restore the Configuration \(Web\)” on page 142](#)

- [“Create a Snapshot of the Gateway State \(Web\)”](#) on page 142
- [“Snapshot Dataset Information \(Web\)”](#) on page 143
- [“Set the Network Management Parameters \(Web\)”](#) on page 144
- [“Set the System Identification Properties \(Web\)”](#) on page 145

Related Information

- [“Performing General Tasks on Oracle ILOM Targets \(CLI\)”](#) on page 67
- [“Performing Oracle ILOM User Tasks \(Web\)”](#) on page 145

▼ Restart the Management Controller (Web)

Note – Restarting the management controller severs any management console link to the management controller. You must reaccess the management controller to regain administrative control.

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

2. Click the Maintenance tab.

3. Click the Reset SP subtab.

The Reset Service Processor window opens.

4. Click Reset SP.

A dialog box opens and asks you to confirm.

5. Click OK.

A message describing the reset action is displayed with a link, and the management controller is reset.

Related Information

- *Gateway Administration*, restarting the management controller
- [“Restart the Management Controller \(CLI\)”](#) on page 68

▼ Set the Date and Time (Web)

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

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** drop-down menus.
6. (Optional) If you want to use a time server, follow these steps:
 - a. Check the **Enabled** box for **Synchronize Time Using NTP**.
 - b. Type the IP address of the first time server into the **Server 1** field.
 - c. Type the IP address of the second time server into the **Server 2** field.
7. Click **Save**.

Related Information

- [“Set the Date and Time \(CLI\)” on page 69](#)
- [“Set the Date and Time \(SNMP\)” on page 241](#)

▼ Set the Time Zone (Web)

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface” on page 118](#).
2. Click the **Configuration** tab.
3. Click the **Timezone** subtab.

The Timezone Settings window opens.
4. Select the time zone from the **Timezone** drop-down menu.
5. Click **Save**.

Related Information

- [“Set the Date and Time \(CLI\)” on page 69](#)
- [“Set the Time Zone \(SNMP\)” on page 241](#)

▼ Enable the Locator LED (Web)

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface” on page 118](#).

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

3. **Click the Indicators subtab.**

The Indicators window opens.

In the Indicators table, the `/SYS/I_LOCATOR` target identifies the Locator LED.

4. **Click the radio button to the left of the target, and from the Actions drop-down menu, select Set LED to On.**

A dialog box opens and asks you to confirm.

5. **Click OK.**

The Locator LED flashes.

Related Information

- [“Enable the Locator LED \(CLI\)” on page 70](#)
- [“Enable the Locator LED \(IPMI\)” on page 264](#)
- [“Disable the Locator LED \(Web\)” on page 137](#)
- [“Display the Gateway Status LEDs States \(Web\)” on page 120](#)

▼ **Disable the Locator LED (Web)**

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

See [“Access Oracle ILOM From the Web Interface” on page 118](#).

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

3. **Click the Indicators subtab.**

The Indicators window opens.

In the Indicators table, the `/SYS/I_LOCATOR` target identifies the Locator LED.

4. **Click the radio button to the left of the target, and from the Actions drop-down menu, select Turn LED Off.**

A dialog box opens and asks you to confirm.

5. **Click OK.**

The Locator LED is unlit.

Related Information

- [“Disable the Locator LED \(CLI\)” on page 71](#)
- [“Disable the Locator LED \(IPMI\)” on page 264](#)
- [“Enable the Locator LED \(Web\)” on page 137](#)
- [“Display the Gateway Status LEDs States \(Web\)” on page 120](#)

▼ Clear the Oracle ILOM Event Log (Web)

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

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

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 Oracle ILOM Event Log \(CLI\)”](#) on page 71
- [“Clear the Oracle ILOM Event Log \(SNMP\)”](#) on page 243
- [“Display the Oracle ILOM Event Log \(Web\)”](#) on page 124
- [“Set the Remote Log Hosts \(Web\)”](#) on page 138

▼ Set the Remote Log Hosts (Web)

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

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

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

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.**

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

5. **Click Save.**

The remote log hosts are set.

Related Information

- [“Set the Remote Log Hosts \(CLI\)” on page 72](#)
- [“Set the Remote Log Hosts \(SNMP\)” on page 243](#)
- [“Display the Remote Log Hosts \(Web\)” on page 130](#)

▼ Configure the DNS Client (Web)

To enable name services within the management controller, Oracle ILOM must be configured as a DNS client.

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface” on page 118](#).

2. Click the Configuration tab.

3. Click the DNS subtab.

The DNS Configuration window opens.

4. If you want the DHCP server to provide the DNS client configuration, check the Enabled box to the right of Auto DNS via DHCP.

Note – If Auto DNS via DHCP is enabled, then the Name Server and Search Path fields are greyed-out.

5. In the DNS Name Server: field, type up to three IP addresses of name servers, separated by commas.

Note – List the IP address in order of search preference.

6. In the DNS Search Path: field, type up to six domains or search suffixes, separated by commas.

Note – List the domains or search suffixes in order of search preference.

7. In the DNS Timeout: and DNS Retries: field, you can configure timeout and retry values.

Note – The default values provide optimal performance.

8. Click Save.

Related Information

- [“Configure the DNS Client \(CLI\)” on page 73](#)
- [“Configure the DNS Client \(SNMP\)” on page 244](#)
- [“Display the DNS Client Status \(Web\)” on page 127](#)

▼ Configure the SMTP Client (Web)

To enable email alerts, you must configure Oracle ILOM as an SMTP client.

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface” on page 118](#).

2. Click the Configuration tab.

3. Click the SMTP Client subtab.

The SMTP Client Settings window opens.

4. Select the Enabled checkbox and provide the SMTP server IP address or hostname, the SMTP server port, and the custom sender string into the respective fields.

5. Click Save.

6. (Optional) Send a test email to verify SMTP client settings.

a. Type an accessible email address into the Address field.

b. Click Send Test.

c. Verify that the email was received.

Related Information

- [“Configure the SMTP Client \(CLI\)” on page 74](#)
- [“Configure the SMTP Client \(SNMP\)” on page 245](#)
- [“Display the SMTP Client Status \(Web\)” on page 128](#)

▼ Back Up the Configuration (Web)

Note – See [“Gateway Configuration Information Backed Up” on page 76](#) for what gateway-specific configuration information is backed up when a passphrase is used.

1. **Access the Oracle ILOM web interface.**
See [“Access Oracle ILOM From the Web Interface”](#) on page 118.
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 drop-down menu.**
5. **Select the transfer protocol from the Transfer Method drop-down menu.**
6. **For the protocol selected, type the file, host IP address, file path, user name, and password into the respective fields.**
7. **If you want to back up sensitive information in addition to the configuration, type a passphrase into the Passphrase and Confirm Passphrase fields.**
8. **Click Run.**
A dialog box opens and asks you to confirm.
9. **Click OK.**
The configuration is backed up in the specified file on the specified host using the specified protocol.

Related Information

- [“Gateway Configuration Information Backed Up”](#) on page 76
- [“Back Up the Configuration \(CLI\)”](#) on page 75
- [“Restore the Configuration \(Web\)”](#) on page 142

▼ **Restore the Configuration (Web)**

1. **Access the Oracle ILOM web interface.**
See [“Access Oracle ILOM From the Web Interface”](#) on page 118.
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 drop-down menu.**
5. **Select the transfer protocol from the Transfer Method drop-down menu.**
6. **For the protocol selected, type 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 so that sensitive information is also restored.

8. **Click Run.**

A dialog box opens and asks you to confirm.

9. **Click OK.**

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

Related Information

- [“Restore the Configuration \(CLI\)” on page 76](#)
- [“Back Up the Configuration \(Web\)” on page 141](#)

▼ **Create a Snapshot of the Gateway State (Web)**

The snapshot utility collects log files, executes various commands and collects their output, and sends the data collected to a user-defined location as a .zip file. The data set selected determines what data is to be included in the snapshot. See [“Snapshot Dataset Information \(Web\)” on page 143](#).

The snapshot describes the state of the gateway at a particular moment in time. This can be used for fault diagnosis.

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

See [“Access Oracle ILOM From the Web Interface” on page 118](#).

2. **Click the Maintenance tab.**

3. **Click the Snapshot subtab.**

The Service Snapshot Utility window opens.

4. **Select the data set from the Data Set drop-down menu.**

See the table in [“Snapshot Dataset Information \(Web\)” on page 143](#).

5. **If you chose the Custom data set, check the data that you want to include in the snapshot.**

6. **If you want only log files, select the Enabled checkbox to the right of Collect Only Log Files From Data Set.**

7. **Select the transfer protocol from the Transfer Method drop-down menu.**

8. **Type the host IP address or host name, file path, user name, and password into the respective fields.**

9. Click Run.

Related Information

- [“Snapshot Dataset Information \(Web\)” on page 143](#)
- [“Create a Snapshot of the Gateway State \(CLI\)” on page 77](#)

Snapshot Dataset Information (Web)

This table provides a listing of the data sets you can choose and the respective data that is included in the snapshot.

Data Set	Description
Normal	Contains Oracle ILOM data, basic operating system data, and gateway configuration data.
FRUID	Contains normal dataset information, with additional FRUID data.
Full	Contains normal dataset information, with additional FRUID data and diagnostic data.
Custom	Contains the user’s choice of Oracle ILOM data, basic operating system data, gateway hardware data, additional FRUID data, and diagnostic data.

The snapshot is stored as a .zip file with a filename of this format:

hostname_IP_address_year-month-dayThour-minute-second.zip

For example:

magnum_123.45.67.89_2011-01-07T14-43-15.zip

Note – The Normal, FRUID, and Full datasets of the snapshot utility are currently equivalent and contain the same data in the snapshot.

Related Information

- [“Create a Snapshot of the Gateway State \(Web\)” on page 142](#)

▼ Set the Network Management Parameters (Web)

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

2. Click the Configuration tab.

3. Click the Network subtab.

The Network Settings window opens.

4. Select the IP Discovery Mode, DHCP, or Static.

5. If you select Static, type the IP address, netmask, and gateway into their respective fields.

6. Click Save.

Note – Changing some network management properties terminates the NET MGT connection to the management controller (web interface). You must re-establish the connection to continue administering the management controller.

7. Re-establish the NET MGT connection to continue administering the management controller.

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

Related Information

- [“Set the Network Management Parameters \(CLI\)”](#) on page 80
- [“Set the Network Parameters \(SNMP\)”](#) on page 246

▼ Set the System Identification Properties (Web)

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

2. Click the System Information tab.

3. Click the Identification Information subtab.

The Identification Information window opens.

4. Type the host name, system identifier, system contact, and system location into their respective fields.

5. Click Save.

Related Information

- [“Set the System Identification Properties \(CLI\)” on page 82](#)
- [“Set the System Identification Properties \(SNMP\)” on page 248](#)
- [“Display System Identification Properties \(Web\)” on page 133](#)

Performing Oracle ILOM User Tasks (Web)

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

- [“Add an Oracle ILOM User Account \(Web\)” on page 145](#)
- [“Change an Oracle ILOM User’s Password and or Role \(Web\)” on page 146](#)
- [“Delete an Oracle ILOM User Account \(Web\)” on page 147](#)

Related Information

- [“Performing Oracle ILOM User Tasks \(CLI\)” on page 83](#)
- [“Performing General Tasks on Oracle ILOM Targets \(Web\)” on page 134](#)

▼ Add an Oracle ILOM User Account (Web)

1. **Access the Oracle ILOM web interface.**
See [“Access Oracle ILOM From the Web Interface” on page 118](#).
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 into the User Name field.**
7. **Select the abilities of the new user from the Roles drop-down menu.**
If a checkbox 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 Oracle ILOM User Account \(CLI\)” on page 84](#)
- [“Add an Oracle ILOM User Account \(SNMP\)” on page 249](#)
- [“Delete an Oracle ILOM User Account \(Web\)” on page 147](#)

▼ Change an Oracle ILOM User’s Password and or Role (Web)

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface” on page 118](#).

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 drop-down menu.

If a checkbox 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 Oracle ILOM User’s Password and or Role \(CLI\)” on page 84](#)

▼ Delete an Oracle ILOM User Account (Web)

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface” on page 118](#).

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 Oracle ILOM User Account \(CLI\)” on page 85](#)
- [“Delete an Oracle ILOM User Account \(SNMP\)” on page 250](#)
- [“Add an Oracle ILOM User Account \(Web\)” on page 145](#)

Managing HTTP Services (Web)

These tasks help you manage the Oracle ILOM HTTP service targets.

- [“Enable the HTTP Service \(Web\)” on page 148](#)
- [“Disable the HTTP Service \(Web\)” on page 148](#)

Related Information

- [“Managing HTTP Services \(CLI\)” on page 86](#)
- [“Managing HTTPS Services \(Web\)” on page 149](#)
- [“Managing SNMP Services \(Web\)” on page 152](#)
- [“Managing IPMI Services \(Web\)” on page 159](#)

▼ Enable the HTTP Service (Web)

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

Note – The HTTP service is disabled and the HTTPS service is enabled by default.

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

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

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 drop-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 86
- [“Set the HTTP Service State \(SNMP\)”](#) on page 251
- [“Disable the HTTP Service \(Web\)”](#) on page 148

▼ **Disable the HTTP Service (Web)**

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

Note – The HTTP service is disabled by default.

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

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

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 drop-down menu.**

6. **Click Save.**

Related Information

- [“Disable the HTTP Service \(CLI\)” on page 87](#)
- [“Set the HTTP Service State \(SNMP\)” on page 251](#)
- [“Enable the HTTP Service \(Web\)” on page 148](#)

Managing HTTPS Services (Web)

These tasks help you manage the Oracle ILOM HTTPS service targets.

- [“Enable the HTTPS Service \(Web\)” on page 149](#)
- [“Install a Custom SSL Certificate \(Web\)” on page 150](#)
- [“Remove the Custom SSL Certificate \(Web\)” on page 151](#)
- [“Disable the HTTPS Service \(Web\)” on page 151](#)

Related Information

- [“Managing HTTPS Services \(CLI\)” on page 88](#)
- [“Managing HTTP Services \(Web\)” on page 147](#)
- [“Managing SNMP Services \(Web\)” on page 152](#)
- [“Managing IPMI Services \(Web\)” on page 159](#)

▼ Enable the HTTPS Service (Web)

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

Note – The HTTPS service is enabled by default.

1. **Access the Oracle ILOM web interface.**
See [“Access Oracle ILOM From the Web Interface” on page 118](#).
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 88](#)
- [“Set the HTTPS Service State \(SNMP\)” on page 251](#)
- [“Disable the HTTPS Service \(Web\)” on page 151](#)

▼ Install a Custom SSL Certificate (Web)

1. Access the Oracle ILOM web interface.
See [“Access Oracle ILOM From the Web Interface” on page 118](#).
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 drop-down menu.
7. For the protocol selected, type 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 89](#)
- [“Remove the Custom SSL Certificate \(Web\)” on page 151](#)

▼ Remove the Custom SSL Certificate (Web)

1. Access the Oracle ILOM web interface.
See [“Access Oracle ILOM From the Web Interface” on page 118](#).
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 89](#)
- [“Install a Custom SSL Certificate \(Web\)” on page 150](#)

▼ **Disable the HTTPS Service (Web)**

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

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

See [“Access Oracle ILOM From the Web Interface” on page 118](#).

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. Clear the **Enabled** checkbox for the **HTTPS** web server.

6. Click **Save**.

Related Information

- [“Disable the HTTPS Service \(CLI\)” on page 90](#)
- [“Set the HTTPS Service State \(SNMP\)” on page 251](#)
- [“Enable the HTTPS Service \(Web\)” on page 149](#)

Managing SNMP Services (Web)

These tasks help you manage the Oracle ILOM SNMP service targets.

- [“Enable the SNMP Service \(Web\)”](#) on page 152
- [“Configure the SNMP Service \(Web\)”](#) on page 153
- [“Add SNMP Service User Accounts \(Web\)”](#) on page 153
- [“Modify SNMP Service User Accounts \(Web\)”](#) on page 154
- [“Delete SNMP Service User Accounts \(Web\)”](#) on page 155
- [“Add SNMP Service Communities \(Web\)”](#) on page 156
- [“Modify SNMP Service Communities \(Web\)”](#) on page 156
- [“Delete SNMP Service Communities \(Web\)”](#) on page 157
- [“Download SNMP Service MIBs \(Web\)”](#) on page 158
- [“Disable the SNMP Service \(Web\)”](#) on page 158

Related Information

- [“Managing SNMP Services \(CLI\)”](#) on page 91
- [“Managing HTTP Services \(Web\)”](#) on page 147
- [“Managing HTTPS Services \(Web\)”](#) on page 149
- [“Managing IPMI Services \(Web\)”](#) on page 159

▼ Enable the SNMP Service (Web)

Note – The SNMP service is enabled by default.

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

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, select the Enabled checkbox for State.

6. Click Save.

Related Information

- [“Enable the SNMP Service \(CLI\)” on page 91](#)
- [“Disable the SNMP Service \(Web\)” on page 158](#)

▼ **Configure the SNMP Service (Web)**

1. **Access the Oracle ILOM web interface.**
See [“Access Oracle ILOM From the Web Interface” on page 118.](#)
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. **Select the Enabled checkbox for Set Requests to enable set requests.**
7. **Select the checkboxes for the protocols you want to enable.**
8. **Click Save.**

Related Information

- [“Configure the SNMP Service \(CLI\)” on page 92](#)

▼ **Add SNMP Service User Accounts (Web)**

1. **Access the Oracle ILOM web interface.**
See [“Access Oracle ILOM From the Web Interface” on page 118.](#)
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 drop-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 drop-down menu.
12. (Optional) Select the privacy protocol from the Privacy Protocol drop-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 93](#)
- [“Delete SNMP Service User Accounts \(Web\)” on page 155](#)

▼ **Modify SNMP Service User Accounts (Web)**

1. **Access the Oracle ILOM web interface.**
See [“Access Oracle ILOM From the Web Interface” on page 118](#).
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 drop-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 drop-down menu.
11. (Optional) Select the privacy protocol from the Privacy Protocol drop-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 94](#)

▼ **Delete SNMP Service User Accounts (Web)**

1. Access the Oracle ILOM web interface.
See [“Access Oracle ILOM From the Web Interface” on page 118](#).
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 95](#)
- [“Add SNMP Service User Accounts \(Web\)” on page 153](#)

▼ Add SNMP Service Communities (Web)

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

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

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 drop-down menu.**

9. **Click Save.**

The community is created and the window closes.

Related Information

- [“Add SNMP Service Communities \(CLI\)”](#) on page 95
- [“Delete SNMP Service Communities \(Web\)”](#) on page 157

▼ Modify SNMP Service Communities (Web)

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

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

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** drop-down menu.

8. Click **Save**.

The community is modified and the window closes.

Related Information

- [“Modify SNMP Service Communities \(CLI\)” on page 96](#)

▼ **Delete SNMP Service Communities (Web)**

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

See [“Access Oracle ILOM From the Web Interface” on page 118](#).

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 96](#)
- [“Add SNMP Service Communities \(Web\)” on page 156](#)

▼ **Download SNMP Service MIBs (Web)**

This procedure creates a compressed file, `ilom-mibs.zip`, that contains these MIBs:

- `ENTITY-MIB.mib`

- SUN-HW-TRAP-MIB.mib
- SUN-ILOM-CONTROL-MIB.mib
- SUN-PLATFORM-MIB.mib
- SUN-FABRIC-MIB.mib
- SUN-DCS-IB-MIB.txt

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

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

Related Information

- [“Download SNMP Service MIBs \(CLI\)”](#) on page 97

▼ Disable the SNMP Service (Web)

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

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, clear the Enabled checkbox for State.

6. Click Save.

Related Information

- [“Disable the SNMP Service \(CLI\)”](#) on page 98

- [“Enable the SNMP Service \(Web\)” on page 152](#)

Managing IPMI Services (Web)

These tasks help you manage the Oracle ILOM IPMI service target.

- [“Enable the IPMI Service \(Web\)” on page 159](#)
- [“Disable the IPMI Service \(Web\)” on page 160](#)

Related Information

- [“Managing IPMI Services \(CLI\)” on page 98](#)
- [“Managing HTTP Services \(Web\)” on page 147](#)
- [“Managing HTTPS Services \(Web\)” on page 149](#)
- [“Managing SNMP Services \(Web\)” on page 152](#)

▼ Enable the IPMI Service (Web)

Note – The IPMI service is enabled by default.

1. **Access the Oracle ILOM web interface.**
See [“Access Oracle ILOM From the Web Interface” on page 118](#).
2. **Click the Configuration tab.**
3. **Click the System Management Access subtab.**
4. **Click the IPMI subtab.**
The IPMI Settings window opens.
5. **Select the Enabled checkbox for State.**
6. **Click Save.**

Related Information

- [“set Command” on page 274](#)
- [“Enable the IPMI Service \(CLI\)” on page 99](#)
- [“Disable the IPMI Service \(Web\)” on page 160](#)

▼ Disable the IPMI Service (Web)

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

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

2. **Click the Configuration tab.**

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

4. **Click the IPMI subtab.**

The IPMI Settings window opens.

5. **Unselect the Enabled checkbox for State.**

6. **Click Save.**

The IPMI service is disabled.

Related Information

- [“set Command”](#) on page 274
- [“Disable the IPMI Service \(CLI\)”](#) on page 99
- [“Enable the IPMI Service \(Web\)”](#) on page 159

Managing Other Aspects With Oracle ILOM (Web)

These tasks help you manage other aspects of Oracle ILOM.

- [“Enable Alerts to Send SNMP Traps \(Web\)”](#) on page 161
- [“Enable Alerts to Send PETs \(Web\)”](#) on page 161
- [“Enable Alerts to Send Email Alerts \(Web\)”](#) on page 162
- [“Disable Alerts \(Web\)”](#) on page 163
- [“Set the CLI Session Timeout \(Web\)”](#) on page 164

Related Information

- [“Managing Other Aspects With Oracle ILOM \(CLI\)”](#) on page 100
- [“Managing Other Aspects With Oracle ILOM \(SNMP\)”](#) on page 250
- [“Performing General Tasks on Oracle ILOM Targets \(Web\)”](#) on page 134

▼ Enable Alerts to Send SNMP Traps (Web)

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

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

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 drop-down menu.**

6. **Select the SNMP Trap alert type from the Type drop-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 drop-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 100
- [“Enable Alerts to Send SNMP Traps \(SNMP\)”](#) on page 252
- [“Enable Alerts to Send PETs \(Web\)”](#) on page 161
- [“Enable Alerts to Send Email Alerts \(Web\)”](#) on page 162
- [“Display the Alert Properties \(Web\)”](#) on page 129
- [“Disable Alerts \(Web\)”](#) on page 163

▼ Enable Alerts to Send PETs (Web)

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

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

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 drop-down menu.**
6. **Select the IPMI PET alert type from the Type drop-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 PETs \(CLI\)” on page 102](#)
- [“Enable Alerts to Send PETs \(SNMP\)” on page 253](#)
- [“Enable Alerts to Send SNMP Traps \(Web\)” on page 161](#)
- [“Enable Alerts to Send Email Alerts \(Web\)” on page 162](#)
- [“Display the Alert Properties \(Web\)” on page 129](#)
- [“Disable Alerts \(Web\)” on page 163](#)

▼ **Enable Alerts to Send Email Alerts (Web)**

1. **Access the Oracle ILOM web interface.**
See [“Access Oracle ILOM From the Web Interface” on page 118](#).
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 drop-down menu.**
6. **Select the email alert type from the Type drop-down menu.**
7. **Type the destination email address into the Email Address field.**
8. **(Optional) Select the Event Class Filter and Event Type Filter from their respective drop-down menus.**
9. **Type a custom sender identifier into the Custom Sender field to override the default value.**
10. **(Optional) Type a message prefix into the Message Prefix field.**

11. Click Save.

The alert is enabled.

Related Information

- [“Enable Alerts to Send Email Alerts \(CLI\)” on page 103](#)
- [“Enable Alerts to Send Email Alerts \(SNMP\)” on page 254](#)
- [“Enable Alerts to Send SNMP Traps \(Web\)” on page 161](#)
- [“Enable Alerts to Send PETs \(Web\)” on page 161](#)
- [“Display the Alert Properties \(Web\)” on page 129](#)
- [“Disable Alerts \(Web\)” on page 163](#)

▼ Disable Alerts (Web)

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface” on page 118](#).

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 drop-down menu.

6. Click Save.

The alert is disabled.

Related Information

- [“Disable Alerts \(CLI\)” on page 104](#)
- [“Disable Alerts \(SNMP\)” on page 256](#)
- [“Enable Alerts to Send SNMP Traps \(Web\)” on page 161](#)
- [“Enable Alerts to Send PETs \(Web\)” on page 161](#)
- [“Enable Alerts to Send Email Alerts \(Web\)” on page 162](#)
- [“Display the Alert Properties \(Web\)” on page 129](#)

▼ Set the CLI Session Timeout (Web)

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

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 Oracle ILOM CLI Session Timeout \(CLI\)”](#) on page 105
- [“Display the CLI Session Timeout \(Web\)”](#) on page 131

▼ Upgrade the Gateway Firmware (Web)

Note – If you are going to downgrade the firmware to a version earlier than 2.0, you must remove user partitions and depopulate the Subnet Manager nodes list. See *Gateway Administration*, removing partitions for firmware downgrade.

1. Acquire the firmware package.

See [“Acquire the Gateway Firmware Package \(CLI\)”](#) on page 107.

2. Open an SSH session and connect to the management controller by specifying the controller’s host name.

For example:

```
% ssh -l root nm2name
root@nm2name's password: password
#
```

where *nm2name* is the host name of the management controller. Initially, the password is changeme.

3. If the Subnet Manager is running on the management controller, disable it with the `disablesm` command.

```
# disablesm
Stopping partitiond daemon.          [ OK ]
Stopping IB Subnet Manager..        [ OK ]
#
```

4. Verify that there is at least 150 MB available in the `/tmp` directory.

```
# df -h /tmp
Filesystem      Size  Used Avail Use% Mounted on
tmpfs           250M  240K  249M  1% /tmp
#
```

In this example, there are 249 MB available. If not enough space is available, you must delete files from the `/tmp` directory.

5. Verify that there is at least 1 MB available in the `/config` directory.

```
# df -h /config
Filesystem      Size  Used Avail Use% Mounted on
/dev/hda2       16M   3.6M   11M   25% /config
#
```

In this example, there are 11 MB available. If not enough space is available, you must delete files from the `/config` directory.

6. Verify that there is at least 1 MB available in the `/var/log` directory.

```
# df -h /var/log
Filesystem      Size  Used Avail Use% Mounted on
/dev/hda3       16M   3.6M   11M   25% /var/log
#
```

In this example, there are 11 MB available. If not enough space is available, you must delete files from the `/var/log` directory.

7. Verify that there is at least 150 MB free memory available.

#	free -m					
	total	used	free	shared	buffers	cached
Mem:	498	104	393	0	12	47
-/+ buffers/cache:		45	453			
Swap:	0	0	0			
#						

In the `-/+ buffers/cache:` row of the `free` column, there should be at least 150 MB free memory. In this example, there are 453 MB available. If not enough memory is available, you must exit nonessential applications that are running.

8. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface” on page 118](#).

9. Click the Maintenance tab.

10. Click the Firmware Upgrade subtab.

The Firmware Upgrade window opens.

11. Click Enter Upgrade Mode.

A dialog box opens and asks you to confirm.

12. Click OK.

The Firmware Upgrade window changes to Upgrade mode and now accepts a URL and file name of the gateway firmware package.

Note – For the specified URL, only the FTP or HTTP protocols are supported.

13. Click Upload.

Oracle ILOM transfers the gateway firmware package to the management controller. Oracle ILOM verifies the package integrity and displays the current versions of the firmware and versions in the package.

14. Click Start Upgrade.

A dialog box opens and asks you to confirm.

15. Click OK.

The upgrade begins and the status of the upgrade is reported.
When the upgrade process ends, a log and summary report are displayed.

16. Click OK.

A final status is displayed, the upgrade either:

- Succeeded
- Partially succeeded
- Failed

17. Reboot the gateway to enable the new firmware.

See *Gateway Administration*, restarting the entire gateway.

Note – The restart process takes between 4 to 5 minutes to complete.

You can monitor the update progress through:

- web browser – `http://gateway_name`
- CLI – `telnet gateway_name 1234`

where *gateway_name* is the host name or IP address of the management controller.

Note – The Oracle ILOM stack requires at least 2 minutes to become operational after a reboot.

18. If the Subnet Manager was previously disabled, open an SSH session, connect to the management controller, and enable the Subnet Manager.

```
% ssh -l root gateway_name
root@gateway_name's password: password
# enablesm
Starting IB Subnet Manager.                [ OK ]
Starting partitiond daemon.                [ OK ]
# exit
```

19. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface”](#) on page 118.

20. Verify the success of the firmware update.

See [“Display the Firmware Version \(Web\)”](#) on page 132.

21. Verify the firmware integrity.

See [“Verify Firmware Integrity \(CLI\)”](#) on page 106.

Related Information

- [“Upgrade the Gateway Firmware \(CLI\)”](#) on page 109

Using the Fabric Monitor

The Fabric Monitor enables you to visually monitor the status of the gateway, the I4 switch chip, and the connectors through a web-based interface. The Fabric Monitor is accessible from the Oracle ILOM web interface.

These topics describe how to use the fabric monitor.

- [“Access the Fabric Monitor” on page 169](#)
- [“Fabric Monitor Features” on page 170](#)
- [“Accessing the Rear Panel Diagram” on page 172](#)
- [“Accessing Status Pane Information” on page 180](#)
- [“Control Panel Function” on page 187](#)
- [“Monitoring Parameters and Status” on page 188](#)

Related Information

- [“Understanding Oracle ILOM on the Gateway” on page 1](#)
- [“Administering Oracle ILOM \(CLI\)” on page 29](#)
- [“Administering Oracle ILOM \(Web\)” on page 115](#)
- [“Administering Oracle ILOM \(SNMP\)” on page 199](#)
- [“Administering Hardware \(IPMI\)” on page 257](#)
- [“Understanding Oracle ILOM Commands” on page 265](#)

▼ Access the Fabric Monitor

1. Access the Oracle ILOM web interface.

See [“Access Oracle ILOM From the Web Interface” on page 118](#).

Note – If the login page is not displayed or an error is displayed, verify that the web interface is enabled. See [“Enable the HTTP Service \(CLI\)” on page 86](#) and [“Enable the HTTPS Service \(CLI\)” on page 88](#).

2. Click the Switch/Fabric Monitoring Tools tab.

The SUN DCS GW Monitor page is displayed.

3. Click Launch SUN DCS GW Monitor.

The Fabric Monitor GUI is displayed.

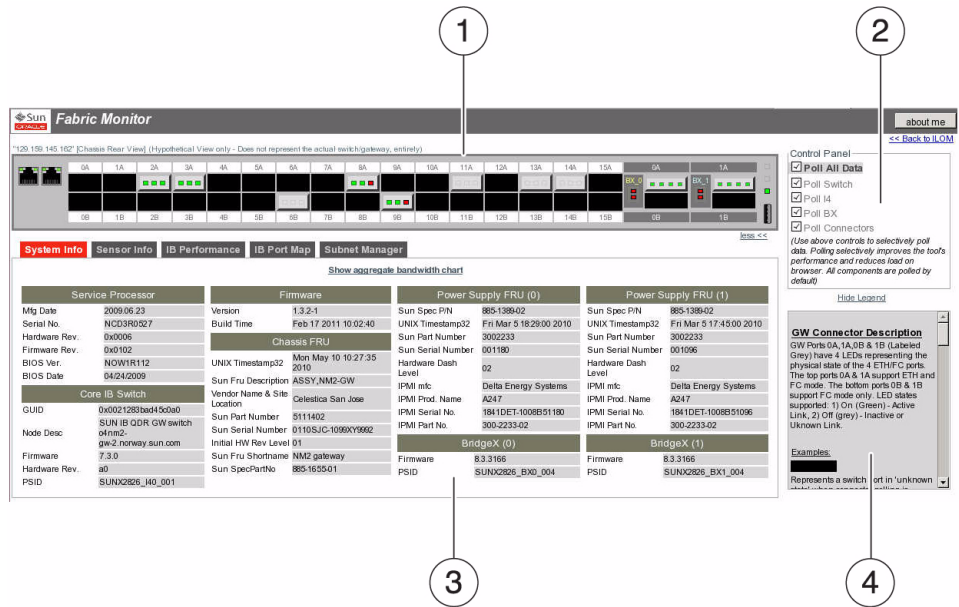
Note – To return to ILOM, click the <<Back to ILOM link in the upper-right corner of the Fabric Monitor.

Related Information

- [“Fabric Monitor Features” on page 170](#)
- [“Accessing the Rear Panel Diagram” on page 172](#)
- [“Accessing Status Pane Information” on page 180](#)
- [“Control Panel Function” on page 187](#)
- [“Monitoring Parameters and Status” on page 188](#)

Fabric Monitor Features

This figure displays the basic aspects of the FM interface.



- 1 Rear panel diagram
- 2 Control panel
- 3 Status pane
- 4 Legend

Note – Both the control panel and legend are hidden by default. Clicking the more>> link makes them visible.

The FM also has status windows for:

- **Connector indicators** – Moving the mouse cursor over an indicator that is orange or red opens a small window that provides the reason for the respective state.
- **InfiniBand connector status** – Clicking on a gray InfiniBand connector opens a window that displays connector FRU, port state, error, and statistical information for that connection.
- **Gateway connector status** – Clicking on a gray gateway connector opens a window that displays connector FRU and port information for that connection.
- **BridgeX port status** – Clicking on a gateway BX indicator opens a window that displays port information for the interface between the I4 switch chip port and the BridgeX chip port.

These status windows are explained in depth in [“Accessing the Rear Panel Diagram”](#) on page 172.

Related Information

- [“Access the Fabric Monitor”](#) on page 169
- [“Accessing the Rear Panel Diagram”](#) on page 172
- [“Accessing Status Pane Information”](#) on page 180
- [“Control Panel Function”](#) on page 187
- [“Monitoring Parameters and Status”](#) on page 188

Accessing the Rear Panel Diagram

The rear panel diagram provides a visual representation of the gateway’s connector and link status. Aspects of the diagram are discussed in these topics:

- [“Rear Panel Diagram Overview”](#) on page 172
- [“InfiniBand Connector Status Window”](#) on page 173
- [“Gateway Connector Status Window”](#) on page 176
- [“BridgeX Port Status Window”](#) on page 178

Related Information

- [“Access the Fabric Monitor”](#) on page 169
- [“Fabric Monitor Features”](#) on page 170
- [“Accessing Status Pane Information”](#) on page 180
- [“Control Panel Function”](#) on page 187
- [“Monitoring Parameters and Status”](#) on page 188

Rear Panel Diagram Overview

This figure provides an example of the rear panel diagram.



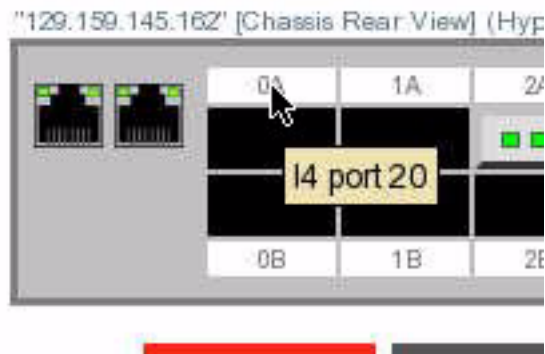
The rear panel diagram displays the presence of connectors and their status within a mockup of the gateway rear panel. The diagram displays the management controller's IP address, and the connector receptacles and their respective connector names. When a cable is attached to a receptacle, a connection is made. That connection is displayed in the diagram as a gray rectangle, with three or four smaller indicators. Moving the mouse cursor over an indicator, clicking on an indicator, or clicking on a connection opens a window that provides additional information about that indicator or connection.

Related Information

- ["InfiniBand Connector Status Window" on page 173](#)
- ["Gateway Connector Status Window" on page 176](#)
- ["BridgeX Port Status Window" on page 178](#)

InfiniBand Connector Status Window

In the rear panel diagram, there are 32 InfiniBand receptacles displayed, labeled 0A to 15A and 0B to 15B. Moving the mouse cursor over a connector name opens a small window that states the respective I4 switch chip port for that connector. This figure provides an example of moving the mouse cursor over the 0A for connection 0A.



When a connector is physically present in an InfiniBand receptacle, the receptacle changes from a black rectangle to a gray rectangle with three indicators.

This table describes the three indicators of the InfiniBand connection rectangle.

Object	Left Indicator	Center Indicator	Right Indicator
Description	Physical link	InfiniBand link quality	InfiniBand link errors
Color	<ul style="list-style-type: none"> • Gray – No link • Green – Link established 	<ul style="list-style-type: none"> • Gray – No activity • Green – QDR • Orange – DDR, SDR 	<ul style="list-style-type: none"> • Gray – No activity • Green – No errors • Red – Errors

Moving the mouse cursor over an indicator that is orange or red opens a small window that states the reason for the respective state:

- A center indicator is orange because the link is at a speed slower than QDR, such as SDR or DDR.
- A right indicator is red because there are errors (symbol, recovery, and so on) on the link.

This figure provides an example of moving the mouse cursor over the red right indicator for connection 8A.



Clicking on the connection opens the InfiniBand connector status window for that connector. This figure provides an example of an InfiniBand connector status window.

Connector: 8A Port: 31

Cable FRU

Property	Value
Identifier	Unknown (ff)
Connector Type	Unknown (ff)
Vendor
Vendor OUI	FFFFFF
Part Number
Revision	...
Serial Number
Date

Switch Port (me)

Property	Value
Device Name	SUN IB QDR GW switch o4nm2- gw-2.norway.sun.com
Device type	Switch
GUID	0x0021283bad45c0a0
LID	0x2
Port	31
Link Status	Active
Link Quality	QDR
Counter Name	Value
SymbolErrors	0
LinkRecoveries	0
LinkDowned	0
RcvErrors	0
RcvRemotePhysErrors	0
RcvSwRelayErrors	1
XmtDiscards	1
XmtConstraintErrors	0
RcvConstraintErrors	0
LinkIntegrityErrors	0
ExcBufOverrunErrors	0
VL15Dropped	0
XmtData	205124661
RcvData	147427717
XmtPkts	322839
RcvPkts	2134715

Peer Port (my peer)

Property	Value
Device Name	o4test55 HCA-1
Device type	HCA
GUID	0x0002c903000213c4
LID	4
Port	1
Link Status	Active
Link Quality	QDR
Counter Name	Value
SymbolErrors	0
LinkRecoveries	0
LinkDowned	0
RcvErrors	0
RcvRemotePhysErrors	0
RcvSwRelayErrors	0
XmtDiscards	0
XmtConstraintErrors	0
RcvConstraintErrors	0
LinkIntegrityErrors	0
ExcBufOverrunErrors	0
VL15Dropped	0
XmtData	147427645
RcvData	205124661
XmtPkts	2134714
RcvPkts	322839

close

At the top of the window are the connector name and the respective I4 switch chip port. There are three sets of information in the window, the cable FRU ID information, information about the I4 switch chip port (Switch Port), and similar information about the port's InfiniBand peer (Peer Port).

The cable FRU ID information includes:

- Identifier
- Connector type
- Vendor
- Vendor OUI
- Part number
- Revision
- Serial number
- Date of manufacture

The port information includes:

- Device name and type
- GUID, LID, and respective port
- Link status and quality
- Symbol errors

- Recovery errors
- Errors of various categories
- Throughput statistics

Clicking Close dismisses the InfiniBand connector status window.

Related Information

- [“Rear Panel Diagram Overview” on page 172](#)
- [“Gateway Connector Status Window” on page 176](#)
- [“BridgeX Port Status Window” on page 178](#)

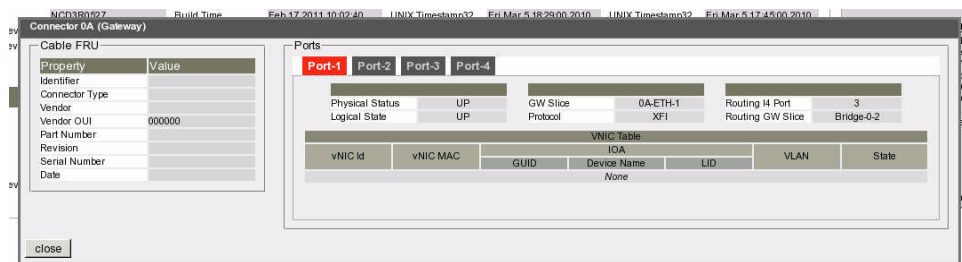
Gateway Connector Status Window

The rear panel diagram displays four gateway receptacles, labeled 0A, 1A, 0B, and 1B. When a connector is physically present in a gateway receptacle, the receptacle changes from a black rectangle to a gray rectangle with four indicators. Each indicator represents one of the four possible ports available at the connection.

This table describes the four indicators of the gateway connection rectangle.

Object	Left Indicator	Left Center Indicator	Right Center Indicator	Right Indicator
Name	Port 1	Port 2	Port 3	Port 4
Description	Physical link 1	Physical link 2	Physical link 3	Physical link 4
Color	<ul style="list-style-type: none"> • Gray – No link • Green – Link established 	<ul style="list-style-type: none"> • Gray – No link • Green – Link established 	<ul style="list-style-type: none"> • Gray – No link • Green – Link established 	<ul style="list-style-type: none"> • Gray – No link • Green – Link established

Clicking on the connection opens the gateway connector status window for that connector. This figure provides an example of a gateway connector status window.



At the top of the window is the connector name. There are two parts of the window, the cable FRU ID information on the left and a smaller status pane for the ports on the right.

The cable FRU ID information includes:

- Identifier
- Connector type
- Vendor
- Vendor OUI
- Part number
- Revision
- Serial number
- Date of manufacture

The smaller status pane has tabs for each of the four ports. Clicking on a tab displays that port's information. How the connector has been configured, for Ethernet or Fibre Channel, determines what information is displayed for each port. Typically, the information includes:

- Physical status and logical state
- Gateway slice (connector) and protocol (speed)
- I4 switch chip routing port and gateway routing slice

Additionally, a table provides information about configured vNICs:

- ID and MAC address
- GUID, device name, and LID
- vLAN attachment
- State

Clicking Close dismisses the gateway connector status window.

Related Information

- [“Rear Panel Diagram Overview” on page 172](#)
- [“InfiniBand Connector Status Window” on page 173](#)
- [“BridgeX Port Status Window” on page 178](#)

BridgeX Port Status Window

Left of the gateway connection rectangles are the BX indicators, which display the status of the BridgeX chip to I4 switch chip connection.

Note – Clicking on the gateway connector name, 0A, 1A, 0B, 1B, either hides or reveals the respective BX indicators. If the BX indicators are not displayed, click on a gateway connector name.

The indicators are labeled BX_0 for connectors 0A and 0B, and BX_1 for connectors 1A and 1B.

This table describes the BX indicators.

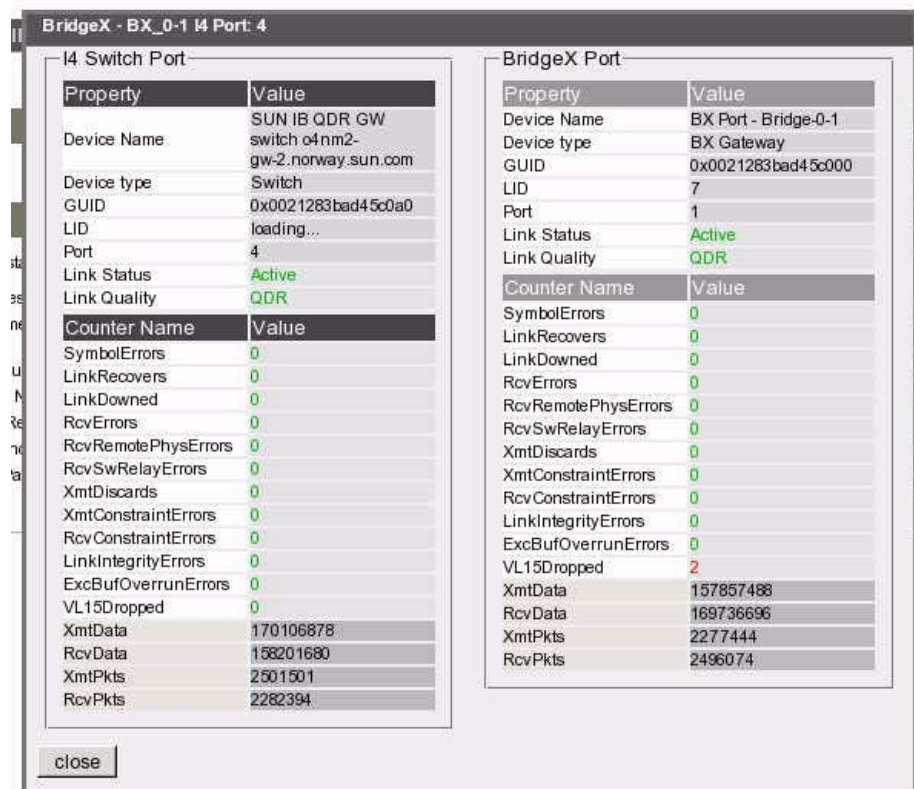
Object	Upper Indicator	Lower Indicator
Description	Physical link 0 connector	Physical link 1 connector
Color	<ul style="list-style-type: none">• Gray – No link• Green – Link established• Red – Link fault	<ul style="list-style-type: none">• Gray – No link• Green – Link established• Red – Link fault

Moving the mouse cursor over a BX indicator opens a small window that provides information about the BridgeX port. If the indicator is red, then the window displays a reason for the respective state.

This figure provides an example of moving the mouse cursor over the red upper indicator for port BX_0.



Clicking on a BX indicator opens the BridgeX port status window for that BridgeX port. This figure provides an example of a BridgeX port status window.



At the top of the window are the BridgeX chip name, the respective BridgeX port, and the attached I4 switch chip port. There are two sets of information in the window, one set for the I4 switch chip port, and another set for the BridgeX port. Each set provides this information about the respective port:

- Device name and type
- GUID, LID, and respective port
- Link status and quality
- Symbol errors
- Recovery errors
- Errors of various categories
- Throughput statistics

Clicking Close dismisses the BridgeX port status window.

Related Information

- [“Rear Panel Diagram Overview” on page 172](#)

- [“InfiniBand Connector Status Window” on page 173](#)
 - [“Gateway Connector Status Window” on page 176](#)
-

Accessing Status Pane Information

At the center of the FM is the status pane, which displays the majority of information regarding the gateway. The status pane has five tabs:

- [“System Info Tab” on page 181](#)
- [“Sensor Info Tab” on page 182](#)
- [“IB Performance Tab” on page 183](#)
- [“IB Port Map Tab” on page 185](#)
- [“Subnet Manager Tab” on page 186](#)

Related Information

- [“Access the Fabric Monitor” on page 169](#)
- [“Fabric Monitor Features” on page 170](#)
- [“Accessing the Rear Panel Diagram” on page 172](#)
- [“Control Panel Function” on page 187](#)
- [“Monitoring Parameters and Status” on page 188](#)

System Info Tab

This figure provides an example of the System Info tab.

System Info		Sensor Info	IB Performance	IB Port Map	Subnet Manager
Show aggregate bandwidth chart					
Service Processor		Firmware		Power Supply FRU (0)	
Mfg Date	2009.06.23	Version	1.3.2-1	Sun Spec P/N	885-1389-02
Serial No.	NCD3R0527	Build Time	Feb 17 2011 10:02:40	UNIX Timestamp32	Fri Mar 5 18:29:00 2010
Hardware Rev.	0x0006	Chassis FRU		Sun Part Number	3002233
Firmware Rev.	0x0102	Sun Fru Description		Sun Serial Number	001180
BIOS Ver.	NOW1R112	UNIX Timestamp32		Hardware Dash Level	02
BIOS Date	04/24/2009	Mon May 10 10:27:35 2010		IPMI mfg.	Delta Energy Systems
Core IB Switch		Vendor Name & Site Location		IPMI Prod. Name	A247
GUID	0x0021283bad45c0a0	Sun Part Number		IPMI Serial No.	1841DET-1008B51180
Node Desc	SUN IB QDR GW switch o4nm2-gw-2.norway.sun.com	Sun Serial Number		IPMI Part No.	300-2233-02
Firmware	7.3.0	Initial HW Rev Level		BridgeX (0)	
Hardware Rev.	a0	Sun Fru Shortname		Firmware	8.3.3166
PSID	SUNX2826_I40_001	Sun SpecPartNo		PSID	SUNX2826_BX0_004
				BridgeX (1)	
				Firmware	8.3.3166
				PSID	SUNX2826_B

The System Info tab displays status information regarding the gateway hardware. The information is categorized in these groups:

- **Service Processor** – Basic information about the management controller
- **Core IB Switch** – Basic information about the I4 switch chip
- **Firmware** – Version and build date
- **Chassis FRU** – FRU ID information about the chassis
- **Power Supply FRU (0)** – FRU ID information about the left power supply
- **Power Supply FRU (1)** – FRU ID information about the right power supply
- **BridgeX (0)** – Firmware information about BridgeX chip 0
- **BridgeX (1)** – Firmware information about BridgeX chip 1

If the Poll I4 checkbox in the control panel is selected (default), then you can click Show aggregate bandwidth chart to display the historic total bandwidth. This figure provides an example of the aggregate bandwidth.

System Info	Sensor Info	IB Performance	IB Port Map	Subnet Manager
-------------	-------------	----------------	-------------	----------------

Voltage Sensors			Power Sensors				Temperature Sensors		
Name	Value	Status	Name	Present	A/C Present	Status	Name	Value	Status
ECB	-	OK	PSU 0	true	true	OK	Back	31	OK
3.3V Main	3.27	OK	PSU 1	true	false	-	Front	29	OK
3.3V Stby	3.35	OK	Fan Sensors				SP	44	OK
12V	11.97	OK	Name	Present	RPM	Status	Switch	44	OK
5V	5.02	OK	FAN 0	true	15151	OK	Bridge-0	48	OK
VBAT	3.21	OK	FAN 1	false	-	-	Bridge-1	54	OK
1.0V	1.01	OK	FAN 2	true	14933	OK	IB Device Sensors		
V1P2 DIG	1.18	OK	FAN 3	false	-	-	Name	Status	
V1P2 ANG	1.18	OK	FAN 4	true	14933	OK	Switch	OK	
1.2V BridgeX	1.19	OK							
1.2V Standby	1.2	OK							
2.5V	2.5	OK							
1.8V	1.78	OK							
I4 1.2V	1.22	OK							

The Sensor Info tab displays status information regarding the gateway sensors. The information is categorized in these groups:

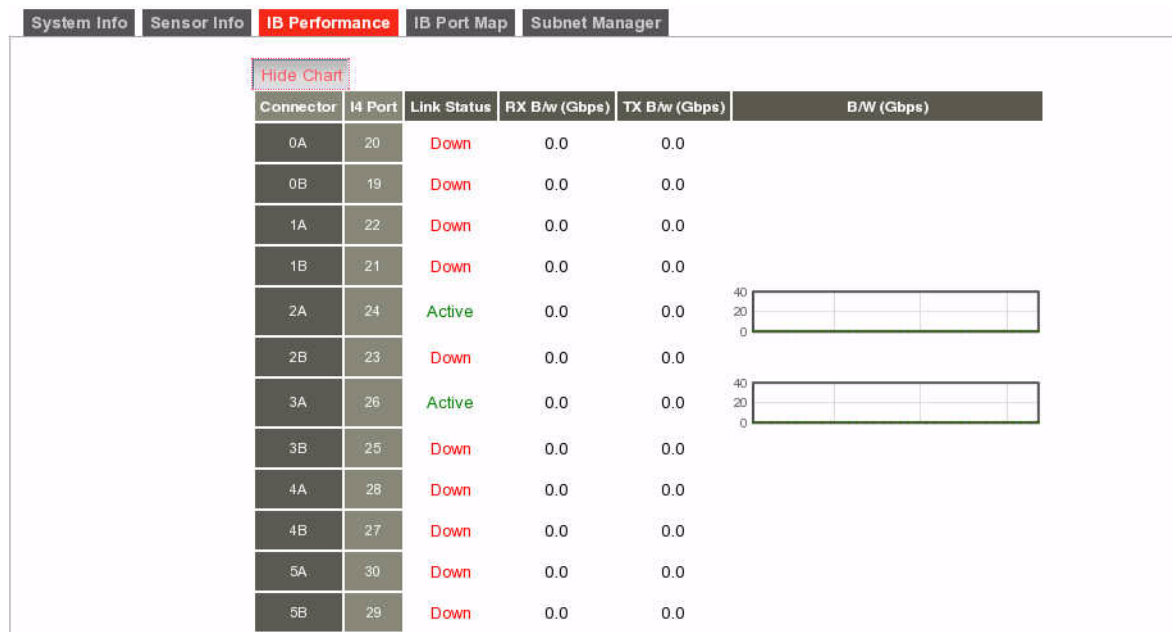
- **Voltage Sensors** – Assorted voltages on the main board
- **Power Sensors** – Presence, AC presence, and status for both power supply slots
- **Fan Sensors** – Presence, RPM, and status for each fan slot
- **Temperature Sensors** – Back, front, management controller, I4 switch chip, and BridgeX chips
- **IB Device Sensors** – I4 switch chip and BridgeX chips status

Related Information

- [“System Info Tab” on page 181](#)
- [“IB Performance Tab” on page 183](#)
- [“IB Port Map Tab” on page 185](#)
- [“Subnet Manager Tab” on page 186](#)

IB Performance Tab

This figure provides an example of the IB Performance tab.



The IB Performance tab displays the status of the I4 switch chip ports. A table describes this information:

- **Connector** – Rear panel connector respective to the I4 switch chip port
- **I4 Port** – Port of the I4 switch chip
- **Link Status** – Present link state of the that port. Either Down (red) or Active (green)
- **RX B/w (Gbps)** – Instantaneous receive link bandwidth for that port
- **TX B/w (Gbps)** – Instantaneous transmit link bandwidth for that port

By clicking Show Chart, a sixth column for the table is displayed:

- **B/W (Gbps)** – Running bandwidth of the link for that port (0 to 40 Gbps)

Note – You must select the Poll I4 checkbox (default) in the control panel to populate the table with current information.

When displaying the B/W (Gbps) column, the added resource demand on the management controller slows its ability to display the information. Clicking Hide Chart removes the bandwidth charts.

By clicking on a column heading, the information in the table is sorted according to that column heading, either in ascending or descending order. For example, clicking the I4 Port heading sorts the information in the table according to the numeric sequence of the I4 ports. Clicking the Link Status heading sorts the information in the table according to the state of the links.

Related Information

- [“System Info Tab” on page 181](#)
- [“Sensor Info Tab” on page 182](#)
- [“IB Port Map Tab” on page 185](#)
- [“Subnet Manager Tab” on page 186](#)

IB Port Map Tab

This figure provides an example of the IB Port Map tab.

System Info		Sensor Info		IB Performance		IB Port Map		Subnet Manager	
Switch Port		Peer Device							
Connector	I4 Port	Type	Name	GUID	LID	Port			
0A	20			0x0000000000000000	-	-			
0B	19			0x0000000000000000	-	-			
1A	22			0x0000000000000000	-	-			
1B	21			0x0000000000000000	-	-			
2A	24	Switch	SUN IB QDR GW switch o4nm2-gw-2.norway.sun.com	0x0021283bad45c0a0	2	26			
2B	23			0x0000000000000000	-	-			
3A	26	Switch	SUN IB QDR GW switch o4nm2-gw-2.norway.sun.com	0x0021283bad45c0a0	2	24			
3B	25			0x0000000000000000	-	-			
4A	28			0x0000000000000000	-	-			
4B	27			0x0000000000000000	-	-			
5A	30			0x0000000000000000	-	-			
5B	29			0x0000000000000000	-	-			
6A	35			0x0000000000000000	-	-			
6B	36			0x0000000000000000	-	-			

The IB Port Map tab displays information about peer devices attached to the gateway. A table describes this information:

- **Connector** – Rear panel connector respective to the I4 switch chip port

- **I4 Port** – Port of the I4 switch chip
- **Type** – Type of peer device attached to the connector or I4 switch chip port
- **Name** – Contents of the peer device's NodeDescription field
- **GUID** – GUID of the peer device
- **LID** – LID assigned to the peer device
- **Port** – Port of the node identified by the GUID or LID

By clicking on a column heading, the information in the table is sorted according to that column heading, either in ascending or descending order. For example, clicking the Connector heading sorts the information in the table according to the numeric sequence of the connectors. Clicking the peer device Name heading sorts the information in the table according to the NodeDescription field of the peer device.

- “System Info Tab” on page 181
- “Sensor Info Tab” on page 182
- “IB Performance Tab” on page 183
- “Subnet Manager Tab” on page 186

This figure provides an example of the Subnet Manager tab.

The Subnet Manager tab displays information about the Subnet Manager within the gateway. Information displayed is categorized into these groups:

- **Active SM Info** – Information about the active Subnet Manager, LID, GUID, activity, priority, and state.
- **Embedded OpenSM Settings** – Information about the management controller's Subnet Manager's configuration.

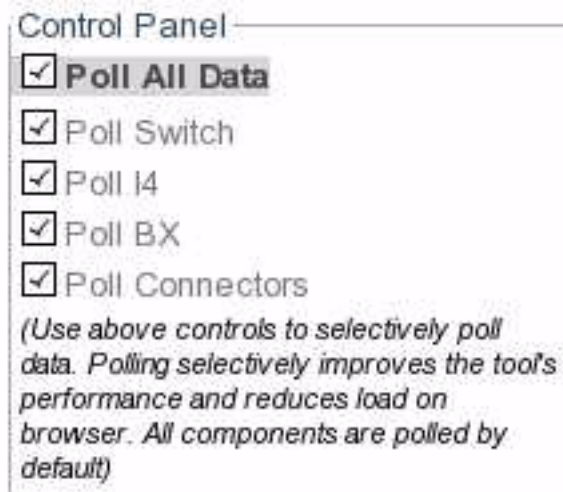
The active Subnet Manager might not be the embedded Subnet Manager within the management controller.

Related Information

- ["System Info Tab" on page 181](#)
- ["Sensor Info Tab" on page 182](#)
- ["IB Performance Tab" on page 183](#)
- ["IB Port Map Tab" on page 185](#)

Control Panel Function

Hidden on the right side of the FM is the control panel. Clicking the more>> link opens the control panel and legend. This figure provides an example of the control panel.



The control panel has five checkboxes that enable you to select what aspect of the gateway is to be monitored. You can select to monitor:

Note – All checkboxes are enabled by default. By clearing the checkboxes that are not necessary for your monitoring needs, you reduce the load on the interface and optimize the operation of the FM.

- **Poll All Data** – Selecting this checkbox enables all polling. Consequently, all checkboxes are selected. When all checkboxes are selected, the added resource demand on the management controller slows its ability to display the information.
- **Poll Switch** – Selecting this checkbox enables you to monitor the status of the gateway hardware and the Subnet Manager. By checking this box, the System Info, Sensor Info, and Subnet Manager tabs of the status pane become active and are populated with information.
- **Poll I4** – Selecting this checkbox enables you to monitor the status of the I4 switch chip and the links its ports negotiate. By checking this box, the IB Performance and IB Port Map tabs of the status pane become active and are populated with information. Additionally, the Show Aggregate Bandwidth Chart link under the System Info tab becomes active.
- **Poll BX** – Selecting this checkbox enables you to monitor the status of the BridgeX chips and the connections from its ports. You must also select the Poll Connectors checkbox to view the status of the BridgeX chips.
- **Poll Connectors** – Selecting this checkbox enables you to monitor the status of the connectors on the gateway rear panel. By checking this box, the rear panel diagram becomes active and displays present connectors and their condition.

Related Information

- [“Access the Fabric Monitor” on page 169](#)
- [“Fabric Monitor Features” on page 170](#)
- [“Accessing the Rear Panel Diagram” on page 172](#)
- [“Accessing Status Pane Information” on page 180](#)
- [“Monitoring Parameters and Status” on page 188](#)

Monitoring Parameters and Status

These tables help you quickly find a gateway parameter or status value using the FM.

- [“Chassis Parameters and Status” on page 189](#)
- [“InfiniBand Connector Parameters and Status” on page 191](#)

- [“Gateway Connector Parameters and Status” on page 194](#)
- [“I4 to Gateway Interface Parameters and Status” on page 195](#)
- [“I4 Switch Chip Port Parameters and Status” on page 196](#)

Related Information

- [“Access the Fabric Monitor” on page 169](#)
- [“Fabric Monitor Features” on page 170](#)
- [“Accessing the Rear Panel Diagram” on page 172](#)
- [“Accessing Status Pane Information” on page 180](#)
- [“Control Panel Function” on page 187](#)

Chassis Parameters and Status

Use this table to determine chassis status with the FM. Find the parameter or status in the left column, then perform the steps from left to right.

Parameter or Status to Monitor	Action in Status Pane	Information Location
Battery voltage.	Click Sensor Info tab.	Look in the first column, Voltage Sensors, in the middle.
BridgeX chip voltage.	Click Sensor Info tab.	Look in the first column, Voltage Sensors, in the lower middle.
BridgeX chip 0 firmware version.	Click System Info tab.	Look in the third column, BridgeX (0), at the top.
BridgeX chip 0 PSID.	Click System Info tab.	Look in the third column, BridgeX (0), at the bottom.
BridgeX chip 0 status.	Click Sensor Info tab.	Look in the third column, IB Device Sensors, in the middle.
BridgeX chip 0 temperature.	Click Sensor Info tab.	Look in the third column, Temperature Sensors, at the bottom.
BridgeX chip 1 firmware version.	Click System Info tab.	Look in the fourth column, BridgeX (1), at the top.
BridgeX chip 1 PSID.	Click System Info tab.	Look in the fourth column, BridgeX (1), at the bottom.
BridgeX chip 1 status.	Click Sensor Info tab.	Look in the third column, IB Device Sensors, at the bottom.
BridgeX chip 1 temperature.	Click Sensor Info tab.	Look in the third column, Temperature Sensors, at the bottom.

Parameter or Status to Monitor	Action in Status Pane	Information Location
Chassis FRU description.	Click System Info tab.	Look in the second column, Chassis FRU, at the top.
Chassis part number.	Click System Info tab.	Look in the second column, Chassis FRU, in the middle.
Chassis serial number.	Click System Info tab.	Look in the second column, Chassis FRU, in the middle.
Chassis temperatures.	Click Sensor Info tab.	Look in the third column, Temperature Sensors.
Controlled handover state.	Click Subnet Manager tab.	Look in the second column, Embedded OpenSM Settings, in the middle.
Fan presence.	Click Sensor Info tab.	Look in the second column, Fan Sensors, second column.
Fan speed.	Click Sensor Info tab.	Look in the second column, Fan Sensors, third column.
Fan status.	Click Sensor Info tab.	Look in the second column, Fan Sensors, fourth column.
I4 switch chip firmware version.	Click System Info tab.	Look in the first column, Core IB Switch, in the middle.
I4 switch chip GUID.	Click System Info tab.	Look in the first column, Core IB Switch, at the top.
I4 switch chip historic aggregate bandwidth.	Click System Info tab. Click Show Aggregate Bandwidth Chart.	Look in the center.
I4 switch chip LID.	Click Subnet Manager tab.	Look in the first column, Active SM Info, at the top.
I4 switch chip status.	Click Sensor Info tab.	Look in the third column, IB Device Sensors, at the top.
I4 switch chip temperature.	Click Sensor Info tab.	Look in the third column, Temperature Sensors, at the bottom.
I4 switch chip voltage.	Click Sensor Info tab.	Look in the first column, Voltage Sensors, at the bottom.
Main board voltages.	Click Sensor Info tab.	Look in the first column, Voltage Sensors.
Management controller BIOS version.	Click System Info tab.	Look in the first column, Service Processor, at the bottom.
Management controller firmware version.	Click System Info tab.	Look in the second column, Firmware.
Management controller serial number.	Click System Info tab.	Look in the first column, Service Processor, at the top.
Power supply presence.	Click Sensor Info tab.	Look in the second column, Power Sensors, second column.

Parameter or Status to Monitor	Action in Status Pane	Information Location
Power supply line voltage presence.	Click Sensor Info tab.	Look in the second column, Power Sensors, third column.
Power supply status.	Click Sensor Info tab.	Look in the second column, Power Sensors, fourth column.
Subnet Manager controlled handover.	Click Subnet Manager tab.	Look in the second column, Embedded OpenSM Settings, in the middle.
Subnet Manager GUID.	Click Subnet Manager tab.	Look in the first column, Active SM Info, at the top.
Subnet Manager LID.	Click Subnet Manager tab.	Look in the first column, Active SM Info, at the top.
Subnet Manager priority.	Click Subnet Manager tab.	Look in the first column, Active SM Info, in the middle. Look in the second column, Embedded OpenSM Settings, in the middle.
Subnet Manager routing algorithm.	Click Subnet Manager tab.	Look in the second column, Embedded OpenSM Settings, in the middle.
Subnet Manager status.	Click Subnet Manager tab.	Look in the first column, Active SM Info, in the middle. Look in the second column, Embedded OpenSM Settings, at the top.
Subnet Manager subnet prefix.	Click Subnet Manager tab.	Look in the second column, Embedded OpenSM Settings, at the bottom.

Related Information

- [“InfiniBand Connector Parameters and Status” on page 191](#)
- [“Gateway Connector Parameters and Status” on page 194](#)
- [“I4 to Gateway Interface Parameters and Status” on page 195](#)
- [“I4 Switch Chip Port Parameters and Status” on page 196](#)

InfiniBand Connector Parameters and Status

Use this table to determine InfiniBand connector status for all connectors with the FM. Find the parameter or status in the left column, then perform the steps from left to right.

Parameter or Status to Monitor	Action at Rear Panel Diagram or Status Pane	Information Location
All connectors - cable present.	Check rear panel diagram.	If gray, connector present. If black, connector absent.
All connectors - current receive bandwidth.	Click IB Performance tab.	Look in the first column, Connector. Look in the fourth column, RX B/w (Gbps).
All connectors - current transmit bandwidth.	Click IB Performance tab.	Look in the first column, Connector. Look in the fifth column, TX B/w (Gbps).
All connectors - link active.	Check rear panel diagram.	If left indicator gray, link down. If left indicator green, link up.
All connectors - link quality.	Check rear panel diagram.	If center indicator gray, no activity. If center indicator green, QDR. If center indicator orange, less than QDR.
All connectors - link errors.	Check rear panel diagram.	If right indicator gray, no activity. If right indicator green, insignificant errors. If right indicator red, significant errors.
All connectors - link state.	Click IB Performance tab.	Look in the first column, Connector. Look in the third column, Link Status.
All connectors - peer device GUID and port.	Click IB Port Map tab.	Look in the first column, Connector. Look in the fifth column, GUID. Look in the seventh column, Port.
All connectors - peer device LID and port.	Click IB Port Map tab.	Look in the first column, Connector. Look in the sixth column, LID. Look in the seventh column, Port.
All connectors - peer device type and name.	Click IB Port Map tab.	Look in the first column, Connector. Look in the third column, Type. Look in the fourth column, Name.
All connectors - running bandwidth.	Click IB Performance tab.	Click Show Chart. Look in the first column, Connector. Look in the sixth column, B/W (Gbps).
All connector to I4 switch chip port mapping.	Click IB Port Map tab.	Look in the first column, Connector. Look in the second column, I4 Port.

Use this table to determine InfiniBand connector status for individual connectors with the FM. Find the parameter or status in the left column, then perform the steps from left to right.

Parameter or Status to Monitor	Action at Rear Panel Diagram or Status Pane	Information Location
Individual connector - data throughput.	Check rear panel diagram. Click connection rectangle.	Look in the second column, Switch Port. Look under Counter Name, at the bottom.
Individual connector - device name and type.	Check rear panel diagram. Click connection rectangle.	Look in the second column, Switch Port. Look under Property, at the top.
Individual connector - FRU ID information.	Check rear panel diagram. Click connection rectangle.	Look in the first column, Cable FRU.
Individual connector - GUID and port.	Check rear panel diagram. Click connection rectangle.	Look in the second column, Switch Port. Look under Property, in the middle.
Individual connector - LID and port.	Check rear panel diagram. Click connection rectangle.	Look in the second column, Switch Port. Look under Property, in the middle.
Individual connector - link status and link quality.	Check rear panel diagram. Click connection rectangle.	Look in the second column, Switch Port. Look under Property, at the bottom.
Individual connector - symbol and recovery errors.	Check rear panel diagram. Click connection rectangle.	Look in the second column, Switch Port. Look under Counter Name, at the top.
Individual connector - peer device data throughput.	Check rear panel diagram. Click connection rectangle.	Look in the third column, Peer Port. Look under Counter Name, at the bottom.
Individual connector - peer device GUID and port.	Check rear panel diagram. Click connection rectangle.	Look in the third column, Peer Port. Look under Property, in the middle.
Individual connector - peer device LID and port.	Check rear panel diagram. Click connection rectangle.	Look in the third column, Peer Port. Look under Property, in the middle.
Individual connector - peer device link status and link quality.	Check rear panel diagram. Click connection rectangle.	Look in the third column, Peer Port. Look under Property, at the bottom.
Individual connector - peer device name and type.	Check rear panel diagram. Click connection rectangle.	Look in the third column, Peer Port. Look under Property, at the top.
Individual connector - peer device symbol and recovery errors.	Check rear panel diagram. Click connection rectangle.	Look in the third column, Peer Port. Look under Counter Name, at the top.

Related Information

- [“Chassis Parameters and Status” on page 189](#)
- [“Gateway Connector Parameters and Status” on page 194](#)
- [“I4 to Gateway Interface Parameters and Status” on page 195](#)

Gateway Connector Parameters and Status

Use this table to determine gateway connector status with the FM. Find the parameter or status in the left column, then perform the steps from left to right.

Parameter or Status to Monitor	Action at Rear Panel Diagram or Status Pane	Information Location
All connectors - cable present.	Check rear panel diagram, right side.	If gray, connector present. If black, connector absent.
All connectors - link active.	Check rear panel diagram, right side.	If indicator gray, link down. If indicator green, link up.
All connectors - link quality.	Check rear panel diagram, right side.	If center indicator gray, no activity. If center indicator green, QDR. If center indicator orange, less than QDR.
All connectors - link errors.	Check rear panel diagram, right side.	If right indicator gray, no activity. If right indicator green, insignificant errors. If right indicator red, significant errors.
Individual connector - FRU ID information.	Check rear panel diagram, right side. Click connection rectangle.	Look in the first column, Cable FRU.
Individual connector port - vNIC ID and MAC.	Check rear panel diagram, right side. Click connection rectangle. Port status pane, click port.	Look in VNIC Table. Look in the first column, VNIC ID. Look in the second column, VNIC MAC.
Individual connector port - vNIC ID and associated vLAN and status.	Check rear panel diagram, right side. Click connection rectangle. Port status pane, click port.	Look in VNIC Table. Look in the first column, VNIC ID. Look in the sixth column, VLAN. Look in the seventh column, State.
Individual connector port - vNIC ID mapping to GUID and LID.	Check rear panel diagram, right side. Click connection rectangle. Port status pane, click port.	Look in VNIC Table. Look in the first column, VNIC ID. Look in the third column, GUID. Look in the fifth column, LID.

Parameter or Status to Monitor	Action at Rear Panel Diagram or Status Pane	Information Location
Individual connector port - physical status and logical state.	Check rear panel diagram, right side. Click connection rectangle. Port status pane, click port.	Look in the left column.
Individual connector port - gateway slice and protocol.	Check rear panel diagram, right side. Click connection rectangle. Port status pane, click port.	Look in the center column.
Individual connector port - routing I4 port and routing gateway slice.	Check rear panel diagram, right side. Click connection rectangle. Port status pane, click port.	Look in the right column.

Related Information

- [“Chassis Parameters and Status” on page 189](#)
- [“InfiniBand Connector Parameters and Status” on page 191](#)
- [“I4 to Gateway Interface Parameters and Status” on page 195](#)
- [“I4 Switch Chip Port Parameters and Status” on page 196](#)

I4 to Gateway Interface Parameters and Status

Use this table to determine I4 to BX interface status with the FM. Find the parameter or status in the left column, then perform the steps from left to right.

Parameter or Status to Monitor	Action at Rear Panel Diagram or Status Pane	Information Location
All I4 to BX interface - link status.	Check rear panel diagram, right side.	If indicator gray, no activity. If indicator green, QDR and insignificant errors. If indicator red, less than QDR or significant errors.
I4 to BX interface - BX data throughput.	Check rear panel diagram, right side. Click BX indicator.	Look in the second column, BridgeX Port. Look under Counter Name, at the bottom.
I4 to BX interface - BX GUID and port.	Check rear panel diagram, right side. Click BX indicator.	Look in the second column, BridgeX Port. Look under Property, in the middle.
I4 to BX interface - BX LID and port.	Check rear panel diagram, right side. Click BX indicator.	Look in the second column, BridgeX Port. Look under Property, in the middle.

Parameter or Status to Monitor	Action at Rear Panel Diagram or Status Pane	Information Location
I4 to BX interface - BX link status and link quality.	Check rear panel diagram, right side. Click BX indicator.	Look in the second column, BridgeX Port. Look under Property, at the bottom.
I4 to BX interface - BX name and type.	Check rear panel diagram, right side. Click BX indicator.	Look in the second column, BridgeX Port. Look under Property, at the top.
I4 to BX interface - BX symbol and recovery errors.	Check rear panel diagram, right side. Click BX indicator.	Look in the second column, BridgeX Port. Look under Counter Name, at the top.
I4 to BX interface - I4 data throughput.	Check rear panel diagram, right side. Click BX indicator.	Look in the first column, I4 Switch Port. Look under Counter Name, at the bottom.
I4 to BX interface - I4 GUID and port.	Check rear panel diagram, right side. Click BX indicator.	Look in the first column, I4 Switch Port. Look under Property, in the middle.
I4 to BX interface - I4 LID and port.	Check rear panel diagram, right side. Click BX indicator.	Look in the first column, I4 Switch Port. Look under Property, in the middle.
I4 to BX interface - I4 link status and link quality.	Check rear panel diagram, right side. Click BX indicator.	Look in the first column, I4 Switch Port. Look under Property, at the bottom.
I4 to BX interface - I4 name and type.	Check rear panel diagram, right side. Click BX indicator.	Look in the first column, I4 Switch Port. Look under Property, at the top.
I4 to BX interface - I4 symbol and recovery errors.	Check rear panel diagram, right side. Click BX indicator.	Look in the first column, I4 Switch Port. Look under Counter Name, at the top.

Related Information

- [“Chassis Parameters and Status” on page 189](#)
- [“InfiniBand Connector Parameters and Status” on page 191](#)
- [“Gateway Connector Parameters and Status” on page 194](#)
- [“I4 Switch Chip Port Parameters and Status” on page 196](#)

I4 Switch Chip Port Parameters and Status

Use this table to determine I4 switch chip port status with the FM. Find the parameter or status in the left column, then perform the steps from left to right.

Parameter or Status to Monitor	Action at Status Pane	Information Location
I4 switch chip port to connector mapping.	Click IB Performance tab. Click I4 Port heading.	Look in the first column, Connector. Look in the second column, I4 Port.
I4 switch chip port - current receive bandwidth.	Click IB Performance tab. Click I4 Port heading.	Look in the second column, I4 Port. Look in the fourth column, RX B/w (Gbps).
I4 switch chip port - current transmit bandwidth.	Click IB Performance tab. Click I4 Port heading.	Look in the second column, I4 Port. Look in the fifth column, TX B/w (Gbps).
I4 switch chip port - link state.	Click IB Performance tab. Click I4 Port heading.	Look in the second column, I4 Port. Look in the third column, Link.
I4 switch chip port - peer device GUID and port.	Click IB Port Map tab. Click I4 Port heading.	Look in the second column, I4 port. Look in the fifth column, GUID. Look in the seventh column, Port
I4 switch chip port - peer device LID and port.	Click IB Port Map tab. Click I4 Port heading.	Look in the second column, I4 port. Look in the sixth column, LID. Look in the seventh column, Port
I4 switch chip port - peer device type and name.	Click IB Port Map tab. Click I4 Port heading.	Look in the second column, I4 port. Look in the third column, Type. Look in the fourth column, Name.
I4 switch chip port - running bandwidth.	Click IB Performance tab. Click I4 Port heading. Click Show Chart.	Look in the second column, I4 Port. Look in the sixth column, B/W (Gbps).

Related Information

- [“Chassis Parameters and Status” on page 189](#)
- [“InfiniBand Connector Parameters and Status” on page 191](#)
- [“Gateway Connector Parameters and Status” on page 194](#)
- [“I4 to Gateway Interface Parameters and Status” on page 195](#)

Administering Oracle ILOM (SNMP)

These topics describe how to administer Oracle ILOM through the Simple Network Management Protocol (SNMP).

- [“SNMP Overview” on page 199](#)
- [“Understanding SNMP Commands” on page 200](#)
- [“Monitoring Oracle ILOM Targets \(SNMP\)” on page 203](#)
- [“Controlling Oracle ILOM Targets \(SNMP\)” on page 240](#)

Related Information

- [“Administering Oracle ILOM \(CLI\)” on page 29](#)
- [“Administering Oracle ILOM \(Web\)” on page 115](#)
- [“Using the Fabric Monitor” on page 169](#)
- [“Administering Hardware \(IPMI\)” on page 257](#)
- [“Understanding Oracle ILOM Commands” on page 265](#)

SNMP Overview

The Oracle ILOM implementation on the management controller within the gateway can communicate the state of and enable remote management of Oracle ILOM through SNMP.

An SNMP client is required to interface with the Oracle ILOM SNMP agent on the management controller. The SNMP client must have the appropriate Oracle ILOM MIBs installed. These MIBs are included in the `SUN_DCS_gw_x.y.z_w.tar.gz` file, the Oracle ILOM firmware package that you downloaded. See [“Acquire the Gateway Firmware Package \(CLI\)” on page 107](#).

The MIBs are also available using the CLI or web interface. See “Download SNMP Service MIBs (CLI)” on page 97 or “Download SNMP Service MIBs (Web)” on page 158.

Using the SNMP protocol, the client sends requests in the form of object identifiers (OIDs) to the server on the management controller. The tables in *Gateway Reference*, understanding MIB OIDs, provide a listing of object identifiers.

For more information about and use of SNMP with Oracle ILOM, refer to the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Protocol Management -- SNMP, IPMI, CIM, WS-MAN*, available online at:

<http://www.oracle.com/pls/topic/lookup?ctx=E19860-01&id=homepage>

Related Information

- “Understanding SNMP Commands” on page 200
- “Monitoring Oracle ILOM Targets (SNMP)” on page 203
- “Controlling Oracle ILOM Targets (SNMP)” on page 240

Understanding SNMP Commands

These topics describe how the SNMP command format is affected by the specified SNMP protocol:

- “SNMP Commands” on page 200
- “V1 and V2c Protocol Command Format” on page 201
- “V3 Protocol Command Format” on page 202

Related Information

- “SNMP Overview” on page 199
- “Monitoring Oracle ILOM Targets (SNMP)” on page 203
- “Controlling Oracle ILOM Targets (SNMP)” on page 240
- “Understanding Oracle ILOM Commands” on page 265

SNMP Commands

You can use several NetSNMP CLI client commands to perform tasks:

- `snmpget` – Returns the value of an SNMP object identifier.
- `snmpset` – Sets the value of an SNMP object identifier.
- `snmpwalk` – Returns values for multiple SNMP object identifiers.

Related Information

- [“V1 and V2c Protocol Command Format” on page 201](#)
- [“V3 Protocol Command Format” on page 202](#)

V1 and V2c Protocol Command Format

The majority of SNMP command examples provided use the V2c protocol for ease of demonstration. To perform the examples, you must enable the `v2c` protocol and sets properties in the Oracle ILOM SNMP service, and the SNMP community `public` has `rw` permission. See these tasks for instructions on how to configure these parameters:

- [“Configure the SNMP Service \(CLI\)” on page 92](#)
- [“Configure the SNMP Service \(Web\)” on page 153](#)
- [“Add SNMP Service Communities \(CLI\)” on page 95](#)
- [“Add SNMP Service Communities \(Web\)” on page 156](#)

The command format for both the V1 and V2c protocols is as follows:

```
$ command -v1|-v2c -c public mc_IP MIB_name::object_id argument
```

where:

- *command* is one of the commands described in [“SNMP Commands” on page 200](#).
- *mc_IP* is the IP address of the management controller.
- *MIB_name* is the name of the MIB.
- *object_id* is the object identifier.
- *argument* is a combination of options and variables that support the object identifier.

Note – When the SNMP command example uses the V2c protocol, the management controller IP address variable *mc_IP* is not defined, as this is different for each gateway installation.

For example:

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlTimezone.0 s "GMT"
```

While simple in execution, the command and returned information is not encrypted or secure.

Related Information

- [“SNMP Commands” on page 200](#)
- [“V3 Protocol Command Format” on page 202](#)

V3 Protocol Command Format

In situations where a secure exchange is required, the V3 protocol supports authentication and encryption. The V3 protocol is enabled on the management controller by default. Some of the SNMP command examples in this domain use the V3 protocol. The command format for the V3 protocol is as follows:

```
$ command -v3 -u snmp_user -l security_level -a authentication_protocol -A authentication_password -x DES -X privacy_password mc_IP MIB_name::object_id argument
```

where:

- *command* is one of the commands described in [“SNMP Commands” on page 200](#).
- *snmp_user* is a configured user of the SNMP services.
- *security_level* is:
 - noAuthNoPriv – There is no authentication or privacy.
 - authNoPriv – There is authentication, but no privacy.
 - authPriv – There is authentication and privacy.
- *authentication_protocol* is either MD5 or SHA.
- *authentication_password* is the *snmp_user*'s authentication password.
- *privacy_password* is the *snmp_user*'s privacy password.
- *mc_IP* is the IP address of the management controller.
- *MIB_name* is the name of the MIB.
- *object_id* is the object identifier.
- *argument* is a combination of options and variables that support the object identifier.

Note – For simplification, when an SNMP command example uses the V3 protocol, the *snmp_user*, *security_level*, *authentication_protocol*, *authentication_password*, and *privacy_password* variables are identified as *usersnmp*, *authPriv*, *MD5*, *authpass*, and *privpass* respectively. You must use unique values for *snmp_user*, *authentication_password*, and *privacy_password* variables, specific to the SNMP users of your gateway. Additionally, the management controller IP address variable *mc_IP* is not defined, as this is different for each gateway installation.

For example:

```
$ snmpset -v3 -u usersnmp -l authPriv -a MD5 -A authpass -x DES -X privpass mc_IP  
SUN-ILOM-CONTROL-MIB::ilomCtrlTimezone.0 s "GMT"
```

Note – See [“Add SNMP Service User Accounts \(CLI\)” on page 93](#) or [“Add SNMP Service User Accounts \(Web\)” on page 153](#) for instructions to configure an SNMP user and their authentication and privacy passwords.

Related Information

- [“SNMP Commands” on page 200](#)
- [“V1 and V2c Protocol Command Format” on page 201](#)

Monitoring Oracle ILOM Targets (SNMP)

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

- [“Performing Daily Tasks \(SNMP\)” on page 204](#)
- [“Checking the Status of Services \(SNMP\)” on page 225](#)
- [“Verifying Other Aspects With Oracle ILOM \(SNMP\)” on page 228](#)

Related Information

- [“Monitoring Oracle ILOM Targets \(CLI\)” on page 39](#)
- [“Monitoring Oracle ILOM Targets \(Web\)” on page 119](#)
- [“Controlling Oracle ILOM Targets \(SNMP\)” on page 240](#)

Performing Daily Tasks (SNMP)

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

- [“Display the Date and Time \(SNMP\)” on page 204](#)
- [“Display the Time Zone \(SNMP\)” on page 205](#)
- [“Display the Aggregate Sensors State \(SNMP\)” on page 205](#)
- [“Display Power Supply Status \(SNMP\)” on page 206](#)
- [“Display Board-Level Voltages \(SNMP\)” on page 208](#)
- [“Display Internal Temperatures \(SNMP\)” on page 212](#)
- [“Display Fan Status \(SNMP\)” on page 215](#)
- [“Display the Sensor Alarm State \(SNMP\)” on page 219](#)
- [“Display the Entity Numbers” on page 220](#)
- [“Display Oracle ILOM Sessions \(SNMP\)” on page 222](#)
- [“Display the Oracle ILOM Event Log \(SNMP\)” on page 223](#)

Related Information

- [“Checking the Status of Services \(SNMP\)” on page 225](#)
- [“Verifying Other Aspects With Oracle ILOM \(SNMP\)” on page 228](#)

▼ 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
$
```

If you use the V3 protocol, type.

```
$ snmpget -v3 -u usersnmp -l authPriv -a MD5 -A authpass -x DES -X privpass 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 \(CLI\)” on page 40](#)
- [“Display the Date \(Web\)” on page 120](#)

- [“Display the Time Zone \(SNMP\)” on page 205](#)

▼ 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)
$
```

If you use the V3 protocol, type.

```
$ snmpget -v3 -u usersnmp -l authPriv -a MD5 -A authpass -x DES -X privpass mc_IP
SUN-ILOM-CONTROL-MIB::ilomCtrlTimezone.0
SUN-ILOM-CONTROL-MIB::ilomCtrlTimezone.0 = STRING: PST (US/Pacific)
$
```

Related Information

- [“Display the Date \(CLI\)” on page 40](#)
- [“Display the Date \(Web\)” on page 120](#)
- [“Display the Date and Time \(SNMP\)” on page 204](#)
- [“Set the Time Zone \(SNMP\)” on page 241](#)

▼ Display the Aggregate Sensors State (SNMP)

Note – The entity numbers used in this procedure are for example only. Your entity numbers might differ, depending on the gateway firmware and configuration.

1. **Determine the entity number of the aggregate sensor.**

See [“Display the Entity Numbers” on page 220](#).

2. From the SNMP client, display the aggregate sensor's state.

```
$ snmpget -v2c -c public mc_IP  
SUN-PLATFORM-MIB::sunPlatDiscreteSensorCurrent.number
```

where *number* is the entity number.

For example, to determine the overall gateway state, use the entity number respective to the /SYS/CHASSIS_STATUS aggregate sensor target. This example uses entity number 35:

```
$ snmpget -v2c -c public mc_IP SUN-PLATFORM-MIB::sunPlatDiscreteSensorCurrent.35  
SUN-PLATFORM-MIB::sunPlatDiscreteSensorCurrent.35 = INTEGER: 1  
$
```

In the output, INTEGER: 1 indicates the sensor is in Deasserted state.
INTEGER: 2 means the sensor is in Asserted state.

Related Information

- [“Display the Aggregate Sensors State \(CLI\)” on page 41](#)
- [“Display the Aggregate Sensors State \(Web\)” on page 120](#)
- [“Display Power Supply Status \(SNMP\)” on page 206](#)
- [“Display Board-Level Voltages \(SNMP\)” on page 208](#)
- [“Display Internal Temperatures \(SNMP\)” on page 212](#)
- [“Display Fan Status \(SNMP\)” on page 215](#)
- [“Display the Sensor Alarm State \(SNMP\)” on page 219](#)
- [“Display the Sensor States \(IPMI\)” on page 258](#)
- [“Display the Entity Numbers” on page 220](#)

▼ Display Power Supply Status (SNMP)

Note – The entity numbers used in this procedure are for example only. Your entity numbers might differ, depending on the gateway firmware and configuration. For more information about entity numbers, see [“Display the Entity Numbers” on page 220](#).

1. From the SNMP client, check for the presence of the power supply.

```
$ snmpget -v2c -c public mc_IP  
SUN-PLATFORM-MIB::sunPlatDiscreteSensorCurrent.number
```

where *number* is the entity number for the /SYS/PSUX/PRSNT presence sensor target for the respective power supply. This example uses entity number 45 for the left power supply:

```
$ snmpget -v2c -c public mc_IP SUN-PLATFORM-MIB::sunPlatDiscreteSensorCurrent.45  
SUN-PLATFORM-MIB::sunPlatDiscreteSensorCurrent.45 = INTEGER: 2  
$
```

In the output, the INTEGER: 2 means the power supply is present. INTEGER: 1 means the power supply is not present.

2. Check for the presence of input power.

```
$ snmpget -v2c -c public mc_IP  
SUN-PLATFORM-MIB::sunPlatDiscreteSensorCurrent.number
```

where *number* is the entity number for the /SYS/PSUX/AC_PRESENT fault sensor target for the respective power supply. This example uses entity number 47 for the left power supply:

```
$ snmpget -v2c -c public mc_IP SUN-PLATFORM-MIB::sunPlatDiscreteSensorCurrent.47  
SUN-PLATFORM-MIB::sunPlatDiscreteSensorCurrent.47 = INTEGER: 1  
$
```

In the output, the INTEGER: 1 means State Deasserted, or input power is present. INTEGER: 2 means State Asserted, or input power is not present.

3. Check for an alert.

```
$ snmpget -v2c -c public mc_IP  
SUN-PLATFORM-MIB::sunPlatDiscreteSensorCurrent.number
```

where *number* is the entity number for the /SYS/PSUX/ALERT fault sensor target for the respective power supply. This example uses entity number 46 for the left power supply:

```
$ snmpget -v2c -c public mc_IP SUN-PLATFORM-MIB::sunPlatDiscreteSensorCurrent.46  
SUN-PLATFORM-MIB::sunPlatDiscreteSensorCurrent.46 = INTEGER: 1  
$
```

In the output, the INTEGER: 1 means State Deasserted, or there are no faults with the power supply. INTEGER: 2 means State Asserted, or there is a fault with the power supply.

Related Information

- [“Display Power Supply Status \(CLI\)” on page 43](#)
- [“Display Power Supply Status \(Web\)” on page 121](#)
- [“Display the Aggregate Sensors State \(SNMP\)” on page 205](#)
- [“Display Board-Level Voltages \(SNMP\)” on page 208](#)
- [“Display Internal Temperatures \(SNMP\)” on page 212](#)
- [“Display Fan Status \(SNMP\)” on page 215](#)
- [“Display the Sensor Alarm State \(SNMP\)” on page 219](#)
- [“Display the Entity Numbers” on page 220](#)

▼ Display Board-Level Voltages (SNMP)

Note – The entity numbers used in this procedure are for example only. Your entity numbers might differ, depending on the gateway firmware and configuration.

Note – The voltage values displayed for this procedure are in millivolts.

1. Determine the entity number of the voltage sensor.

See [“Display the Entity Numbers” on page 220](#).

2. Display the basic board-level voltage data.

```
$ snmpget -v2c -c public mc_IP  
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.number
```

where *number* is the entity number.

For example, to display the current 3.3 VDC voltage, use the entity number respective to the /SYS/MB/V_3.3VMain voltage sensor target. This example uses entity number 4:

```
$ snmpget -v2c -c public mc_IP SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.4  
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.4 = INTEGER: 3249  
$
```

The 3.3 VDC voltage displayed in the output of the example is 3249 millivolts, or 3.249 volts.

3. Display comprehensive board-level voltages.

```
$ snmpwalk -v2c -c public mc_IP SUN-PLATFORM-MIB::sunPlatNumericSensorTable  
SUN-PLATFORM-MIB::sunPlatNumericSensorBaseUnits.4 = INTEGER: volts(6)  
SUN-PLATFORM-MIB::sunPlatNumericSensorBaseUnits.6 = INTEGER: volts(6)  
SUN-PLATFORM-MIB::sunPlatNumericSensorBaseUnits.7 = INTEGER: volts(6)  
SUN-PLATFORM-MIB::sunPlatNumericSensorBaseUnits.8 = INTEGER: volts(6)  
SUN-PLATFORM-MIB::sunPlatNumericSensorBaseUnits.10 = INTEGER: volts(6)  
SUN-PLATFORM-MIB::sunPlatNumericSensorBaseUnits.11 = INTEGER: volts(6)  
SUN-PLATFORM-MIB::sunPlatNumericSensorBaseUnits.13 = INTEGER: volts(6)  
SUN-PLATFORM-MIB::sunPlatNumericSensorBaseUnits.15 = INTEGER: volts(6)  
.  
.  
.  
SUN-PLATFORM-MIB::sunPlatNumericSensorExponent.4 = INTEGER: -3  
SUN-PLATFORM-MIB::sunPlatNumericSensorExponent.6 = INTEGER: -3  
SUN-PLATFORM-MIB::sunPlatNumericSensorExponent.7 = INTEGER: -3  
SUN-PLATFORM-MIB::sunPlatNumericSensorExponent.8 = INTEGER: -3  
SUN-PLATFORM-MIB::sunPlatNumericSensorExponent.10 = INTEGER: -3  
SUN-PLATFORM-MIB::sunPlatNumericSensorExponent.11 = INTEGER: -3  
SUN-PLATFORM-MIB::sunPlatNumericSensorExponent.13 = INTEGER: -3  
SUN-PLATFORM-MIB::sunPlatNumericSensorExponent.15 = INTEGER: -3  
.  
.  
.  
SUN-PLATFORM-MIB::sunPlatNumericSensorRateUnits.4 = INTEGER: none(1)  
SUN-PLATFORM-MIB::sunPlatNumericSensorRateUnits.6 = INTEGER: none(1)  
SUN-PLATFORM-MIB::sunPlatNumericSensorRateUnits.7 = INTEGER: none(1)  
SUN-PLATFORM-MIB::sunPlatNumericSensorRateUnits.8 = INTEGER: none(1)
```

```

SUN-PLATFORM-MIB::sunPlatNumericSensorRateUnits.10 = INTEGER: none(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorRateUnits.11 = INTEGER: none(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorRateUnits.13 = INTEGER: none(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorRateUnits.15 = INTEGER: none(1)
.
.
.
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.4 = INTEGER: 3266
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.6 = INTEGER: 3351
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.7 = INTEGER: 11965
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.8 = INTEGER: 5018
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.10 = INTEGER: 3213
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.11 = INTEGER: 1006
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.13 = INTEGER: 1216
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.15 = INTEGER: 2503
.
.
.
SUN-PLATFORM-MIB::sunPlatNumericSensorRestoreDefaultThresholds.4 = INTEGER:
reset(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorRestoreDefaultThresholds.6 = INTEGER:
reset(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorRestoreDefaultThresholds.7 = INTEGER:
reset(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorRestoreDefaultThresholds.8 = INTEGER:
reset(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorRestoreDefaultThresholds.10 = INTEGER:
reset(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorRestoreDefaultThresholds.11 = INTEGER:
reset(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorRestoreDefaultThresholds.13 = INTEGER:
reset(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorRestoreDefaultThresholds.15 = INTEGER:
reset(1)
.
.
.
$

```

4. Look through the output for the entity numbers respective to the voltage sensors.

You can also filter the output of the `snmpwalk` command for a specific entity number. This is an example of filtering the `snmpwalk` command output:

```
$ snmpwalk -v2c -c public mc_IP SUN-PLATFORM-MIB::sunPlatNumericSensorTable
|grep -F '.number ='
```

where *number* is the entity number.

Note – The manner in which you can filter the output varies according to your operating system.

To filter voltage information for the 3.3 VDC main voltage, use the entity number respective to the `/SYS/MB/V_3.3VMain` voltage sensor target. This filtering example uses entity number 4:

```
$ snmpwalk -v2c -c public mc_IP SUN-PLATFORM-MIB::sunPlatNumericSensorTable
|grep -F '.4 ='
SUN-PLATFORM-MIB::sunPlatNumericSensorBaseUnits.4 = INTEGER: volts(6)
SUN-PLATFORM-MIB::sunPlatNumericSensorExponent.4 = INTEGER: -3
SUN-PLATFORM-MIB::sunPlatNumericSensorRateUnits.4 = INTEGER: none(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.4 = INTEGER: 3266
SUN-PLATFORM-MIB::sunPlatNumericSensorNormalMin.4 = INTEGER: 0
SUN-PLATFORM-MIB::sunPlatNumericSensorNormalMax.4 = INTEGER: 255
SUN-PLATFORM-MIB::sunPlatNumericSensorAccuracy.4 = INTEGER: 0
SUN-PLATFORM-MIB::sunPlatNumericSensorLowerThresholdNonCritical.4 = INTEGER:
3112
SUN-PLATFORM-MIB::sunPlatNumericSensorUpperThresholdNonCritical.4 = INTEGER:
3402
SUN-PLATFORM-MIB::sunPlatNumericSensorLowerThresholdCritical.4 = INTEGER: 3060
SUN-PLATFORM-MIB::sunPlatNumericSensorUpperThresholdCritical.4 = INTEGER: 3454
SUN-PLATFORM-MIB::sunPlatNumericSensorLowerThresholdFatal.4 = INTEGER: 2958
SUN-PLATFORM-MIB::sunPlatNumericSensorUpperThresholdFatal.4 = INTEGER: 3539
SUN-PLATFORM-MIB::sunPlatNumericSensorHysteresis.4 = Gauge32: 0
SUN-PLATFORM-MIB::sunPlatNumericSensorEnabledThresholds.4 = BITS: FC
lowerThresholdNonCritical(0) upperThresholdNonCritical(1)
lowerThresholdCritical(2) upperThresholdCritical(3) lower
SUN-PLATFORM-MIB::sunPlatNumericSensorRestoreDefaultThresholds.4 = INTEGER:
reset(1)
$
```

Related Information

- [“Display Board-Level Voltages \(CLI\)” on page 44](#)
- [“Display Board-Level Voltages \(Web\)” on page 122](#)

- “Display the Aggregate Sensors State (SNMP)” on page 205
- “Display Power Supply Status (SNMP)” on page 206
- “Display Internal Temperatures (SNMP)” on page 212
- “Display Fan Status (SNMP)” on page 215
- “Display the Sensor Alarm State (SNMP)” on page 219
- “Display the Entity Numbers” on page 220

▼ Display Internal Temperatures (SNMP)

Note – The entity numbers used in this procedure are for example only. Your entity numbers might differ, depending on the gateway firmware and configuration.

Note – The temperature values displayed for this procedure are in degrees celsius.

1. Determine the entity number of the temperature sensor.

See “Display the Entity Numbers” on page 220.

2. Display the basic temperature data.

```
$ snmpget -v2c -c public mc_IP  
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.number
```

where *number* is the entity number.

For example, to display the current I4 switch chip temperature, use the entity number respective to the /SYS/MB/T_I4A temperature sensor target. This example uses entity number 27.

```
$ snmpget -v2c -c public mc_IP SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.27  
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.27 = INTEGER: 36  
$
```

The I4 switch chip temperature displayed in the output of the example is 36 degrees celsius.

Note – Temperature readings can vary and are influenced by the gateway environment and loading.

3. Display comprehensive temperature information:

```
$ snmpwalk -v2c -c public mc_IP SUN-PLATFORM-MIB::sunPlatNumericSensorTable
SUN-PLATFORM-MIB::sunPlatNumericSensorBaseUnits.4 = INTEGER: volts(6)
SUN-PLATFORM-MIB::sunPlatNumericSensorBaseUnits.6 = INTEGER: volts(6)
SUN-PLATFORM-MIB::sunPlatNumericSensorBaseUnits.7 = INTEGER: volts(6)
SUN-PLATFORM-MIB::sunPlatNumericSensorBaseUnits.8 = INTEGER: volts(6)

.
.
.
SUN-PLATFORM-MIB::sunPlatNumericSensorExponent.4 = INTEGER: -3
SUN-PLATFORM-MIB::sunPlatNumericSensorExponent.6 = INTEGER: -3
SUN-PLATFORM-MIB::sunPlatNumericSensorExponent.7 = INTEGER: -3
SUN-PLATFORM-MIB::sunPlatNumericSensorExponent.8 = INTEGER: -3
.
.
.
SUN-PLATFORM-MIB::sunPlatNumericSensorExponent.24 = INTEGER: 0
SUN-PLATFORM-MIB::sunPlatNumericSensorExponent.25 = INTEGER: 0
SUN-PLATFORM-MIB::sunPlatNumericSensorExponent.26 = INTEGER: 0
SUN-PLATFORM-MIB::sunPlatNumericSensorExponent.27 = INTEGER: 0
SUN-PLATFORM-MIB::sunPlatNumericSensorExponent.28 = INTEGER: 0
SUN-PLATFORM-MIB::sunPlatNumericSensorExponent.29 = INTEGER: 0
.
.
.
SUN-PLATFORM-MIB::sunPlatNumericSensorRateUnits.24 = INTEGER: none(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorRateUnits.25 = INTEGER: none(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorRateUnits.26 = INTEGER: none(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorRateUnits.27 = INTEGER: none(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorRateUnits.28 = INTEGER: none(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorRateUnits.29 = INTEGER: none(1)
.
.
.
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.24 = INTEGER: 31
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.25 = INTEGER: 29
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.26 = INTEGER: 45
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.27 = INTEGER: 44
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.28 = INTEGER: 49
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.29 = INTEGER: 55
.
.
.
SUN-PLATFORM-MIB::sunPlatNumericSensorRestoreDefaultThresholds.24 = INTEGER:
reset(1)
```

```

SUN-PLATFORM-MIB::sunPlatNumericSensorRestoreDefaultThresholds.25 = INTEGER:
reset(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorRestoreDefaultThresholds.26 = INTEGER:
reset(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorRestoreDefaultThresholds.27 = INTEGER:
reset(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorRestoreDefaultThresholds.28 = INTEGER:
reset(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorRestoreDefaultThresholds.29 = INTEGER:
reset(1)
.
.
.
$

```

4. Look through the output for the entity numbers respective to the temperature sensors.

You can also filter the output of the `snmpwalk` command for a specific entity number. This is an example of filtering the `snmpwalk` command output:

```

$ snmpwalk -v2c -c public mc_IP SUN-PLATFORM-MIB::sunPlatNumericSensorTable
|grep -F '.number ='

```

where *number* is the entity number.

Note – The manner in which you can filter the output varies according to your operating system.

To filter temperature information for the I4 switch chip, use the entity number respective to the `/SYS/MB/T_I4A` temperature sensor target. This filtering example uses entity number 27:

```

$ snmpwalk -v2c -c public mc_IP SUN-PLATFORM-MIB::sunPlatNumericSensorTable
|grep -F '.27 ='
SUN-PLATFORM-MIB::sunPlatNumericSensorBaseUnits.27 = INTEGER: degC(3)
SUN-PLATFORM-MIB::sunPlatNumericSensorExponent.27 = INTEGER: 0
SUN-PLATFORM-MIB::sunPlatNumericSensorRateUnits.27 = INTEGER: none(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.27 = INTEGER: 36
SUN-PLATFORM-MIB::sunPlatNumericSensorNormalMin.27 = INTEGER: 0
SUN-PLATFORM-MIB::sunPlatNumericSensorNormalMax.27 = INTEGER: 255
SUN-PLATFORM-MIB::sunPlatNumericSensorAccuracy.27 = INTEGER: 0
SUN-PLATFORM-MIB::sunPlatNumericSensorLowerThresholdNonCritical.27 = INTEGER:
0
SUN-PLATFORM-MIB::sunPlatNumericSensorUpperThresholdNonCritical.27 = INTEGER:
0
SUN-PLATFORM-MIB::sunPlatNumericSensorLowerThresholdCritical.27 = INTEGER: 0

```

```
SUN-PLATFORM-MIB::sunPlatNumericSensorUpperThresholdCritical.27 = INTEGER: 70
SUN-PLATFORM-MIB::sunPlatNumericSensorLowerThresholdFatal.27 = INTEGER: 0
SUN-PLATFORM-MIB::sunPlatNumericSensorUpperThresholdFatal.27 = INTEGER: 100
SUN-PLATFORM-MIB::sunPlatNumericSensorHysteresis.27 = Gauge32: 0
SUN-PLATFORM-MIB::sunPlatNumericSensorEnabledThresholds.27 = BITS: 14
upperThresholdCritical(3) upperThresholdFatal(5)
SUN-PLATFORM-MIB::sunPlatNumericSensorRestoreDefaultThresholds.27 = INTEGER:
reset(1)
$
```

Related Information

- [“Display Internal Temperatures \(CLI\)” on page 47](#)
- [“Display Internal Temperatures \(Web\)” on page 122](#)
- [“Display the Aggregate Sensors State \(SNMP\)” on page 205](#)
- [“Display Power Supply Status \(SNMP\)” on page 206](#)
- [“Display Board-Level Voltages \(SNMP\)” on page 208](#)
- [“Display Fan Status \(SNMP\)” on page 215](#)
- [“Display the Sensor Alarm State \(SNMP\)” on page 219](#)
- [“Display the Entity Numbers” on page 220](#)

▼ Display Fan Status (SNMP)

Note – The entity numbers used in this procedure are for example only. Your entity numbers might differ, depending on the gateway firmware and configuration. For more information about entity numbers, see [“Display the Entity Numbers” on page 220](#).

Note – The fan speed values displayed for this procedure are in RPM.

1. From the SNMP client, check for the presence of the fan.

```
$ snmpget -v2c -c public mc_IP  
SUN-PLATFORM-MIB::sunPlatDiscreteSensorCurrent.number
```

where *number* is the entity number for the /SYS/FANx/PRSNT presence sensor target for the respective fan. This example uses entity number 53 for the left fan (FAN1):

```
$ snmpget -v2c -c public mc_IP SUN-PLATFORM-MIB::sunPlatDiscreteSensorCurrent.53  
SUN-PLATFORM-MIB::sunPlatDiscreteSensorCurrent.53 = INTEGER: 2  
$
```

In the output, the INTEGER: 2 means the fan is present. INTEGER: 1 means the fan is not present.

2. Check the speed of the fan.

```
$ snmpget -v2c -c public mc_IP  
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.number
```

where *number* is the entity number for the /SYS/FANx/TACH speed sensor target for the respective fan. This example uses entity number 54 for the left fan (FAN1):

```
$ snmpget -v2c -c public mc_IP SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.54  
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.54 = INTEGER: 12099  
$
```

The FAN1 speed displayed in the output of the example is 12099 RPM.

Note – Fan speed readings can vary and are influenced by the gateway environment and loading.

3. Display comprehensive fan information.

```
$ snmpwalk -v2c -c public mc_IP SUN-PLATFORM-MIB::sunPlatNumericSensorTable  
SUN-PLATFORM-MIB::sunPlatNumericSensorBaseUnits.4 = INTEGER: volts(6)  
SUN-PLATFORM-MIB::sunPlatNumericSensorBaseUnits.6 = INTEGER: volts(6)  
SUN-PLATFORM-MIB::sunPlatNumericSensorBaseUnits.7 = INTEGER: volts(6)  
SUN-PLATFORM-MIB::sunPlatNumericSensorBaseUnits.8 = INTEGER: volts(6)  
SUN-PLATFORM-MIB::sunPlatNumericSensorBaseUnits.10 = INTEGER: volts(6)  
.  
.
```

```

.
SUN-PLATFORM-MIB::sunPlatNumericSensorBaseUnits.54 = INTEGER: rpm(20)
SUN-PLATFORM-MIB::sunPlatNumericSensorBaseUnits.57 = INTEGER: rpm(20)
SUN-PLATFORM-MIB::sunPlatNumericSensorBaseUnits.60 = INTEGER: rpm(20)
.
.
.
SUN-PLATFORM-MIB::sunPlatNumericSensorExponent.54 = INTEGER: 0
SUN-PLATFORM-MIB::sunPlatNumericSensorExponent.57 = INTEGER: 0
SUN-PLATFORM-MIB::sunPlatNumericSensorExponent.60 = INTEGER: 0
.
.
.
SUN-PLATFORM-MIB::sunPlatNumericSensorRateUnits.54 = INTEGER: none(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorRateUnits.57 = INTEGER: none(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorRateUnits.60 = INTEGER: none(1)
.
.
.
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.54 = INTEGER: 12208
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.57 = INTEGER: 11772
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.60 = INTEGER: 12099
.
.
.
SUN-PLATFORM-MIB::sunPlatNumericSensorRestoreDefaultThresholds.54 = INTEGER:
reset(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorRestoreDefaultThresholds.57 = INTEGER:
reset(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorRestoreDefaultThresholds.60 = INTEGER:
reset(1)
$

```

4. Look though the output for the entity numbers respective to the fans.

You can also filter the output of the `snmpwalk` command for a specific entity number. This is an example of filtering the `snmpwalk` command output.:

```

$ snmpwalk -v2c -c public mc_IP SUN-PLATFORM-MIB::sunPlatNumericSensorTable
|grep -F '.number ='

```

where *number* is the entity number.

Note – The manner in which you can filter the output varies according to your operating system.

To filter speed information for the left fan (FAN1), use the entity number respective to the /SYS/FAN1/TACH speed sensor target. This filtering example uses entity number 54:

```
$ snmpwalk -v2c -c public mc_IP SUN-PLATFORM-MIB::sunPlatNumericSensorTable
|grep -F '.54 ='
SUN-PLATFORM-MIB::sunPlatNumericSensorBaseUnits.54 = INTEGER: rpm(20)
SUN-PLATFORM-MIB::sunPlatNumericSensorExponent.54 = INTEGER: 0
SUN-PLATFORM-MIB::sunPlatNumericSensorRateUnits.54 = INTEGER: none(1)
SUN-PLATFORM-MIB::sunPlatNumericSensorCurrent.54 = INTEGER: 12208
SUN-PLATFORM-MIB::sunPlatNumericSensorNormalMin.54 = INTEGER: 0
SUN-PLATFORM-MIB::sunPlatNumericSensorNormalMax.54 = INTEGER: 255
SUN-PLATFORM-MIB::sunPlatNumericSensorAccuracy.54 = INTEGER: 0
SUN-PLATFORM-MIB::sunPlatNumericSensorLowerThresholdNonCritical.54 = INTEGER:
6322
SUN-PLATFORM-MIB::sunPlatNumericSensorUpperThresholdNonCritical.54 = INTEGER:
0
SUN-PLATFORM-MIB::sunPlatNumericSensorLowerThresholdCritical.54 = INTEGER: 0
SUN-PLATFORM-MIB::sunPlatNumericSensorUpperThresholdCritical.54 = INTEGER:
26705
SUN-PLATFORM-MIB::sunPlatNumericSensorLowerThresholdFatal.54 = INTEGER: 0
SUN-PLATFORM-MIB::sunPlatNumericSensorUpperThresholdFatal.54 = INTEGER: 0
SUN-PLATFORM-MIB::sunPlatNumericSensorHysteresis.54 = Gauge32: 0
SUN-PLATFORM-MIB::sunPlatNumericSensorEnabledThresholds.54 = BITS: 90
lowerThresholdNonCritical(0) upperThresholdCritical(3)
SUN-PLATFORM-MIB::sunPlatNumericSensorRestoreDefaultThresholds.54 = INTEGER:
reset(1)
$
```

Related Information

- [“Display Fan Status \(CLI\)” on page 48](#)
- [“Display Fan Status \(Web\)” on page 123](#)
- [“Display the Aggregate Sensors State \(SNMP\)” on page 205](#)
- [“Display Power Supply Status \(SNMP\)” on page 206](#)
- [“Display Board-Level Voltages \(SNMP\)” on page 208](#)
- [“Display Internal Temperatures \(SNMP\)” on page 212](#)
- [“Display Fan Status \(SNMP\)” on page 215](#)
- [“Display the Sensor Alarm State \(SNMP\)” on page 219](#)
- [“Display the Entity Numbers” on page 220](#)

▼ Display the Sensor Alarm State (SNMP)

Note – The entity numbers used in this procedure are for example only. Your entity numbers might differ, depending on the gateway firmware and configuration.

1. Determine the entity number of the sensor.

See [“Display the Entity Numbers” on page 220](#).

2. From the SNMP client, display the sensor’s alarm state.

```
$ snmpget -v2c -c public mc_IP  
SUN-PLATFORM-MIB::sunPlatEquipmentAlarmStatus.number
```

where *number* is the entity number.

For example, to determine the overall gateway alarm state, use the entity number respective to the /SYS/CHASSIS_STATUS aggregate sensor target. This example uses entity number 35:

```
$ snmpget -v2c -c public mc_IP SUN-PLATFORM-MIB::sunPlatEquipmentAlarmStatus.35  
SUN-PLATFORM-MIB::sunPlatEquipmentAlarmStatus.35 = INTEGER: cleared(7)  
$
```

In the output, the `INTEGER: cleared(7)` indicates the alarm state for the sensor is clear. These alarm states are possible:

- `INTEGER: critical(1)` – A critical alarm has occurred.
- `INTEGER: major(2)` – A major alarm has occurred.
- `INTEGER: minor(3)` – A minor alarm has occurred.
- `INTEGER: indeterminate(4)` – The alarm is indeterminate, or not applicable.
- `INTEGER: cleared(7)` – The alarm has been cleared.

Related Information

- [“Display the Aggregate Sensors State \(CLI\)” on page 41](#)
- [“Display the Aggregate Sensors State \(Web\)” on page 120](#)
- [“Display the Aggregate Sensors State \(SNMP\)” on page 205](#)
- [“Display Power Supply Status \(SNMP\)” on page 206](#)
- [“Display Board-Level Voltages \(SNMP\)” on page 208](#)
- [“Display Internal Temperatures \(SNMP\)” on page 212](#)
- [“Display Fan Status \(SNMP\)” on page 215](#)

- “Display the Sensor States (IPMI)” on page 258
- “Display the Entity Numbers” on page 220

▼ Display the Entity Numbers

This procedure outputs the entity numbers and their respective Oracle ILOM targets.

Note – The entity numbers displayed in this procedure are for example only. Your entity numbers might differ, depending on the gateway firmware and configuration.

1. From the SNMP client, type.

```
$ snmpwalk -v2c -c public mc_IP ENTITY-MIB::entPhysicalName
ENTITY-MIB::entPhysicalName.1 = STRING: /SYS
ENTITY-MIB::entPhysicalName.2 = STRING: /SYS/MB
ENTITY-MIB::entPhysicalName.3 = STRING: /SYS/MB/V_ECB
ENTITY-MIB::entPhysicalName.4 = STRING: /SYS/MB/V_3.3VMain
ENTITY-MIB::entPhysicalName.5 = STRING: /SYS/MB/V_3.3VMainOK
.
.
.
ENTITY-MIB::entPhysicalName.61 = STRING: /SYS/I_POWER
ENTITY-MIB::entPhysicalName.62 = STRING: /SYS/I_ATTENTION
ENTITY-MIB::entPhysicalName.63 = STRING: /SYS/I_LOCATOR
$
```

You can also filter the output of the `snmpwalk` command to display just entity numbers and their respective Oracle ILOM targets. This is an example of filtering the `snmpwalk` command output:

Note – The manner in which you can filter the output varies according to your operating system.

```
$ snmpwalk -v2c -c public mc_IP ENTITY-MIB::entPhysicalName | awk -F"me." '{print
$2}' | awk '{print $1 " " " $4}'
1 /SYS
2 /SYS/MB
3 /SYS/MB/V_ECB
4 /SYS/MB/V_3.3VMain
5 /SYS/MB/V_3.3VMainOK
.
.
```

```
.  
61 /SYS/I_POWER  
62 /SYS/I_ATTENTION  
63 /SYS/I_LOCATOR  
$
```

2. Use the entity numbers for daily tasks.

See:

- “Display the Aggregate Sensors State (SNMP)” on page 205
- “Display Power Supply Status (SNMP)” on page 206
- “Display Board-Level Voltages (SNMP)” on page 208
- “Display Internal Temperatures (SNMP)” on page 212
- “Display Fan Status (SNMP)” on page 215
- “Display the Sensor Alarm State (SNMP)” on page 219

Related Information

- “Display Gateway FRU ID (SNMP)” on page 232
- “Display Power Supply FRU ID (SNMP)” on page 234
- “Display the System Components (SNMP)” on page 236

▼ Display Oracle ILOM Sessions (SNMP)

- From the SNMP client, type.

```
$ snmpwalk -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlSessions
SUN-ILOM-CONTROL-MIB::ilomCtrlSessionsUsername.118 = STRING: user1
SUN-ILOM-CONTROL-MIB::ilomCtrlSessionsUsername.119 = STRING: root
SUN-ILOM-CONTROL-MIB::ilomCtrlSessionsUsername.126 = STRING: root
SUN-ILOM-CONTROL-MIB::ilomCtrlSessionsConnectionType.118 = INTEGER: web(2)
SUN-ILOM-CONTROL-MIB::ilomCtrlSessionsConnectionType.119 = INTEGER: shell(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlSessionsConnectionType.126 = INTEGER: other(3)
SUN-ILOM-CONTROL-MIB::ilomCtrlSessionsLoginTime.118 = STRING:
2010-1-20,12:14:27.0
SUN-ILOM-CONTROL-MIB::ilomCtrlSessionsLoginTime.119 = STRING:
2010-1-20,12:17:40.0
SUN-ILOM-CONTROL-MIB::ilomCtrlSessionsLoginTime.126 = STRING:
2010-1-20,12:27:4.0
$
```

If you use the V3 protocol, type.

```
$ snmpwalk -v3 -u usersnmp -l authPriv -a MD5 -A authpass -x DES -X privpass
mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlSessions
SUN-ILOM-CONTROL-MIB::ilomCtrlSessionsUsername.118 = STRING: user1
SUN-ILOM-CONTROL-MIB::ilomCtrlSessionsUsername.119 = STRING: root
SUN-ILOM-CONTROL-MIB::ilomCtrlSessionsUsername.126 = STRING: root
SUN-ILOM-CONTROL-MIB::ilomCtrlSessionsConnectionType.118 = INTEGER: web(2)
SUN-ILOM-CONTROL-MIB::ilomCtrlSessionsConnectionType.119 = INTEGER: shell(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlSessionsConnectionType.126 = INTEGER: other(3)
SUN-ILOM-CONTROL-MIB::ilomCtrlSessionsLoginTime.118 = STRING:
2010-1-20,12:14:27.0
SUN-ILOM-CONTROL-MIB::ilomCtrlSessionsLoginTime.119 = STRING:
2010-1-20,12:17:40.0
SUN-ILOM-CONTROL-MIB::ilomCtrlSessionsLoginTime.126 = STRING:
2010-1-20,12:27:4.0
$
```

The output displays three users. user1 is using the web interface, and the root user is using the CLI interface.

Related Information

- [“Display the Oracle ILOM Sessions \(CLI\)” on page 50](#)
- [“Display the Oracle ILOM Sessions \(Web\)” on page 123](#)
- [“Display Oracle ILOM User Accounts \(SNMP\)” on page 230](#)

▼ Display the Oracle 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::ilomCtrlEventLogType.4 = INTEGER: log(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogType.5 = INTEGER: log(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogTimestamp.1 = STRING:
2010-1-20,10:22:28.0
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogTimestamp.2 = STRING:
2010-1-20,10:22:50.0
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogTimestamp.3 = STRING:
2010-1-20,10:22:56.0
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogTimestamp.4 = STRING:
2010-1-20,10:23:20.0
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogTimestamp.5 = STRING:
2010-1-20,10:23:20.0
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::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::ilomCtrlEventLogSeverity.4 = INTEGER: minor(4)
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogSeverity.5 = INTEGER: minor(4)
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogDescription.1 = STRING: user1 : Set :
object = /logs/event/clear : value = true : success
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogDescription.2 = STRING: root : Create :
object = /users/user4 : value = N/A : success
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogDescription.3 = STRING: root : Set :
object = /users/user4/password : value = ***** : success
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogDescription.4 = STRING: root : Set :
object = /services/snmp/users/snmpuser/permission : value = rw : success
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogDescription.5 = STRING: root : Set :
object = /services/snmp/users/snmpuser/adminstate : value = enabled : success
$
```

If you use the V3 protocol, type.

```
$ snmpwalk -v3 -u usersnmp -l authPriv -a MD5 -A authpass -x DES -X privpass
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::ilomCtrlEventLogType.4 = INTEGER: log(1)
```

```
SUN-ILOM-CONTROL-MIB::ilomCtrlEventLogType.5 = INTEGER: log(1)
.
.
.
$
```

Related Information

- [“Display the Oracle ILOM Event Log \(CLI\)” on page 51](#)
- [“Display the Oracle ILOM Event Log \(Web\)” on page 124](#)
- [“Display the System Event Log \(IPMI\)” on page 261](#)
- [“Clear the Oracle ILOM Event Log \(SNMP\)” on page 243](#)
- [“Set the Remote Log Hosts \(SNMP\)” on page 243](#)

Checking the Status of Services (SNMP)

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

- [“Display the HTTP Service Status \(SNMP\)” on page 225](#)
- [“Display the HTTPS Service Status \(SNMP\)” on page 226](#)
- [“Display the DNS Client Status \(SNMP\)” on page 226](#)
- [“Display the SMTP Client Status \(SNMP\)” on page 227](#)
- [“Display the NTP State \(SNMP\)” on page 227](#)
- [“Display the NTP Servers \(SNMP\)” on page 228](#)

Related Information

- [“Performing Daily Tasks \(SNMP\)” on page 204](#)
- [“Verifying Other Aspects With Oracle ILOM \(SNMP\)” on page 228](#)

▼ 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 52
- “Display the HTTP Service Status (Web)” on page 125
- “Display the HTTPS Service Status (SNMP)” on page 226
- “Set the HTTP Service State (SNMP)” on page 251

▼ 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 53
- “Display the HTTPS Service Status (Web)” on page 125
- “Display the HTTP Service Status (SNMP)” on page 225

▼ Display the DNS Client Status (SNMP)

- From the SNMP client, type.

```
$ snmpwalk -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlDNS
SUN-ILOM-CONTROL-MIB::ilomCtrlDNSNameServers.0 = STRING: 129.158.227.31,
129.158.227.32
SUN-ILOM-CONTROL-MIB::ilomCtrlDNSSearchPath.0 = STRING: india.sun.com,
norway.sun.com
SUN-ILOM-CONTROL-MIB::ilomCtrlDNSdhcpAutoDns.0 = INTEGER: true(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlDNSTimeout.0 = INTEGER: 5
SUN-ILOM-CONTROL-MIB::ilomCtrlDNSRetries.0 = INTEGER: 1
$
```

Related Information

- “Display the DNS Client Status (CLI)” on page 56
- “Display the DNS Client Status (Web)” on page 127
- “Configure the DNS Client (SNMP)” on page 244

▼ Display the SMTP Client Status (SNMP)

1. From the SNMP client, display the state of the SMTP client.

Note – This example shows that the SMTP client is not enabled.

```
$ snmpget -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlSMTPEnabled.0
SUN-ILOM-CONTROL-MIB::ilomCtrlSMTPEnabled.0 = INTEGER: false(2)
$
```

2. Display the SMTP server IP address.

```
$ snmpget -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlSMTPServerIP.0
SUN-ILOM-CONTROL-MIB::ilomCtrlSMTPServerIP.0 = IpAddress: 10.18.223.35
$
```

3. Display the SMTP server port.

```
$ snmpget -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlSMTPPortNumber.0
SUN-ILOM-CONTROL-MIB::ilomCtrlSMTPPortNumber.0 = INTEGER: 25
$
```

Related Information

- [“Display the SMTP Client Status \(CLI\)” on page 57](#)
- [“Display the SMTP Client Status \(Web\)” on page 128](#)
- [“Configure the SMTP Client \(SNMP\)” on page 245](#)

▼ Display the NTP State (SNMP)

- From the SNMP client, type.

```
$ snmpget -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlNTPEnabled.0
SUN-ILOM-CONTROL-MIB::ilomCtrlNTPEnabled.0 = INTEGER: true(1)
$
```

Note – The `true(1)` in the output signifies that NTP is enabled.

Related Information

- [“Display the NTP Servers \(CLI\)” on page 57](#)

- “Display the Network Time Protocol Servers (Web)” on page 128
- “Display the NTP Servers (SNMP)” on page 228
- “Set the Network Time Protocol State (SNMP)” on page 242

▼ Display the NTP Servers (SNMP)

- From the SNMP client, type.

```
$ snmpget -v2c -c public mc_IP
SUN-ILOM-CONTROL-MIB::ilomCtrlDeviceNTPServerOneIP.0
SUN-ILOM-CONTROL-MIB::ilomCtrlDeviceNTPServerOneIP.0 = IPAddress: 123.45.67.90
$ snmpget -v2c -c public mc_IP
SUN-ILOM-CONTROL-MIB::ilomCtrlDeviceNTPServerTwoIP.0
SUN-ILOM-CONTROL-MIB::ilomCtrlDeviceNTPServerTwoIP.0 = IPAddress: 0.0.0.0
$
```

Note – The IP address of 0.0.0.0 for NTP server two in the output signifies that a second NTP server is not configured.

Related Information

- “Display the NTP Servers (CLI)” on page 57
- “Display the Network Time Protocol Servers (Web)” on page 128
- “Display the NTP State (SNMP)” on page 227
- “Set the Network Time Protocol Servers (SNMP)” on page 242

Verifying Other Aspects With Oracle ILOM (SNMP)

These tasks display the status of aspects of Oracle ILOM not included in “Performing Daily Tasks (SNMP)” on page 204 or “Checking the Status of Services (SNMP)” on page 225.

- “Display the Alert Properties (SNMP)” on page 229
- “Display Oracle ILOM User Accounts (SNMP)” on page 230
- “Display the Remote Log Hosts (SNMP)” on page 231
- “Display the Network Management Configuration (SNMP)” on page 231
- “Display Gateway FRU ID (SNMP)” on page 232
- “Display Power Supply FRU ID (SNMP)” on page 234

- “Display the System Components (SNMP)” on page 236
- “Display the Additional System Component Information (SNMP)” on page 238
- “Display the Firmware Version (SNMP)” on page 239
- “Display System Identification Properties (SNMP)” on page 239

Related Information

- “Performing Daily Tasks (SNMP)” on page 204
- “Checking the Status of Services (SNMP)” on page 225

▼ Display the Alert Properties (SNMP)

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

- 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 60](#)
- [“Display the Alert Properties \(Web\)” on page 129](#)
- [“Enable Alerts to Send SNMP Traps \(SNMP\)” on page 252](#)
- [“Modify Alert SNMP Version \(SNMP\)” on page 255](#)
- [“Disable Alerts \(SNMP\)” on page 256](#)

▼ Display Oracle 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."ilom-admin" = STRING: "(Not
Viewable)"
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserPassword."ilom-operator" = STRING:
"(Not Viewable)"
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserRoles."root" = STRING: "aucro"
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserRoles."ilom-admin" = STRING: "aucro"
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserRoles."ilom-operator" = STRING: "o"
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserRowStatus."root" = INTEGER: active(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserRowStatus."ilom-admin" = INTEGER:
active(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserRowStatus."ilom-operator" = INTEGER:
active(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserCLIMode."root" = INTEGER: default(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserCLIMode."ilom-admin" = INTEGER:
default(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlLocalUserCLIMode."ilom-operator" = INTEGER:
default(1)
$
```

Note – The output identifies three users. Of them, users root and ilom-admin have an administrative role.

Related Information

- [“Display the Oracle ILOM User Accounts \(CLI\)” on page 61](#)
- [“Display the Oracle ILOM User Accounts \(Web\)” on page 130](#)
- [“Add an Oracle ILOM User Account \(SNMP\)” on page 249](#)
- [“Delete an Oracle ILOM User Account \(SNMP\)” on page 250](#)

▼ Display the Remote Log Hosts (SNMP)

- From the SNMP client, type.

```
$ snmpget -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlRemoteSyslogDest1.0
SUN-ILOM-CONTROL-MIB::ilomCtrlRemoteSyslogDest1.0 = IPAddress: 123.45.67.89
$ snmpget -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlRemoteSyslogDest2.0
SUN-ILOM-CONTROL-MIB::ilomCtrlRemoteSyslogDest2.0 = IPAddress: 0.0.0.0
$
```

Related Information

- [“Display the Remote Log Hosts \(CLI\)” on page 62](#)
- [“Display the Remote Log Hosts \(Web\)” on page 130](#)
- [“Set the Remote Log Hosts \(SNMP\)” on page 243](#)

▼ 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 63](#)
- [“Display the Network Management Configuration \(Web\)” on page 131](#)
- [“Set the Network Parameters \(SNMP\)” on page 246](#)

▼ Display Gateway FRU ID (SNMP)

Note – The entity number for the /SYS gateway container target might change with different firmware releases or gateway configurations. Verify the gateway entity number (1) with the procedure in [“Display the Entity Numbers” on page 220](#).

1. From the SNMP client, type.

```

$ snmpwalk -v2c -c public mc_IP ENTITY-MIB::entPhysicalTable
ENTITY-MIB::entPhysicalDescr.1 = STRING: Sun Datacenter InfiniBand Switch GW
ENTITY-MIB::entPhysicalDescr.2 = STRING: Motherboard
ENTITY-MIB::entPhysicalDescr.3 = STRING: Fault Sensor
ENTITY-MIB::entPhysicalDescr.4 = STRING: Voltage Sensor
ENTITY-MIB::entPhysicalDescr.5 = STRING: Fault Sensor
.
.
.
ENTITY-MIB::entPhysicalVendorType.1 = OID: SNMPv2-SMI::zeroDotZero
.
.
.
ENTITY-MIB::entPhysicalContainedIn.1 = INTEGER: 0
.
.
.
ENTITY-MIB::entPhysicalClass.1 = INTEGER: chassis(3)
.
.
.
ENTITY-MIB::entPhysicalParentRelPos.1 = INTEGER: -1
.

```

```

.
.
ENTITY-MIB::entPhysicalName.1 = STRING: /SYS
.
.
.
ENTITY-MIB::entPhysicalHardwareRev.1 = STRING:
.
.
.
ENTITY-MIB::entPhysicalFirmwareRev.1 = STRING: 2.0.5-1
.
.
.
$

```

2. Look through the output for entity number 1.

You can also filter the output of the `snmpwalk` command for entity number 1. This is an example of filtering the `snmpwalk` command output:

Note – The manner in which you can filter the output varies according to your operating system.

```

$ snmpwalk -v2c -c public mc_IP ENTITY-MIB::entPhysicalTable | grep -F '.1 ='
ENTITY-MIB::entPhysicalDescr.1 = STRING: Sun Datacenter InfiniBand Switch GW
ENTITY-MIB::entPhysicalVendorType.1 = OID: SNMPv2-SMI::zeroDotZero
ENTITY-MIB::entPhysicalContainedIn.1 = INTEGER: 0
ENTITY-MIB::entPhysicalClass.1 = INTEGER: chassis(3)
ENTITY-MIB::entPhysicalParentRelPos.1 = INTEGER: -1
ENTITY-MIB::entPhysicalName.1 = STRING: /SYS
ENTITY-MIB::entPhysicalHardwareRev.1 = STRING:
ENTITY-MIB::entPhysicalFirmwareRev.1 = STRING: 2.0.5-1
ENTITY-MIB::entPhysicalSoftwareRev.1 = STRING:
ENTITY-MIB::entPhysicalSerialNum.1 = STRING: 0110SJC-1099XY9992
ENTITY-MIB::entPhysicalMfgName.1 = STRING: Sun Microsystems, Inc.
ENTITY-MIB::entPhysicalModelName.1 = STRING: 5111402
ENTITY-MIB::entPhysicalAlias.1 = STRING:
ENTITY-MIB::entPhysicalAssetID.1 = STRING:
ENTITY-MIB::entPhysicalIsFRU.1 = INTEGER: true(1)
$

```

Related Information

- [“Display Gateway FRU ID \(CLI\)” on page 64](#)
- [“Display System Component FRU ID \(Web\)” on page 132](#)
- [“Display FRU ID Information \(IPMI\)” on page 262](#)

- [“Display the Entity Numbers” on page 220](#)

▼ Display Power Supply FRU ID (SNMP)

Note – You can only display FRU ID information for currently present power supplies.

Note – The entity numbers for the /SYS/PSUx power supply FRU targets might change with different firmware releases or gateway configurations. Verify the power supply entity numbers with the procedure in [“Display the Entity Numbers” on page 220](#).

1. From the SNMP client, type.

```
$ snmpwalk -v2c -c public mc_IP ENTITY-MIB::entPhysicalTable
ENTITY-MIB::entPhysicalDescr.1 = STRING: Sun Datacenter InfiniBand Switch GW
ENTITY-MIB::entPhysicalDescr.2 = STRING: Motherboard
ENTITY-MIB::entPhysicalDescr.3 = STRING: Fault Sensor
ENTITY-MIB::entPhysicalDescr.4 = STRING: Voltage Sensor
ENTITY-MIB::entPhysicalDescr.5 = STRING: Fault Sensor
.
.
.
ENTITY-MIB::entPhysicalDescr.44 = STRING: Power Supply FRU
.
.
.
ENTITY-MIB::entPhysicalDescr.48 = STRING: Power Supply FRU
.
.
.
ENTITY-MIB::entPhysicalVendorType.44 = OID: SNMPv2-SMI::zeroDotZero
.
.
.
ENTITY-MIB::entPhysicalVendorType.48 = OID: SNMPv2-SMI::zeroDotZero
.
.
.
ENTITY-MIB::entPhysicalContainedIn.44 = INTEGER: 1
.
.
.
```

```

ENTITY-MIB::entPhysicalContainedIn.48 = INTEGER: 1
.
.
.
ENTITY-MIB::entPhysicalClass.44 = INTEGER: powerSupply(6)
.
.
.
ENTITY-MIB::entPhysicalClass.48 = INTEGER: powerSupply(6)
.
.
.
ENTITY-MIB::entPhysicalParentRelPos.44 = INTEGER: 1
.
.
.
ENTITY-MIB::entPhysicalParentRelPos.48 = INTEGER: 2
.
.
.
ENTITY-MIB::entPhysicalName.44 = STRING: /SYS/PSU0
.
.
.
ENTITY-MIB::entPhysicalName.48 = STRING: /SYS/PSU1
.
.
.
$

```

2. Look though the output for the entity numbers respective to the power supplies.

You can also filter the output of the `snmpwalk` command for a specific entity number. This is an example of filtering the `snmpwalk` command output.:

```
$ snmpwalk -v2c -c public mc_IP ENTITY-MIB::entPhysicalTable | grep -F '.number ='
```

where *number* is the entity number.

Note – The manner in which you can filter the output varies according to your operating system.

To filter voltage information for the left power supply (PSU0), use the entity number respective to the /SYS/PSU0 power supply FRU target. This filtering example uses entity number 44:

```
$ snmpwalk -v2c -c public mc_IP ENTITY-MIB::entPhysicalTable | grep -F '.44 ='
ENTITY-MIB::entPhysicalDescr.44 = STRING: Power Supply FRU
ENTITY-MIB::entPhysicalVendorType.44 = OID: SNMPv2-SMI::zeroDotZero
ENTITY-MIB::entPhysicalContainedIn.44 = INTEGER: 1
ENTITY-MIB::entPhysicalClass.44 = INTEGER: powerSupply(6)
ENTITY-MIB::entPhysicalParentRelPos.44 = INTEGER: 1
ENTITY-MIB::entPhysicalName.44 = STRING: /SYS/PSU0
ENTITY-MIB::entPhysicalHardwareRev.44 = STRING:
ENTITY-MIB::entPhysicalFirmwareRev.44 = STRING:
ENTITY-MIB::entPhysicalSoftwareRev.44 = STRING: 02
ENTITY-MIB::entPhysicalSerialNum.44 = STRING: 001180
ENTITY-MIB::entPhysicalMfgName.44 = STRING: Delta Energy Systems
ENTITY-MIB::entPhysicalModelName.44 = STRING: 3002233
ENTITY-MIB::entPhysicalAlias.44 = STRING: A247
ENTITY-MIB::entPhysicalAssetID.44 = STRING:
ENTITY-MIB::entPhysicalIsFRU.44 = INTEGER: true(1)
$
```

Related Information

- [“Display Power Supply FRU ID \(CLI\)” on page 65](#)
- [“Display System Component FRU ID \(Web\)” on page 132](#)
- [“Display FRU ID Information \(IPMI\)” on page 262](#)
- [“Display the Entity Numbers” on page 220](#)

▼ Display the System Components (SNMP)

1. From the SNMP client, type.

```
$ snmpwalk -v2c -c public mc_IP ENTITY-MIB::entPhysicalName
ENTITY-MIB::entPhysicalName.1 = STRING: /SYS
ENTITY-MIB::entPhysicalName.2 = STRING: /SYS/MB
ENTITY-MIB::entPhysicalName.3 = STRING: /SYS/MB/V_ECB
ENTITY-MIB::entPhysicalName.4 = STRING: /SYS/MB/V_3.3VMain
ENTITY-MIB::entPhysicalName.5 = STRING: /SYS/MB/V_3.3VMainOK
ENTITY-MIB::entPhysicalName.6 = STRING: /SYS/MB/V_3.3VStby
ENTITY-MIB::entPhysicalName.7 = STRING: /SYS/MB/V_12V
```

```

.
.
.
ENTITY-MIB::entPhysicalName.61 = STRING: /SYS/I_POWER
ENTITY-MIB::entPhysicalName.62 = STRING: /SYS/I_ATTENTION
ENTITY-MIB::entPhysicalName.63 = STRING: /SYS/I_LOCATOR
$

```

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

2. Display the physical entity descriptions.

```

$ snmpwalk -v2c -c public mc_IP ENTITY-MIB::entPhysicalDescr
ENTITY-MIB::entPhysicalDescr.1 = STRING: Sun Datacenter InfiniBand Switch GW
ENTITY-MIB::entPhysicalDescr.2 = STRING: Motherboard
ENTITY-MIB::entPhysicalDescr.3 = STRING: Fault Sensor
ENTITY-MIB::entPhysicalDescr.4 = STRING: Voltage Sensor
ENTITY-MIB::entPhysicalDescr.5 = STRING: Fault Sensor
ENTITY-MIB::entPhysicalDescr.6 = STRING: Voltage Sensor
ENTITY-MIB::entPhysicalDescr.7 = STRING: Voltage Sensor
.
.
.
ENTITY-MIB::entPhysicalDescr.61 = STRING: Indicator
ENTITY-MIB::entPhysicalDescr.62 = STRING: Indicator
ENTITY-MIB::entPhysicalDescr.63 = STRING: Indicator
$

```

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

3. Display the physical entity classes.

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

```

$ snmpwalk -v2c -c public mc_IP ENTITY-MIB::entPhysicalClass
ENTITY-MIB::entPhysicalClass.1 = INTEGER: chassis(3)
ENTITY-MIB::entPhysicalClass.2 = INTEGER: container(5)
ENTITY-MIB::entPhysicalClass.3 = INTEGER: sensor(8)
ENTITY-MIB::entPhysicalClass.4 = INTEGER: sensor(8)
ENTITY-MIB::entPhysicalClass.5 = INTEGER: sensor(8)
ENTITY-MIB::entPhysicalClass.6 = INTEGER: sensor(8)
ENTITY-MIB::entPhysicalClass.7 = INTEGER: sensor(8)

```

```

.
.
.
ENTITY-MIB::entPhysicalClass.61 = INTEGER: other(1)
ENTITY-MIB::entPhysicalClass.62 = INTEGER: other(1)
ENTITY-MIB::entPhysicalClass.63 = INTEGER: other(1)
$

```

Related Information

- [“Display System Component FRU ID \(Web\)” on page 132](#)
- [“Display the Additional System Component Information \(SNMP\)” on page 238](#)
- [“Display the Entity Numbers” on page 220](#)

▼ 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: indeterminate(4)
.
.
.
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 has been truncated to display the information for the first two entities.

Related Information

- [“Display the System Components \(SNMP\)” on page 236](#)

▼ Display the Firmware Version (SNMP)

- From the SNMP client, display the firmware version.

```
$ snmpget -v2c -c public mc_IP ENTITY-MIB::entPhysicalFirmwareRev.1
ENTITY-MIB::entPhysicalFirmwareRev.1 = STRING: 2.0.5-1
$
```

Related Information

- [“Display the Firmware Version \(CLI\)” on page 66](#)
- [“Display the Oracle ILOM Version \(Web\)” on page 133](#)
- [“Display the Entity Numbers” on page 220](#)

▼ Display System Identification Properties (SNMP)

1. From the SNMP client, display the host name.

```
$ snmpget -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlHostName.0
SUN-ILOM-CONTROL-MIB::ilomCtrlHostName.0 = STRING: us-gw-1
$
```

2. Display the system identifier.

```
$ snmpget -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlSystemIdentifier.0
SUN-ILOM-CONTROL-MIB::ilomCtrlSystemIdentifier.0 = STRING: (none)
$
```

Related Information

- [“Display System Identification Properties \(CLI\)” on page 66](#)
- [“Display System Identification Properties \(Web\)” on page 133](#)
- [“Set the System Identification Properties \(SNMP\)” on page 248](#)

Controlling Oracle ILOM Targets (SNMP)

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

- [“Performing General Tasks \(SNMP\)” on page 240](#)
- [“Performing User Tasks \(SNMP\)” on page 248](#)
- [“Managing Other Aspects With Oracle ILOM \(SNMP\)” on page 250](#)

Related Information

- [“Controlling Oracle ILOM Targets \(CLI\)” on page 67](#)
- [“Controlling Oracle ILOM Targets \(Web\)” on page 134](#)
- [“Monitoring Oracle ILOM Targets \(SNMP\)” on page 203](#)

Performing General Tasks (SNMP)

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

- [“Set the Date and Time \(SNMP\)” on page 241](#)
- [“Set the Time Zone \(SNMP\)” on page 241](#)
- [“Set the Network Time Protocol State \(SNMP\)” on page 242](#)
- [“Set the Network Time Protocol Servers \(SNMP\)” on page 242](#)
- [“Clear the Oracle ILOM Event Log \(SNMP\)” on page 243](#)
- [“Set the Remote Log Hosts \(SNMP\)” on page 243](#)
- [“Configure the DNS Client \(SNMP\)” on page 244](#)
- [“Configure the SMTP Client \(SNMP\)” on page 245](#)
- [“Set the Network Parameters \(SNMP\)” on page 246](#)
- [“Set the System Identification Properties \(SNMP\)” on page 248](#)

Related Information

- [“Performing User Tasks \(SNMP\)” on page 248](#)
- [“Managing Other Aspects With Oracle ILOM \(SNMP\)” on page 250](#)

▼ 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 and Time \(CLI\)” on page 69](#)
- [“Set the Date and Time \(Web\)” on page 136](#)
- [“Display the Date and Time \(SNMP\)” on page 204](#)

▼ Set the Time Zone (SNMP)

- From the SNMP client, type.

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlTimezone.0 s  
"timezone"
```

where *timezone* is the time zone. For example, to set for Greenwich Mean Time:

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlTimezone.0 s "GMT"  
SUN-ILOM-CONTROL-MIB::ilomCtrlTimezone.0 = STRING: GMT  
$
```

Related Information

- [“Set the Date and Time \(CLI\)” on page 69](#)
- [“Set the Time Zone \(Web\)” on page 136](#)
- [“Display the Time Zone \(SNMP\)” on page 205](#)

▼ Set the Network Time Protocol State (SNMP)

- From the SNMP client, type.

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlNTPEnabled.0 i state
```

where *state* is either 1 for enabled or 2 for disabled. For example, to enable NTP:

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlNTPEnabled.0 i 1
SUN-ILOM-CONTROL-MIB::ilomCtrlNTPEnabled.0 = INTEGER: true(1)
$
```

Related Information

- [“Set the Network Time Protocol Servers \(SNMP\)” on page 242](#)
- [“Display the NTP State \(SNMP\)” on page 227](#)

▼ Set the Network Time Protocol Servers (SNMP)

- From the SNMP client, type.

```
$ snmpset -v2c -c public mc_IP
SUN-ILOM-CONTROL-MIB::ilomCtrlDeviceNTPServernumberIP.0 = "IP_address"
```

where:

- *number* is the string for the number of the server, either One or Two.
- *IP_address* is the IP address of the NTP server.

For example, to set the NTP server One to the address of 123.45.67.90:

```
$ snmpset -v2c -c public mc_IP
SUN-ILOM-CONTROL-MIB::ilomCtrlDeviceNTPServerOneIP.0 = "123.45.67.90"
SUN-ILOM-CONTROL-MIB::ilomCtrlDeviceNTPServerOneIP.0 = IpAddress: 123.45.67.90
$
```

Note – Setting the NTP server IP address parameter to 0.0.0.0 effectively disables that parameter.

Related Information

- [“Set the Date and Time \(CLI\)” on page 69](#)
- [“Set the Date and Time \(Web\)” on page 136](#)

- “Set the Network Time Protocol State (SNMP)” on page 242
- “Display the NTP Servers (SNMP)” on page 228

▼ Clear the Oracle 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 Oracle ILOM Event Log (CLI)” on page 71
- “Clear the Oracle ILOM Event Log (Web)” on page 138
- “Display the Oracle ILOM Event Log (SNMP)” on page 223
- “Set the Remote Log Hosts (SNMP)” on page 243

▼ Set the Remote Log Hosts (SNMP)

The Oracle ILOM implementation in the management controller provides a protocol for transmitting Oracle 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

- “Set the Remote Log Hosts (CLI)” on page 72
- “Set the Remote Log Hosts (Web)” on page 138
- “Display the Remote Log Hosts (SNMP)” on page 231

▼ Configure the DNS Client (SNMP)

To enable name services within the management controller, Oracle ILOM must be configured as a DNS client.

1. From the SNMP client, set whether the DNS client will be configured via the DHCP server (1), or configured locally (2).

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlDNSdhcpAutoDns.0 i
2
SUN-ILOM-CONTROL-MIB::ilomCtrlDNSdhcpAutoDns.0 = INTEGER: false(2)
$
```

2. If configured locally, set the name server IP addresses.

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlDNSNameServers.0 s
'IP_address'
```

where *IP_addresses* are a comma delimited list of up to three IP addresses of name servers in search order.

For example:

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlDNSNameServers.0 s
'123.45.67.89,123.45.67.90'
SUN-ILOM-CONTROL-MIB::ilomCtrlDNSNameServers.0 = STRING: 123.45.67.89,
123.45.67.90
$
```

3. If configured locally, set the search path.

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlDNSSearchPath.0 s 'domains'
```

where *domains* are a comma delimited list of up to six domains or search suffixes in search order.

For example:

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlDNSSearchPath.0 s 'india.sun.com,norway.sun.com'
SUN-ILOM-CONTROL-MIB::ilomCtrlDNSSearchPath.0 = STRING:
india.sun.com,norway.sun.com
$
```

Note – The timeout value and number of retries are configurable. The default values of 5 and 1, respectively, provide for optimal performance.

Related Information

- [“Configure the DNS Client \(CLI\)” on page 73](#)
- [“Configure the DNS Client \(Web\)” on page 139](#)
- [“Display the DNS Client Status \(SNMP\)” on page 226](#)

▼ Configure the SMTP Client (SNMP)

To enable email alerts, you must configure Oracle ILOM as an SMTP client.

1. From the SNMP client, set the SMTP server IP address.

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlSMTPServerIP.0 a "IP_address"
```

where *IP_address* is the IP address of the SMTP server. For example:

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlSMTPServerIP.0 a 123.45.67.89
SUN-ILOM-CONTROL-MIB::ilomCtrlSMTPServerIP.0 = IPAddress: 123.45.67.89
$
```

2. Set the SMTP server port.

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlSMTPPortNumber.0 i
port
```

where *port* is the port of the SMTP server. For example:

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlSMTPPortNumber.0 i
25
SUN-ILOM-CONTROL-MIB::ilomCtrlSMTPPortNumber.0 = INTEGER: 25
$
```

3. Enable the SMTP client.

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlSMTPEnabled.0 i 1
SUN-ILOM-CONTROL-MIB::ilomCtrlSMTPEnabled.0 = INTEGER: true(1)
$
```

Related Information

- [“Configure the SMTP Client \(CLI\)” on page 74](#)
- [“Configure the SMTP Client \(Web\)” on page 140](#)
- [“Display the SMTP Client Status \(SNMP\)” on page 227](#)

▼ Set the Network Parameters (SNMP)

1. From the SNMP client, set the network parameter.

```
$ snmpset -v2c -c public mc_IP
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkPendingIpparameter.\"SP/network\" type \"value\"
```

where:

- *parameter* is the network parameter to configure:
 - Discovery – The IP address discovery method, 1 for static or 2 for DHCP.
 - Address – The IP address of the management controller, if static discovery is configured.
 - Gateway – The IP address of the subnet gateway.
 - Netmask – The netmask for the subnet.
- *type* is the type of parameter, i for discovery and a for all others

- *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 80](#)

- [“Set the Network Management Parameters \(Web\)” on page 144](#)
- [“Display the Network Management Configuration \(SNMP\)” on page 231](#)

▼ Set the System Identification Properties (SNMP)

1. From the SNMP client, set the host name.

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlHostName.0 s
"hostname"
```

where *hostname* is the host name of the gateway. For example:

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlHostName.0 s
"us-gw-1"
SUN-ILOM-CONTROL-MIB::ilomCtrlHostName.0 = STRING: us-gw-1
$
```

2. Set the system identifier.

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlSystemIdentifier.0
s "identity"
```

where *identity* is the string to identify the gateway. For example:

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlSystemIdentifier.0
s "blr-03-gw-1"
SUN-ILOM-CONTROL-MIB::ilomCtrlSystemIdentifier.0 = STRING: blr-03-gw-1
$
```

Related Information

- [“Set the System Identification Properties \(CLI\)” on page 82](#)
- [“Set the System Identification Properties \(Web\)” on page 145](#)
- [“Display System Identification Properties \(SNMP\)” on page 239](#)

Performing User Tasks (SNMP)

These tasks enable you to add and delete Oracle ILOM users.

- [“Add an Oracle ILOM User Account \(SNMP\)” on page 249](#)
- [“Delete an Oracle ILOM User Account \(SNMP\)” on page 250](#)

Related Information

- [“Performing General Tasks \(SNMP\)” on page 240](#)
- [“Managing Other Aspects With Oracle ILOM \(SNMP\)” on page 250](#)

▼ Add an Oracle ILOM User Account (SNMP)

1. From the SNMP client, type.

```
$ 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\"  
$
```

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 Oracle ILOM User Account \(CLI\)” on page 84](#)
- [“Add an Oracle ILOM User Account \(Web\)” on page 145](#)
- [“Delete an Oracle ILOM User Account \(SNMP\)” on page 250](#)
- [“Display Oracle ILOM User Accounts \(SNMP\)” on page 230](#)

▼ Delete an Oracle 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 Oracle ILOM User Account \(CLI\)” on page 85](#)
- [“Delete an Oracle ILOM User Account \(Web\)” on page 147](#)
- [“Add an Oracle ILOM User Account \(SNMP\)” on page 249](#)
- [“Display Oracle ILOM User Accounts \(SNMP\)” on page 230](#)

Managing Other Aspects With Oracle ILOM (SNMP)

These tasks help you manage the Oracle ILOM services.

- [“Set the HTTP Service State \(SNMP\)” on page 251](#)
- [“Set the HTTPS Service State \(SNMP\)” on page 251](#)
- [“Enable Alerts to Send SNMP Traps \(SNMP\)” on page 252](#)
- [“Enable Alerts to Send PETs \(SNMP\)” on page 253](#)
- [“Enable Alerts to Send Email Alerts \(SNMP\)” on page 254](#)
- [“Modify Alert SNMP Version \(SNMP\)” on page 255](#)
- [“Disable Alerts \(SNMP\)” on page 256](#)

Related Information

- [“Managing Other Aspects With Oracle ILOM \(CLI\)” on page 100](#)
- [“Managing Other Aspects With Oracle ILOM \(Web\)” on page 160](#)
- [“Performing General Tasks \(SNMP\)” on page 240](#)

▼ 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 86
- “Disable the HTTP Service (CLI)” on page 87
- “Enable the HTTP Service (Web)” on page 148
- “Disable the HTTP Service (Web)” on page 148
- “Display the HTTP Service Status (SNMP)” on page 225

▼ Set the HTTPS Service State (SNMP)

- From the SNMP client, type.

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlHttpsEnabled.0 i state
```

where *state* is either 1 for enabled or 2 for disabled. For example, to enable the HTTPS service:

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlHttpsEnabled.0 i 1
SUN-ILOM-CONTROL-MIB::ilomCtrlHttpsEnabled.0 = INTEGER: true(1)
$
```

Related Information

- “Enable the HTTPS Service (CLI)” on page 88
- “Disable the HTTPS Service (CLI)” on page 90
- “Enable the HTTPS Service (Web)” on page 149
- “Disable the HTTPS Service (Web)” on page 151
- “Display the HTTPS Service Status (SNMP)” on page 226

▼ 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"
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertDestinationPort.number = port
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSeverity.number = severity
```

where:

- *number* is the number of the alert.
- *IP_address* is the IP address of the host to receive the trap.
- *port* is the destination port.
- *severity* is the severity of the alert.

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 100](#)
- [“Enable Alerts to Send SNMP Traps \(Web\)” on page 161](#)
- [“Enable Alerts to Send PETs \(SNMP\)” on page 253](#)
- [“Enable Alerts to Send Email Alerts \(SNMP\)” on page 254](#)
- [“Display the Alert Properties \(SNMP\)” on page 229](#)
- [“Disable Alerts \(SNMP\)” on page 256](#)

▼ Enable Alerts to Send PETs (SNMP)

- From the SNMP client, type.

```
$ snmpset -v2c -c public mc_IP
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertDestinationIP.number = "IP_address"
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertType.number = 3
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSeverity.number = severity
```

where:

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

For example, to enable alert 2 to send PET 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::ilomCtrlAlertType.2 = 3
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSeverity.2 = 4
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertDestinationIP.2 = IPAddress: 123.45.67.90
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertType.2 = INTEGER: ipmipet(3)
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSeverity.2 = INTEGER: minor(4)
$
```

Related Information

- [“Enable Alerts to Send PETs \(CLI\)” on page 102](#)
- [“Enable Alerts to Send PETs \(Web\)” on page 161](#)
- [“Enable Alerts to Send SNMP Traps \(SNMP\)” on page 252](#)
- [“Enable Alerts to Send Email Alerts \(SNMP\)” on page 254](#)
- [“Display the Alert Properties \(SNMP\)” on page 229](#)
- [“Disable Alerts \(SNMP\)” on page 256](#)

▼ Enable Alerts to Send Email Alerts (SNMP)

- From the SNMP client, type.

```
$ snmpset -v2c -c public mc_IP
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertDestinationEmail.number = "email_address"
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertType.number = 1
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertEmailCustomSender.number =
"ilom-gwl-hostname" SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSeverity.number = severity
```

where:

- *number* is the number of the alert.
- *email_address* is the fully qualified email address to receive the trap.
- *hostname* is the host name of the management controller.
- *severity* is the severity of the alert.

For example, to enable alert 2 to send to user@yahoo.com:

```
$ snmpset -v2c -c public mc_IP
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertDestinationEmail.2 = "user@yahoo.com"
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertType.2 = 1
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertEmailCustomSender.2 = "ilom-gwl-hostname"
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSeverity.2 = 4
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertDestinationEmail.2 = STRING: user@yahoo.com
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertType.2 = INTEGER: email(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertEmailCustomSender.2 = STRING:
ilom-gwl-hostname
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSeverity.2 = INTEGER: minor(4)
$
```

Related Information

- [“Enable Alerts to Send Email Alerts \(CLI\)” on page 103](#)
- [“Enable Alerts to Send Email Alerts \(Web\)” on page 162](#)
- [“Enable Alerts to Send SNMP Traps \(SNMP\)” on page 252](#)
- [“Enable Alerts to Send PETs \(SNMP\)” on page 253](#)
- [“Display the Alert Properties \(SNMP\)” on page 229](#)
- [“Disable Alerts \(SNMP\)” on page 256](#)

▼ Modify Alert SNMP Version (SNMP)

- From the SNMP client, type.

```
$ snmpset -v2c -c public mc_IP  
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSNMPVersion.number = version
```

where:

- *number* is the number of the alert.
- *version* is the SNMP version, 1 is v1, 2 is v2c, or 3 is v3.

For example, to modify alert 2 for SNMP version v2c:

```
$ snmpset -v2c -c public mc_IP SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSNMPVersion.2  
= 2  
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSNMPVersion.2 = INTEGER: v2c(2)  
$
```

Note – You can modify all alert configuration parameters using SNMP. Refer to the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Protocol Management -- SNMP, IPMI, CIM, WS-MAN*, for more information.

Related Information

- [“Enable Alerts to Send SNMP Traps \(SNMP\)” on page 252](#)
- [“Enable Alerts to Send PETs \(SNMP\)” on page 253](#)
- [“Enable Alerts to Send Email Alerts \(SNMP\)” on page 254](#)
- [“Display the Alert Properties \(SNMP\)” on page 229](#)
- [“Disable Alerts \(SNMP\)” on page 256](#)

▼ 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 104](#)
- [“Disable Alerts \(Web\)” on page 163](#)
- [“Display the Alert Properties \(SNMP\)” on page 229](#)
- [“Enable Alerts to Send SNMP Traps \(SNMP\)” on page 252](#)
- [“Enable Alerts to Send PETs \(SNMP\)” on page 253](#)
- [“Enable Alerts to Send Email Alerts \(SNMP\)” on page 254](#)
- [“Modify Alert SNMP Version \(SNMP\)” on page 255](#)

Administering Hardware (IPMI)

These topics describe how to administer the hardware of the gateway using the `ipmitool` utility.

- [“ipmitool Overview” on page 257](#)
- [“Display the Sensor States \(IPMI\)” on page 258](#)
- [“Display the Sensor Information \(IPMI\)” on page 259](#)
- [“Display the System Event Log \(IPMI\)” on page 261](#)
- [“Display FRU ID Information \(IPMI\)” on page 262](#)
- [“Display Gateway Status LED States \(IPMI\)” on page 263](#)
- [“Enable the Locator LED \(IPMI\)” on page 264](#)
- [“Disable the Locator LED \(IPMI\)” on page 264](#)

Related Information

- [“Administering Oracle ILOM \(CLI\)” on page 29](#)
- [“Administering Oracle ILOM \(Web\)” on page 115](#)
- [“Using the Fabric Monitor” on page 169](#)
- [“Administering Oracle ILOM \(SNMP\)” on page 199](#)
- [“Understanding Oracle ILOM Commands” on page 265](#)

ipmitool Overview

The Oracle ILOM implementation on the management controller within the gateway provides an IPMI server, which can communicate the state of the gateway hardware through the Intelligent Platform Management Interface.

An IPMI client is required to interface with the Oracle ILOM IPMI stack on the management controller. You must have administrator privileges to interface with the stack and the IPMI service must be enabled on the gateway.

The `ipmitool` utility is the IPMI client used in these topics and has this format:

```
$ ipmitool -v -I lan -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 management 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 Oracle ILOM, refer to the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Protocol Management -- SNMP, IPMI, CIM, WS-MAN*, available online at:

<http://www.oracle.com/pls/topic/lookup?ctx=E19860-01&id=homepage>

▼ Display the Sensor States (IPMI)

- From the IPMI client, type.

Note – This example is a portion of the full output.

```
$ 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 Deasserted]
Sensor ID           : PSU0/PRSNT (0x2)
Entity ID           : 10.0
Sensor Type (Discrete): Entity Presence
States Asserted     : Availability State
                     [Device Present]
.
.
```

```

.
Sensor ID           : COOLING_REDUN (0x2b)
Entity ID           : 7.0
Sensor Type (Discrete): OEM reserved #c0
States Asserted     : Digital State
                    [State Deasserted]
Sensor ID           : CABLE_CONN_STAT (0x2c)
Entity ID           : 7.0
Sensor Type (Discrete): OEM reserved #c0
States Asserted     : Digital State
                    [State Deasserted]
$

```

Related Information

- [“Display the Aggregate Sensors State \(CLI\)” on page 41](#)
- [“Display the Aggregate Sensors State \(Web\)” on page 120](#)
- [“Display the Aggregate Sensors State \(SNMP\)” on page 205](#)
- [“Display the Sensor Alarm State \(SNMP\)” on page 219](#)
- [“Display the Sensor Information \(IPMI\)” on page 259](#)

▼ Display the Sensor Information (IPMI)

- From the IPMI client, type.

Note – This example is a portion of the full output.

```

$ 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
Sensor Reading      : 0h
Event Message Control : Per-threshold
States Asserted     : Digital State
                    [State Asserted]
Assertions Enabled  : Digital State
                    [State Deasserted]
                    [State Asserted]
Sensor ID           : PSU0/PRSNT (0x2)
Entity ID           : 10.0 (Power Supply)

```

```

Sensor Type (Discrete): Entity Presence
Sensor Reading          : 0h
Event Message Control  : Per-threshold
States Asserted        : Availability State
                        [Device Present]
Assertions Enabled      : Availability State
                        [Device Absent]
                        [Device Present]
.
.
.
Sensor ID               : COOLING_REDUN (0x2b)
Entity ID               : 7.0 (System Board)
Sensor Type (Discrete): OEM reserved #c0
Sensor Reading          : 0h
Event Message Control  : Per-threshold
States Asserted        : Digital State
                        [State Deasserted]
Assertions Enabled      : Digital State
                        [State Deasserted]
                        [State Asserted]
Sensor ID               : CABLE_CONN_STAT (0x2c)
Entity ID               : 7.0 (System Board)
Sensor Type (Discrete): OEM reserved #c0
Sensor Reading          : 0h
Event Message Control  : Per-threshold
States Asserted        : Digital State
                        [State Deasserted]
Assertions Enabled      : Digital State
                        [State Deasserted]
                        [State Asserted]
$

```

Related Information

- [“Display the Sensor States \(IPMI\)” on page 258](#)
- [“Display the Sensor Alarm State \(SNMP\)” on page 219](#)

▼ 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 Oracle ILOM Event Log \(CLI\)” on page 51](#)
- [“Display the Oracle ILOM Event Log \(Web\)” on page 124](#)
- [“Display the Oracle ILOM Event Log \(SNMP\)” on page 223](#)

▼ Display FRU ID Information (IPMI)

- From the IPMI client, type.

```
$ ipmitool -v -I lan -H mc_IP -U ilom-admin fru print
Password: password
FRU Device Description : Builtin FRU Device (ID 0)
  Product Manufacturer : Sun Microsystems
  Product Name         : ILOM
  Product Version      : 2.0.5-1

FRU Device Description : SYS (ID 4)
  Product Manufacturer : Sun Microsystems
  Product Name         : Sun Datacenter InfiniBand Switch GW
  Product Part Number  : 5413495
  Product Serial       : 0110SJC-09183P0022

FRU Device Description : PSU0 (ID 5)
  Board Mfg            : Delta Energy Systems
  Board Product        : A236
  Board Serial         : 006541
  Board Part Number    : 3002234
  Board Extra          : sun_spec_part_number - 885-1390-01

FRU Device Description : PSU1 (ID 6)
  Board Mfg            : Delta Energy Systems
  Board Product        : A236
  Board Serial         : 006653
  Board Part Number    : 3002234
  Board Extra          : sun_spec_part_number - 885-1390-01

FRU Device Description : MB (ID 7)
  Board Extra          : ComEx: manufacturing_date - 2009.02.20
  Product Manufacturer : Sun Microsystems
  Product Name         : Sun Datacenter InfiniBand Switch GW
  Product Part Number  : 5413495
  Product Serial       : 0110SJC-09183P0022
  Product Extra        : ComEx: serial_number - NCD2T0271
$
```

In the output, the FRU Device Description field identifies the FRUs:

- Builtin FRU Device (ID 0) – Oracle ILOM firmware
- SYS (ID 4) – Management controller
- PSU0 (ID 5) – Power supply 0

- PSU1 (ID 6) – Power supply 1
- MB (ID 7) – Motherboard

Related Information

- “Display Gateway FRU ID (CLI)” on page 64
- “Display Power Supply FRU ID (CLI)” on page 65
- “Display System Component FRU ID (Web)” on page 132
- “Display Gateway FRU ID (SNMP)” on page 232
- “Display Power Supply FRU ID (SNMP)” on page 234

▼ Display Gateway Status LED States (IPMI)

- From the IPMI client, type.

```
$ ipmitool -v -I lan -H mc_IP -U ilom-admin sunoem sbled get
Password: password
I_POWER          | ON
I_ATTENTION      | OFF
I_LOCATOR        | OFF
$
```

In the output, the Power LED is on, and the Attention and Locator LEDs are off.

Related Information

- “Display Gateway Status LEDs States (CLI)” on page 40
- “Display the Gateway Status LEDs States (Web)” on page 120
- “Enable the Locator LED (IPMI)” on page 264
- “Disable the Locator LED (IPMI)” on page 264

▼ Enable the Locator LED (IPMI)

- From the IPMI client, type.

```
$ ipmitool -v -I lan -H mc_IP -U ilom-admin sunoem sbled set I_LOCATOR ON
Password: password
I_LOCATOR      | ON
$
```

The Locator LEDs is lit.

Related Information

- [“Enable the Locator LED \(CLI\)” on page 70](#)
- [“Enable the Locator LED \(Web\)” on page 137](#)
- [“Disable the Locator LED \(IPMI\)” on page 264](#)
- [“Display Gateway Status LED States \(IPMI\)” on page 263](#)

▼ Disable the Locator LED (IPMI)

- From the IPMI client, type.

```
$ ipmitool -v -I lan -H mc_IP -U ilom-admin sunoem sbled set I_LOCATOR OFF
Password: password
I_LOCATOR      | OFF
$
```

The Locator LEDs is unlit.

Related Information

- [“Disable the Locator LED \(CLI\)” on page 71](#)
- [“Disable the Locator LED \(Web\)” on page 137](#)
- [“Enable the Locator LED \(IPMI\)” on page 264](#)
- [“Display Gateway Status LED States \(IPMI\)” on page 263](#)

Understanding Oracle ILOM Commands

Only the `ilom-admin` user of the Oracle ILOM shell can run all of the Oracle ILOM commands on the Sun Network QDR InfiniBand Gateway Switch. The format of the Oracle ILOM commands is typically as follows:

-> `command [option] [target] [property=value] . . .`

where:

- *command* is the command being issued.
- *option* is any option to that command.
- *target* is the target and path to act upon.
- *property* is the property of the target to change.
- *value* is what to change the property to.

Command Syntax	Links
<code>cd [-default] [target]</code>	“cd Command” on page 266
<code>create [target] [property=value property=value . . .]</code>	“create Command” on page 267
<code>delete [-script] [target]</code>	“delete Command” on page 268
<code>dump [-destination URI] [target]</code>	“dump Command” on page 269
<code>exit</code>	“exit Command (ILOM)” on page 270
<code>help [-o terse verbose] [command legal targets target target property]</code>	“help Command (ILOM)” on page 271
<code>load [-force] [-o verbose] [-script] -source URI [target]</code>	“load Command” on page 272
<code>reset [-script] [target]</code>	“reset Command” on page 273

Command Syntax	Links
<code>set [target]property=value[property=value...]</code>	“set Command” on page 274
<code>show [-d targets properties commands all] [-l 1 2 3...255 all] [-o table] [target] [property property...]</code>	“show Command” on page 275
<code>version</code>	“version Command (ILOM)” on page 277

Related Information

- *Gateway Command Reference*
- [“Administering Oracle ILOM \(CLI\)” on page 29](#)
- [“Administering Oracle ILOM \(Web\)” on page 115](#)
- [“Using the Fabric Monitor” on page 169](#)
- [“Administering Oracle ILOM \(SNMP\)” on page 199](#)
- [“Administering Hardware \(IPMI\)” on page 257](#)

cd Command

Changes the current target.

Syntax

```
cd [-default] target
```

where *target* is the target and path to act upon.

Description

This Oracle ILOM command changes the Oracle 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

This example shows how to change to the `/SP/logs/event/list` target with the `cd` command.

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

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

-> show
/SP/logs/event/list
Targets:
Properties:
Commands:
  cd
  s      how
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
.
.
.
->
```

create Command

Creates a target or property.

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 Oracle ILOM command creates the specified target with the specified properties. Your user must have administrator (a) privileges to use this command.

Example

This 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 268](#)

delete Command

Deletes a target.

Syntax

```
delete [-script] [target]
```

where *target* is the target and path to act upon.

Description

This Oracle 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

This example shows how to delete the `/SP/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 267](#)

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 Oracle 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

This 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 272](#)

exit Command (ILOM)

Terminates the Oracle ILOM session.

Syntax

```
exit
```

Description

This Oracle ILOM command exits the Oracle ILOM shell and either:

- Returns the `root` user to the Linux `root` user prompt of the management controller.

- Logs off the `ilom-admin` user or `ilom-operator` user from the management controller.

Example

This example shows how to exit the Oracle ILOM session using the `exit` command.

```
-> exit  
#
```

Related Information

- *Gateway Reference*, `exit` command

help Command (ILOM)

Provides help with Oracle ILOM commands.

Syntax

```
help [-o terse|verbose] [command | legal | targets | target | target property]
```

where:

- *command* is the Oracle 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 Oracle 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

This 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

- *Gateway Reference*, `help` command

load Command

Transfers a file from a remote location to update a target.

Syntax

```
load [-force] [-o verbose] [-script] -source URI [target]
```

where:

- *URI* is the uniform resource indicator.
- *target* is the target and path to act upon.

Description

This Oracle 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

This table describes the options to the `load` command and their purposes:

Option	Purpose
<code>-force</code>	Disables the version number check for firmware updates.
<code>-o</code>	Enables verbose output.
<code>-script</code>	Skips confirmation of the action and proceeds as if <code>y</code> was specified.

Example

This 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 269](#)

reset Command

Resets a target.

Syntax

```
reset [-script] [target]
```

where *target* is the target and path to act upon.

Description

This Oracle ILOM command resets a resettable *target* to default conditions. If no *target* is specified, the current target is affected. The `-script` option skips confirmation of the action and proceeds as if `yes` was specified. Your user must have administrator (a) privileges to use this command.

Example

This example shows how to reset the custom SSL certificate with the `reset` command.

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

Related Information

- [“set Command” on page 274](#)

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 change the property to.

Description

This Oracle 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

This 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 275](#)
- [“reset Command” on page 273](#)

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 Oracle ILOM command displays information about targets, their properties, and associated commands. If no *target* is specified, information about the current target is displayed.

Options

This table describes the options to the show command and their purposes:

Option	Purpose
-d	Specifies what information to display. <ul style="list-style-type: none">• <i>targets</i> – The subtargets of the target.• <i>properties</i> – The properties of the target.• <i>commands</i> – The supported commands of the target.• <i>all</i> – 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

This example shows how to display the Oracle 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 274](#)

version Command (ILOM)

Displays version information.

Syntax

```
version
```

Description

This Oracle ILOM command displays the version information within the management controller.

Example

This example shows how to display the version information with the `version` command.

```
-> version  
SP firmware 1.3  
SP firmware build number: 47111  
SP firmware date: Wed Nov 11 18:21:29 IST 2009  
SP filesystem version: 0.1.22  
->
```

Related Information

- *Gateway Reference*, version command

Index

A

- accessing
 - ILOM
 - from CLI, 30
 - from web, 118
 - NET MGT port, 30
 - SER MGT port, 31
- acquiring
 - gateway firmware, 107
- adding
 - from CLI
 - ILOM user, 84
 - SNMP communities, 95
 - SNMP users, 93
 - from SNMP
 - ILOM user, 249
 - from web
 - ILOM user, 145
 - SNMP communities, 156
 - SNMP users, 153
- administering
 - hardware from IPMI, 257
 - ILOM
 - from CLI, 29
 - from SNMP, 199
 - from web, 115
- aggregate sensor states, 42
- alerts
 - from CLI
 - disabling, 104
 - displaying, 60
 - send emails, 103
 - send PETs, 102
 - send traps, 100
 - from SNMP
 - disabling, 256
 - displaying, 229

- send emails, 254
 - send PETs, 253
 - send traps, 252
 - SNMP version, 255
- from web
 - disabling, 163
 - displaying, 129
 - send emails, 162
 - send PETs, 161
 - send traps, 161

B

- backing up
 - configuration
 - from CLI, 75
 - from web, 141
 - configuration information, 76
- board level voltages, 46
- BridgeX chips
 - status window, 178

C

- cd command, 266
- changing password
 - ILOM user
 - from CLI, 84
 - from web, 146
- chassis
 - monitoring, 189
- clear
 - ILOM event log
 - from CLI, 71
 - from SNMP, 243
 - from web, 138
- CLI
 - acquiring gateway firmware, 107
 - adding

- ILOM user, 84
- SNMP communities, 95
- SNMP users, 93
- backing up configuration, 75
- changing ILOM password, 84
- clearing ILOM event log, 71
- configuring
 - DNS client, 73
 - SMTP client, 74
- creating snapshot, 77
- deleting
 - ILOM user, 85
 - SNMP communities, 96
 - SNMP users, 95
- disabling
 - alerts, 104
 - HTTP, 87
 - HTTPS, 90
 - IPMI, 99
 - log hosts, 72
 - SNMP, 98
- displaying
 - aggregate sensors state, 41
 - alerts, 60
 - board voltages, 44
 - CLI timeout, 64
 - date, 40
 - DNS client status, 56
 - fan speed, 48
 - fan status, 48
 - gateway FRU ID, 64
 - gateway status LEDs, 40
 - help, 59
 - host name, 66
 - HTTP status, 52
 - HTTPS status, 53
 - ILOM event log, 51
 - ILOM sessions, 50
 - ILOM users, 61
 - ILOM version, 66
 - internal temperatures, 47
 - IPMI status, 56
 - log hosts, 62
 - network management configuration, 63
 - NTP servers, 57
 - other aspects, 58
 - power supply FRU ID, 65
 - power supply status, 43
 - service status, 52
 - SMTP client status, 57, 227
 - SNMP communities, 55
 - SNMP status, 54
 - SNMP users, 54
 - SSL certificates, 53
 - system identity, 66
 - target properties, 60
- downloading
 - SNMP MIBs, 97
- enabling
 - alerts send emails, 103
 - alerts send PETs, 102
 - alerts send traps, 100
 - HTTP, 86
 - HTTPS, 88
 - IPMI, 99
 - log hosts, 72
 - SNMP, 91
- interface overview, 29
- management controller
 - reset, 68
 - restart, 68
- managing
 - HTTP, 86
 - HTTPS, 88
 - IPMI, 98
 - other aspects, 100
 - SNMP, 91
- modifying
 - SNMP communities, 96
 - SNMP users, 94
- performing
 - daily tasks, 39
 - general tasks, 67
 - ILOM user tasks, 83
- restoring configuration, 76
- setting
 - CLI timeout, 105
 - date, 69
 - host name, 82
 - log hosts, 72
 - network management configuration, 80
 - NTP servers, 69
 - SNMP configuration, 92
 - system identity, 82
- snapshot dataset information, 79
- SSL certificate
 - installing, 89
 - removing, 89

- upgrading gateway firmware, 105, 109
- command
 - create, 84, 93, 95
 - delete, 85, 95, 96
 - dump, 97
 - fwverify, 106
 - help, 59, 60
 - ILOM
 - cd, 266
 - create, 267
 - delete, 268
 - dump, 269
 - exit, 270
 - help, 271
 - load, 272
 - reset, 273
 - set, 274
 - show, 275
 - version, 277
 - load, 89, 109
 - SNMP, 200
 - version, 66
- configuring
 - DNS client
 - from CLI, 73
 - from SNMP, 244
 - from web, 139
 - SMTP client
 - from CLI, 74
 - from SNMP, 245
 - from web, 140
- connector
 - status window
 - gateway, 176
 - InfiniBand, 173
- connector status
 - gateway, 176
 - InfiniBand, 173
- controlling
 - ILOM targets
 - from CLI, 67
 - from SNMP, 240
 - from web, 134
- create command, 84, 93, 95, 267
- creating
 - snapshot
 - from CLI, 77
 - from web, 142

D

- date
 - displaying
 - from CLI, 40
 - from web, 120
 - setting
 - from CLI, 69
 - from SNMP, 241
 - from web, 136
- delete command, 85, 95, 96, 268
- deleting
 - from CLI
 - ILOM user, 85
 - SNMP communities, 96
 - SNMP users, 95
 - from web
 - ILOM user, 147
 - SNMP communities, 157
 - SNMP users, 155
- disabling
 - from CLI
 - alerts, 104
 - HTTP, 87
 - HTTPS, 90
 - IPMI, 99
 - log hosts, 72
 - SNMP, 98
 - from SNMP
 - alerts, 256
 - HTTP, 251
 - HTTPS, 251
 - log hosts, 243
 - NTP, 242
 - from web
 - alerts, 163
 - HTTP, 148
 - HTTPS, 151
 - IPMI, 160
 - log hosts, 138
 - SNMP, 158
- Locator LED
 - from CLI, 71
 - from IPMI, 264
 - from web, 137
- displaying
 - entity numbers, 220
 - firmware
 - ILOM, 66, 133

- version, 132
- from CLI
 - aggregate sensors state, 41
 - alerts, 60
 - board voltages, 44
 - CLI timeout, 64
 - date, 40
 - DNS client status, 56
 - fan speed, 48
 - fan status, 48
 - gateway FRU ID, 64
 - gateway status LEDs, 40
 - help, 59
 - host name, 66
 - HTTP status, 52
 - HTTPS status, 53
 - ILOM event log, 51
 - ILOM sessions, 50
 - ILOM users, 61
 - ILOM version, 66
 - internal temperatures, 47
 - IPMI status, 56
 - log hosts, 62
 - network management configuration, 63
 - NTP servers, 57
 - other aspects, 58
 - power supply FRU ID, 65
 - power supply status, 43
 - service status, 52
 - SMTP client status, 57, 227
 - SNMP communities, 55
 - SNMP status, 54
 - SNMP users, 54
 - SSL certificates, 53
 - system identity, 66
 - target properties, 60
- from IPMI
 - aggregate sensor information, 259
 - aggregate sensor state, 258
 - FRU ID, 262
 - gateway status LEDs, 263
 - system event log, 261
- from SNMP
 - aggregate sensor state, 205, 219
 - alerts, 229
 - board voltages, 208
 - date and time, 204
 - DNS client status, 226
 - fan speed, 215
 - fan status, 215
 - gateway FRU ID, 232
 - host name, 239
 - HTTP status, 225
 - HTTPS status, 226
 - ILOM event log, 223
 - ILOM sessions, 222
 - ILOM users, 230
 - ILOM version, 239
 - internal temperatures, 212
 - log hosts, 231
 - network management configuration, 231
 - NTP servers, 228
 - NTP state, 227
 - other aspects, 228
 - physical entities, 236
 - physical entity classes, 236
 - physical entity descriptions, 236
 - physical entity information, 238
 - power supply FRU ID, 234
 - power supply status, 206
 - system components, 236
 - system identity, 239
 - time zone, 205
- from web
 - aggregate sensor, 120
 - alerts, 129
 - board voltages, 122
 - CLI timeout, 131
 - component FRU ID, 132
 - date, 120
 - DNS client status, 127
 - fan speed, 123
 - fan status, 123
 - firmware version, 132
 - gateway status, 120
 - host name, 133
 - HTTP status, 125
 - HTTPS status, 125
 - ILOM event log, 124
 - ILOM sessions, 123
 - ILOM users, 130
 - ILOM version, 133
 - internal temperatures, 122
 - IPMI status, 127
 - log hosts, 130
 - network management configuration, 131
 - NTP servers, 128
 - other aspects, 129

- power supply status, 121
- service status, 124
- SMTP client status, 128
- SNMP communities, 127
- SNMP status, 126
- SNMP users, 126
- SSL certificates, 125
- system identity, 133
- displaying from Fabric Monitor
 - all connectors
 - bandwidth, 191
 - I4 mapping, 191
 - link status, 191
 - peer information, 191
 - presence, 191
 - battery voltage, 189
 - BridgeX
 - errors, 195
 - GUID, 195
 - LID, 195
 - link status, 195
 - name, 195
 - throughput, 195
 - chassis
 - FRU ID, 189
 - part number, 189
 - serial number, 189
 - temperature, 189
 - connector
 - errors, 191
 - FRU ID, 191
 - GUID, 191
 - LID, 191
 - link status, 191
 - name and type, 191
 - peer information, 191
 - throughput, 191
 - fan
 - speed, 189
 - status, 189
 - gateway
 - cable FRU ID, 194
 - cable presence, 194
 - link status, 194
 - port status, 194
 - routing, 194
 - vNIC information, 194
 - I4
 - bandwidth, 189, 196
 - firmware, 189
 - GUID, 189
 - LID, 189
 - link status, 196
 - mapping, 196
 - peer information, 196
 - temperature, 189
 - voltage, 189
 - main board voltage, 189
 - management controller
 - BIOS, 189
 - firmware, 189
 - serial number, 189
 - power supply status, 189
 - Subnet Manager
 - algorithm, 189
 - GUID, 189
 - LID, 189
 - priority, 189
 - status, 189
- DNS client
 - configuring
 - from CLI, 73
 - from SNMP, 244
 - from web, 139
- downloading
 - SNMP MIBs
 - from CLI, 97
 - from web, 158
- dump command, 97, 269

E

- email
 - from CLI, 103
 - from SNMP, 254
 - from web, 162
- enabling
 - from CLI
 - alerts send emails, 103
 - alerts send PETs, 102
 - alerts send traps, 100
 - HTTP, 86
 - HTTPS, 88
 - IPMI, 99
 - log hosts, 72
 - SNMP, 91
 - from SNMP
 - alerts send emails, 254

- alerts send PETs, 253
- alerts send traps, 252
- HTTP, 251
- HTTPS, 251
- log hosts, 243
- NTP, 242
- from web
 - alerts send emails, 162
 - alerts send PETs, 161
 - alerts send traps, 161
 - HTTP, 148
 - HTTPS, 149
 - IPMI, 159
 - log hosts, 138
 - SNMP, 152
- Locator LED
 - from CLI, 70
 - from IPMI, 264
 - from web, 137
- entity numbers
 - displaying, 220
- exit command, 270

F

Fabric Monitor

- accessing, 169
- all connectors
 - bandwidth, 191
 - I4 mapping, 191
 - link status, 191
 - peer information, 191
 - presence, 191

- battery voltage, 189

BridgeX

- errors, 195
- GUID, 195
- LID, 195
- link status, 195
- name, 195
- throughput, 195

chassis

- FRU ID, 189
- part number, 189
- serial number, 189
- temperature, 189

connector

- errors, 191
- FRU ID, 191

- GUID, 191
- LID, 191
- link status, 191
- name and type, 191
- peer information, 191
- throughput, 191
- control panel, 187
- fan
 - speed, 189
 - status, 189
- features, 170
- gateway
 - cable FRU ID, 194
 - cable presence, 194
 - link status, 194
 - port status, 194
 - routing, 194
 - vNIC information, 194
- I4
 - bandwidth, 189, 196
 - firmware, 189
 - GUID, 189
 - LID, 189
 - link status, 196
 - mapping, 196
 - peer information, 196
 - temperature, 189
 - voltage, 189
- main board voltage, 189
- management controller
 - BIOS, 189
 - firmware, 189
 - serial number, 189
- monitoring
 - chassis, 189
 - gateway, 194
 - InfiniBand, 191
 - interface, 195
 - switch chip, 196
- power supply status, 189
- Subnet Manager
 - algorithm, 189
 - GUID, 189
 - LID, 189
 - priority, 189
 - status, 189
- tab
 - IB Performance, 183
 - IB Port Map, 185

- Sensor Info, 182
- Subnet Manager, 186
- System Info, 181
- using, 169

firmware

- overview, 106
- verifying integrity, 106
- version
 - from CLI, 66
 - from SNMP, 239
 - from web, 132

FRU ID

- component, 132, 262
- gateway, 64, 232, 262
- power supply, 65, 234, 262

fwverify command, 106

G

gateway

- configuration back up
 - from CLI, 75
 - from web, 141
- configuration restore
 - from CLI, 76
 - from web, 142
- LEDs
 - from CLI, 40
 - from IPMI, 263
- monitoring, 194

H

help command, 59, 60, 271

host name

- displaying
 - from CLI, 66
 - from SNMP, 239
 - from web, 133
- setting
 - from CLI, 82
 - from web, 145

hostname

- setting
 - from SNMP, 248

HTTP

- from CLI
 - disabling, 87
 - enabling, 86
 - managing, 86

- from web
 - disabling, 148
 - enabling, 148
 - managing, 147

HTTPS

- from CLI
 - disabling, 90
 - enabling, 88
 - managing, 88
- from web
 - disabling, 151
 - enabling, 149
 - managing, 149

I

identity

- displaying
 - from CLI, 66
 - from SNMP, 239
 - from web, 133
- setting
 - from CLI, 82
 - from SNMP, 248
 - from web, 145

ILOM

- accessing
 - from CLI, 30
 - from web, 118
 - NET MGT port, 30
 - SER MGT port, 31
- CLI, 29
- command
 - help, 59
 - reference, 265
- displaying from CLI
 - event log, 51
 - sessions, 50
 - users, 61
 - version, 66
- displaying from SNMP
 - event log, 223
 - sessions, 222
 - users, 230
 - version, 239
- displaying from web
 - event log, 124
 - sessions, 123
 - users, 130

- version, 133
- from CLI
 - adding user, 84
 - administering, 29
 - changing password, 84
 - controlling targets, 67
 - deleting user, 85
 - event log clearing, 71
 - interface, 29
 - user tasks, 83
- from SNMP
 - adding user, 249
 - administering, 199
 - controlling, 240
 - deleting user, 250
 - event log clearing, 243
 - interface, 199
 - monitoring, 203
 - user tasks, 248
- from web
 - adding user, 145
 - administering, 115
 - changing password, 146
 - controlling targets, 134
 - deleting user, 147
 - event log clearing, 138
 - interface, 115
 - user tasks, 145
- overview, 1
- properties
 - fan, 11
 - general, 22
 - general system, 9
 - indicator, 12
 - power supply, 13
 - service, 25
 - temperature, 15
 - user, 27
 - voltage, 17
- supported features, 2
- switching
 - between shells, 32
 - from Linux, 38
 - to Linux, 36
- targets
 - description, 5
 - overview, 4
 - understanding, 4
- understanding, 1

- InfiniBand
 - connector status, 173
 - monitoring, 191
- installing
 - SSL certificate
 - from CLI, 89
 - from web, 150
- internal temperature sensor, 48
- IPMI, 257
 - displaying
 - aggregate sensor information, 259
 - aggregate sensor state, 258
 - FRU ID, 262
 - gateway status LEDs, 263
 - system event log, 261
 - from CLI
 - disabling, 99
 - enabling, 99
 - managing, 98
 - from web
 - disabling, 160
 - enabling, 159
 - managing, 159
 - interface, 257
 - overview, 257
- ipmitool utility, 257, 258, 259, 261, 262

L

- load command, 89, 109, 272
- Locator LED
 - disabling
 - from CLI, 71
 - from IPMI, 264
 - from web, 137
 - enabling
 - from CLI, 70
 - from IPMI, 264
 - from web, 137

M

- management controller
 - reset
 - from CLI, 68
 - from web, 135
 - restart
 - from CLI, 68
 - from web, 135
- managing

- from CLI
 - HTTP, 86
 - HTTPS, 88
 - IPMI, 98
 - other aspects, 100
 - SNMP, 91
- from SNMP
 - other aspects, 250
- from web
 - HTTP, 147
 - HTTPS, 149
 - IPMI, 159
 - other aspects, 160
 - SNMP, 152
- modifying
 - from CLI
 - SNMP communities, 96
 - SNMP users, 94
 - from SNMP
 - alerts, 255
 - from web
 - SNMP communities, 156
 - SNMP users, 154
- monitoring
 - chassis, 189
 - gateway, 194
 - ILOM targets
 - from CLI, 39
 - from SNMP, 203
 - from web, 119
 - InfiniBand, 191
 - interface, 195
 - parameters and status, 188
 - switch chip, 196

N

- network management configuration
 - displaying
 - from CLI, 63
 - from SNMP, 231
 - from web, 131
 - setting
 - from CLI, 80
 - from web, 144
- NTP servers
 - displaying
 - from CLI, 57
 - from SNMP, 228

- from web, 128
- setting
 - from CLI, 69
 - from SNMP, 242
 - from web, 136

O

- overview
 - CLI, 29
 - firmware, 106
 - ILOM, 1
 - commands, 29
 - SNMP interface, 199
 - targets, 4
 - IPMI, 257
 - web interface, 115

P

- password, 84, 146
- performing
 - from CLI
 - daily tasks, 39
 - general tasks, 67
 - ILOM user tasks, 83
 - from SNMP
 - daily tasks, 204
 - general tasks, 240
 - ILOM user tasks, 248
 - from web
 - daily tasks, 119
 - general tasks, 134
 - ILOM user tasks, 145

PET

- from CLI, 102
- from SNMP, 253
- from web, 161

R

- rear panel diagram, 172
- removing
 - SSL certificate
 - from CLI, 89
 - from web, 151
- reset command, 89, 273
- resetting
 - management controller
 - from CLI, 68

- from web, 135
- restarting
 - management controller
 - from CLI, 68
 - from web, 135
- restoring configuration
 - from CLI, 76
 - from web, 142

S

- set command, 274
- setting
 - from CLI
 - CLI timeout, 105
 - date, 69
 - host name, 82
 - log hosts, 72
 - network management configuration, 80
 - NTP servers, 69
 - SNMP configuration, 92
 - system identity, 82
 - from SNMP
 - date, 241
 - host name, 248
 - HTTP state, 251
 - HTTPS state, 251
 - log hosts, 243
 - network parameters, 246
 - NTP servers, 242
 - NTP state, 242
 - system identity, 248
 - time zone, 241
 - from web
 - CLI timeout, 164
 - date, 136
 - host name, 145
 - log hosts, 138
 - network management configuration, 144
 - NTP servers, 136
 - SNMP configuration, 153
 - system identity, 145
 - time zone, 136
- show command, 275
- SMTP client
 - configuring
 - from CLI, 74
 - from SNMP, 245
 - from web, 140

- displaying status, 227
- snapshot dataset information
 - CLI, 79
 - web, 143
- SNMP
 - administering ILOM, 199
 - checking services, 225
 - clearing ILOM event log, 243
 - commands, 200
 - understanding, 200
 - V1 format, 201
 - V2c format, 201
 - V3 format, 202
 - configuring
 - DNS client, 244
 - SMTP client, 245
 - disabling
 - alerts, 256
 - HTTP, 251
 - HTTPS, 251
 - log hosts, 243
 - NTP, 242
 - displaying
 - aggregate sensor state, 205, 219
 - alerts, 229
 - board voltages, 208
 - date and time, 204
 - DNS client status, 226
 - fan speed, 215
 - fan status, 215
 - gateway FRU ID, 232
 - host name, 239
 - HTTP status, 225
 - HTTPS status, 226
 - ILOM event log, 223
 - ILOM sessions, 222
 - ILOM users, 230
 - ILOM version, 239
 - internal temperatures, 212
 - log hosts, 231
 - network management configuration, 231
 - NTP servers, 228
 - NTP state, 227
 - other aspects, 228
 - physical entities, 236
 - physical entity classes, 236
 - physical entity descriptions, 236
 - physical entity information, 238
 - power supply FRU ID, 234

- power supply status, 206
- system components, 236
- system identity, 239
- time zone, 205
- enabling
 - alerts send emails, 254
 - alerts send PETs, 253
 - alerts send traps, 252
 - HTTP, 251
 - HTTPS, 251
 - log hosts, 243
 - NTP, 242
- from CLI
 - adding communities, 95
 - adding users, 93
 - deleting communities, 96
 - deleting users, 95
 - disabling, 98
 - downloading MIBs, 97
 - enabling, 91
 - managing, 91
 - modifying communities, 96
 - modifying users, 94
 - setting configuration, 92
- from web
 - adding communities, 156
 - adding users, 153
 - deleting communities, 157
 - deleting users, 155
 - disabling, 158
 - downloading MIBs, 158
 - enabling, 152
 - managing, 152
 - modifying communities, 156
 - modifying users, 154
 - setting configuration, 153
- ILOM
 - controlling, 240
 - monitoring, 203
- ILOM user
 - adding, 249
 - deleting, 250
- managing other aspects, 250
- modify alerts, 255
- overview, 199
- performing
 - daily tasks, 204
 - general tasks, 240
 - user tasks, 248
- setting
 - date, 241
 - host name, 248
 - HTTP state, 251
 - HTTPS state, 251
 - log hosts, 243
 - network parameters, 246
 - NTP servers, 242
 - NTP state, 242
 - system identity, 248
 - time zone, 241
- SSL certificate
 - from CLI
 - installing, 89
 - removing, 89
 - from web
 - installing, 150
 - removing, 151
- switch chip
 - monitoring, 196
- switching
 - between shells, 32
 - ILOM to Linux, 36
 - Linux to ILOM, 38

T

- targets, 5
 - controlling
 - from CLI, 67
 - from SNMP, 240
 - from web, 134
 - monitoring
 - from CLI, 39
 - from SNMP, 203
 - from web, 119
 - properties
 - displaying, 60
 - fan, 11
 - general, 22
 - general system, 9
 - indicator, 12
 - power supply, 13
 - service, 25
 - temperature, 15
 - user, 27
 - voltage, 17
- trap
 - from CLI, 100

- from SNMP, 252
- from web, 161

U

- understanding
 - ILOM, 1
 - commands, 265
 - targets, 4
 - SNMP commands, 200
- upgrading
 - gateway firmware
 - from CLI, 105, 109
 - from web, 164

V

- verifying
 - firmware integrity, 106
- version command, 66, 277

W

- web
 - adding
 - ILOM user, 145
 - SNMP communities, 156
 - SNMP users, 153
 - backing up
 - configuration, 141
 - changing ILOM password, 146
 - clearing ILOM event log, 138
 - configuring
 - DNS client, 139
 - SMTP client, 140
 - creating snapshot, 142
 - deleting
 - ILOM user, 147
 - SNMP communities, 157
 - SNMP users, 155
 - disabling
 - alerts, 163
 - HTTP, 148
 - HTTPS, 151
 - IPMI, 160
 - log hosts, 138
 - SNMP, 158
 - displaying
 - aggregate sensor, 120
 - alerts, 129
 - board voltages, 122

- CLI timeout, 131
- component FRU ID, 132
- date, 120
- DNS client status, 127
- fan speed, 123
- fan status, 123
- firmware version, 132
- gateway status, 120
- host name, 133
- HTTP status, 125
- HTTPS status, 125
- ILOM event log, 124
- ILOM sessions, 123
- ILOM users, 130
- ILOM version, 133
- internal temperatures, 122
- IPMI status, 127
- log hosts, 130
- network management configuration, 131
- NTP servers, 128
- other aspects, 129
- power supply status, 121
- service status, 124
- SMTP client status, 128
- SNMP communities, 127
- SNMP status, 126
- SNMP users, 126
- SSL certificates, 125
- system identity, 133
- downloading
 - SNMP MIBs, 158
- enabling
 - alerts send emails, 162
 - alerts send PETs, 161
 - alerts send traps, 161
 - HTTP, 148
 - HTTPS, 149
 - IPMI, 159
 - log hosts, 138
 - SNMP, 152
- interface overview, 115
- management controller
 - reset, 135
 - restart, 135
- managing
 - HTTP, 147
 - HTTPS, 149
 - IPMI, 159
 - other aspects, 160

- SNMP, 152
- modifying
 - SNMP communities, 156
 - SNMP users, 154
- performing
 - daily tasks, 119
 - general tasks, 134
 - ILOM user tasks, 145
- restoring configuration, 142
- setting
 - CLI timeout, 164
 - date, 136
 - host name, 145
 - log hosts, 138
 - network management configuration, 144
 - NTP servers, 136
 - SNMP configuration, 153
 - system identity, 145
 - time zone, 136
- snapshot dataset information, 143
- SSL certificate
 - installing, 150
 - removing, 151
- upgrading gateway firmware, 164

