Oracle Integrated Lights Out Manager (ILOM) 3.1

User's Guide

Part No.: E24523-10
September 2013

Please
Recycle

Adobe PostScript

Contents

Using This Documentation

Use this guide in conjunction with other guides in the Oracle Integrated Lights Out Manager (ILOM) 3.1 Documentation Library. This guide is intended for technicians, system administrators, and authorized Oracle service providers, and users who have experience managing system hardware.

Related Documentation

Documentation	Links
All Oracle products	http://www.oracle.com/documentation
Oracle Integrated Lights Out Manager (ILOM) 3.1 Documentation Library	http://www.oracle.com/pls/topic/lookup?ctx=ilom31

Documentation	Links
System management, single-system management (SSM) security, and diagnostic documentation	http://www.oracle.com/technetwork/documentation/sys-mgmt-networking-190072.html
Oracle Hardware Management Pack 2.2	http://www.oracle.com/pls/topic/lookup?ctx=ohmp

Note: To locate Oracle ILOM 3.1 documentation that is specific to your server platform, refer to the Oracle ILOM section of the administration guide that is available for your server.

Documentation Feedback

Provide feedback on this documentation at:

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

Product Downloads

Updates to the Oracle ILOM 3.1 firmware are available through standalone software updates that you can download from the My Oracle Support (MOS) web site for each Oracle server or blade chassis system. To download these software updates from the MOS web site, see the instructions that follow.

▼ Download Product Software and Firmware

1. **Go to** http://support.oracle.com**.**
2. **Sign in to My Oracle Support.**
3. **At the top of the page, click the Patches and Updates tab.**
4. **In the Patch Search panel, at the top of the Search tab, select Product or Family (Advanced).**

5. **In the Product Is list box, type a full or partial product name until a list of product matches appears in the list box, and then select the product of interest.**

   Example Product Names: `Sun Fire X4470 M2 Server` or `Sun Enterprise SPARC T5120`

6. **In the Release Is list box:**

   a. **Click the down arrow in the Release Is list box to display a list of matching product folders.**

      A list of one or more product software releases appears.

   b. **Select the check box next to the software release of interest.**

      For example: `X4170 M2 SW 1.4` or `Sun SPARC Enterprise T5120`

7. **Click Search.**

   A Patch Search Results screen appears displaying a list of patch names and descriptions.

8. **In the Patch Search Results screen, select the Patch Name of interest.**

   For example: `X4170 M2 SW 1.4. ILOM and BIOS (Patch)` or `Firmware SPARC Enterprise T5120 Sun System Firmware 7.1.3.2`

9. **In the Patch Name selection, click one of the following actions:**
   - **Readme –** Opens the selected patch Readme file.
   - **Add to Plan** – Adds the selected patch to a new or existing plan.
   - **Download** – Downloads the selected patch.

Oracle ILOM 3.1 Firmware Version Numbering Scheme

Oracle ILOM 3.1 uses a firmware version numbering scheme that helps you to identify the firmware version you are running on your server or chassis monitoring module (CMM). This numbering scheme includes a five-field string, for example, `a.b.c.d.e`, where:

- `a` – Represents the major version of Oracle ILOM.
- `b` – Represents a minor version of Oracle ILOM.
- `c` – Represents the update version of Oracle ILOM.
- `d` – Represents a micro version of Oracle ILOM. Micro versions are managed per platform or group of platforms. See your platform product notes for details.

- `e` – Represents a nano version of Oracle ILOM. Nano versions are incremental iterations of a micro version.

For example, Oracle ILOM 3.1.2.1.a would designate:

- Oracle ILOM 3 as the major version
- Oracle ILOM 3.1 as a minor version
- Oracle ILOM 3.1.2 as the second update version
- Oracle ILOM 3.1.2.1 as a micro version
- Oracle ILOM 3.1.2.1.a as a nano version of 3.1.2.1

Tip – To identify the Oracle ILOM firmware version installed on your server or CMM, click System Information > Firmware in the web interface, or type `version` in the command-line interface.

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`

Oracle ILOM Overview

Description	Links
Refer to these topics for an overview of Oracle ILOM features, functionality, and supported browsers.	• "About Oracle ILOM" on page 2 • "Oracle ILOM Features and Functionality" on page 2 • "Supported Management Interfaces" on page 4 • "Supported Operating System Web Browsers" on page 5
Refer to this topic for information about integrating third-party management tools.	• "Integration With Other Management Tools" on page 6

Related Information

- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Setting Up a Management Connection to Oracle ILOM and Logging In" on page 1
- *Oracle ILOM 3.1 Protocol Management Reference Guide*, "SNMP Overview" on page 1
- *Oracle ILOM 3.1 Protocol Management Reference Guide*, "Server Managment Using IPMI" on page 111

About Oracle ILOM

Oracle Integrated Lights Out Manager (ILOM) provides advanced service processor (SP) hardware and software that you can use to manage and monitor your Oracle hardware. Oracle ILOM is pre-installed on all Oracle rackmount servers, blade servers, and chassis monitoring modules (CMMs). Oracle ILOM is a vital management tool in the data center and can be integrated with other data center management tools already installed on the server.

Oracle ILOM enables you to experience a single, consistent, and standards-based service processor across all Oracle servers and CMMs. This means you will have:

- Single, consistent system management interfaces for operators
- Support for rich and standard protocol
- Third-party management tools and interfaces
- Integrated system management functions at no extra cost

The Oracle ILOM service processor (SP) runs its own embedded operating system and has a dedicated Ethernet port, which together provide out-of-band management capability. Oracle ILOM automatically initializes as soon as power is applied to the server. It provides a full-featured, browser-based web interface and has an equivalent command-line interface (CLI). There is also an industry-standard SNMP interface and IPMI interface.

Related Information

- "Oracle ILOM Features and Functionality" on page 2
- "Supported Management Interfaces" on page 4
- "Supported Operating System Web Browsers" on page 5
- "Integration With Other Management Tools" on page 6

Oracle ILOM Features and Functionality

Oracle ILOM offers a full set of features, functions, and protocols that will help you monitor and manage your server systems.

TABLE: Oracle ILOM Features and Functionality

Oracle ILOM Feature	What You Can Do
Newly designed web and command-line interfaces	Display high-level information in a simple, standardized format that is common across x86 SP, SPARC SP, and CMM platforms.
Dedicated service processor and resources	• Manage the server without consuming system resources. • Continue to manage the server using standby power even when the server is powered off.
Simple Oracle ILOM initial configuration	• Oracle ILOM automatically learns the network address of the server SP or CMM using IPv4 and IPv6 default settings. • Configure BIOS settings on the x86 SP platform.
Downloadable firmware updates	• Download firmware updates using the browser-based web interface.
Remote hardware monitoring	• Monitor system health and system event logs. • Monitor hardware event logs. • Monitor audit event logs. • Monitor customer-replaceable units (CRUs) and field-replaceable units (FRUs), including power supplies, fans, host bus adapters (HBAs), PCI devices, disks, CPUs, memory, and motherboard. • Monitor environmental temperatures (component temperatures).
Hardware and FRU inventory and presence	• Identify installed CRUs and FRUs and their status. • Identify part numbers, versions, and product serial numbers. • Identify NIC card MAC addresses.
Remote KVMS	• Redirect the system serial console through serial port and LAN. • Access keyboard, video, and mouse (KVM) on remote x86 systems and on some SPARC systems. • Redirect the OS graphical console to a remote client browser. • Connect a remote CD/DVD/floppy to the system for remote storage.
System power control and monitoring	• Power the system on or off, either locally or remotely. • Force power-off for immediate shutdown or perform a graceful shutdown to shut down the host operating system before power-off. • Monitor power management and power history charts through the web interface.

TABLE: Oracle ILOM Features and Functionality *(Continued)*

Oracle ILOM Feature	What You Can Do
Configuration and management of user accounts	• Configure local user accounts. • Authenticate user accounts using LDAP, LDAP/SSL, RADIUS, and Active Directory.
Error and fault management	• Log events in a consistent method for all "service" data. • Monitor hardware and system-related errors, as well as ECC memory errors, reported on a dedicated user interface page, and into SP logs, syslog, and remote log host. • Oracle ILOM automatically clears most fault conditions after you perform a service action to address the fault.
System alerts, including SNMP traps, IPMI PETs, remote syslog, and email alerts	• Monitor components using industry-standard SNMP commands and the IPMItool utility.

Supported Management Interfaces

This documentation provides conceptual and procedural information for the Oracle ILOM web and command-line interfaces. However, to access all of the Oracle ILOM features and functions, you can choose to use any of, or a combination of all, the following interfaces and protocols.

- **Web interface** – The web interface enables you to access the Oracle ILOM SP or CMM through a web browser. From the Oracle ILOM web interface, you can perform daily system management operations remotely. Additionally, from the web interface, you can launch tools to redirect KVMS, or to perform maintenance and diagnostic operations.
- **Command-line interface (CLI)** – Using an SSH client, you can access the Oracle ILOM CLI on the server SP or CMM. This command-line interface enables you to perform server management operations remotely using industry-standard DMTF-style keyboard commands and scripting protocols.
- **Intelligent Platform Management Interface (IPMI)** – IPMI is an open, industry-standard interface that was designed for the management of server systems over a number of different types of networks. IPMI functionality includes field-replaceable unit (FRU) inventory reporting, system monitoring, logging of system events, system recovery (including system resets and power-on and power-off capabilities), and alerting.
- **WS-Management/CIM** – As of version 3.0.8, Oracle ILOM supports the use of the Distributed Management Task Force (DMTF) Web Services for Management (WS-Management) protocol and Common Information Model (CIM). The support

for these DMTF standards in Oracle ILOM enables developers to build and deploy network management applications to monitor and manage information about Oracle system hardware.

- **Simple Network Management Protocol (SNMP) interface** – Oracle ILOM also provides an SNMP v3 interface for third-party applications such as HP OpenView and IBM Tivoli. Some of the MIBs supported by Oracle ILOM include:
  - SUN-PLATFORM-MIB
  - SUN-ILOM-CONTROL-MIB
  - SUN-HW-TRAP-MIB
  - SUN-ILOM-PET-MIB
  - SNMP-FRAMEWORK-MIB (9RFC2271.txt)
  - SNMP-MPD-MIB (RFC2572)
  - System and SNMP groups from SNMPv2-MIB (RFC1907)
  - entPhysicalTable from ENTITY-MIB (RFC2737)

Related Information

- "Log In to the Oracle ILOM Web Interface" on page 11
- "Log In to the Oracle ILOM CLI" on page 11
- *Oracle ILOM 3.1 Protocol Management Reference Guide,* "Server Managment Using IPMI" on page 111
- *Oracle ILOM 3.1 Protocol Management Reference Guide,* "Server Management Using WS-Management and CIM" on page 133
- *Oracle ILOM 3.1 Protocol Management Reference Guide,* "SNMP Overview" on page 1
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting Up a Management Connection to Oracle ILOM and Logging In" on page 1

Supported Operating System Web Browsers

Oracle ILOM supports the following operating system web browsers.

Note – For a list of operating systems supported by the Oracle server, refer to the server administration guide or product notes.

TABLE: Supported Web Browsers

Operating System	Web Browser
Oracle Solaris 10	• Mozilla 1.4 and 1.7 • Firefox 3.6.x and 6
Linux (Oracle, Red Hat, SuSE, Ubuntu 10.10)	• Firefox 3.6.x and 6
Microsoft Windows (XP Service Pack 2, Windows 7)	• Internet Explorer 7.x, 8.x (for Windows XP Service Pack 2), and 9 (for Windows 7) • Firefox 3.6.x and 6
Macintosh (OSX v10.6 and later)	• Firefox 3.6.x and 6 • Safari – all

Related Information

- "Redesigned Web Interface as of Oracle ILOM 3.1" on page 14
- "Log In to the Oracle ILOM Web Interface" on page 11

Integration With Other Management Tools

You can easily integrate Oracle ILOM with other management tools and processes. A description of the supported third-party system management tools and their support for Oracle systems is available at:

`http://www.oracle.com/technetwork/server-storage/servermgmt/tech/isv-hardware-connectors/index.html`

For information about the Oracle Enterprise Ops Center management tool, see "About Oracle Enterprise Manager Ops Center" on page 7.

About Oracle Enterprise Manager Ops Center

Oracle Enterprise Manager Ops Center can help you discover new and existing Oracle systems on your network. For instance, you can use Oracle Enterprise Manager Ops Center to:

- Update the server to the latest firmware and BIOS image.
- Provision the operating environment with off-the-shelf distributions or Oracle Solaris images.
- Manage updates and configuration changes.
- Remotely control key aspects of the service processor such as boot control, power status, and indicator lights.

For more information about Oracle Enterprise Manager Ops Center, go to: http://www.oracle.com/in/products/enterprise-manager/enterprise-manager-opscenter-044497-en-in.html

Getting Started With Oracle ILOM 3.1

Description	Links
Refer to this section for topics describing instructions for logging in to the Oracle ILOM CLI and web interfaces.	• "Logging In to Oracle ILOM" on page 10
Refer to this section for topics describing the newly redesigned Oracle ILOM 3.1 web interface, as well as topics describing navigation options available for a managed device.	• "Navigating the Redesigned 3.1 Web Interface" on page 13
Refer to this section for topics describing the updated Oracle ILOM 3.1 CLI namespace, as well as topics describing instructions for issuing CLI commands.	• "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22

Related Information

- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Setting Up a Management Connection to Oracle ILOM and Logging In" on page 1
- *Oracle ILOM 3.1 Protocol Management Reference Guide*, "Server Managment Using IPMI" on page 111
- *Oracle ILOM 3.1 Protocol Management Reference Guide*, "SNMP Overview" on page 1

Logging In to Oracle ILOM

Network Requirements for Logging In

Before logging in to Oracle ILOM over a network connection, you must:

- **Establish a physical network management connection to the server SP or CMM from an internal trusted network or dedicated secure management or private network.**
- **Obtain the network address assigned to the server SP or CMM**.

  The accepted input format for entering IPv4 and IPv6 addresses are as follows:

Note – When entering an IPv6 address or Link-Local IPv6 address, the address must be enclosed within brackets to work correctly. However, when you specify an IPv6 address to log in to Oracle ILOM using SSH, *do not* enclose the IPv6 address in brackets.

  - **IPv4 address** – `192.0.2.0`
  - **IPv6 address** – `[2001:db8:0:0:0:0:0:0/32]`
  - **IPv6 address using SSH and root user account** – **`ssh root@`***ipv6address*
  - **Link-Local IPv6 address** – `[e80::214:4fff:feca:5f7e/64]`
  - **DNS host domain address** – `company.com`
- **If you do not have an Oracle ILOM user account, you will need to obtain a user account from your Oracle ILOM system administrator.**

Related Information

- "Supported Operating System Web Browsers" on page 5
- "Log In to the Oracle ILOM Web Interface" on page 11
- "Log In to the Oracle ILOM CLI" on page 11
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting Up a Management Connection to Oracle ILOM and Logging In" on page 1

- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting Up and Maintaining User Accounts" on page 27

▼ Log In to the Oracle ILOM Web Interface

Before You Begin

Meet the requirements described in "Network Requirements for Logging In" on page 10.

1. **In a web browser, type the IPv 4 or IPv 6 address for the server SP or CMM.**

   The Oracle Integrated Lights Out Manager Login page appears.

2. **Type a user name and password, and then click Log In.**

Note – To enable first-time login and access to Oracle ILOM, a default Administrator account and its password are provided with the system. To build a secure environment, you must change the default password (`changeme`) for the default Administrator account (`root`) after your initial login to Oracle ILOM. If this default Administrator account has since been changed, contact your system administrator for an Oracle ILOM user account.

Related Information

- "Supported Operating System Web Browsers" on page 5
- "Network Connection Issues: Oracle ILOM Interfaces" on page 64
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Resolving Web Browser Security Settings" on page 111
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting Up a Management Connection to Oracle ILOM and Logging In" on page 1
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Default Timeout for CLI and Web Sessions" on page 75
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Password Recovery for root Account" on page 35

▼ Log In to the Oracle ILOM CLI

Before You Begin

Meet the requirements described in "Network Requirements for Logging In" on page 10.

1. **Using a Secure Shell (SSH) session, log in to Oracle ILOM in one of the following ways:**

   - **If you are logging in with the default `root` account password**, type the following at the system prompt:

     `$` **`ssh root@`***system-ip-address*

Note – To enable first-time login and access to Oracle ILOM, a default Administrator account and its password are provided with the system. To build a secure environment, you must change the default password (`changeme`) for the default Administrator account (`root`) after your initial login to Oracle ILOM. If this default Administrator account has since been changed, contact your system administrator for an Oracle ILOM user account.

   - **If you are logging in with a user account that was created for you** by the system administrator, type the following at the system prompt:

     `$` **`ssh`** *system-ip-address*

   If Oracle ILOM is operating in a dual-stack network environment, you can enter the *system-ip-address* in either an IPv4 or IPv6 address format.

2. **At the system prompt, type the password of your user account (for the default `root` account, this is `changeme`).**

   `Password:` *password*

   The Oracle ILOM CLI prompt appears (->).

   For example:

```
Oracle(R) Integrated Lights Out Manager

Version 3.1.0.0 r54408

Copyright (c) 2011, Oracle and/or its affiliates. All rights
reserved.

->
```

Related Information

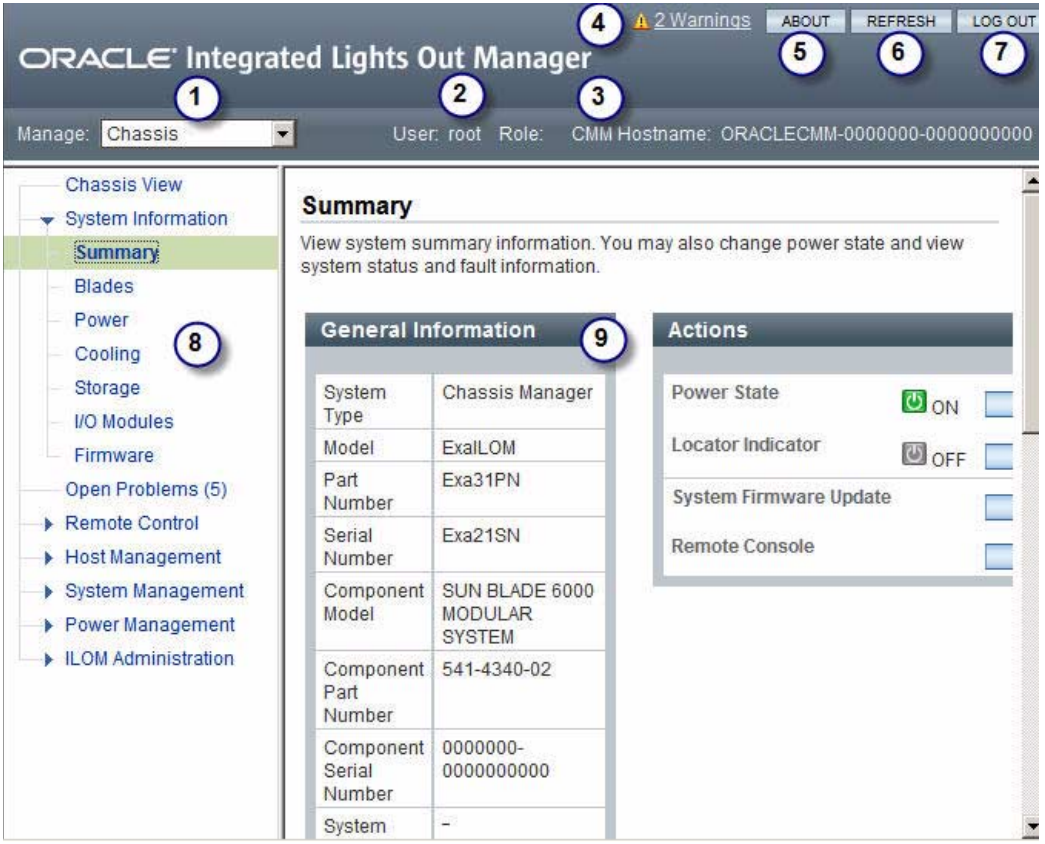
- "Network Connection Issues: Oracle ILOM Interfaces" on page 64
- "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting Up a Management Connection to Oracle ILOM and Logging In" on page 1
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Default Timeout for CLI and Web Sessions" on page 75

- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Password Recovery for root Account" on page 35

Navigating the Redesigned 3.1 Web Interface

Redesigned Web Interface as of Oracle ILOM 3.1

FIGURE: Redesigned 3.1 Web Interface



Number	Description
1	**Manage list box** – Appears only with a CMM connection to Oracle ILOM. Click the arrow to view the blades in the chassis, and click a blade to manage that blade.
2	**User and Role fields** – Displays the user name and role of the user who is currently logged in to the web interface.
3	**CMM Hostname (for CMM connection) or Server (for SP connection)** – Displays the host name of the CMM or server SP.

Number	Description
4	**Warning message** – Displays the number of warnings that Oracle ILOM has detected on the CMM or SP that you are managing. You can define warning thresholds and define when and where you receive alerts from the ILOM Administration > Notifications page. For more information, refer to *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting Up Alert Notifications and Syslog Server for Event Logging" on page 167.
5	**About button** – Click to view product copyright information.
6	**Refresh button** – Click to refresh the information in the content pane of the interface. The Refresh button does not save new data that you might have entered or selected on the page.
7	**Log Out button** – Click to end the current session of the web interface.
8	**Navigation pane** – A hierarchical menu that enables you to navigate through the web interface, replacing the navigation tabs from the Oracle ILOM 3.0 web interface.
9	**Content pane** – Displays the content of each page to which you navigate.

Web Interface Navigation Options for Managed Devices

The following table describes the web interface navigation options available for managed devices.

Note – The CMM and SP navigation options presented in the web interface might differ slightly depending on the Oracle ILOM firmware version currently installed on the managed device.

TABLE: Web Interface Navigation Options for Managed Devices

First-Level Menu	Second- and Third-Level Menu	What You Can Do	Managed Device
Chassis View		View a graphical representation of the front and rear view of the chassis, including the blades and monitoring modules installed in the chassis.	CMM
System Information			
	Summary	View summary information about the system. You can also perform the following actions: • Turn the system power state off or on. • Locate the system in the chassis by turning on or off the system indicator LED. • Update the system firmware. • Launch the Remote Console. • View overall system status and problem count for the entire system.	Server SP CMM
	Blades	View summary and detailed information about the blades, monitoring modules, and NEMs in the blade chassis.	CMM
	Processors	View summary and detailed information about the processors in the system.	Server SP
	Memory	View summary and detailed information about the memory installed in the system.	Server SP
	Power	View summary and detailed information about the power supplies in the system.	Server SP CMM
	Cooling	View summary and detailed information about the fans that cool the system.	Server SP

TABLE: Web Interface Navigation Options for Managed Devices *(Continued)*

First-Level Menu	Second- and Third-Level Menu	What You Can Do	Managed Device
	Storage	View summary information about the storage in the SP or CMM. Oracle ILOM reports on the following storage: • Disks • Volumes (including logical volumes) • Controllers • Expanders	Server SP CMM
	I/O Modules	View summary and detailed information about the I/O modules in the system.	CMM
	Networking	View summary and detailed information about system networking.	Server SP
	PCI Devices	View summary and detailed information about the PCI devices in the system.	Server SP
	Firmware	View the current firmware levels and choose to upgrade the firmware, if needed.	Server SP CMM
Open Problems		View information about systems and subsystems that are in a faulted state.	Server SP CMM
Remote Control			
	Redirection	Manage the host remotely by redirecting the system console to your local machine.	Server SP CMM
	KVMS	Enable or disable the remote management state of the keyboard, video, mouse, or storage device.	Server SP
Host Management			
	Power Control	Select a power state: Immediate Power Off, Graceful Shutdown and Power Off, Power On, Power Cycle, or Reset.	Server SP CMM

TABLE: Web Interface Navigation Options for Managed Devices *(Continued)*

First-Level Menu	Second- and Third-Level Menu	What You Can Do	Managed Device
	Diagnostics	Enable or disable diagnostics for x86 processor–based systems or SPARC processor–based systems.	Server SP
	Host Control	View and configure the host control information. Configure the boot device at the next system power-on.	Server SP
System Management			
	BIOS	Manage the BIOS configuration backup and restore.	Server SP
	SAS Zoning	Enable or disable Zone Manager settings and reset the Zone Manager password.	CMM
	Policy	Enable or disable system policies, such as managing the chassis power, forcing power supply fans to run on high or low, and monitoring specific power supplies.	Server SP CMM
Power Management			
	Consumption	View power consumption metrics for actual power and permitted power, as well as set power consumption thresholds to generate email alerts or SNMP notifications.	Server SP CMM
	Limit	View or configure server power limits.	Server SP
	Allocation	View system power requirements for capacity planning.	Server SP CMM
	Settings	Configure policy options for power consumption on SPARC servers.	SPARC
	Redundancy	View and configure CMM power supply redundancy options.	CMM
	Statistics	View power statistical data for the Oracle server or blade chassis server.	Server SP CMM

TABLE: Web Interface Navigation Options for Managed Devices *(Continued)*

First-Level Menu	Second- and Third-Level Menu	What You Can Do	Managed Device
	History	View a history of rolling averages for power consumption.	Server SP CMM
ILOM Administration			
	Identification	Enter or change the service processor identification information by assigning a host name or system identifier.	Server SP CMM
	Logs > Event	View various details about each particular event, including the event ID, class, type, severity, date and time, and description of the event.	Server SP CMM
	Logs > Audit	View interface-related user actions such as user logins, logouts, configuration changes, and so on.	Server SP CMM
	Management Access > Web Server	Edit or update the web server settings, such as the HTTP web server or the HTTP port.	Server SP CMM
	Management Access > SSL Certificate	View information about the default SSL certificate, or optionally find and enter a new SSL certificate.	Server SP CMM
	Management Access > SNMP	Edit or update SNMP settings.	Server SP CMM
	Management Access > SSH Server	Configure Secure Shell (SSH) server access and key generation.	Server SP CMM
	Management Access > IPMI	Use a command-line interface to monitor and control your server platform, as well as to retrieve information about your server platform.	Server SP CMM
	Management Access > CLI	Configure the CLI settings. The Session Time-out value indicates the number of idle minutes that can lapse before automatic CLI logout occurs.	Server SP CMM

TABLE: Web Interface Navigation Options for Managed Devices *(Continued)*

First-Level Menu	Second- and Third-Level Menu	What You Can Do	Managed Device
	Management Access > WS-MAN	Configure the WS-Management settings. WS-Management is a Web Services and SOAP–based protocol for managing servers and devices.	Server SP
	Management Access > Banner Messages	View and configure a message that appears prior to login and the login message that appears after user login.	Server SP CMM
	User Management > Active Sessions	View the users who are currently logged in to Oracle ILOM, and the type of session each user initiated.	Server SP CMM
	User Management > User Accounts	Add, delete, or modify local Oracle ILOM user accounts.	Server SP CMM
	User Management > LDAP	Configure Oracle ILOM access for LDAP users.	Server SP CMM
	User Management > LDAP/SSL	Configure Oracle ILOM access for LDAP users with enhanced security settings enabled by Secure Socket Layer (SSL) technology.	Server SP CMM
	User Management > RADIUS	Configure Oracle ILOM access for RADIUS users.	Server SP CMM
	User Management > Active Directory	Configure Oracle ILOM access for Active Directory users.	Server SP CMM
	Connectivity > Network	View and edit the IPv4 and IPv6 network settings for Oracle ILOM and for local interconnect interface settings.	Server SP CMM
	Connectivity > DNS	Specify host names, and have those host names resolved into IP addresses using the Domain Name Service (DNS).	Server SP CMM
	Connectivity > Serial Port	View and edit the baud rate of the internal and external serial ports.	Server SP CMM
	Configuration Management > Backup/Restore	Back up and restore the service processor configuration to a remote host or removable storage device in a secure manner.	Server SP CMM

TABLE: Web Interface Navigation Options for Managed Devices *(Continued)*

First-Level Menu	Second- and Third-Level Menu	What You Can Do	Managed Device
	Configuration Management > Reset Defaults	Manage the service processor configuration data.	Server SP CMM
	Notifications > Alerts	View details about each alert, and change the list of configured alerts.	Server SP CMM
	Notifications > Syslog	Configure the server addresses to which the syslog messages will be sent.	Server SP CMM
	Notifications > SMTP Client	Configure the state of the SMTP client, which is used for sending email notifications of alerts.	Server SP CMM
	Date and Time > Clock	View and edit the Oracle ILOM clock time manually, or synchronize the Oracle ILOM clock with an NTP server.	Server SP CMM
	Date and Time > Timezone	Specify a particular time zone so that time stamps displayed by the service processor can be correlated to logs created elsewhere (for example, in the Oracle Solaris Operating System).	Server SP CMM
	Maintenance > Firmware Upgrade	Start the process to obtain an upgrade of the Oracle ILOM firmware.	Server SP CMM
	Maintenance > Reset Components	Reset the service processor and CMM components.	Server SP CMM
	Maintenance > Snapshot	Collect environmental, log, error, and FRUID data and send it to a USB flash drive, or an external host using the CLI, or as a downloaded file.	Server SP CMM

CMM Web Interface: Blade Server Views

The CMM web interface supports blade servers running Oracle ILOM firmware version 3.0.x and 3.1.x. If you click a blade server running Oracle ILOM 3.1 in the CMM web interface, the newly designed 3.1 web interface appears. If you click a blade server running Oracle ILOM 3.0 in the CMM web interface, the legacy 3.0 web interface appears.

Navigating the Command-Line Interface (CLI) Namespace Targets

Case Insensitivity in the Oracle ILOM 3.1 and Later CLI

As of Oracle ILOM 3.1, the Oracle ILOM command-line interface is case insensitive, that is, Oracle ILOM does not distinguish between uppercase and lowercase characters. The following are exceptions to this rule:

- targets and properties under the `/SYS` legacy target for server service processors (SPs)
- targets and properties under the `/CH` legacy target for chassis monitoring modules (CMMs)
- command verbs, such as `show`, `set`, and `start`
- property values

Oracle ILOM 3.1 CLI Namespace Targets

The Oracle ILOM 3.1 CLI namespace is a hierarchical tree that contains every manageable object for a managed device.

The following table describes the CLI namespace targets available in Oracle ILOM 3.1. The targets listed in the following table are at the highest level in the hierarchy.

Namespace Target	Managed Device	Description
/SP	All servers	On rackmount or blade servers, the targets and properties under this target are used for configuring the Oracle ILOM service processor (SP) and for viewing logs, managing components, and accessing consoles. You can access the blade server /SP target from the chassis monitoring module (CMM) CLI. For more information, see "Managing Blade Servers From the CMM CLI" on page 26.
/CMM	All CMMs	On a blade chassis, this target replaces /SP and is used for configuring the Oracle ILOM chassis monitoring module (CMM).
/HOST	All servers	On rackmount or blade servers, the targets and properties under this target are used to monitor and manage the host operating system.
/System	All servers and CMMs	On rackmount servers, blade servers, or blade chassis, the targets and properties under this target are used to monitor inventory status and environmental sensors. Some management tasks, such as firmware maintenance and service tasks, are available. The targets under this target directly correspond to the names of the hardware components (for either the server or chassis depending on whether you logged in to an SP or CMM), some of which are printed on the physical hardware.
/Servers	All CMMs	On a blade chassis, the targets and properties under this target are used to monitor inventory status and environmental sensors, as well as to manage components of blades in the chassis. Targets you would normally see when logged into the blade service processor are available (such as /SP, /HOST, /System, and so forth). Legacy targets (such as /SYS and /STORAGE) would also be visible if enabled for the server.

Namespace Target	Managed Device	Description
/SYS (3.0 legacy target)	All servers and CMMs	This is a pre-Oracle ILOM 3.1 legacy target, and is only visible when CLI legacy_targets are enabled (from the SP or CMM). On rackmount or blade servers, this target type is similar to the /System target, but includes all targets available for Oracle ILOM 3.0. The targets and properties under this target are always available (whether you see them or not) to ensure backward compatibility with existing Oracle ILOM user scripts.
/STORAGE (3.0 legacy target)	All servers and CMMs	• For a rackmount or blade server, this is a pre-Oracle ILOM 3.1 legacy target, and is only visible when CLI legacy_targets are enabled from the SP. This target is similar to the /System/Storage target and was available with earlier versions of Oracle ILOM. The targets and properties under this target are always available (whether they are visible or hidden) to ensure backward compatibility with existing Oracle ILOM user scripts. • For a blade chassis, this target is used to manage chassis storage (that is, storage on storage blades). Chassis storage can be assigned to blade servers in the chassis.
/CH (3.0 legacy target)	All CMMs	This is a pre-Oracle ILOM 3.1 legacy target, and is only visible when CLI legacy_targets are enabled from the CMM. On a blade chassis, the targets and properties below this target are used to monitor inventory status and environmental sensors, as well as to access and manage components (such as BL, which indicates an installed server or storage blade). The targets under this target directly correspond to the names of the hardware components.

For more information on available targets, see:

- "Default Oracle ILOM 3.1 Targets" on page 24
- "Show or Hide Oracle ILOM 3.0 CLI Legacy Targets" on page 27
- "Navigating to Targets and Listing Their Properties and Supported Commands" on page 29
- "Show or Hide Oracle ILOM 3.0 CLI Legacy Targets" on page 27

Default Oracle ILOM 3.1 Targets

Here is an example of the namespace hierarchy for a server and blade chassis that ships with Oracle ILOM 3.1 or later installed. Actual targets displayed vary from system to system. Legacy targets are hidden by default.

TABLE: Oracle ILOM 3.1 CLI Targets

Server (Connected through SP)	Blade Chassis (Connected through CMM)
/HOST	**/STORAGE**
bootmode (SPARC only)	sas_zoning
console	**/System**
diag	Cooling
domain (SPARC only)	Power
provisioning (x86 only)	Storage
tpm (SPARC only)	Firmware
	Open_Problems
	IO_Modules
	Blades
/System	**/CMM**
Cooling	alertmgmt
Processors	cli
Memory	clients
Power	clock
Storage	config
PCI_Devices	diag
Firmware	faultmgmt
Networking	firmware
Open_Problems	logs
BIOS (x86 only)	network
IO_Modules	policy
	powermgmt
	preferences
	serial
	services
	sessions
	users

TABLE: Oracle ILOM 3.1 CLI Targets *(Continued)*

Server (Connected through SP)	Blade Chassis (Connected through CMM)
/SP	**/Servers**
alertmgmt	Blade_0
cli	Blade_1
clients	Blade_2
clock	Blade_3
config	Blade_4
diag	Blade_5
faultmgmt	Blade_6
firmware	Blade_7
logs	Blade_8
network	Blade_9
policy	
powermgmt	
preferences	
serial	
services	
sessions	
users	

For more information on available targets, see:

- "Oracle ILOM 3.1 CLI Namespace Targets" on page 23
- "Show or Hide Oracle ILOM 3.0 CLI Legacy Targets" on page 27

Managing Blade Servers From the CMM CLI

In Oracle ILOM 3.0 and earlier, a chassis monitoring module (CMM) command-line interface (CLI) session provided limited information about blade servers in the chassis. To manage a blade server, you had to log in to the blade server service processor (SP), or launch a CLI session for the SP from the CMM CLI as follows:

```
start /CH/BLn/SP/cli
```

As of Oracle ILOM 3.1, you can manage a blade server directly from the CMM CLI if Single Sign-On is enabled on the blade server SP. When Single Sign-On is enabled, the `/Servers/Blades/Blade_`*n* target on the CMM is equivalent to the `/` target on the blade server SP. You still have the option of logging in to the blade server SP directly.

Related Information

- "Show or Hide Oracle ILOM 3.0 CLI Legacy Targets" on page 27

Show or Hide Oracle ILOM 3.0 CLI Legacy Targets

As of Oracle ILOM 3.1, the `/SYS`, `/STORAGE` (for servers), and `/CH` (for blade chassis) namespaces have been replaced by `/System`. The `/System` namespace is a simplified version of `/SYS`, redesigned for clarity and ease of use.

You can still issue commands to the `/SYS`, `/STORAGE`, and `/CH` namespace targets on systems running Oracle ILOM 3.1, even though these legacy targets might be hidden. This backward compatibility ensures that commands and scripts that were valid in Oracle ILOM 3.0 will continue to work in Oracle ILOM 3.1.

You can optionally unhide the `/SYS`, `/STORAGE` and `/CH` namespace targets by issuing one of the following commands.

- For a server service processor, type:

  ```
  set /SP/cli legacy_targets=enabled
  ```

- For a blade chassis CMM, type:

  ```
  set /CMM/cli legacy_targets=enabled
  ```

  When you enable legacy targets on the CMM and Single-Sign On on a blade server SP, you can manage the blade server directly from the `/CH/BL`*n* target in the CMM CLI. For more information, see "Managing Blade Servers From the CMM CLI" on page 26.

Note – For systems that upgrade to Oracle ILOM 3.1 from an earlier version of Oracle ILOM, legacy targets are enabled by default.

The following table lists examples of legacy targets that are applicable to Oracle servers and CMMs:

Server (Connected through SP)	Blade Chassis (Connected through CMM)
/SYS	**/CH**
MB	CMM
MB_ENV	MIDPLANE
SP	BL*n* (server blades have HOST, System, and SP targets)
USBBD	BL*n* (storage blades have HDD and enclosure targets)
DVD	NEM*n*
PSn	FM*n*
DBPn	PS*n*
PWRBS	T_AMB
INSTSW	HOT
SASBP	VPS
PDB	OK
CONNBD	SERVICE
FANBD	TEMP_FAULT
VPS_CPUS	LOCATE
VPS_MEMORY	
VPS	
T_AMB	
OK	
LOCATE	
SERVICE	
PS_FAULT	
TEMP_FAULT	
FAN_FAULT	
/STORAGE	
raid	

Related Information

- "Oracle ILOM 3.1 CLI Namespace Targets" on page 23
- "Navigating to Targets and Listing Their Properties and Supported Commands" on page 29
- "Using the Command-Line Interface" on page 111
- "Show or Hide Oracle ILOM 3.0 CLI Legacy Targets" on page 27

Navigating to Targets and Listing Their Properties and Supported Commands

Use the `help targets` command to list all available targets in the CLI namespace for your system with a brief description:

`help targets`

Use the `cd` command to navigate the namespace hierarchy. For example, to navigate to the `services` target under `/SP`, type:

`cd /SP/services`

Use the `show` command (or `ls`) to list the targets immediately under the current target and the commands that can be used with the current target. For example, after navigating to the `services` target, issue the `show` command to view the targets and commands for the `services` target:

```
-> show

 /SP/services
 Targets:
 http
 https
 ipmi
 kvms
 servicetag
 snmp
 ssh
 sso
 wsman

 Properties:

 Commands:
 cd
 show

->
```

Note – You can issue commands from anywhere in the CLI hierarchy as long as you use a fully qualified path and the command is supported by the intended target. In the previous example, you could have entered **`show /SP/services`** to yield the same result.

If a target has properties, the `show` command is also used to list the current properties.

The `show` command output can be displayed in a simple list:

```
-> show http
/SP/services/http
 Targets:

 Properties:
 port = 80
 secureredirect = enabled
 servicestate = disabled
 sessiontimeout = 15

 Commands:
 cd
 set
 show

->
```

The `show` command output can also be displayed in a table:

```
-> show -o table http
Target               | Property               | Value
---------------------+------------------------+--------------
/SP/services/http    | port                   | 80
/SP/services/http    | secureredirect         | enabled
/SP/services/http    | servicestate           | disabled
/SP/services/http    | sessiontimeout         | 15

->
```

For any target, you can use the `help` command to display properties, supported values, and roles required to configure target properties.

Note – Not all targets have configurable properties. Some are view only.

For example, to obtain help information for the `http` target, which is used to configure the Oracle ILOM internal web server for HTTP access, type:

```
-> help /SP/services/http

 /SP/services/http : HTTP service
```

```
  Targets:

  Properties:
  port : Port number for http service
  port : User role required for set = a

  secureredirect : HTTP secure redirect
  secureredirect : Possible values = enabled, disabled
  secureredirect : User role required for set = a

  servicestate : HTTP service state
  servicestate : Possible values = enabled, disabled
  servicestate : User role required for set = a

  sessiontimeout : Timeout in minutes for http session
  sessiontimeout : Possible values = Range: 1-720 minutes
  sessiontimeout : User role required for set = a

->
```

Related Information

- "Case Insensitivity in the Oracle ILOM 3.1 and Later CLI" on page 22
- "Oracle ILOM 3.1 CLI Namespace Targets" on page 23
- "Show or Hide Oracle ILOM 3.0 CLI Legacy Targets" on page 27
- "Using the Command-Line Interface" on page 111

Collecting System Information, Monitoring Health Status, and Initiating Host Management

Description	Links
Refer to this section for topics describing how to gather system information and view subcomponent health details.	• "Collecting Information, Status, and Initiating Common Actions" on page 34
Refer to this section for topics describing how to view open problems and determine required service actions.	• "Administering Open Problems" on page 41
Refer to this section for topics describing how to access and manage logging entries for system events and user actions.	• "Managing Oracle ILOM Log Entries" on page 45
Refer to this section for topics describing how to perform common system management actions from the web interface.	• "Performing Commonly Used Host Management Actions (Web)" on page 50

Related Information

- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Configuring Host Server Management Actions" on page 147
- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Setting System Management Power Source Policies" on page 175
- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Setting Up Alert Notifications and Syslog Server for Event Logging" on page 167

Collecting Information, Status, and Initiating Common Actions

Oracle ILOM interfaces provide easy-to-access properties for viewing system information and administering commonly used host management actions, for example:

- From the web interface Summary page or from the CLI `/System` target, you can, at a glance, collect system-specific information describing the managed device, determine the health state of the managed device, and view open problems, if detected on a managed device.
- From the Actions panel on the Summary page, you can view and modify commonly used host management properties such as the host power state and Locator LED indicator state. Or, you can initiate commonly used system management actions such as performing a firmware update or launching the Oracle ILOM Remote Console.

For instructions on how to collect device information, monitor the health of the managed device, or to perform commonly used host management tasks, see these topics:

- "View System-Level Information and Health Status (Web)" on page 34
- "View Subcomponent-Level Information and Health Status (Web)" on page 35
- "View System-Level Information and Health Status (CLI)" on page 36
- "View Subcomponent-Level Information and Health Status (CLI)" on page 37
- "Health State: Definitions" on page 40
- "Performing Commonly Used Host Management Actions (Web)" on page 50

▼ View System-Level Information and Health Status (Web)

The system-level health status properties for the host server or the CMM are viewable from the Summary page in the web interface.

1. **To view system-level health status details, click System Information > Summary.**

   The Summary page appears.

2. **To collect system information about the managed device, review the entries shown in the General Information table.**

   Entries shown in the General Information table can include model number, serial number, system type, firmware currently installed, primary operating system installed, host MAC address, IP address for the managed SP or CMM, and MAC address for the managed SP or CMM.

Note – The property value for the Primary Operating System installed on the managed device is shown only when the Oracle ILOM Hardware Management Pack is installed on the managed device.

---

3. **To identify problems detected on the managed device or to view the total problem count, review the entries shown in the Status table.**

   The overall health status and total problem count appear at the top of the table.

   To view additional information about a subcomponent category reported in the Status table, click the link in the Subsystem column.

4. **To view the firmware history installed on the managed device, click System Information > Firmware.**

Related Information

- "Health State: Definitions" on page 40
- "View Subcomponent-Level Information and Health Status (Web)" on page 35
- "Administering Open Problems" on page 41

▼ View Subcomponent-Level Information and Health Status (Web)

The subcomponent-level health status properties for the host server or the CMM are viewable from the Summary page in the web interface.

1. **To view subcomponent-level health status properties, click System Information > *subcomponent-category-name*.**

   For example:

   - The SP navigation pane shows subcomponent names for: Processors, Memory, Power, Cooling, Networking, Storage, and PCIe devices.

     To view the subcomponent-level health status details for storage devices, click System Information > Storage.

   - The CMM navigation pane shows subcomponent names for: Blades, Power, Cooling, Storage, and I/O Modules.

To view the subcomponent-level heath status details for I/O modules, click System Information > I/O Modules.

2. **On the subcomponent category page, you can:**
   - Determine the overall health for the subcomponent category and the number of subcomponents installed for each category.
   - Determine the health details and the installed location for each subcomponent currently installed on the managed device.
   - View further information about the installed subcomponent by clicking the Details link in the table.

Note – In the DIMM Details page, as of Oracle ILOM 3.1.2, the following format will be used to describe the value for the DIMM Part Number = *Oracle_part number*, *vendor_part_number*. For example: `5111616-01,M393B5270DH0-YK0`; *where:* `5111616-01` is the Oracle part number and `M393B5270DH0-YK0` is the vendor part number.

Related Information

- "Health State: Definitions" on page 40
- "Administering Open Problems" on page 41

▼ View System-Level Information and Health Status (CLI)

The host system-level health status CLI properties are viewable at the `/System` target.

Note – Alternatively, you can issue the CLI legacy `/SYS` target in place of the `/System` target if the managed device previously supported ILOM 3.0.x. If the managed device did not previously support a version of Oracle ILOM 3.0, the legacy `/SYS` target, in Oracle ILOM 3.1, is disabled by default. To enable the CLI legacy `/SYS` target, see "Show or Hide Oracle ILOM 3.0 CLI Legacy Targets" on page 27.

- **To collect system-level information or to verify the system health status, type:**

  `show /System`

  For example:

```
Properties:
 health = OK
health_details = -
open_problems_count = 0
power_state = On
locator_indicator = Off
model = SUN FIRE X4270 M3
type = Rack Mount
part_number = 07011205
serial_number = 0328MSL-1119T4002F
system_identifier = (none)
system_fw_version = ILOM: 3.1.0.0
primary_operating_system = Not Available
host_primary_mac_address = Not Available
ilom_address = 10.123.45.255
ilom_mac_address = 00:12:34:D5:F2:F6
actual_power_consumption = 123 watts
action = (none)
```

Note – The property value for the primary operating system installed on the managed device is shown only when the Oracle ILOM Hardware Management Pack is installed on the managed device.

Related Information

- "Health State: Definitions" on page 40
- "View Subcomponent-Level Information and Health Status (CLI)" on page 37
- "Administering Open Problems" on page 41

▼ View Subcomponent-Level Information and Health Status (CLI)

The host health status CLI properties for sub-components are viewable under the `/System` target.

- **To access subcomponent-level health details from the CLI, type:**

  `show /System/`*subcomponent-category-name*

  Where *subcomponent-category-name* equals one of the subcomponent target names under `show /System`.

  For example:

  - To view server subcomponent health status for memory, type:

    `show /System/Memory`

```
 /System/Memory
 Targets:
DIMMs

Properties:
health = OK
health_details = -
installed_memory = 16 GB
installed_dimms = 2
max_dimms = 16

Commands:
cd
show
```

  - To view server subcomponent health status for a specific DIMM, type:

    `show /System/Memory/DIMMs/DIMM_`*n*

```
/System/Memory/DIMMs/DIMM_0
   Targets:

   Properties:
       health = OK
       health_details = -
       part_number = 001-0003
       serial_number = 00AD0111232F6E432B
       location = P0/D0 (CPU 0 DIMM 0)
       manufacturer = Hynix Semiconductor Inc.
       memory_size = 8 GB

   Commands:
       cd
       show
```

Note – In the DIMM_*n* properties, as of Oracle ILOM 3.1.2, the following format will be used to describe the value for the part_number = *Oracle_part number*, *vendor_part_number*. For example: 5111616-01,M393B5270DH0-YK0; *where:* 5111616-01 is the Oracle part number and M393B5270DH0-YK0 is the vendor part number.

- To view health status details for all blades in a blade system chassis, type:

  show -level all /System/Blades

```
 /System/Blades
 Targets:
 Blade_0
 Blade_1

Properties:
 health = Service Required
 health_details = BL1 (Blade 1) is faulty.
 Type 'show /System/Open_Problems' for details.
 installed_blades = 2
 max_blades = 10

/System/Blades/Blade_0
 Targets:

 Properties:
 health = OK
 health_details = -
 type = Storage Blade
 model = ASSY,BLADE,X6275
 location = BL0 (Blade 0)
 actual_power_consumption = 10 watts
 system_identifier = (none)
 address = Not Available
 part_number = 375-3604-01
 serial_number = Not Available

/System/Blades/Blade_1
 Targets:

 Properties:
 health = Service Required
 health_details = A device necessary to support a configuration
 has failed. Type 'show /System/Open_Problems' for details.
 type = Server Blade
 model = SUN BLADE X6270 M2 SERVER MODULE
 location = BL1 (Blade 1)
```

```
  actual_power_consumption = 56 watts
  system_identifier = ORACLESP-1044FMN00B
  address = Not Available
  part_number = 511-1418-03
  serial_number = 000000-1042B903A6

Commands:
cd
show
```

Related Information

- "Health State: Definitions" on page 40
- "Administering Open Problems" on page 41

Health State: Definitions

Health Status State	Description
OK	The system or subcomponent is in good working order.
Service Required	Oracle ILOM detected a problem on the managed device that will require a service action to resolve the issue. If this status appears at the system level, view the open problems detected on the managed device. If this status appears in the Open Problems table, refer to the URL provided in the table for further details.
Not Available	Oracle ILOM is unable to provide a health status for this component. Oracle ILOM might require the Hardware Management Pack to be installed. For more information, see the Oracle Hardware Management documentation library at: http://www.oracle.com/pls/topic/lookup?ctx=ohmp
Offline	Offline applies to the Prepare to Remove action state of a chassis subcomponent. This status appears when the action property is set to Prepare to Remove and the physical subcomponent is not physically removed from the chassis. **Note -** Not all chassis subcomponents managed by Oracle ILOM support properties for service actions (Prepare to Remove or Return to Service).

Related Information

- "Administering Open Problems" on page 41

Administering Open Problems

Oracle ILOM automatically detects system hardware faults and environmental conditions on a managed device. If a problem occurs on a managed system, Oracle ILOM automatically:

- Illuminates the Server Action LED on the physical device.
- Identifies the faulted condition in an easy-to-read Open Problems table.
- Records system information about the fault condition in the event log.

Upon the repair (or the replacement) of a faulty server component or a faulty Oracle blade chassis field-replaceable unit (FRU), Oracle ILOM automatically clears the fault state from the Open Problems table.

For further information about administering open problems that are detected and reported in Oracle ILOM interfaces, see these topics:

- "Open Problems Terminology" on page 41
- "View Open Problems Detected on a Managed Device" on page 42

Open Problems Terminology

Term	Definition
Faulted state	A *faulted state* indicates the component is present but is unusable or degraded because one or more problems have been diagnosed by Oracle ILOM. Oracle ILOM automatically disables the component to prevent damage to the system.
Open Problems	*Open Problems* refers to the Open Problems page in the web interface or the Open Problems tabular output shown in the CLI. When a problem is detected on a managed device, Oracle ILOM identifies the problem in the Open Problems CLI output or web interface table.
Oracle ILOM Fault Management Shell	The *Oracle ILOM Fault Management Shell* enables Oracle Services personnel to diagnose system problems and, if necessary, to override fault states. Customers should not use this shell unless requested to do so by Oracle Services.

▼ View Open Problems Detected on a Managed Device

Open problems detected on a host server or blade system chassis are viewable from either the Open Problems web page or the `/System/Open_problems` CLI target.

Before You Begin

- Faults reported in the Open Problems table for server components or blade chassis FRUs are automatically cleared upon repair or replacement of the component.
- Faults reported in the Open Problems table for blade chassis customer-replaceable units (CRUs) must be manually cleared from the Open Problems table after repair or replacement of the faulty CRU. For instructions, see "Clear Faults for Undetected Replaced or Repaired Hardware Components" on page 103.

To view host server or blade system chassis open problems using the CLI or web interface, follow this step:

1. **Perform one of the following:**
   - **Web:**

     Click System Information > Open Problems.
   - **CLI:**

     Type: **`show /System/Open_Problems`**
2. **The Open Problems web page and the CLI target report the following information:**
   - The total number of problems detected
   - The time stamp, name, and CLI target for each faulted component
   - The URL for troubleshooting a faulted component

Related Information

- "Managing Oracle Hardware Faults Through the Oracle ILOM Fault Management Shell" on page 95
- "Administering Service Actions: Oracle Blade Chassis NEMs" on page 43
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Performing Firmware Updates" on page 194
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Reset Power to Server SP, NEM SP, or CMM" on page 202

Administering Service Actions: Oracle Blade Chassis NEMs

Oracle ILOM provides a set of properties for removing or returning some Oracle blade chassis network express modules (NEMs) to service. For further information about using these NEM service properties, see these topics:

NEM Service Action Properties

NEM Property	Description
Prepare to Remove (`action=prepare_to_remove`)	Notifies Oracle ILOM that the physical NEM will be removed from the blade chassis NEM slot for repair.
Return to Service (`action=return_to_service`)	Notifies Oracle ILOM that the NEM that was physically removed for repair is returned to the blade chassis NEM slot and is ready for service.

▼ Prepare to Remove or Return a NEM to Service (Web)

Use the CMM properties in the Oracle ILOM web interface to prepare a blade system chassis for when a NEM is being removed or returned to service.

Note – Not all Oracle blade chassis NEMs, managed by Oracle ILOM, support service action states for removing or returning a NEM to service.

Before You Begin

- Review "NEM Service Action Properties" on page 43.
- The Reset and Host Control (`r`) role is required in Oracle ILOM to modify the service action state for a NEM.

1. **In the CMM web interface, click System Information > I/O Modules.**

2. **In the Network Express Module table, perform these step:**

   a. **Click the radio button adjacent to the NEM that needs to be removed or returned to service.**

      To deselect a radio button in the table, click the deselect icon that appears at the top of the radio button column.

   b. **Click the action list box and select one of the following: Prepare to Remove or Return to Service.**

      A confirmation dialog box appears.

   c. **In the confirmation dialog box, click Yes to continue.**

      The health status state for the NEM is updated according to the selected action. For more information, see "Health State: Definitions" on page 40.

▼ Prepare to Remove or Return a NEM to Service (CMM CLI)

Use the CMM properties in the Oracle ILOM CLI to prepare a blade system chassis for when a NEM is being removed or returned to service.

Note – Not all blade system chassis NEMs, managed by Oracle ILOM, support service action states for removing or returning a NEM to service.

Before You Begin

- Review "NEM Service Action Properties" on page 43.
- The Reset and Host Control (`r`) role is required in Oracle ILOM to modify the service action state for a NEM.

1. **In the CMM CLI, type one of the following command to remove or return a NEM to service:**

   `set /Systems/IO_Modules/NEMs/NEM`_n **`action=`***prepare_to_remove* | *return to service*

   Where:

   NEM_*n* equals the NEM slot number in the blade chassis.

   A prompt appears confirming that you want to proceed with the modifications.

Note – Alternatively, you can issue the CLI legacy `/SYS` target in place of the `/System` target if the managed device previously supported ILOM 3.0.x. If the managed device did not previously support a version of Oracle ILOM 3.0, the legacy `/SYS` target, in Oracle ILOM 3.1, is disabled by default. For information on how to enable the CLI legacy `/SYS` target, see "Show or Hide Oracle ILOM 3.0 CLI Legacy Targets" on page 27.

2. **At the prompt, type `Yes` to continue.**

   The health status state for the NEM is updated according to the service action set.

3. **To verify the updated health state for the NEM, type:**

   `show /Systems/IO_Modules/NEMs/NEM_`*n*` health`

   For more information about health states, see "Health State: Definitions" on page 40.

Related Information

- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Update Blade Chassis Component Firmware Images" on page 199
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Reset Power to Server SP, NEM SP, or CMM" on page 202

Managing Oracle ILOM Log Entries

Oracle ILOM maintains three system management logs: event log, audit log, and syslog. For further details about these logs, see these topics:

Oracle ILOM: Log Descriptions

Log	Description
Event	The *event log* tracks informational, warning, or error messages about a managed device such as the addition or removal of a component or the failure of a component. The event properties recorded in the event log can include: the severity of the event, the event provider (class), and the date and time the event was logged. The event log is helpful for troubleshooting the system when problems occur. It is also helpful for monitoring the performance of the managed device.
Audit	The *audit log* tracks all interface-related user actions such as, user logins, logouts, configuration changes, and password changes. The user interfaces monitored for user actions include: Oracle ILOM web interface, CLI, Fault Management Shell (captive shell), the Restricted shell, as well as SNMP and IPMI client interfaces. The audit log in Oracle ILOM is helpful for auditing user activity to ensure that no privilege violations have occurred.
Syslog	The *syslog* defines a set of common features for event logging and a protocol for transmitting the log entries to a remote host. The syslog in Oracle ILOM is helpful if you want to combine events from multiple Oracle ILOM sessions within a single place. The entries recorded in the syslog contain all the same information that you would see the local event log. **Note -** The syslog feature in Oracle ILOM is, disabled by default. For instructions on how to configure the syslog properties in Oracle ILOM, refer to *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Setting Up Alert Notifications and Syslog Server for Event Logging" on page 167.

Oracle ILOM: Log Entries

Column Entry	Description
Event ID	The number of the event, in sequence from number 1.
Date and Time	The day and time the event occurred. If the Network Time Protocol (NTP) server is enabled to set the Oracle ILOM time, the Oracle ILOM clock uses Universal Coordinated Time (UTC). For more information about time stamps, see "Oracle ILOM: Log Time Stamps" on page 47.

Column Entry	Description
Class	• **Audit/ Log** – Commands that result in a configuration change. Description includes user, command, command parameters, and success/failure. • **IPMI/Log** – Any event that is placed in the IPMI SEL is also put in the management log. • **Chassis/State** – For changes to the inventory and general system state. • **Chassis/Action** – Category for shutdown events for server module/chassis, hot insert/removal of FRU components, as well as Reset Parameters button when pushed. • **Fault/Fault** – For Fault Management faults. Description gives the time fault was detected and the suspect component. • **Fault/Repair** – For Fault Management repairs. Description gives component.
Type	• **Log** – Appears for event log. • **UI** – Appears for audit log.
Severity	Debug, Down, Critical, Major, or Minor.

Oracle ILOM: Log Time Stamps

Local system time stamps, by default, are captured in Oracle ILOM log files by using the host server system clock UTC/GMT time zone. However, if a log file is viewed from a remote client that is located in a different time zone, Oracle ILOM automatically adjusts the time stamps in the log files to reflect the local time zone of the remote client and the host system. In this case, two time stamps appear in the log for each listed event entry.

In addition to supporting local system time stamps, Oracle ILOM enables you to capture remote router time stamps using a Network Time Protocol (NTP) server. For information about the way to modify how Oracle ILOM captures time stamps for logged entries, refer to the *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting Properties for SP or CMM Clock" on page 110.

▼ View and Clear Log Entries (Web)

Event and audit log entries for a host server or blade system chassis are viewable from the server SP or CMM web interface.

Before You Begin

- Admin (a) role privileges are required to clear log entries.

To view and clear log entries using the server SP or CMM web interface, follow these steps:

1. **To view the event and audit log entries, click ILOM Administration > Logs, and then click the Event or Audit tab.**

   The Event Log or Audit Log page appears, depending on the tab you clicked.

2. **To clear all log entries shown in the event or audit log, click the Clear Log button on the log table, and then click OK in the message box that appears.**

   The log is cleared of all its entries.

Related Information

- "Filter Log Entries" on page 49
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Configuring Syslog for Event Logging" on page 173
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting Properties for SP or CMM Clock" on page 110

▼ View and Clear Log Entries (CLI)

Event and audit log entries for a host server or blade system chassis are viewable from the server SP CLI.

Before You Begin

- Admin (a) role privileges are required to clear log entries.

To view and clear log entries using the server SP or CMM CLI, follow these steps:

1. **To view a tabular CLI list of event and audit log entries, type one of the following:**

   - **`show /SP/Logs/event/list`**
   - **`show /CMM/Logs/event/list`**
   - **`show /SP/Logs/audit/list`**
   - **`show /CMM/Logs/audit/list`**

   To scroll through the list, press any key except the q key.

2. **To clear log entries shown, use the `clear=true` command, and then type `y` at the prompt.**

   Examples:

- **set /SP/Logs/event/ clear=true**
- **set /CMM/Logs/event clear=true**
- **set /SP/Logs/audit clear=true**
- **set /CMM/Logs/audit clear=true**

Related Information

- "Filter Log Entries" on page 49
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Configuring Syslog for Event Logging" on page 173
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting Properties for SP or CMM Clock" on page 110

▼ Filter Log Entries

Properties for filtering the server SP or CMM log entries are available in the CLI and web interface.

To filter log entries for the server SP or CMM, follow these steps:

- **To filter the event or audit log entries, do one of the following:**
  - **Web:**

    Click the controls at the top of the log table.
  - **CLI:**

    Issue the show command followed by one or more these filter properties: Class, Type, Severity.

    For example:

    - To filter the log entries by Class, type:

      show /*SP* | *CMM***/logs/***event* | *audit***/list Class==***value*
    - To filter the log entries by Class and Type, type:

      show /*SP* | *CMM***/logs/***event* | *audit***/list Class==***value* **Type==***value*
    - To filter the log entries using all the filter properties, type:

      show /*SP* | *CMM***/logs/***event* | *audit***/list Class==***value* **Type==***value* **Severity==***value*

    Where:

    - *SP* | *CMM* appears, type either **SP** or **CMM**.
    - *event* | *audit* appears, type either **event** to filter the event log, or type **audit** to filter the audit log.

Related Information

- "View and Clear Log Entries (Web)" on page 47
- "View and Clear Log Entries (CLI)" on page 48

Performing Commonly Used Host Management Actions (Web)

The Oracle ILOM web interface provides an Actions panel on the Summary page that you can use to:

- View and change the state of commonly used system properties such as the power state and the Locator Indicator LED state on a managed device.
- Update the firmware image currently installed on the managed device.
- Launch the Oracle ILOM Remote Console or the x86 Oracle System Assistant.

Note – The web interface feature for launching the Oracle ILOM Remote Console from the Actions panel is not available from the Oracle ILOM CMM. The web interface feature for launching the Oracle ILOM System Assistant from the Actions panel is available only from the Oracle ILOM x86 server SPs.

For further details about initiating these commonly used host management actions from the Actions panel on the web interface Summary page, see these topics:

- "View and Modify the Device Power State From the Actions Panel (Web)" on page 51
- "View and Modify the Device Locator State From the Actions Panel (Web)" on page 52
- "Update the Device Firmware From the Actions Panel (Web)" on page 52
- "Launch the Oracle ILOM Remote Console From the Actions Panel (Web)" on page 55
- "Launch the x86 Oracle System Assistant" on page 57

▼ View and Modify the Device Power State From the Actions Panel (Web)

The Power state property for the host server or CMM is viewable and configurable from the Actions panel in the web interface Summary page.

Before You Begin

- Admin (a) role privileges are required in Oracle ILOM to modify the power state on a managed device.

Note – Alternatively, you can modify the power state for a managed device from the Host Management > Remote Power Control page, or from the CLI `/System` target. For details about using these alternative methods to control the power state, see the topics in the Related Information section following this procedure.

---

1. **To view the power state for a managed device, click System Information > Summary.**

   The current power state for the managed device appears in the Actions panel.

2. **To modify the power state shown for a managed device, do one of the following:**

   - **If Power state is set to ON in Actions Panel**– Click the Turn Off button to perform a graceful shutdown of the operating system prior to powering off the host server.

Note – If the power to the host server fails to shut down, you can force a power shutdown by clicking Immediate Power Off on the Host Management Power Control page.

   - **If Power state is set to Off in Actions Panel** – Click the Turn On button to return power to the host server.

   A prompt appears confirming that you want to proceed; click Yes to continue or No to cancel the action.

Related Information

- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Controlling Host Power to Server or Blade System Chassis" on page 148

▼ View and Modify the Device Locator State From the Actions Panel (Web)

The Locator Indicator state property for the host server or CMM is viewable and configurable from the Actions panel in the web interface Summary page.

Before You Begin

- User Management (u) privileges are required in Oracle ILOM to modify the Locator Indicator state.
- The physical Locator Indicator LED on a managed device is typically located on both the front and back panel of the device.

Note – Alternatively, you can view and modify the Locator Indicator state from CLI `/System` target. For instructions, see the topics in the Related Information section following this procedure.

---

1. **To view the current Locator Indicator state on the managed device, then click System Information > Summary.**

   The current Locator Indicator state for the managed device appears in the Actions panel.

2. **To modify the state shown in the Actions panel for Locator Indictor, click the Turn** *Off* | *ON* **button for Locator.**

   A prompt appears confirming that you want to proceed; click Yes to continue or No to cancel the action.

Related Information

- *Oracle ILOM 3.1 Quick Start Guide,* "Locate a Managed Device Using the Locator LED" on page 27
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Configuring Host Server Management Actions" on page 147

▼ Update the Device Firmware From the Actions Panel (Web)

The System Firmware Update property for the host server or CMM is viewable and configurable from the Actions panel in the web interface Summary page.

Before You Begin

- If required by your platform, shut down the host operating system prior to updating the firmware image on the server SP.

- Admin (a) role privileges are required to clear log entries.
- The firmware update process takes several minutes to complete. During this time, do not perform other Oracle ILOM tasks. When the firmware update is complete, the system will reboot.

Note – Alternatively, you can launch the firmware update process from the web interface: ILOM Administration > Maintenance > Firmware Upgrade page. You can also launch the firmware update process from the Oracle ILOM CLI. For details, see the topics in the Related Information section following this procedure.

To initiate the firmware update process from the Actions panel on the web interface Summary page:

1. **Determine the current firmware version installed on the server SP or CMM.**

   From the web interface, click System Information > Summary and view the System Firmware Version Installed value in the General Information table.

2. **Open a new web browser tab or window and navigate to the following site to download the Oracle ILOM firmware image:**

   `http://support.oracle.com/`

   For detailed instructions on downloading software updates from the My Oracle Support web site, see "Download Product Software and Firmware" on page x.

Note – Updating the system firmware image on a managed device to a prior firmware release is not recommended. However, if an earlier firmware release is required, Oracle ILOM will support the firmware update process to any prior firmware release that is available from the download site.

---

3. **Place the firmware image on a server supporting one of the following protocols: TFTP, FTP, HTTP, HTTPS.**

   For web interface firmware updates, you should copy the image to the system on which the Oracle ILOM web browser is running.

4. **To update the Oracle ILOM firmware image from the Actions panel in the web interface Summary page, click System Information Summary, and do the following:**

   a. **In the Actions panel, click the Update button for System Firmware Update.**

      The Firmware Upgrade page appears.

   b. **Click Enter Upgrade Mode in the Firmware Upgrade page.**

      An Upgrade Verification dialog box appears, indicating that other users who are logged in will lose their session when the update process is complete.

c. In the Upgrade verification dialog box, click OK to continue.

The Firmware Upgrade page appears.

5. Perform the following actions:

a. Specify the image location by performing one of the following:

- Click Browse to select the location of the firmware image you want to install.
- If supported on your system, click Specify URL. Then, in the text field, type the URL that will locate the firmware image.

b. Click the Upload button to upload and validate the file, and then wait for the file to upload and validate.

The Firmware Verification page appears.

6. Enable any of the following options:

- **Preserve Configuration** – Enable this option if you want to save your existing configuration in Oracle ILOM and restore that existing configuration after the update process is complete.
- **Delay BIOS upgrade until next server power-off** – Enable this option if you want to postpone the BIOS upgrade until the next time the system reboots.

Note – The Delay BIOS upgrade option appears only for firmware updates on Oracle x86 servers.

Note – For Oracle x86 servers, Oracle ILOM prompts you to preserve the current BIOS properties on the managed device. If you answer Yes, Oracle ILOM will preserve the current BIOS properties after completing the firmware update. If you answer No, Oracle ILOM will set the BIOS properties to factory defaults after completing the firmware update.

---

7. Click Start Upgrade to start the upgrade process, or click Exit to cancel the process.

When you click Start Upgrade, the upload process starts, and a prompt to continue the process appears.

8. At the prompt, click OK to continue.

The Update Status page appears providing details about the update progress. When the update indicates 100%, the firmware upload is complete.

When the upload is complete, the system automatically reboots.

Note – The Oracle ILOM web interface might not refresh properly after the update is complete. If the Oracle ILOM web page is missing information or displays an error message, you might be viewing a cached version of the page from the version previous to the update. Clear your browser cache and refresh your browser before continuing.

9. **Reconnect to the Oracle ILOM SP or CMM web interface. Click System Information > Summary to verify that the firmware version on the SP or CMM corresponds to the firmware version you installed.**

Related Information

- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Performing Firmware Updates" on page 194
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Recover From a Network Failure During Firmware Update" on page 202
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Update the Server SP or CMM Firmware Image" on page 196
- *Oracle ILOM 3.1 Protocol Management Reference Guide,* "Update Oracle ILOM Firmware (SNMP)" on page 93

▼ Launch the Oracle ILOM Remote Console From the Actions Panel (Web)

A Remote Console button for launching the Oracle ILOM Remote Console is provided in the Actions panel of the Summary page for both the server SP and CMM.

x86 system administrators can use the Actions panel Remote Console button to launch a video-based redirection session. SPARC system administrators can use the Actions panel Remote Console button to launch a video-based or a serial-based redirection session. CMM system administrators can use the Actions panel Remote Console button to launch a separate redirection session for each managed blade system server SP.

The Oracle ILOM Remote Console provides remote redirection for these host server devices: keyboard, video, mouse, and storage.

Before You Begin

- For first-time-use, the following requirements must be met:
  - The Java Runtime Environment (1.5 or later) must be installed on your local system. To download the Java 1.5 Runtime Environment, go to `http://java.com`.

- Registration of the 32-bit JDK browser plug-in. For details, see *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "First-Time Setup for Oracle ILOM Remote Console" on page 118.
- Verification that the default KVMS settings provided in Oracle ILOM match your desktop environment. For details, see *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "First-Time Setup for Oracle ILOM Remote Console" on page 118.

- The Actions panel Remote Console button on a SPARC server SP launches a video-based redirection session by default, unless the property for a serial redirection session is enabled on the Remote Control >Launch Redirection web page.

To launch the Oracle ILOM Remote Console from the Actions panel in the web interface, perform this step:

1. **To access the Actions panel in the web interface, click System Information > Summary page.**

   The Actions panel appears in the upper right corner of the Summary page.

Note – Alternatively, the Oracle ILOM Remote Console can be launched in the web interface by clicking the Launch Remote Console button on the Remote Control > Launch redirection web page.

---

2. **To launch the Oracle ILOM Remote Console from the Actions panel, click the Launch button for Remote Console.**

Note – If the web browser 32-bit JDK plug-in was not configured for first-time-use, a dialog for "`Opening jnlpgenerator.cli`" appears. Prior to clicking OK to proceed, review the browser JDK plug-in configuration options described in *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "First-Time Setup for Oracle ILOM Remote Console" on page 118.

   The Oracle ILOM Remote Console window appears displaying the redirection session for the host server SP.

Note – If the redirection session was launched from the CMM, a separate redirection session (tab) for each server SP appears in the Oracle ILOM Remote Console window.

   The redirection session displays the host server desktop in its present state. For example, if the host server is powering-up, a set of boot messages appear; if the host server operating system is powered-on, a desktop log in dialog appears; if the host server is not powered-on, a blank screen appears.

3. **To use the Oracle ILOM Remote Console, use the options in the Redirection, Device, and Keyboard menus.**

   For complete details about the menu options in the Oracle ILOM Remote Console, refer to *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Launching and Using the Oracle ILOM Remote Console" on page 125.

Related Information

- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Using Remote KVMS Consoles for Host Server Redirection" on page 117
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Optionally Set a Lock Mode to Secure the Host Server Desktop" on page 122

▼ Launch the x86 Oracle System Assistant

Oracle System Assistant is a tool that offers features for provisioning servers, including operating system installation, firmware updates, RAID configuration, and more. For more information about these features, refer to the administration guide for your x86 server.

Before You Begin

- The Launch option for Oracle System Assistant appears in Oracle ILOM only when Oracle System Assistant is present on the host x86 server.
- Power off the host operating system on the host server. If you do not power off the host OS prior to performing this procedure, Oracle ILOM will prompt you to power off the host before launching the Oracle System Assistant.
- When launching Oracle System Assistant, you will be prompted to launch a new Oracle ILOM Remote Console session. Therefore, prior to launching Oracle System Assistant, ensure that the setup requirements for launching and using the Oracle ILOM Remote Console (JDK version, browser Java plug-in, and KVMS settings) are met. For more information about these requirements, see "Launch the Oracle ILOM Remote Console From the Actions Panel (Web)" on page 55.
- The Admin (a) role is required in Oracle ILOM to launch Oracle System Assistant. The Console (c) role is required to launch the Oracle ILOM Remote Console.

This procedure provides both web and CLI instructions.

- **To launch Oracle System Assistant, perform one of the following Oracle ILOM interface procedures:**

Oracle ILOM Interface	Launch Oracle System Assistant Procedure
Web	1. In the Actions panel, which is located in the System Information > Summary page, click the Launch button for Oracle System Assistant. One or more of the following prompts appear: **Power off host prompt**: This prompt appears only if the power on the host server was not powered-off prior to performing this procedure. Click OK to power-off the host server. **Launch a new Oracle ILOM Remote Console prompt**: This prompt appears prior to launching the Oracle ILOM Remote Console. **Note** – You might encounter the following behavior: 1) an alert message appears stating, "cannot get power state" and 2) a powered-off state is shown for Power in the Actions panel. If you encounter this behavior, it is because Oracle ILOM is temporarily unable to obtain the host server information. In this situation, click OK in the alert message to continue launching Oracle System Assistant. When you return to the Summary page, click Refresh to update the host power state shown in the Actions panel. 2. Oracle ILOM launches Oracle System Assistant in the Oracle ILOM Remote Console window. Refer to the x86 server administration guide for instructions for using the Oracle System Assistant.
CLI	1. In the Oracle ILOM CLI, type: **`start /HOST/provisioning/system-assistant`** The following prompt appears: `Are you sure that you want to start /HOST/provisioning/system-assistant (y/n)?` 2. Type **`y`** to launch Oracle System Assistant (or type **`n`** to cancel the operation). Oracle ILOM launches Oracle System Assistant. Refer to the x86 server administration guide for instructions for using Oracle System Assistant.

Related Information

- Administration guide for Oracle x86 server, Oracle System Assistant

Applying Host and System Management Actions

Description	Link
Refer to this section for links to Oracle ILOM configuration topics that describe how to set properties for host management actions.	• "Administering Host Management Configuration Actions" on page 60
Refer to this section for links to Oracle ILOM configuration topics that describe how to set properties for server management actions.	• "Administering System Management Configuration Actions" on page 61

Related Information

- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Setting System Management Power Source Policies" on page 175
- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Maintaining x86 BIOS Configuration Parameters" on page 215
- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Configuring Host Server Management Actions" on page 147
- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Performing Oracle ILOM Maintenance and Configuration Management Tasks" on page 193

Administering Host Management Configuration Actions

Description	Link
Refer to this section for instructions on controlling rackmount and blade chassis power properties.	• *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Controlling Host Power to Server or Blade System Chassis" on page 148
Refer to this section for instructions on controlling the next boot device.	• *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting Next Boot Device on x86 Host Server" on page 153
Refer to this section for instructions on enabling SP diagnostics on a managed server.	• *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting Host Diagnostic Tests to Run" on page 149
Refer to these sections for instructions on managing SPARC host boot, host domains, KeySwitch, and TPM properties.	• *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting Boot Behavior on SPARC Host Server" on page 155 • *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Overriding SPARC Host Boot Mode" on page 158 • *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Managing SPARC Host Domains" on page 162 • *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting SPARC Host KeySwitch State" on page 164 • *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting SPARC Host TPM State" on page 165

Administering System Management Configuration Actions

Description	Link
Refer to this section for instructions on backing up and restoring BIOS properties on an x86 managed server.	• *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Maintaining x86 BIOS Configuration Parameters" on page 215
Refer to this section for instructions on setting system management policies on a managed device.	• *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting System Management Power Source Policies" on page 175
Refer to this section for instructions on managing SAS storage devices installed in an Oracle blade chassis.	• *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "SAS Zoning Chassis Blade Storage Resources" on page 231
Refer to this section for instructions for backing up and restoring the Oracle ILOM configuration, and resetting the server SP, NEM SP, or CMM.	• *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Performing Oracle ILOM Maintenance and Configuration Management Tasks" on page 193

Troubleshooting Oracle ILOM Managed Devices

Description	Links
Refer to this topic for suggestions for resolving issues when establishing a management connection to Oracle ILOM.	• "Network Connection Issues: Oracle ILOM Interfaces" on page 64
Refer to this topic for a list of offline and online tools that you can use to observe and debug a managed system.	• "Tools for Observing and Debugging System Behavior" on page 65
Refer to this section for topics providing instructions for enabling and running Oracle ILOM SP diagnostic tools.	• "Enabling and Running Oracle ILOM Diagnostic Tools" on page 66

Related Information

- "Managing Oracle Hardware Faults Through the Oracle ILOM Fault Management Shell" on page 95
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting Host Diagnostic Tests to Run" on page 149
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Suggested Resolutions for Network Connectivity Issues" on page 111
- *Oracle x86 Server Diagnostics Guide For Servers With Oracle ILOM 3.1*
- Service manual for Oracle server or CMM

Network Connection Issues: Oracle ILOM Interfaces

If you are experiencing difficulties establishing a network connection to Oracle ILOM interfaces, refer to the following information for suggested resolutions.

TABLE: Troubleshooting Connectivity Issues

Problem	Suggested Resolution
Unable to access the Oracle ILOM web interface using an IPv6 address.	Ensure that the IPv6 address in the URL is enclosed by brackets, for example: `https://[2001:db8:0:0:0:0:0:0]`
Unable to download a file using an IPv6 address.	Ensure that the IPv6 address in the URL is enclosed by brackets, for example: `load -source tftp://[2001:db8:0:0:0:0:0:0]/desktop.pkg`
Unable to access Oracle ILOM using IPv6 from a network client.	If on a separate subnet, try the following: • Verify that Oracle ILOM has a dynamic or static address (not just a Link-Local address). • Verify that the network client has an IPv6 address configured (not just a Link-Local address). If on the same or a separate subnet, try the following: • Ensure that setting for `IPv6 State` is enabled on the Network Settings page in the Oracle ILOM web interface or under the `/SP/network/ipv6` target in the Oracle ILOM CLI. • Verify that the appropriate network service, in Oracle ILOM, is enabled: SSH, HTTP, or HTTPS. In the web interface, click ILOM Administration > Connectivity to verify and change network connectivity settings • Use an industry-standard network diagnostic tool like IPv6 Ping or Traceroute to test the network connection to the managed device. Run `ping6` from the web interface or CLI. Or, run `traceroute` from the service Oracle ILOM restricted shell.

TABLE: Troubleshooting Connectivity Issues *(Continued)*

Problem	Suggested Resolution
Unable to access Oracle ILOM using IPv4 from a network client.	Ensure that the setting for State is enabled on the Network Settings page in the Oracle ILOM web interface or under the `/SP/network` target in the Oracle ILOM CLI. Other suggestions for diagnosing IPv4 network issues, include the following: • Verify that a LAN connection to the physical management port (NET MGMT) is established. • Verify that the appropriate network service, in Oracle ILOM, is enabled: SSH, HTTP, or HTTPS. In the web interface, click ILOM Administration > Connectivity to verify and change network connectivity settings. • Use an industry-standard network diagnostic tool like IPv4 Ping or Traceroute to test the network connection to the managed device. Run `ping4` from the web interface or the CLI. Or, run `traceroute` from the service Oracle ILOM restricted shell.
Unable to access the Oracle ILOM web interface using the Internet Explorer 6 (IE6) web browser.	Internet Explorer 6 users must upgrade browsers or upload custom certificate keys to use SSL in the Oracle ILOM web interface. For instructions on how to upload a custom SSL certificate, refer to *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Modifying Default Settings for Network Deployment and Administration" on page 69.

Tools for Observing and Debugging System Behavior

A collection of online and offline diagnostic tools are provided with Oracle ILOM to assist IT administrators and Oracle Services personnel who verify server behavior, troubleshoot problems, and perform repair or replacement service actions. For a list of Oracle ILOM diagnostic tools, their usages, and where to locate additional information about them, see the following table.

TABLE: Suggested Diagnostic Tools

To Perform:	Use:	For Details, See:
x86 host diagnostic tests	• Oracle ILOM Host Management Diagnostics: Pc-Check	• *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Setting Host Diagnostic Tests to Run" on page 149 • "Enabling x86 Diagnostics to Run at Boot" on page 71

TABLE: Suggested Diagnostic Tools *(Continued)*

To Perform:	Use:	For Details, See:
x86 processor interrupt for non-recoverable errors or to debug system status	• Oracle ILOM Host Management Diagnostics: NMI	• "Generating x86 Processor Interrupt: Debugging System Status" on page 67
SPARC host diagnostic tests	• Oracle ILOM Host Management Diagnostics	• "Enabling SPARC Diagnostics to Run at Boot" on page 74
Service processor snapshots	• Oracle ILOM Snapshot*	• "Taking a Snapshot: Oracle ILOM SP State" on page 68
Fault management	• Oracle ILOM Open Problems output • Oracle ILOM Fault Management Shell*	• "Administering Open Problems" on page 41 • "Protecting Against Hardware Faults: Oracle ILOM Fault Manager" on page 96
Host operating system management	• Oracle ILOM CLI	• *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Starting and Stopping a Host Serial Redirection Session" on page 144 Supported Oracle ILOM CLI targets for launching a host console include: `SP/console` or `host/console`
Oracle ILOM Recovery Tasks — x86 Preboot Menu	• Oracle ILOM Preboot Menu†	• *Oracle x86 Server Diagnostics Guide For Servers With Oracle ILOM 3.1*, "Fixing Problems With Oracle ILOM"

* Diagnostic tool designed for authorized Oracle Services personnel.

† Available on Oracle x86 managed servers only.

Enabling and Running Oracle ILOM Diagnostic Tools

Oracle ILOM provides various diagnostic tools to help resolve unexpected system performance or faulty component behavior on a managed device. For details on how to use these tools, see these topics:

- "Generating x86 Processor Interrupt: Debugging System Status" on page 67
- "Taking a Snapshot: Oracle ILOM SP State" on page 68
- "Enabling x86 Diagnostics to Run at Boot" on page 71
- "Enabling SPARC Diagnostics to Run at Boot" on page 74

Generating x86 Processor Interrupt: Debugging System Status

Sending a nonmaskable interrupt (NMI) to the host operating system can cause the host to stop responding and wait for input from an external debugger. Therefore, you should use this feature only when requested to do so by Oracle Services personnel.

▼ Generate a Nonmaskable Interrupt

Before You Begin

- Obtain permission from Oracle Services prior to performing this procedure.
- To generate an NMI from Oracle ILOM interfaces, you need the Admin(a) role enabled.
- The setting for generating a nonmaskable interrupt from Oracle ILOM might not be supported on all managed servers.

Caution – Depending on the host OS configuration, generating a nonmaskable interrupt (NMI) might cause the OS to crash, stop responding, or wait for external debugger input.

- **To generate a processor interrupt, do one of the following:**
  - From the Oracle ILOM web interface, click Host Management > Diagnostics, and then click Generate NMI.
  - **From the Oracle ILOM CLI**, type:

    `set /HOST/diag generate_host_nmi = true`

    For example:

```
-> cd /HOST
/HOST

-> show
/HOST
    Targets:
        diag

    Properties:
        generate_host_nmi = (Cannot show property)

    Commands:
        cd
        set
```

```
          show

-> set generate_host_nmi=true
set 'generate_host_nmi' to 'true'
```

Taking a Snapshot: Oracle ILOM SP State

The Oracle ILOM Service Snapshot utility enables you to produce a snapshot of the server processor at any instant in time.

Caution – The purpose of the Oracle ILOM Service Snapshot utility is to collect data for use by Oracle Services personnel to diagnose system problems. Customers should not run this utility unless requested to do so by Oracle Services personnel.

The Oracle ILOM Service Snapshot utility gathers SP state data. The utility collects log files, runs various commands and collects their output, and sends the data collection as a downloaded file to a user-defined location.

The Service Snapshot utility FRUID data set option enables Oracle Services personnel to analyze data in a binary format about field-replaceable hardware installed on a server. This FRUID option is not for customer use, unless an authorized Oracle Services representative instructs a customer to use the option.

For snapshot instructions, refer to one of these topics:

- "Take a Snapshot of the Oracle ILOM SP State (Web)" on page 68
- "Take a Snapshot of the Oracle ILOM SP State (CLI)" on page 69

▼ Take a Snapshot of the Oracle ILOM SP State (Web)

Before You Begin

- The Admin (a) role is required to modify Service Snapshot properties.

Caution – The purpose of the Service Snapshot utility is to collect data for use by Oracle Services personnel to diagnose system problems. Customers should not run this utility unless requested to do so by Oracle Services.

1. **To access the Service Snapshot Utility page, click ILOM Administration > Maintenance > Snapshot.**
2. **Define the snapshot settings and run the Service Snapshot utility:**
   a. **To specify a Data Set, specify one of the following:**

- Normal – Collect information about Oracle ILOM, host operating system, and hardware configuration.
- FRUID – Collect information about installed FRUs, in addition to the data set collected for Normal.
- Full – Collect the maximum information about the server. This option could cause the server to reset.
- Custom – Collect specific information about the server such as, hardware data, Oracle ILOM data, basic OS data, basic diagnostic data, and FRU data.

b. To specify output properties, specify the following:

- Collect Log Files For Data Set – Enable (select) this option to collect log files.
- Encrypt Output File – Enable (select) this option to encrypt the output file.

c. To specify a Transfer Method for the output files, select one of the following:

- Browser – Download the files according to your browser settings.
- SFTP – Specify a host server, directory path to the server, and the user name and password for the host server.
- FTP – Specify a host server, directory path to the server, and the user name and password for the host server.

d. To run the Service Snapshot utility, click Run.

When the snapshot is complete, a dialog box appears prompting you to save the output file.

3. To specify a file name for the snapshot and where to save the file, specify a file name and a directory in the Save As dialog box, and then click OK.

▼ Take a Snapshot of the Oracle ILOM SP State (CLI)

Caution – The purpose of the Oracle ILOM Service Snapshot utility is to collect data for use by Oracle Services personnel to diagnose system problems. Customers should not run this utility unless requested to do so by Oracle Services.

Before You Begin

- To collect SP data using the Service Snapshot utility, you need the Admin `(a)` role enabled.
- Review the following CLI snapshot properties:

Property	Value	Description
data	`normal`	Collect information about Oracle ILOM, operating system, and hardware.
	`FRUID`	Collect information about FRUs currently configured on your server in addition to the data collected by the `normal` option.
	`full`	Collect the maximum data about the system. **Note -** Using this option might reset the host operating system.
	• `normal-logonly` • `fruid-logonly` • `full-logonly`	Collect only log files.

uri	Any valid target directory location	Specify the transfer method of the output files. The URI format is as follows:
		`protocol://username:password@host/directory`
		Where `protocol` can be one of these transfer methods: SFTP or FTP.
		For example, to store the snapshot information in the directory named `data` on the host, define the URI as follows:
		`ftp://joe:`*mypasswd@host-ip-address*`/data`
		The directory `data` is relative to the user's login, so the directory would probably be `/home/joe/data`.

To take a snapshot of the Oracle ILOM SP state from the Oracle ILOM CLI:

1. **Log in to the Oracle ILOM CLI server SP.**
2. **To view the snapshot properties, type:**

   `show SP/diag/snapshot`
3. **To define the data set collection, type:**

   `set /SP/diag/snapshot dataset=`*data*
4. **To define the encryption mode, type:**

   `set /SP/diag/snapshot encrypt_output=`*true* | *false*

Note – When the encryption mode is set to `true`, you must type an encryption password at the prompt in order to start the data collection. Then later, you must type an encryption password at the prompt in order to decrypt the output file.

5. **To start the data collection, type:**

   `set /SP/diag/snapshot dump_uri=`*uri*

Enabling x86 Diagnostics to Run at Boot

Use Pc-Check diagnostics to test and detect problems on all motherboard components, hard disk drives, ports, and slots.

- "Enable x86 Diagnostics to Run at Boot (Web)" on page 71
- "Enable x86 Diagnostics to Run at Boot (CLI)" on page 72

▼ Enable x86 Diagnostics to Run at Boot (Web)

Before You Begin

- To diagnose x86 systems hardware issues, you need the Reset and Host Control (`r`) role enabled.
- If you choose to run diagnostics in Manual mode, or if you want to monitor the progress of diagnostic tests in Enabled or Extended mode, do one of the following:
  - Start a host console redirection.
  - Set up a serial console.
  - Connect a keyboard, video, and mouse to your system.

To configure PC-Check diagnostics:

1. **Click Host Management > Diagnostics.**

   The Diagnostics page appears.

2. **In the Run Diagnostics on Boot list box, select one of the following levels of diagnostics to run:**
   - **Disabled (default)**– PC-Check will not run diagnostic test during host start-up. The server remains in normal operation mode.
   - **Enabled** – PC-Check runs a predefined test suite without user intervention at host startup. Upon completion, the host will boot from the next device on the BIOS Boot Device Priority list. Use this mode to run quick diagnostic tests for first-time field installation or prior to installing mission-critical applications to verify system quality. The basic PC-Check tests typically take up to 5 minutes to complete.

- **Extended** – PC-Check runs a comprehensive test suite upon host startup. Use this mode after installing the system for the first time, after physically transporting the system, any time you add components, and prior to installing production operating systems and mission-critical applications. The extended PC-Check tests typically take 20 to 40 minutes to complete.
- **Manual** – The PC-Check diagnostic tests menu appears upon host startup. Use this mode to select tests from the PC-Check menu or to select predefined test suites through the Immediate Burn-in test menu. Test times depend on the tests selected.

3. **Click Save.**

   a. **Click Host Management > Power Control.**

      The Server Power Control page appears.

   b. **In the Select Action list box, select Power Cycle, and then click Save.**

      If you initiated a redirection session, the redirected display will initially show the host startup messages, and then it shows the progress of the diagnostic tests.

Note – On UEFI platforms running PC-Check, if the Configuration Sync Status in the System Management > BIOS page is Reboot_needed, a warm reset will also initiate diagnostic tests.

---

   c. **If a license agreement appears, click Enter to continue.**

4. **If you chose to run diagnostics in Manual mode, select Show Results Summary in the PC-Check menu to view the output files.**

▼ Enable x86 Diagnostics to Run at Boot (CLI)

Before You Begin

- To diagnose x86 system hardware issues, you need the Reset and Host Control (`r`) role enabled.

To configure PC-Check diagnostics:

1. **From the Oracle ILOM CLI, type one of the following `set` commands to specify the level of diagnostics to run:**
   - **`set /Host/diag state=disabled`** (default) – PC-Check will not run diagnostic tests during host start-up. The server remains in normal operation mode.

     For example:

- **set /HOST/diag state=enabled** – PC-Check runs a predefined test suite without user intervention at host startup. Upon completion, the host will boot from the next device on the BIOS Boot Device Priority list. Use this mode to run quick diagnostic tests for first-time field installation or prior to installing mission-critical applications to verify system quality. The basic PC-Check tests typically take up to 5 minutes to complete.
- **set /HOST/diag state=extended** – PC-Check runs a comprehensive test suite upon host startup. Use this mode after installing the system for the first time, after physically transporting the system, any time you add components, and prior to installing production operating systems and mission-critical applications. The extended PC-Check tests typically take 20 to 40 minutes to complete.
- **set /HOST/diag state=manual** – The PC-Check diagnostic tests menu appears upon host startup. Use this mode to select tests from the PC-Check menu or to select predefined test suites through the Immediate Burn-in test menu. Test times depend on the tests selected.

```
-> cd /HOST/diag/
/HOST/diag

-> show /HOST/diag
    Targets:

    Properties:
        state = disabled

    Commands:
        cd
        set
        show

-> set state=extended
OR
-> set state=enabled
OR
-> set state=manual

-> show
    Targets:

    Properties:
        state = enabled

    Commands:
        cd
        set
        show
```

2. **Power cycle the server:**

   a. **Type `stop /System`.**

   b. **Type `start /System`.**

      The diagnostic tests are run when you power on the server.

Note – On UEFI platforms running PC-Check, if the Configuration Sync Status in the System Management > BIOS page is Reboot_needed, a warm reset will also initiate diagnostic tests.

---

3. **If you chose to run diagnostics in Manual mode, select Show Results Summary in the PC-Check menu to view the output files.**

Enabling SPARC Diagnostics to Run at Boot

On an Oracle SPARC system using Oracle ILOM, you can enable the diagnostic mode, specify triggers and the level of diagnostics, as well as the verbosity of the diagnostic output. For more information about SPARC platform diagnostics, see your platform-specific service manual.

- "Enable SPARC Diagnostics to Run at Boot (Web)" on page 74
- "Enable SPARC Diagnostics to Run at Boot (CLI)" on page 75

▼ Enable SPARC Diagnostics to Run at Boot (Web)

Before You Begin

- The Reset and Host control (`r`) role is required to modify the SPARC diagnostic properties in Oracle ILOM on SPARC systems.

To enable SPARC diagnostics tests to run when powering on the system:

1. **From the Oracle ILOM web interface, click Host Management > Diagnostics.**

   The Diagnostics page appears.

2. **To specify a trigger for when the diagnostics tests are run, select one of the following:**
   - Power On – Run diagnostics when power is applied.
   - HW Change – Run diagnostics upon a user-invoked power reset.
   - Error Reset – Run diagnostics upon any error-invoked power reset.

3. **To specify the test level for each trigger, select one of the following:**

- Min – Run the minimum level of diagnostics to verify the system.
- Max – Run the maximum set of diagnostics to fully verify system health (the default value).

4. **To specify the verbosity reported for each trigger, select one of the following:**
   - None – Do not print output to the system console when diagnostics are run, unless a fault is detected.
   - Min – Print limited output to the system console when diagnostics are run.
   - Normal – Print a moderate amount of output to the system console when diagnostics are run, including the name and results for each test.
   - Debug – Print extensive debugging output to the system console when diagnostics are run, including devices being tested and debugging output for each test.
5. **To specify the mode to enable diagnostics, select one of the following:**
   - Off – Disable all triggers for running diagnostic tests.
   - Normal – (Default) Run diagnostic tests based on the trigger specified in Step 2.
6. **To save modifications on this page, click Save.**

▼ Enable SPARC Diagnostics to Run at Boot (CLI)

Before You Begin

- The Reset and Host control (`r`) role is required to modify the SPARC diagnostic properties in Oracle ILOM on SPARC systems.
- Use the `/HOST/diag` host mode property to control whether diagnostics are enabled and to specify which diagnostic mode is enabled.

To enable SPARC server diagnostics tests to run when power on the system:

1. **To specify triggers for running the SPARC diagnostic tests, type:**

   `set /HOST/diag trigger=`*value*

   Where *value* can be one of the following:
   - `none` – Do not run diagnostic tests.
   - `user-reset` – Run diagnostics upon a user-invoked power reset.
   - `power-on-reset` – Run diagnostics when power is applied to the host operating system.
   - `error-reset` – Run diagnostics upon any error-invoked power reset.
   - `all-resets` – Run diagnostics whenever a power reset occurs.
2. **To specify the level of diagnostics to run, perform the following:**

- For when the host operating system powers on, type:

  set /HOST/diag power_on_level=*value*

- For when the host operating system is reset by the user, type:

  set /HOST/diag user_reset_level=*value*

- For when the host operating system is reset due to a system error, type:

  set /HOST/diag error_reset_level=*value*

Where *value* is one of the following:

- `min` – Run the minimum set of diagnostics to partially verify the health of the system.
- `max` – (Default) Run the maximum set of diagnostics to fully verify the health of the system.

3. **To specify the report verbosity when diagnostics are run, perform one of the following:**

   - For when the host is powered on, type:

     set /HOST/diag power_on_verbosity=*value*

   - For when the host is reset by the user, type:

     set /HOST/diag user_reset_verbosity=*value*

   - For when the host is reset due to a system error, type:

     set /HOST/diag error_reset_verbosity=*value*

   Where *value* is one of the following:

   - `none` – Do not print output to the system console while diagnostics are run, unless a fault is detected.
   - `min` – Print limited output to the system console while diagnostics are run.
   - `normal` – (Default) Print a moderate amount of output to the system console while diagnostics are ran.
   - `max` – Print the full output to the system console while diagnostics are run, including the name and results for each test.
   - `debug` – Print extensive debugging output to the system console while diagnostics are run, including device testing and debugging output for each test.

4. **To specify the diagnostics mode, type:**

   set /HOST/diag mode=*value*

   Where *value* is one of the following:

   - `off` – Prevent the diagnostic tests from running.
   - `normal` – (Default) Run the diagnostic tests based upon the triggers specified in Step 1.

Real-Time Power Monitoring Through Oracle ILOM Interfaces

Description	Link
Refer to this section for topics describing terminology, properties, and instructions for viewing power consumption metrics for a managed device using Oracle ILOM interfaces.	• "Monitoring Power Consumption" on page 78
Refer to this section for topics describing properties, hardware components, monitoring considerations, and instructions for viewing power allocation metrics for a managed device using Oracle ILOM interfaces.	• "Monitoring Power Allocations" on page 81
Refer to these sections for topics describing instructions for viewing power statistics, power history metrics, and graphs using Oracle ILOM interfaces.	• "Analyzing Power Usage Statistics" on page 90 • "Comparing Power History Performance" on page 92

Related Information

- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting the CMM Power Supply Redundancy Policy" on page 191
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting Power Alert Notifications and Managing System Power Usage" on page 181
- *Oracle ILOM 3.1 Protocol Management Reference Guide,* "Monitor and Manage System Power (SNMP)" on page 85

Monitoring Power Consumption

The Power Consumption properties, shown in the Oracle ILOM interfaces, enable you to acquire:

- Input power wattage value currently being consumed by a managed device.
- Maximum power wattage value a managed device is permitted to consume.
- Power consumption threshold wattages set for generating power event notifications.

For additional details about the power consumption properties presented by Oracle ILOM, see the following topics:

- "View Power Consumption Properties for a Managed Device" on page 78
- "Power Consumption Terminology and Properties" on page 79

▼ View Power Consumption Properties for a Managed Device

Before You Begin

Review "Power Consumption Terminology and Properties" on page 79.

- **To view the power consumption properties from the SP or CMM web interface or CLI, do one of the following:**
  - **From the SP or CMM web interface**, click Power Management > Consumption.
  - **From the SP or CMM CLI**, type the `show` command followed by the appropriate target and property.

    For example:

    - **`show /`***SP*`|`*CMM*`/powermgmt actual_power`**
    - **`show /`***SP*`|`*CMM*`/powermgmt permitted_power`**
    - **`show /`***SP*`|`*CMM*`/powermgmt threshold`***1*`|`*2*
    - **`show /CMM/System/VPS`**

    Where:

    - *SP*`|`*CMM* appears, type **`SP`** if the managed device is an Oracle server, or type **`CMM`** if the managed device is an Oracle blade chassis.
    - *1*`|`*2* appears, type **1** to view threshold 1, or type **2** to view threshold 2.

Related Information

- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Setting Power Consumption Alert Notifications" on page 182
- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Setting CMM Power Grant and SP Power Limit Properties" on page 184
- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Setting SP Advanced Power Capping Policy to Enforce Power Limit" on page 187
- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Setting the CMM Power Supply Redundancy Policy" on page 191

Power Consumption Terminology and Properties

TABLE: Power Consumption Terminology

Terms		Description
Real-time power monitoring		Oracle ILOM enables *real-time power monitoring*, within one second accuracy, by polling hardware interfaces (CMM, SP, power supply units (PSUs), and so forth) at any instance in time to present continuously updated power monitoring metrics in Oracle ILOM interfaces.
Power Consumption		*Power consumption* refers to either the input power consumed by the managed device or the output power provided by the PSUs.
	• Input power	• *Input power* is the power that is pulled into the chassis power supply units from an external power source.
	• Output power	• *Output power* is the amount of power provided from the power supply units to the chassis components.
Power Consumption per managed device		The *power consumption* metric, appearing in Oracle ILOM interfaces, depends on the following hardware configurations:
	• Rackmount	• *Rackmount server power consumption* is the sum of input power being consumed by the rackmount chassis power supplies.
	• Blade server	• *Blade server power consumption* is the sum of power being consumed by its local components.
	• CMM	• *CMM power consumption* is the sum of input power being consumed by the blade chassis power supplies.

TABLE: Power Consumption Properties in Oracle ILOM Interfaces

Power Metric Property	Managed Device	Description
Actual Power (*/SP|CMM*/powermgmt actual_power)	x86 SP SPARC SP CMM	The read-only *Actual Power* property value, shown in Oracle ILOM interfaces, indicates the consumed power wattage by the managed device (blade chassis, rackmounted server, or blade server).
Target Limit (/SP/powermgmt/budget powerlimit)	x86 SP SPARC SP	The read-only *Target Limit* property value, shown in Oracle ILOM interfaces, displays the current Target Limit value (wattage or percentage) set on the server. *Important power monitoring considerations:* • Oracle ILOM uses the set target limit value to determine the power budgeting parameters allowed for a server. • Not all Oracle x86 servers will show a power management Target Limit property in the Oracle ILOM interfaces. When a Target Limit property is not supported by a server, Oracle ILOM determines the power budgeting parameters for that server based on the power-consuming hardware components installed on the server. • If the Target Limit property is supported (shown) in Oracle ILOM interfaces and a property value is not set, the property value `Not Configured` appears in the Oracle ILOM interfaces. For more information about power budgeting or instructions for setting a Target Limit, refer to the *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Set SP Power Target Limit Properties" on page 185.
Peak Permitted (*/SP|CMM*/powermgmt permitted_power)	x86 SP SPARC SP CMM	The read-only *Peak Permitted* property value, shown in Oracle ILOM interfaces, displays the maximum power wattage a managed device can consume: • For an Oracle rackmounted or blade server, the peak permitted value represents the maximum input power that the server can consume. • For a blade chassis, the peak permitted value represents the maximum power the blade chassis can consume.

TABLE: Power Consumption Properties in Oracle ILOM Interfaces *(Continued)*

Power Metric Property	Managed Device	Description
Event Notification Threshold *Default setting*s: disabled • Threshold 1 = 0 watts • Threshold 2 = 0 watts (*/SP*|*CMM*/`powermgmt threshold` *1*|*2 = 0*)	x86 SP SPARC SP CMM	The user-defined *Notification Threshold* properties, shown in Oracle ILOM interfaces, display the power wattage value set to trigger an alert notification. When enabled, an alert notification is triggered by Oracle ILOM when the power consumption wattage on a managed device exceeds the user-defined threshold value. **Note -** Event notifications generated by Oracle ILOM are dependent on whether email alert properties are properly configured in Oracle ILOM interfaces. For more information, refer to *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting Power Alert Notifications and Managing System Power Usage" on page 181.

Monitoring Power Allocations

The Power Management Allocation Plan, shown in Oracle ILOM interfaces, can aid your efforts in planning an energy-efficient data center. The properties shown in the Allocation Plan enable you to effectively monitor and acquire the precise power metrics allocated to a single managed device, or the individual components installed on a managed device.

For more details about the power metric properties shown in the Allocation Plan, see the following topics:

- "Power Allocation Plan Properties per Managed Device" on page 84
- "Power Allocated Components and Monitoring Considerations" on page 88
- "View the Power Allocation Plan for a Managed Device" on page 81

▼ View the Power Allocation Plan for a Managed Device

Before You Begin

- Review "Power Allocation Plan Properties per Managed Device" on page 84
- Review "Power Allocated Components and Monitoring Considerations" on page 88

1. **To view the Power Allocation Plan properties from the CMM or SP web interface, click Power Management > Allocation.**

   The Power Allocation Plan for the managed device appears.

2. **To view the Power Allocation Plan properties from the SP CLI, perform the following:**

   - View SP System Power Specification properties:

     a. **To view the Allocated Power and Peak Permitted power property values, type:**

        `show /SP/powermgmt/ allocated_power permitted_power`

     b. **To view property value for Target Limit (this property is not supported on all servers), type:**

        `show /SP/powermgmt/budget powerlimit`

     c. **To view the property for Power Supply Maximum, type:**

        `show /SP/powermgmt/ available_power`

Note – The power wattage property value for Installed Hardware Minimum on an Oracle CPU blade server is viewable only from the Allocation Plan in the Oracle ILOM web interface.

   - View SP Per Component Map properties:

     a. **To view a list of power allocated components configured on a managed server, type:**

        `show /SP/powermgmt/powerconf/`

     b. **To view power allocated property values for a specific server component, type:**

        `show /SP/powermgmt/powerconf/`*component_type***`/`***component_name*

        Where *component_type* is the name of the component category and *component_name* is the name of the component.

        Example:

        To view the power allocated to a specific CPU, you would type:

        `show /SP/powermgmt/powerconf/CPUs/CPU`*n*

        Where *n* is the installed location number of the CPU.

3. **To view the Power Allocation Plan properties from the CMM CLI, perform the following:**

   - View CMM System Power Specification properties:

a. To view the Allocated Power and Peak Permitted power property values, type:

```
show /CMM/powermgmt/ allocated_power permitted_power
```

b. To view the Power Supply Maximum property value, type:

```
show /CMM/powermgmt available_power
```

c. To view the Redundant Power property value, type:

```
show /CMM/powermgmt redundant_power
```

- View CMM Blade Power Map properties:

a. To view the Grantable Power properties, type:

```
show /CMM/powermgmt/ grantable_power
```

Note – The property for Unfilled Grant Requests is only viewable from the Allocation Plan in the ILOM web interface.

---

b. To view the Grant Limit and Granted Limit property values per blade slot, type:

show /CMM/powermgmt/powerconf/bladeslots BL*n*

Where *n* is the blade slot location in the Oracle blade chassis.

c. To view the Required Power property for a specific blade slot, type:

show /CMM/powermgmt/advanced/*n*

Where *n* is the blade slot location in the Oracle blade chassis.

d. To view the Granted Power property value for all chassis blade slots and the Reserved Power property value for all I/O chassis blade slots, type:

```
show /CMM/powermgmt/powerconf/bladeslots granted_power
reserved_power
```

e. To view power allocated property values for a specific component installed in a chassis slot, type:

show /CMM/powermgmt/powerconf/*component-type***/***component-name*

Where *component_type* is the name of the component category and *component-name* is the name of the component

Example:

show /CMM/powermgmt/powerconf/NEMs/NEM*n*

Where *n* is the NEM slot location in the Oracle blade chassis.

Related Information

- "Power Allocation Plan Properties per Managed Device" on page 84
- "Power Allocated Components and Monitoring Considerations" on page 88
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting CMM Power Grant and SP Power Limit Properties" on page 184
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting SP Advanced Power Capping Policy to Enforce Power Limit" on page 187
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting the CMM Power Supply Redundancy Policy" on page 191

Power Allocation Plan Properties per Managed Device

TABLE: System Power Specification Properties (Power Allocation)

Power Metric Property (read-only)	Managed Device	Description
Power Supply Maximum (`/`*SP*`|`*CMM*`/powermgmt available_power`)	x86 SP CMM	The *Power Supply Maximum* property value, shown in Oracle ILOM interfaces, represents the maximum input power wattage that the power supplies are capable of drawing from the power outlets.
Redundant Power (`/CMM/powermgmt redundant_power`)	CMM	The *Redundant Power* property value, shown in Oracle ILOM interfaces, represents the available power wattage currently not allocated to the blade chassis power supplies. **Note -** The power wattage for the redundant power property is configurable through the CMM Power Supply Redundancy Policy. For further details, refer to *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Set CMM Power Supply Redundancy Policy" on page 191.
Installed Hardware Minimum	Blade SP	The *Installed Hardware Minimum* property value, shown in Oracle ILOM web interface, represents the minimum input power wattage consumed by the hardware components installed on the server.

TABLE: System Power Specification Properties (Power Allocation) *(Continued)*

Power Metric Property (read-only)	Managed Device	Description
Peak Permitted (*/SP|CMM*/powermgmt permitted_power)	x86 SP SPARC SP CMM	The *Peak Permitted* property value, shown in Oracle ILOM interfaces, represents the maximum power wattage consumption guaranteed to the managed device. For instance: • For Oracle x86 and SPARC servers, the Peak Permitted property represents the maximum input power wattage that the server can consume at any instant. • For Oracle CMMs, the Peak Permitted property represents the maximum input power wattage a blade server can consume at any instant. *Important monitoring considerations:* • Not all Oracle x86 server SPs support the property for Target Limit in the Oracle ILOM interfaces. In these instances, the same property value (wattage) shown for Peak Permitted is derived by the power consuming hardware components installed on the managed server. • For a server SP, Oracle ILOM derives the wattage value shown for Peak Permitted from the property values shown for Allocated Power and Target Limit. If the Target Limit property is not supported, Oracle ILOM derives the Peak Permitted property value from the power consuming hardware components installed on the managed server. For further information about budgeting power that is consumed by a managed device, refer to *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Setting Power Alert Notifications and Managing System Power Usage" on page 181.
Allocated Power (*/SP|CMM*/powermgmt allocated_power)	x86 SP SPARC SP CMM	The *Allocated Power* property value, shown in Oracle ILOM interfaces, represents the maximum input power wattage allocated to a managed device. For example: • For an Oracle rackmounted server, the Allocated Power property value represents the total sum of the maximum power allocated to all installed chassis components and hot-pluggable components configured on the rackmount server. • For an Oracle blade chassis, the Allocated Power property value represents: 1) the maximum power wattage that is allocated to all installed chassis components, and 2) the maximum power wattage granted to all chassis server blades.

TABLE: System Power Specification Properties (Power Allocation) *(Continued)*

Power Metric Property (read-only)	Managed Device	Description
Target Limit (`/SP/powermgmt/budget powerlimit`)	x86 SP SPARC SP	The *Target Limit* property value, shown in Oracle ILOM interfaces, displays the power limit value (wattage or percentage) configured on the server. *Important power monitoring considerations:* • Oracle ILOM uses the set power limit value to determine the power budgeting parameters allowed for an Oracle server. • When a power limit is not configured in Oracle ILOM, the read-only Target Limit property value `Not Configured` appears in the Power Allocation Plan. • Not all Oracle x86 server SPs support a Target Limit property in Oracle ILOM interfaces. When a Target Limit property is not supported, Oracle ILOM will determine the Peak Permitted wattage value based on the power consuming hardware components installed on the managed server. For more information about power budgeting or instructions for configuring a power limit, refer to *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting Power Alert Notifications and Managing System Power Usage" on page 181.

TABLE: Per Component Power Map Properties (SP Power Allocation)

Power Metric Property (read-only)	Managed Device	Description
Allocated Power (`/SP/powermgmt allocated_power`)	x86 SP SPARC SP	The *Allocated Power* property value, shown in Oracle ILOM SP interfaces, represents the total sum of power wattage allocated to either: 1) a server component category (CPUs), or 2) an individual component installed on the server (MB_P0).
Can be capped	x86 SP SPARC SP	A Yes or No property value, per server component, appears in the Oracle ILOM SP web interface to indicate whether a power budget limit can be set for that server component. **Note -** If power budgeting (Target Limit property) is not supported by the managed server, the "Can be capped" property will not appear in the Power Management Allocation Plan. For further information about power budgeting, refer to *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting Power Alert Notifications and Managing System Power Usage" on page 181.

TABLE: Blade Slot Power Summary (CMM Power Allocation)

Power Metric Property (read-only)	Managed Device	Description
Grantable Power (`/CMM/powermgmt grantable_power`)	CMM blade slot	The *Grantable Power* property value, shown in the Oracle ILOM CMM interface, represents the remaining power wattage that the CMM can allocate to the blade chassis slots without exceeding the grant limit.
Unfilled Grant Requests	CMM blade slot	The *Unfilled Grant Requests* property value, shown in the Oracle ILOM CMM web interface, represents the ungranted power wattage that the CMM has been requested to grant to the chassis blade slots.

TABLE: Blade Power Grants (CMM Power Allocation)

Power Metric Property	Managed Device	Description
Grant Limit (`/CMM/powermgmt/powerconf/ bladeslots/BL`*n* `grant_limit`)	CMM blade slot	The user-defined *Grant Limit* property value, shown in Oracle ILOM CMM interfaces, represents the maximum sum of power wattage the CMM can grant to a blade slot. For instructions on setting the Grant Limit property, refer to *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Set CMM Blade Slot Grant Limit Property" on page 184.
Required Power (`/CMM/powermgmt/advanced/`*n* `value`)	CMM blade slot	The read-only *Required Power* property value, shown in Oracle ILOM CMM interfaces, represents the maximum sum of power wattage required for either: 1) all blade slots, or 2) an individual blade slot.
Granted Power (`/CMM/powermgmt/powerconf/ bladeslots granted_power` or `/CMM/powermgmt/powerconf/b ladeslots/BL`*n* `granted_power`	CMM blade slot	The read-only *Granted Power* property value, shown in the Oracle ILOM CMM interfaces, represents the maximum sum of power wattage the CMM has granted to either: 1) all blade slots requesting power, or 2) an individual blade slot requesting power.

TABLE: Chassis Component Properties (CMM only)

Power Metric Property (read-only)	Managed Device	Description
Allocated Power (`CMM/powermgmt/powerconf/`*`component_type/component_name`*`allocated_power`)	CMM component	The read-only *Allocated Power* property value, shown in Oracle ILOM CMM interfaces, represents the total sum of power wattage allocated to either: 1) an Oracle blade chassis category (fans), or 2) an individual chassis component installed (fan0). **Note -** If the Oracle blade chassis configuration supports I/O blade servers, Oracle ILOM will also display the maximum sum of power wattage reserved for all I/O blade servers.

Power Allocated Components and Monitoring Considerations

- TABLE: Server SP Power Allocated Components on page 88
- TABLE: CMM Power Allocated Components on page 89
- TABLE: Power Allocations Monitoring Considerations on page 89

TABLE: Server SP Power Allocated Components

Server Component	Allocated Power	Applicable to Oracle x86 and SPARC Servers	Applicable to Oracle Blade Servers
All server power consuming components	X	X	X
CPUs	X	X	X
Memory Modules, such as DIMMs	X	X	X
I/O Modules such as such as HDDs, PEMs* REMs*, RFEMs*	X	X	X
Motherboard (MB)	X	X	X
Power Supply Units (PSUs)	X	X	Does not apply†
Fans (FM)	X	X	Does not apply+

* These server related I/O modules (PEMs REMs and RFEMs) apply only to an Oracle blade chassis configuration.

† When these devices (PSUs and FM) are installed in an Oracle blade chassis, they are allocated power by the CIMM.

TABLE: CMM Power Allocated Components

CMM Component	Granted Power (Watts)	Grant Limit (Watts)	Grantable Power (Watts)
All CMM power-consuming components (aggregate value for all powered entities listed)	X	X	X
Blade slots (BL#)	X	X*	Does not apply
CMM	X	Does not apply	Does not apply
Network Express Modules (NEMs)	X	Does not apply	Does not apply
Power Supply Units (PSUs)		Does not apply	Does not apply
Fans (FM)		Does not apply	Does not apply

* The Grant Limit allocated to blade slots is user configurable.

TABLE: Power Allocations Monitoring Considerations

Power Allocated Components	Oracle ILOM Power Allocation Behavior
Oracle rackmounted servers	Power allocated to an Oracle rackmounted server is the maximum power the rackmount chassis components are capable of consuming. This value represents the maximum power wattage consumed by the processors, memory, I/O, fans, as well as the power loss across the power supplies. If the rackmount chassis contains slots for hot-pluggable components, the Power Allocated property value shown represents the maximum power wattage required for the most power-consuming component that can be installed in the hot-pluggable slot.
Oracle blade servers	Power to an Oracle blade server is allocated by the CMM when a request for power is made by the blade server. The blade server requests power whenever it is powered on, and releases power to the CMM whenever it is powered off. The CMM allocates power to the blade server if the grantable power is sufficient to meet the blade server's request. In addition, the CMM will verify whether a Grant Limit is set for the corresponding blade slot. If a Grant Limit is set for the corresponding blade slot, the CMM will allocate power to the blade server only when the power wattage request is less than or equal to the Grant Limit property set for the blade slot.
Oracle auto-powered I/O blades	Since Oracle I/O blade servers are not managed by an SP, I/O blade servers will not seek permission to power-on from the CMM. When an I/O blade server is installed in an Oracle blade chassis, the I/O blade server will automatically power on.

TABLE: Power Allocations Monitoring Considerations *(Continued)*

Power Allocated Components	Oracle ILOM Power Allocation Behavior
Hot-pluggable chassis components	Oracle ILOM automatically displays a pre-allocated maximum power value for any known hot-pluggable component that is installed in a hot-plug designated chassis slot location. For example: • For rackmount hot-pluggable slots, Oracle ILOM displays the known maximum power wattage value required for a hot-pluggable component. • For blade hot-pluggable slots, Oracle ILOM displays the maximum power value required for any Oracle I/O blade server that could be installed in the blade chassis slot. However, if the Oracle blade chassis does not support I/O blade servers, Oracle ILOM displays the maximum power wattage value required for a CPU blade server. To determine which components or slots in a rackmount chassis or blade chassis are hot-pluggable, refer to the Oracle server or blade chassis documentation.
Chassis component categories	For chassis component categories that include multiple instances of the same component, Oracle ILOM presents the total sum of power allocated for a component category (fans), as well as the total sum of power allocated to an individual component (fan0).
Power supply unit (PSU)	Oracle ILOM automatically allocates power to the power supply to account for power losses between the wall outlet and the managed device.

Analyzing Power Usage Statistics

To help analyze the power consumed by a managed device, Oracle ILOM provides power statistic usage properties in bar graphs and tabular output. For more details, see these topics:

- "Rolling Average Power Statistics Graphs and Metrics" on page 91
- "View Power Statistics Bar Graphs and Metrics" on page 91

Rolling Average Power Statistics Graphs and Metrics

Oracle ILOM presents power metrics and bar graphs depicting a rolling average of power consumption in 15-, 30-, and 60-second intervals per managed device. These power usage metrics and bar graphs are particularly useful for analyzing energy consumption by a managed device.

▼ View Power Statistics Bar Graphs and Metrics

1. **To display the power usage metrics and bar graph from the CMM or SP web interface, click Power Management > Statistics.**
   - View the power wattage values and time intervals presented in the bar graph and in the Power History table.
   - For the CMM bar graph, you can toggle the graph display between the chassis power usage and the blade server power usage.

Note – Power statistics graphs are not available for Oracle I/O blade servers installed in an Oracle blade chassis. Power history metrics appearing in the Power Usage Averages table will show a **No Data** property value for each I/O blade server installed in a blade chassis.

---

2. **To access the CMM power statistics for 15-, 30-, and 60-second intervals from the CMM CLI, type:**

   ```
   show /CH/VPS/history
   ```

Note – Power usage statistics for 15-, 30-, and 60-second intervals are not available from the SP CLI. However, if the `/SYS` CLI legacy target is supported on the managed server SP, you can view the power statistics from the `/SYS/VPS/history` CLI target. The `/SYS` legacy target is, by default, hidden. To reveal the `/SYS` legacy target, see "Show or Hide Oracle ILOM 3.0 CLI Legacy Targets" on page 27.

Related Information

- "Power History Graphs and Metrics" on page 92
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting CMM Power Grant and SP Power Limit Properties" on page 184
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting SP Advanced Power Capping Policy to Enforce Power Limit" on page 187

- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Setting the CMM Power Supply Redundancy Policy" on page 191

Comparing Power History Performance

To help compare the power usage over time for a managed device, Oracle ILOM provides history statistics in bar graphs and tabular output. For more details, see:

- "Power History Graphs and Metrics" on page 92
- "View Power History Graphs and Metrics" on page 92

Power History Graphs and Metrics

Oracle ILOM presents history metrics and a series of bar graphs depicting the minimum, average, and maximum power consumption in:

- 1-hour intervals for a managed device
- 14-day intervals for a managed device
- 1-minute intervals in the last hour for a managed device
- 1-hour intervals in the last 14 days for a managed device

The power history metrics and graphs presented by Oracle ILOM are particularly helpful when comparing the best, average, and worst energy performance of a managed device.

▼ View Power History Graphs and Metrics

1. **To display the power history metrics and bar graphs from the CMM or SP web interface, click Power Management > History.**
   - **SP** – You can toggle the graph display between a 1-hour interval and a 14-day interval.
   - **CMM** – You can change the graph display by click the following options:
     - **Hardware options**: Toggle the power usage between chassis power usage and blade power usage.

Note – Power history graphs are not available for Oracle I/O blade servers installed in an Oracle blade chassis. Power history metrics appearing in the Power History table will show a **No Data** property value for each I/O blade server installed in a blade chassis.

- **Time period:** Toggle history between 1-hour and 14-day intervals.
- **Graph series**: Toggle the graph series between Minimum power consumed (watts), Average power consumed (watts), Maximum power consumed (watts), or select a combination of these options.

2. **To view additional power history sample sets from the SP or CMM web interface, click the links under the Sample Set column in the Power History table:**

   The Sample Set links enable you to view a bar graph depicting power consumption wattages in 1-minute intervals over the last hour, or 1-hour intervals over the last 14 days.

Note – The power history metrics and graphs presented by Oracle ILOM are not available from the SP CLI. However, you can from the CMM CLI view the power history consumption metrics by minute or hour and view the time stamps and power wattages for these sample sets by typing these `show` commands:

```
show /CH/VPS/history/0
show /CH/VPS/history/0/list
```

Related Information

- "Rolling Average Power Statistics Graphs and Metrics" on page 91
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting CMM Power Grant and SP Power Limit Properties" on page 184
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting SP Advanced Power Capping Policy to Enforce Power Limit" on page 187
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Set CMM Power Supply Redundancy Policy" on page 191

Managing Oracle Hardware Faults Through the Oracle ILOM Fault Management Shell

Description	Links
Refer to this section for topics describing hardware fault notifications, corrective action, and auto clearing of faults.	• "Protecting Against Hardware Faults: Oracle ILOM Fault Manager" on page 96
Refer to these sections for instructions for launching and running fault management commands from the Oracle ILOM Fault Management Shell.	• "Oracle ILOM Fault Management Shell" on page 97 • "Using fmadm to Administer Active Oracle Hardware Faults" on page 100 • "View Information About Active Faulty Components (fmadm faulty)" on page 100 • "Using fmdump to View Historical Fault Management Logs" on page 105 • "Using fmstat to View the Fault Management Statistics Report" on page 107

Related Information

- *Oracle x86 Server Diagnostics Guide For Servers With Oracle ILOM 3.1*
- Service manual for Oracle server

Protecting Against Hardware Faults: Oracle ILOM Fault Manager

The Fault Manager in Oracle ILOM is intended to help with problems that might occur on an Oracle ILOM managed device. For instance, the Fault Manager detects and interprets errors and determines whether a fault or defect is present on a managed system. When a determination is made, the Fault Manager issues a list of suspected hardware components that might be the cause of the problem.

For additional information about how Oracle ILOM helps to enhance uptime when hardware faults are detected on a managed device, see:

- "Hardware Fault Notifications" on page 96
- "Hardware Fault Corrective Action" on page 97
- "Fault Events Cleared: Repaired Hardware" on page 97

Hardware Fault Notifications

Notifications indicating that a hardware fault or defect has been diagnosed appears in the Open Problems tabular output, which is viewable by Oracle hardware customers from the Oracle ILOM interfaces. In addition to the hardware fault notifications provided in the Open Problems output, the Fault Manager also logs event messages to the event log and the Fault Management logs. Customers can view the event log from the Oracle ILOM interfaces. Oracle Services personnel can view the Fault Management logs from the Oracle ILOM Fault Management Shell.

Note – You can also configure notification of fault events by using the Simple Network Management Protocol (SNMP) or Simple Mail Transfer Protocol (SMTP). For SNMP configuration details, refer to *Oracle ILOM 3.1 Protocol Management Reference Guide,* "Configuring SNMP Settings in Oracle ILOM" on page 9. For SMTP configuration details, refer to *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Configure SMTP Client for Email Alerts" on page 172.

Hardware Fault Corrective Action

When notified of a diagnosed problem, always consult the recommended knowledge article for additional details. An http:// reference is provided to the recommended knowledge article in the event notification in the Open Problems output, as well in the event messages in the log files.

Fault Events Cleared: Repaired Hardware

Fault events and notifications in Oracle ILOM are automatically cleared when the repaired or replaced resource is an associated with a field-replaceable unit (FRU). When a repaired or replaced resource is not associated with a FRU, Oracle ILOM is unable to detect the repair or replacement; therefore, the fault event notification is not cleared automatically in the Open Problems output or in the log files. For information about clearing fault events in Oracle ILOM for undetected repairs or replacements, see "Clearing Faults for Repairs or Replacements" on page 101.

Oracle ILOM Fault Management Shell

The Oracle ILOM Fault Management Shell enables Oracle Services personnel to view and manage fault activity detected on a managed device.

For further information about how to use the Oracle ILOM Fault Management Shell, see these topics:

- "Fault Management Terminology" on page 98
- "Launch a Fault Management Shell Session (CLI)" on page 99

Caution – The purpose of the Oracle ILOM Fault Management Shell is to help Oracle Services personnel diagnose system problems. Customers should not launch this shell or run fault management commands in the shell unless requested to do so by Oracle Services.

Fault Management Terminology

Term	Description
Proactive self-healing	Proactive self-healing is a fault management architecture and methodology for automatically diagnosing, reporting, and handling software and hardware fault conditions. Proactive self-healing reduces the time required to debug a hardware or software problem and provides the administrator or Oracle Services personnel with detailed data about each fault. The architecture consists of an event management protocol, the Fault Manager, and fault-handling agents and diagnosis engines.
Diagnosis engines	The fault management architecture, in Oracle ILOM, includes *diagnosis engines* that broadcast fault events for detected system errors. For a list of diagnosis engines supported in the fault management architecture for Oracle ILOM, see "fmstat Report Example and Description" on page 107.
Health states	Oracle ILOM associates the following *health states* with every resource for which telemetry information has been received. The possible states presented in Oracle ILOM interfaces include: • **ok** – The hardware resource is present in the chassis and in use. No known problems have been detected. • **unknown** – The hardware resource is not present or not usable, but no known problems are detected. This management state can indicate that the suspect resource is disabled by the system administrator. • **faulted** – The hardware resource is present in the chassis but is unusable since one or more problems have been detected. The hardware resource is disabled (offline) to prevent further damage to the system. • **degraded** – The hardware resource is present and usable, but one or more problems have been detected. If all affected hardware resources are in the same state, this status is reflected in the event message at the end of the list. Otherwise, a separate health state is provided for each affected resource.
Fault	A *fault* indicates that a hardware component is present but is unusable or degraded because one or more problems have been diagnosed by the Oracle ILOM Fault Manager. The component has been disabled to prevent further damage to the system.
Managed device	A *managed device* can be an Oracle rackmounted server, blade server, or blade chassis.
FRU	A *FRU* is a field-replaceable unit (such as a drive, memory DIMM, or printed circuit board).
CRU	A *CRU* is a customer-replaceable unit (such as a NEM in an Oracle blade chassis.).

Term	Description
Universal unique identifier (UUID)	A *UUID* is used to uniquely identify a problem across any set of systems.

▼ Launch a Fault Management Shell Session (CLI)

Before You Begin

- Oracle hardware customers should seek permission from Oracle Services prior to performing this procedure.
- Admin (a) role privileges are required to launch the Fault Management Shell from the Oracle ILOM CLI.

To launch the Oracle ILOM Fault Management Shell:

1. **If you have not done so, log into the CLI, as described in** "Log In to the Oracle ILOM CLI" on page 11**.**

   The Oracle ILOM CLI prompt (->) appears.

2. **To launch a Fault Management Shell session, type:**

   ```
   start /SP/faultmgmt/shell
   ```

   One of the following Fault Management Shell command prompts appears:

   - faultmgmtsp> appears for Oracle SP managed devices.
   - *faultmgmtcmm*> appears for Oracle CMM managed devices.

Note – After you start the Fault Management Shell and until you exit the Fault Management Shell, you can issue only commands that are specific to the Fault Management Shell.

---

3. **To run Fault Management Shell commands, perform any of the following:**
   - Administer active faulty components (display faulty components or clear faults for undetected repairs or replacements); see "Using fmadm to Administer Active Oracle Hardware Faults" on page 100.
   - View historical fault management activity; see "Using fmdump to View Historical Fault Management Logs" on page 105.
   - View a statistical report of fault management operations; see "Using fmstat to View the Fault Management Statistics Report" on page 107.

4. **To display help information for one of following external commands, type:**

   `help fmadm`

   `help fmdump`

   `help fmstat`

5. **To exit the Fault Management Shell, at the `faultmgmt` prompt, type:**

   `exit`

Note – To issue standard Oracle ILOM CLI commands, you must first exit the Fault Management Shell.

Related Information

- "Using fmadm to Administer Active Oracle Hardware Faults" on page 100
- "Using fmdump to View Historical Fault Management Logs" on page 105
- "Using fmstat to View the Fault Management Statistics Report" on page 107

Using `fmadm` to Administer Active Oracle Hardware Faults

Use the `fmadm` utility in the Fault Management Shell to view and manage active Oracle hardware faults that are conventionally maintained by the Oracle ILOM Fault Manager. For further details on how to view and manage fault behavior using the `fmadm` utility, see these topics:

- "View Information About Active Faulty Components (fmadm faulty)" on page 100
- "Clearing Faults for Repairs or Replacements" on page 101

▼ View Information About Active Faulty Components (`fmadm faulty`)

Note – For Oracle hardware customers, the preferred method for viewing active information about faulty components is to view the health state of a component in the Open Problems tabular output, which is provided in the Oracle ILOM CLI and web interface.

---

1. **If you have not done so, launch the Fault Management Shell from the CLI, as described in** "Launch a Fault Management Shell Session (CLI)" on page 99**.**

   The `faultmgmtsp>` or `faultmgmtcmm>` prompt appears.

2. **To view information about active faulty hardware components reported for a managed device, type:**

   `fmadm faulty` <*display_option*>

   For example, to view:

   - All active faulty components, type:

     `fmadm faulty -a`

   - Active faulty FRUs, type:

     `fmadm faulty -f`

   - Active fault FRUs and their fault management states, type:

     `fmadm faulty -r`

   - One-line fault summary for each fault event, type:

     `fmadm faulty -s`

   - Fault diagnosis events that match a specific universal unique identifier (UUID), type:

     `fmadm faulty -u` <*uuid*>

3. **When applicable, refer to the `http://` referenced knowledge article in the `fmadm faulty` output for further instructions for resolving a reported problem.**

Related Information

- "Fault Management Terminology" on page 98
- "Clear Faults for Undetected Replaced or Repaired Hardware Components" on page 103
- "Administering Open Problems" on page 41

Clearing Faults for Repairs or Replacements

After you replace or repair a faulted component on a managed device, the Oracle ILOM Fault Manager automatically detects the repair or replacement and clear the associated fault message from the system. However, if the replaced or repaired hardware component is not associated with a FRU serial number, the corrective service action is not detected by Oracle ILOM, nor are the fault event messages associated with the undetected repair cleared from the Oracle ILOM interfaces.

Note – The Oracle ILOM Fault Manager is unable to detect repair or replacement service actions for Oracle blade chassis customer-replaceable units (CRUs).

With the permission of Oracle Services personnel, a customer can issue `fmadm` repair commands from the Oracle ILOM Fault Management Shell to manually clear fault messages for undetected repair or replacement service actions. For more information, see these topics:

- "fmadm Command Usage and Syntax" on page 102
- "Clear Faults for Undetected Replaced or Repaired Hardware Components" on page 103

`fmadm` Command Usage and Syntax

fmadm Repair Command	Use to:
`acquit` *fru*|*cru*	Notify the Oracle ILOM Fault Manager that the specified faulted component is not to be considered suspect in any fault events that have been detected. The `fmadm acquit` command should be used only at the direction of a documented Oracle hardware repair procedure. **Syntax example:** To instruct the Fault Manager to ignore a suspect fan module in a rackmounted server chassis, type: **`fmadm acquit /SYS/FANBD/FM`***n*
`acquit` *uuid*	Notify the Oracle ILOM Fault Manager that the faulted event identified by the *uuid* resource can be safely ignored. The `fmadm acquit` command should be used only at the direction of a documented Oracle hardware repair procedure. **Syntax example:** To instruct the Fault Manager to ignore the event identified by 6d76a0f4-b5f5-623c-af8b-9d7b53812ea1, type: **`fmadm acquit 6d76a0f4-b5f5-623c-af8b-9d7b53812ea1`**

fmadm Repair Command	Use to:
`repaired` *fru*|*cru*	Notify the Oracle ILOM Fault Manager that a repair procedure has been performed on the specified field-replaceable unit or customer-replaceable unit. The `fmadm repaired` command should be used in those cases where Oracle ILOM's Fault Manager is unable to detect the repaired FRU. **Syntax example:** To notify the Fault Manager that a fan module in a rackmount server chassis has been repaired, type: **`fmadm repaired /SYS/FANBD/FM`***n* **Note -** The `repair` command is equivalent to the `repaired` command.
`replaced` *fru*|*cru*	Notify the Oracle ILOM Fault Manager that the specified faulted field-replaceable unit or customer-replaceable unit has been replaced. This command should be used in those cases where Oracle ILOM is unable to automatically detect the replacement. **Syntax example:** To notify the Fault Manager that a fan module in a rackmount server chassis has been replaced, type: **`fmadm replaced /SYS/FANBD/FM`***n*

▼ Clear Faults for Undetected Replaced or Repaired Hardware Components

Before You Begin

- Oracle hardware customers should seek permission from Oracle Services prior to performing this procedure.
- Review "fmadm Command Usage and Syntax" on page 102.
- If a fault event is cleared prior to completing the corrective service action required for the faulty component, the Oracle ILOM Fault Manager diagnoses the fault and redisplays the fault event in the Oracle ILOM Open Problems table, as well as in the Oracle ILOM Fault Management log files.

To clear faults for undetected hardware repairs or replacement:

1. **If you have not done so, launch a Fault Management Shell from the Oracle ILOM CLI, as described in** "Launch a Fault Management Shell Session (CLI)" on page 99**.**

   The `faultmgmtsp>` or `faultmgmtcmm>` prompt appears.

2. **Identify and display information about active suspect components; see** "View Information About Active Faulty Components (fmadm faulty)" on page 100**.**

3. **To manually clear a fault for an undetected replaced or repaired hardware components, type the appropriate repair commands:**

- To indicate that a suspect component has been replaced or removed, type:

  `fmadm replaced` <*fru* | *cru*>

- To indicate that a suspect component has been physically repaired to resolve the reported problem (for example, reseating a component or fixing a bent pin), type:

  `fmadm repaired` <*fru* | *cru*>

- To indicate that a suspect component is not the cause of the problem, type:

  `fmadm acquit` <*fru* | *cru* | *uuid*>

  Where <*fru* | *cru* | *uuid*> appears, type the system path to the suspect chassis FRU or CRU; or type the associated universal unique identifier (*uuid*) for the resource reported in the problem.

Note – A replacement takes precedence over repair, and both replacement and repair take precedence over acquittal. Thus, you can acquit a component and then subsequently repair it, but you cannot acquit a component that has already been repaired.

For syntax descriptions and examples, see "fmadm Command Usage and Syntax" on page 102.

4. **To display the exit code for the last executed fault management command, type:**

   `echo $?`

   One of the following echo codes appears:

Code	Description
0	Successful completion.
1	An error occurred. Errors include a failure to communicate with Oracle ILOM or insufficient privileges to perform the requested operation.

Related Information

- "Fault Management Terminology" on page 98
- "View Information About Active Faulty Components (fmadm faulty)" on page 100
- "Administering Open Problems" on page 41

Using `fmdump` to View Historical Fault Management Logs

The Oracle ILOM Fault Manager maintains historical information about system problems in two sets of log files for Oracle Services personnel use. A log file set can consist of active system events together with a possible number of older system events.

- "Log File Display Commands and Log Descriptions" on page 105
- "View Fault Management Log Files (fmdump)" on page 105

Log File Display Commands and Log Descriptions

Display command	Target log	Description
`fmdump`	Fault log	The fault management *fault log* records human-readable fault diagnosis information and the problems possibly related to the symptoms. A time stamp and description is provided for each event recorded.
`fmdump -e`	Error log	The fault management *error log* records error telemetry and the symptoms of problems detected by the system. Each problem recorded, identifies: • A time stamp for when the problem was detected. • A universal unique identifier (UUID) that uniquely identifies a particular problem across any set of systems. • An http:// identifier that provides access to a corresponding knowledge article posted on the Oracle support web site.

Caution – Do not base administrative service actions on content in the fault management historical log files, but rather on the active `fmadm faulty` output. The fault management log files contain historical events, which should not be considered active events for faults or defects.

▼ View Fault Management Log Files (`fmdump`)

Before You Begin

- Oracle hardware customers should seek permission from Oracle Services prior to performing this procedure.

- Review "Log File Display Commands and Log Descriptions" on page 105.

To view the fault management log files:

1. **If you have not done so, launch a Fault Management Shell from the CLI, as described in "Launch a Fault Management Shell Session (CLI)" on page 99.**

   The `faultmgmtsp>` or `faultmgmtcmm>` prompt appears.

2. **To display the contents maintained in a fault management log file set, perform one of the following:**
   - To display the fault log, type:

     `fmdump`
   - To display a fault log for a specific universal unique identifier (uuid), type:

     `fmdump -u` *<uuid>*
   - To display the error log, type:

     `fmdump -e`

Note – For the fault log, in particular, it is important to recognize that `fmdump` shows all problems ever diagnosed and is not limited to active problems diagnosed. To view active faults only, issue the `fmadm faulty` command.

---

3. **To rotate the log display, type one of following:**
   - To rotate the fault log display, type:

     `fmadm rotate fltlog`
   - To rotate the error log display, type:

     `fmadm rotate errlog`

4. **To display the exit code for the last executed fault management command, type:**

   `echo $?`

   One of the following echo codes appears:

Code	Description
0	Successful completion. All records in the log file were examined successfully.
1	Invalid command-line options were specified.

Related Information

- "Fault Management Terminology" on page 98
- "View Information About Active Faulty Components (fmadm faulty)" on page 100
- "Administering Open Problems" on page 41

Using `fmstat` to View the Fault Management Statistics Report

The Oracle ILOM Fault Manager maintains a viewable statistics report about diagnosis engines and agents participating in fault management operations. For more details about this report, see:

- "fmstat Report Example and Description" on page 107
- "View the Fault Management Statistics Report (fmstat)" on page 109

`fmstat` Report Example and Description

- "fmstat Report Example" on page 108
- "fmstat Report Property Descriptions" on page 108

`fmstat` Report Example

```
faultmgmtsp> fmstat
fdd statistics    2011-02-03/19:12:51

engine               status    evts_in  evts_out  errors
repair               empty           8         0       0
hysteresis           empty           0         0       0
SERD                 empty           0         0       0
simple               empty          12         0       0
```

`fmstat` Report Property Descriptions

Property	Description
`engine`	The *engine* column in the `fmstat` tabular output identifies the name of the diagnosis engine: • **repair** – Rule that indicates a fault should be considered repaired if a specified ereport is logged. For example, the fault `fault.chassis.power.inadequate@/sys` would be considered repaired if `ereport.chassis.boot.power-off-requested@/system` was logged. • **hysteresis** – Rule to diagnose a fault if ereport *A* (initiation) is logged and ereport *B* (cancellation) is not logged within some specified time afterward. For example, ereport A is `ereport.fan.speed-low-asserted` and ereport B is `ereport.fan.speed-low-deasserted`. The time limit between the initiation/cancellation can be no greater than 10 seconds. • **SERD** – Soft error rate discrimination (SERD) is used in tracking multiple occurrences of an ereport. If more than *N* ereports show up within time period *T*, the fault is diagnosed. For example, if too many correctable memory error ereports are logged within a specific time frame, a DIMM fault is diagnosed. • **simple** – Rule to allow one ereport to result in the diagnosis of multiple faults. For example, an ereport for an uncorrectable memory error can be diagnosed to the faults for two DIMMs in a DIMM pair.
`status`	The *status* column in the `fmstat` tabular output identifies the current state of the diagnosis engine, which can include: `uninit`, `empty`, `enqueued`, `busy`, or `exiting`.

Property	Description
`evts_in`	The *evts_in* column in the `fmstat` tabular output identifies the number of events received by the engine as relevant to a diagnosis.
`evts_out`	The *evts_out* column in the `fmstat` tabular output identifies the number of faults detected and posted by the engine.
`errors`	The *errors* column in the `fmstat` tabular output identifies the number of internal errors detected by the engine.

▼ View the Fault Management Statistics Report (`fmstat`)

Before You Begin

- Oracle hardware customers should seek permission from Oracle Services prior to performing this procedure.
- Review "fmstat Report Example and Description" on page 107.

To view statistics for fault management operations:

1. **If you have not done so, launch the Fault Management Shell from the CLI, as described in "Launch a Fault Management Shell Session (CLI)" on page 99.**

   The `faultmgmtsp>` or `faultmgmtcmm>` prompt appears.

2. **To view the fault management statistics report, type:**

   `fmstat`

Related Information

- "Fault Management Terminology" on page 98
- "Using fmadm to Administer Active Oracle Hardware Faults" on page 100
- "Clearing Faults for Repairs or Replacements" on page 101
- "Using fmdump to View Historical Fault Management Logs" on page 105
- "Administering Open Problems" on page 41

Using the Command-Line Interface

Description	Links
Refer to this topic for information about the Distributed Management Task Force command-line protocol.	"About the Command-Line Interface (CLI)" on page 112
Refer to this topic for information about supported CLI syntax, commands, options	"CLI Reference For Supported DMTF Syntax, Command Verbs, Options" on page 112
Refer to this section for topics describing how to execute commands to change target properties.	"CLI Reference For Executing Commands to Change Properties" on page 119
Refer to this section for topics describing where management tasks are performed in the target namespace hierarchy.	"CLI Reference For Mapping Management Tasks to CLI Targets" on page 122

Related Information

- "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22

About the Command-Line Interface (CLI)

The Oracle ILOM CLI is based on the Distributed Management Task Force (DMTF) *Server Management Command-Line Protocol Specification (SM CLP), version 11.0a.8 Draft*. You can view the entire specification at the following site:

`http://www.dmtf.org/`

In Oracle ILOM, the SM CLP provides a user interface for managing your servers regardless of server state, method of access, or installed operating system.

The server management CLP architecture models a hierarchical namespace, which is a predefined tree that contains every managed object in the system. In this model, a small number of commands operate on a large namespace of targets, which can be modified by options and properties. This namespace defines the targets for each command verb.

The server management CLP is also suitable for scripting environments. Using a scripting tool, such as Expect, you can automate testing and facilitate provisioning (such as common configuration and firmware updates) on multiple servers.

For more information about managing objects in the Oracle ILOM CLI namespace, see "Oracle ILOM 3.1 CLI Namespace Targets" on page 23.

Related Information

- "CLI Reference For Executing Commands to Change Properties" on page 119
- "CLI Reference For Mapping Management Tasks to CLI Targets" on page 122

CLI Reference For Supported DMTF Syntax, Command Verbs, Options

Supported CLI Syntax

The supported syntax entered in the Oracle ILOM CLI to execute commands is in the form of:

`<verb>` [`<-option>`] [`<target>`] [`<property>`=<property_value>

Where:

- <verb> — The term verb refers to a specific command or an action being performed. For instance, the use of a command verb enables the retrieving and managing of data (**`set`**, **`show`**), creating or deleting data (**`create`**, **`delete`**), modifying the state of a managed component (**`set`**, **`reset`**, **`start`**, **`stop`**), managing the current CLI session (**`cd`**, **`version`**, **`exit`**), as well as providing command information (**`help`**).

Note – Only one command verb can be issued on a command line.

- <-option> — The term option refers to the command `-option` that is used to modify the action or behavior of a command verb. For instance, the use of an option can provide features for changing the CLI output format, applying a command to nested levels, or executing a script to perform one or more actions.

  When entering an option on the command line, it can appear immediately after the command verb, and it must always be proceeded by a hyphen (-).

Note – Not all command verbs support options. Therefore, there might be zero or more options supported for an issued command verb.

- <target> — The term target refers to the address or path for the issued command verb. For instance, a target can reference individual managed components (for example, a disk, a power supply, a memory module), or a collection of managed components (for example, system).

  When entering a target on the command line, it can appear after the command verb but only one target can be referenced for each issued command verb.
- <property> — The term property is the attribute of the target that might contain values that are needed to process the command. A property identifies a target's class which is retrieved or acted upon by the command.
- =<property_value> — The assignment operator (=) is used to indicate a desired value to be assigned to a specified property.

Related Information

- "Case Insensitivity in the Oracle ILOM 3.1 and Later CLI" on page 22

Basic CLI Commands and Options

The Oracle ILOM CLI supports the following basic commands and options.

Note – The options that are enclosed in squared brackets ([]) are optional, those that are enclosed in angle brackets (<>) are keywords, and those that are separated by a pipe (|) indicate a choice of a keyword or option.

Command	Command Options	Description
`cd`	[`-default`] <*target*>	Navigates the target namespace. **`-default`** — Selects the initial default target.
`create`	<*target*> [<*property*>=<*value*>]	Creates a target and property values in the namespace (for example, to add a user and specify the user's `role` and `password`).
`delete`	[`-script`] <*target*>	Removes an object from the namespace (for example, to delete a user account). **`-script`** — Skips warnings and prompts normally associated with the command (assumes "yes" for prompts).
`dump`	-destination <URI> [-force] [<target>]	Transfers a file from a target to a remote location specified by the URI (for example, a configuration or service snapshot). **`-f`**|**`-force`** — Overrides internal checks and dumps the requested file. **`-destination`** <*URI*> — Specifies the required destination path using the uniform resource identifier (URI) format.
`exit`	None.	Terminates a CLI session.
`help`	[`-format wrap|nowrap`] [`-output terse|verbose`]	Displays Help information for commands, targets, and target properties. **`-format wrap`**|**`nowrap`** — Specifies the screen format for help. **`-o`**|**`-output terse`**|**`verbose`** — Specifies the amount of help text to b e displayed.

Command	Command Options	Description
`load`	[`-output verbose`] [`-force`] [`-script`] `-source` <*URI*>	Transfers a file from an indicated source to an indicated target (for example, a configuration or firmware image). **`-o`**|**`-output verbose`** — Specifies the amount of information text to be displayed. **`-f`**|**`-force`** — Overrides internal checks and dumps the requested file. **`-script`** — Skips warnings and prompts normally associated with the command (assumes "yes" for prompts). **`-source`** <*URI*> — Specifies the required source path using the uniform resource identifier (URI) format.
`reset`	• For X86: [`-script`] <*target*> • For SPARC: [`-script`] [`-force`] <*target*>	Reset a target (for example, the power to a host server or to the service processor). **`-f`**|**`-force`** — Specify the action will be performed immediately. **`-script`** — Skips warnings and prompts normally associated with the command (assumes "yes" for prompts).
`set`	[<*target*>] <*property*>=<*value*> [<*property*>=<*value*>]	Sets target properties to the specified value.
`show`	[`-display targets|properties|commands|all`] |[`-a`] [`-level 1|2|3...255|all`] [`-format wrap|nowrap`] [`-output table`] [`-t`] [<*target*>] [<*property*> <*property*>]	Displays information about targets and properties. **`-d`**|**`-display`** — Specifies the information to be displayed. **`-a`** — Same as `-display all`. **`-l`**|**`-level`** — Specifies the relative level in the target hierarchy to which the action will apply. **`-format wrap`**|**`nowrap`** — Specifies screen format. **`-o`**|**`-output table`** — Specifies to display the output in table format. **`-t`** - Same as `-level all -output table`.

Command	Command Options	Description
`start`	[`-script`] [`-force`] <*target*>	Starts the target (for example, the host system, or an Oracle ILOM internal shell). **`-script`** — Skips warnings and prompts normally associated with the command (assumes "yes" for prompts). **`-f`** | **`-force`** — Overrides internal checks and performs the action immediately.
`stop`	[`-script`] [`-force`] <*target*>	Stops the target (for example, the host system). **`-script`** — Skips warnings and prompts normally associated with the command (assumes 'yes' for prompts). **`-f`** | **`-force`** — Overrides internal checks and performs the action immediately.
`version`	None.	Displays the service processor firmware version.

Related Information

- "Basic Command-Line Editing Keystrokes" on page 117
- "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22
- "CLI Reference For Executing Commands to Change Properties" on page 119
- "CLI Reference For Mapping Management Tasks to CLI Targets" on page 122

Basic Command-Line Editing Keystrokes

The Oracle ILOM CLI supports the following command-line editing keystrokes:

TABLE: Cursor Movement CLI Editing Keystrokes

To:	Press:
Move the cursor to the right.	**Right arrow** -or- **Ctrl+f**
Move the cursor to the left.	**Left arrow** -or- **Ctrl+b**
Move the cursor to the beginning of the command line.	**Ctrl+a**
Move the cursor to the end of the command line.	**Ctrl+e**
Move the cursor forward by one word.	**Esc+f**
Move the cursor backward by one word.	**Esc+b**

TABLE: Text Deletion CLI Editing Keystrokes

To:	Press:
Delete the character before the cursor.	**Backspace** -or- **Ctrl+h**
Delete the character at the cursor.	**Ctrl+d**
Delete the characters starting from the cursor location to the end of the command line.	**Ctrl+k**
Delete the word before the cursor.	**Ctrl+w** -or- **Esc+h** -or- **Esc+Backspace**
Delete the word at the cursor.	**Esc+d**

TABLE: Text Input CLI Editing Keystrokes

To:	Press:
Complete the input of the target or property name.	**Tab**
Abort the command-line input.	**Ctrl**+**c**
Complete the end of multi-line input when using the commands for: `load -source console` or `set load_uri=console`.	**Ctrl**+**z**

TABLE: Command History CLI Editing Keystrokes

To:	Press:
Display the command-line history.	**Ctrl**+**L**
Scroll backward through the command-line history.	**Up arrow** -or- **Ctrl**+**p**
Scroll forward through the command-line history.	**Down arrow** -or- **Ctrl**+**n**

Related Information

- "Basic CLI Commands and Options" on page 114
- "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22
- "CLI Reference For Executing Commands to Change Properties" on page 119
- "CLI Reference For Mapping Management Tasks to CLI Targets" on page 122

CLI Reference For Executing Commands to Change Properties

You can execute most CLI commands by specifying the command, the target, and property values to change. You can choose to execute commands that change single or multiple properties on the same command line. Some properties that can interrupt Oracle ILOM connectivity also require you to confirm the change before the change can take affect in Oracle ILOM.

For further details about executing CLI commands, see the following topics:

- "Executing Commands to Change Target Properties" on page 119
- "Executing Commands That Require Confirmation" on page 120

Executing Commands to Change Target Properties

You can choose to execute commands to change target properties by performing any of the following methods:

- Navigating to the target, looking at its properties, and executing a command.

  For example, to set the HTTP user session time-out for the Oracle ILOM web server to 30 minutes:

```
-> cd /SP/services/http
/SP/services/http

-> show

 /SP/services/http
 Targets:

 Properties:
 port = 80
 secureredirect = disabled
 servicestate = enabled
 sessiontimeout = 15

 Commands:
 cd
 set
```

```
 show

-> set sessiontimeout=30
```

- Entering the command and the full path to the target, from anywhere in the namespace, to change a single property.

  For example:

```
-> set /SP/services/http sessiontimeout=30
```

- Entering the command and the full path to the target, from anywhere in the namespace, to change multiple properties.

  For example:

```
-> set /SP/services/http servicestate=disable secureredirect=
enabled
```

Related Information

- "Executing Commands to Change Target Properties" on page 119
- "Executing Commands That Require Confirmation" on page 120
- "Managing Blade Servers From the CMM CLI" on page 26

Executing Commands That Require Confirmation

For targets where a change in properties can interrupt current user sessions, configuration includes committing the pending change to take affect.

For example, changing the IP network settings for the SP in Oracle ILOM will cause an interruption to the current user sessions. Therefore, you will be required to commit any changes you have made to the IP properties before your changes can take affect in Oracle ILOM.

An example of the process used to commit changes for IP properties appears below:

1. View the current network settings.

```
-> show /SP/network

/SP/network
 Targets:
 interconnect
 ipv6
```

```
  test

  Properties:
  commitpending = (Cannot show property)
  dhcp_clientid = none
  dhcp_server_ip = none
  ipaddress = 192.0.2.22
  ipdiscovery = static
  ipgateway = 192.0.2.1
  ipnetmask = 10.255.255.0
  macaddress = 00:28:25:E7:18:0C
  managementport = MGMT
  outofbandmacaddress = 00:28:25:E7:18:0C
  pendingipaddress = 192.0.2.22
  pendingipdiscovery = static
  pendingipgateway = 192.0.2.1
  pendingipnetmask = 10.255.255.0
  pendingmanagementport = MGMT
  sidebandmacaddress = 00:28:25:E7:18:0D
  state = enabled

  Commands:
  cd
  set
  show

 ->
```

2. To change the settings, first enter the new (pending) information.

```
 ->set /SP/network pendingipdiscovery=static pendingipaddress=
nnn.nn.nn.nn pendingipgateway=nnn.nn.nn.nn pendingipnetmask=nnn.nn.nn.nn
```

3. Then, after you have confirmed that the new settings are correct, commit the new settings and have them take effect immediately:

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

Note – You can also combine the commit property with the pending information in a single command.

Note – If you are connecting to Oracle ILOM over a LAN, you will have to reconnect to Oracle ILOM after committing any IP property changes.

Related Information

- "Executing Commands to Change Target Properties" on page 119
- "Managing Blade Servers From the CMM CLI" on page 26
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting Up a Management Connection to Oracle ILOM and Logging In" on page 1

CLI Reference For Mapping Management Tasks to CLI Targets

Refer to the topics in this section to help identify the applicable CLI namespace targets for the following Oracle ILOM management tasks.

Management Connection Tasks and Applicable CLI Targets

Use the following table to help identify the applicable CLI namespace targets for Oracle ILOM management connection tasks.

For additional information about setting up a management connection to Oracle ILOM, see the topics listed in the Related Information section that appears after the table.

Note – Not all CLI management connection targets are available on all managed systems.

Task	Description	Targets Containing the Necessary Properties	User Role Required to Configure Properties

Configure the Oracle ILOM Ethernet port.	• Enable/disable Ethernet access
	• Select to use the service processor NET MGT port or a host network port (not supported on all systems)
		`/SP/network`
		or
		`/CMM/network`
			Admin (`a`)

Configure the Oracle ILOM NET MGT Ethernet port for IPv4.	• Configure the port for DHCP
	• Configure the port for static IP
		`/SP/network`
		or
		`/CMM/network`
			Admin (`a`)

For dual-stack IPv4/IPv6, configure the Oracle ILOM NET MGT Ethernet port for IPv6.	• Configure the port for autoconfiguration
	• Configure the port for DHCPv6
	• Configure a static IPv6 address for the port
	• View IPv6 dynamic addresses
		`/SP/network`
		`ipv6`
		or
		`/CMM/network`
		`ipv6`
			Admin (`a`)

Test the network port.	• Send an IPv4 or IPv6 test ping	`/SP/network`
		`test`
		or
		`/CMM/network`
		`test`
			Read only (`o`)

Task	Description	Targets Containing the Necessary Properties	User Role Required to Configure Properties
Configure domain name service (DNS) resolution support for Oracle ILOM.	• Enable DNS resolution • Configure the IP address for the name server • Configure the domain search path • Configure name search attempts	/SP/clients dns	Admin (a)
Configure the Oracle ILOM internal USB Ethernet port.	• Configure the interconnect port for host management (recommended) • Configure the interconnect port for static IP	/SP/network interconnect	Admin (a)
Configure the Oracle ILOM SER MGT serial port.	• Configure the external SER MGT port settings • Configure host internal port settings • Pass ownership of the SER MGT port between the service processor and the host **Note -** Passing ownership of the SER MGT port to the host should be done only if an Ethernet connection to Oracle ILOM is also available.	/SP/serial external host portsharing	Admin (a)

Related Information

- "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting Up a Management Connection to Oracle ILOM and Logging In" on page 1
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Configure a Dedicated Network Management Connection to Oracle ILOM" on page 3
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Configure a Sideband Management Connection to Oracle ILOM" on page 5
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Manually Configure the Local Interconnect" on page 10
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Configure a Dedicated Local Management Connection to Oracle ILOM" on page 7

Network Deployment Tasks and Applicable CLI Targets

Use the following table to help identify the applicable CLI namespace targets for Oracle ILOM network deployment tasks.

For additional information about modifying default network deployment properties in Oracle ILOM, see the topics listed in the Related Information section that appears after the table.

Task	Description	Targets Containing the Necessary Properties	User Role Required to Configure Properties
Configure Oracle ILOM web management access.	• Configure web HTTP access • Configure web HTTPS access and authentication • Configure web session time-out • Configure CLI SSH access and authentication • Configure Single Sign On (When done through the CMM, you can access all blade chassis components with one login.)	/SP/services http https ssh sso or /CMM/services http https ssh sso	Admin (a)
Configure CLI session time-out.	• Configure CLI session time-out	/SP/cli or /CMM/cli	Admin (a)
View details on Oracle ILOM user sessions.	• View currently logged in users (name, roles) • Obtain details of session	/SP/sessions or /CMM/sessions	Read only (o)

Task	Description	Targets Containing the Necessary Properties	User Role Required to Configure Properties

Set management protocol support.	• Configure the IPMI service
	• Configure the SNMP service (including MIB access)
	• Configure WS-Management access
	Note - In order for SNMP Set Request operations to succeed, you need to use an SNMP v1 or v2c community or an SNMP v3 user account with read-write (rw) privileges.
	Note - WS-Management is done through a WS-Management client outside of Oracle ILOM. The `wsman` HTTP/HTTPS ports must be different from the Oracle ILOM web HTTP/HTTPS ports.
		`/SP/services`
		`ipmi`
		`snmp`
		`wsman`
		or
		`/CMM/services`
		`ipmi`
		`snmp`
		`wsman`
			Admin (a)

Set system description information.	• Specify the host name and system description
	• Specify a system identifier (used with DHCP)
	• Specify location and contact information
		`/SP`
		or
		`/CMM`
			Admin (a)

Set banner messages.	• Create connection messages
	• Create login messages
		`/SP/preferences`
		`banner`
		or
		`/CMM/preferences`
		`banner`
			Admin (a)

Set the Oracle ILOM date and time.	• Set the date and time
	• Set the time zone
	• View the service processor uptime statistic
	• Enable Network Time Protocol sync (NTP server must be configured)
		`/SP/clock`
		or
		`/CMM/clock`
			Admin (a)

Set NTP server.	• Enable NTP servers (using IP or DNS host name)	`/SP/clients`
		`ntp`
		or
		`/CMM/clients`
		`ntp`
			Admin (a)

Related Information

- "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22
- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Modifying Default Settings for Network Deployment and Administration" on page 69
- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Management Access Deployment Options" on page 70
- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Connectivity Deployment Options" on page 74
- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Use of Web Server Certificates and SSH Server-Side Keys" on page 75
- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Default Timeout for CLI and Web Sessions" on page 75
- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Serial Management Port Owner" on page 77

User Management Tasks and Applicable CLI Targets

Use the following table to help identify the applicable CLI namespace targets for Oracle ILOM user management tasks.

For additional information about setting up local or remote directory user accounts in Oracle ILOM, see the topics listed in the Related Information section that appears after the table.

Task	Description	Targets Containing the Necessary Properties	User Role Required to Configure Properties
Manage Oracle ILOM users locally (up to 10 per service processor).	• Add, delete users • Set user access role • Set user password • Upload user-generated SSH keys	/SP/users or /CMM/users	• User management (u) to manage other users • Read only (o) to manage your own account
Configure user roles and authentication using an authentication server.	• Configure Active Directory for user or user group access and authentication • Configure LDAP for user access and authentication • Configure LDAP/SSL for user or user group access and authentication • Configure RADIUS for user access and authentication	/SP/clients activedirectory ldap ldapssl radius or /CMM/clients activedirectory ldap ldapssl radius	User management (u)
Set physical presence security for Oracle ILOM default password recovery.	• The check physical presence state is enabled by default. Enforce a physical presence check (pressing the system Locate button) to allow the default Oracle ILOM password to be reset **Note -** Resetting the Oracle ILOM default password must be performed through a connection to the system's SER MGT port.	/SP or /CMM check_physical_presence=	User Management (u)

Related Information

- "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting Up and Maintaining User Accounts" on page 27
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Supported User Authentication Configuration Options" on page 28
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Assignable Oracle ILOM User Roles" on page 30
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Single Sign-On Service (Enabled by Default)" on page 32

- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "CLI Authentication Using Local User SSH Key" on page 34
- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Password Recovery for root Account" on page 35

System Power-On Policy Tasks and Applicable CLI Targets

Use the following table to help identify the applicable CLI namespace targets for Oracle ILOM SP power-on and CMM power supply policy tasks.

For detail information about setting SP and CMM power source policies in Oracle ILOM, see the topics listed in the Related Information section that appears after the table.

Task	Description	Targets Containing the Necessary Properties	User Role Required to Configure Properties

Set server power-on and cooling-down policies.
or
`Set CMM power supply policies.`
	•	`/SP/policy`
		or
		`/CMM/policy`
			Admin (a)

Related Information

- "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22
- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Power-On and Cooling-Down Policies Configurable From the Server SP" on page 176
- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "System Management Power Supply Policies Configurable From CMM" on page 178

System Power Usage Policy Tasks and CLI Targets

Use the following table to help identify the applicable CLI namespace targets for Oracle ILOM system power usage policy tasks and alert notification tasks.

For detail information about setting SP and CMM power usage policies and alert notification in Oracle ILOM, see the topics listed in the Related Information section that appears after the table.

Note – Power usage policies are server-specific, therefore, some policies might not be available for all Oracle servers.

Task	Description	Targets Containing the Necessary Properties	User Role Required to Configure Properties
Set power consumption alert notification. **Note -**	Configure values for alert notification threshold properties.	*/SP|CMM* `/powermgmt` `threshold1=`*n* `threshold2=`*n*	Admin (a)

Set server power management policies.	• View current power consumption and settings
	• Configure thresholds for power alerts
	• Configure power policy (maximum performance, power conservation)
	• Configure power limiting and violation actions when power limit is exceeded
	• View individual component power (CPU, memory, IO, motherboard)
	• Configure power limiting for individual components, if supported
		`/SP/powermgmt`
		`budget`
		`powerconf`
			Admin (a)

Set blade chassis power consumption policies.	• View current chassis power consumption and settings
	• Configure chassis power supply redundancy policy (affects available power)
	• Configure thresholds for power alerts
	• View individual component power (blade slots, NEMs, Fans, PSUs, CMM)
	• Configure power limiting for individual components, if supported
		`/CMM/powermgmt`
		`powerconf`
		`advanced`
			Admin (a)

Related Information

- "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting Power Consumption Alert Notifications" on page 182

- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Set SP Power Target Limit Properties" on page 185
- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Setting SP Advanced Power Capping Policy to Enforce Power Limit" on page 187
- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Set Power Management Settings for Power Policy on SPARC Servers" on page 189
- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Set CMM Power Supply Redundancy Policy" on page 191

Firmware Update Tasks and Applicable CLI Targets

Use the following table to help identify Oracle ILOM firmware update tasks and CLI targets.

For detail information about how to perform Oracle ILOM firmware updates, see the topics listed in the Related Information section that appears after the table.

Task	Description	Targets Containing the Necessary Properties	User Role Required to Configure Properties
Check system BIOS version (x86 only).	• View system BIOS information	`/System/BIOS`	Read only (o)
Check Oracle ILOM firmware version.	• View service processor firmware information	`/SP` or `/CMM`	Read only (o)
Update firmware from the device service processor.	• Load service processor firmware image • Load system BIOS image (x86 only) **Note -** After a firmware update, the system will power off. SPARC servers must be powered off before performing an update. **Note -** Updating the chassis CMM firmware does not also update other chassis component firmware, such as blade servers or NEMs.	`/SP/firmware` or `/CMM/firmware`	Admin (a)

Task	Description	Targets Containing the Necessary Properties	User Role Required to Configure Properties

Update server blade and storage blade firmware from the chassis.	• Load service processor firmware image
	• Load system BIOS image (x86 only)
	Note - After a firmware update, the system will power off. SPARC servers must be powered off before performing an update.
		`/Servers/Blades`
		`Blade_`*n*
		or
		`/System/Firmware/Other_Firmware`
		`Firmware_`*n* `(choose an associated Blade)`
			Admin (a)

Update NEM firmware from the chassis.	• Load service processor firmware image • Load SAS firmware image (for SAS-NEMs only) **Note -** NEMs that do not have service processors will not be shown as they do not have firmware that can be upgraded.	`/System/Firmware/Other_Firmware` `Firmware_`*n* `(choose an associated NEM)`	Admin (a)
Update blade chassis component firmware using legacy targets.	• Load service processor firmware image • Load system BIOS image (x86 only) • Load SAS firmware image (for SAS-NEMs only) **Note -** After a firmware update, the system will power off. SPARC servers must be powered off before performing an update.	`/CH` `BL`*n* `NEM`*n*	Admin (a)

Related Information

- "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Performing Firmware Updates" on page 194
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Firmware Upgradable Devices" on page 194

Firmware Back Up and Restore Tasks and Applicable CLI Targets

Use the following table to help identify the applicable CLI namespace target for Oracle ILOM back up or restore configuration tasks or to reset Oracle ILOM configuration to factory defaults.

For detail information about backing up or restoring the SP configuration in Oracle ILOM, see the topics listed in the Related Information section that appears after the table.

Task	Description	Targets Containing the Necessary Properties	User Role Required to Configure Properties
Save or restore Oracle ILOM configurations.	• Save Oracle ILOM configurations (all user-configured settings) and dump them to a file • Restore Oracle ILOM configurations (all user-configured settings) and load them from a file	`/SP/config`	User roles determine how much configuration data gets backed up or restored. For the most complete backup or restore, you need: • Admin (`a`) • User Management (`u`) • Console (`c`) • Reset and Host • Control (`r`) • Read Only (`o`)

Reset Oracle ILOM configurations to the defaults.	• Reset `all` user-configured settings to defaults and delete log files
	• Reset user-configured settings to `factory` defaults and keep log files
	• Cancel a pending reset request by specifying `none` (must be done before SP reboot)
		`/SP`
		or
		`/CMM`
			Admin (`a`)

Related Information

- "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22
- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Backing Up, Restoring, or Resetting the Oracle ILOM Configuration" on page 203

- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Password Recovery for root Account" on page 35

x86 BIOS Back Up and Restore Tasks and Applicable CLI Targets

Use the following table to help identify the applicable CLI namespace targets for Oracle ILOM x86 BIOS configuration tasks.

For detail information about backing up or restoring the x86 BIOS configuration in Oracle ILOM, see the topics listed in the Related Information section that appears after the table.

Task	Description	Targets Containing the Necessary Properties	User Role Required to Configure Properties
Save/restore system BIOS configurations (x86 only).	• Save Oracle ILOM configurations (all user-configured settings) and dump them to a file • Restore Oracle ILOM configurations (all user-configured settings) and load them from a file • Check system BIOS configuration sync status with service processor • Cancel a request to restore or a request to reset system BIOS configurations	`/System/BIOS Config`	• Admin (`a`) for save or restore • Reset and Host Control (`r`) for restore
Reset system BIOS configurations to the defaults (x86 only).	• Reset BIOS configurations to `factory` defaults • Cancel a pending reset request by specifying the cancel action (must be done before server power cycle)	`/System/BIOS`	• Admin (`a`) for save or restore • Reset and Host Control (`r`) for restore

Related Information

- "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Maintaining x86 BIOS Configuration Parameters" on page 215
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Requirements for BIOS Configuration Tasks" on page 222

System Health Status Tasks and Applicable CLI Targets

Use the following table to help identify the applicable CLI tasks for Oracle ILOM system and component-level health status tasks.

Task	Description	Targets Containing the Necessary Properties	User Role Required to View Properties
View system details from a server's service processor.	• View system details (model, status, version, configuration information) • View open problems requiring attention • View processor information (number, speed, cores, status) • View memory information (number, size, status) • View power details (model, status, input/output) • View cooling information (number, temperature, status) • View storage information (number, size, status, disks, controllers, volumes, expanders) • View network information (installed network interface cards, model, status, MAC address) • View PCIe device information (on-board devices, add-on devices) • View the service processor firmware version • View the system BIOS version (x86 only) • View RAID expansion module (REM) and fabric expansion module (FEM) information	/System Open_Problems Processors Memory Power Cooling Storage Networking PCI_Devices Firmware BIOS IO_Modules	Read only (o)
View system details from a blade chassis CMM.	• View system details (model, status, version, configuration information) • View open problems requiring attention • View information on installed blades • View power details (model, status, input/output) • View cooling information (number, temperature, status) • View storage information (number, size, status, of chassis managed disks) • View network express module (NEM) information (blade chassis only) • View the firmware versions of chassis components	/System Open_Problems Blades Power Cooling Storage IO_Modules Firmware	Read only (o)

Related Information

- "Collecting System Information, Monitoring Health Status, and Initiating Host Management" on page 33

Event and Audit Log Tasks and Applicable CLI Targets

Use the following table to help identify the applicable CLI namespace targets for Oracle ILOM log entry tasks.

Task	Description	Targets Containing the Necessary Properties	User Role Required to Configure Properties

Manage logs.	• View the event log
	• View the audit log
	• Filter events (by `class==`, `type==` and `severity==`)
	• Clear the log
	Note - For a list of filter property values, see the web interface ILOM Administration > Logs page.
		`/SP/logs`
		`audit`
		`event`
		or
		`/CMM/logs`
		`audit`
		`event`
			• Read only (`o`) to view
			• Admin (`a`) to clear

Configure log centralization using a syslog server.	• Configure the address or domain name of the primary and secondary syslog server that will maintain copy of Oracle ILOM logs	`/SP/syslog`
		or
		`/CMM/syslog`
			Admin (`a`)

Related Information

- "Oracle ILOM: Log Entries" on page 46
- "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22

Alert Notification Tasks and Applicable CLI Targets

Use the following table to help identify the applicable CLI namespace tasks for Oracle ILOM alert notification tasks.

For detail information about how to set alert notifications in Oracle ILOM, see the topic listed in the Related Information section that appears after the table.

Task	Description	Targets Containing the Necessary Properties	User Role Required to Configure Properties

Configure alerts (up to 15).	• Set the alert type (IPMI PET, Email, SNMP trap)
	• Set the alert level
	• Set the alert destination
	• Test the alert rule
	Note - The SNMP and IPMI services must be configured to receive SNMP and IPMI alerts.
		`/SP/alertmgmt rules`
		or
		`/CMM/alertmgmt rules`
			• Read only (o) to view
			• Admin (a) to clear

Configure an SMTP server for email alerts.	• Configure the SMTP server details to enable email alerts (using IP or DNS host name)
	• Send a test email
		`/SP/clients smtp`
		or
		`/CMM/clients smtp`
			Admin (a)

Related Information

- "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Configure SMTP Client for Email Alerts" on page 172
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting Power Consumption Alert Notifications" on page 182

Host Server Management Tasks and Applicable CLI Targets

Use the following table to help identify the applicable CLI targets for host server management action tasks.

For detail information about how to perform host management actions in Oracle ILOM, see the topic listed in the Related Information section that appears after the table.

Task	Description	Targets Containing the Necessary Properties	User Role Required to Configure Properties
Power on, off, or reset the system from the SP.	• Power on (start) the system • Power off (stop) the system • `Reset` the system	`/System`	Reset and Host Control (`r`)
Power on or off the blade chassis from the CMM.	• Power on (start) the chassis • Power off (stop) the chassis	`/System`	Reset and Host Control (`r`)

Reset (restart) the Oracle ILOM service processor.	• Reset the SP or CMM	`/SP`
		or
		`/CMM`
			Reset and Host Control (`r`)

Turn on/off the system locate LED.	• Turn on (start) the locator indicator • Turn off (stop) the locator indicator	`/System`	Admin (`a`)
Set boot device (x86 only).	• Set boot device - default, PXE, disk, diagnostic partition, CD-ROM, BIOS, floppy	`/HOST`	Reset and Host Control (`r`)
Set domain boot device (SPARC only).	• Set auto boot for both the host controller and guest domains at startup • Set boot guests to enable or disable guest domain booting at startup	`/HOST/domain`	Reset and Host Control (`r`)
Set boot recovery mode (SPARC only).	• Set auto restart policy • Set auto run on error mode • Set boot failure recovery mode • Set boot restart policy • Set boot time out • Set maximum boot failures	`/HOST`	Reset and Host Control (`r`)
Set trusted platform module (TPM) device (SPARC only).	• Enable TPM • Disable TPM • Clear TPM state **Note -** Actual TPM targets vary from system to system.	`/HOST/tpm`	Reset and Host Control (`r`)

Related Information

- "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22

- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Configuring Host Server Management Actions" on page 147

Remote KVMS Service State Tasks and Applicable CLI Target

Use the following table to help identify the applicable CLI namespace targets for Oracle ILOM KVMS tasks.

Task	Description	Targets Containing the Necessary Properties	User Role Required to Configure Properties
Configure the SP remote KVMS.	• Enable the KVMS • Configure display quality (for the web interface video remote console only) • Configure mouse mode (web interface video remote console only) • Configure console lock mode (web interface video remote console only)	`/SP/services kvms`	Admin (a)

Related Information

- "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Configuring Host Server Management Actions" on page 147

Host Serial Console Session Tasks and Applicable CLI Target

Use the following table to help identify the applicable CLI namespace targets for the starting or ending a host serial console session.

Note – This feature is for text-only serial console redirection. For full video graphics console redirection, use the Oracle ILOM Remote Console web interface.

Task	Description	Targets Containing the Necessary Properties	User Role Required to Configure Properties
Start remote host serial console session.	• Start or end serial console session (KVMS must be enabled) • View console history • View most recent server console bootlog • Set console text and viewing properties	`/HOST/console`	Console (c)

Related Information

- "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22
- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Using Remote KVMS Consoles for Host Server Redirection" on page 117

Host Diagnostic Tasks and Applicable CLI Targets

Use the following table to help identify the applicable CLI namespace targets for Oracle ILOM host diagnostic tasks.

Task	Description	Targets Containing the Necessary Properties	User Role Required to Configure Properties
Configure system diagnostics for an x86 system.	• Enable diagnostics mode (runs Pc-Check at next system restart) • Configure extended mode for Pc-Check diagnostics (run all diagnostic tests) • Configure manual mode for Pc-Check diagnostics (select the diagnostic tests to run) **Note -** To run and view diagnostics, launch the Oracle ILOM Remote Console from the web interface, and then restart the system.	`/HOST/diag`	Reset and Host Control (`r`)
Configure system diagnostics for a SPARC system.	• Enable diagnostics mode to run power-on self-test (POST) at next system restart • Configure trigger for running POST diagnostics (power on, hardware change, error reset) • Specify the diagnostics level (maximum or minimum tests) • Configure verbosity of test messages **Note -** To run and view diagnostics, launch the Oracle ILOM Remote Console from the web interface, and then restart the system.	`/HOST/diag`	Reset and Host Control (`r`)

Related Information

- "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22
- "Troubleshooting Oracle ILOM Managed Devices" on page 63
- *Oracle ILOM 3.1 Configuration and Maintenance Guide,* "Setting Host Diagnostic Tests to Run" on page 149

Fault Management Shell Session Task and Applicable CLI Target

Use the following table to help identify the CLI namespace target for the Oracle ILOM Fault Management Shell.

All components faults reported in Oracle ILOM are automatically cleared upon the service repair or replacement of the component. For detail information about the Oracle ILOM Fault Management Shell or the open problems reported in Oracle ILOM, see the topics in the Related Information section that appears after the following table.

Note – The purpose of the Oracle ILOM Fault Management Restricted Shell is to help Oracle Services personnel diagnose system problems. Customers should not run commands in the shell unless requested to do so by Oracle Service. For detail information

---

Task	Description	Targets Containing the Necessary Properties	User Role Required to Configure Properties
Launch the Fault Management shell to diagnose problems (as instructed by Oracle Service).	• Initiate (start) a Fault Management Shell session • Display error logs and previous commands • Obtain fault statistics using a diagnostic engine • Inform Oracle ILOM of repaired and replaced FRUs	`/SP/faultmgmt shell`	Admin (a)

Related Information

- "Managing Oracle Hardware Faults Through the Oracle ILOM Fault Management Shell" on page 95
- "Administering Open Problems" on page 41

NEM Service Action Tasks and Applicable CLI Target

Use the following table to help identify the applicable CLI namespace task for the preparing to remove or return a NEM to service.

Task	Description	Targets Containing the Necessary Properties	User Role Required to Configure Properties
Perform NEM service actions.	• Prepare to remove a NEM • Return a NEM to service • Clear fault state **Note -** Only certain components, such as NEMs, support service actions through Oracle ILOM.	`/System/IO_Modules/NEMs` `NEM_`*n*	Admin (a)

Related Information

- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Reset Power to Server SP, NEM SP, or CMM" on page 202
- "NEM Service Action Properties" on page 43

Server Blade SAS Zoning Tasks and Applicable CLI Target

Use the following table to help identify the applicable CLI namespace target for the Oracle ILOM blade chassis SAS zoning task.

For detail information about how to perform SAS storage zoning in Oracle ILOM, see the topic in the Related Information section that appears after the following table.

Task	Description	Targets Containing the Necessary Properties	User Role Required to Configure Properties
Manage chassis storage.	• Assign storage blade disks to server blades using the Sun Blade Zone Manager • Reset storage zoning configurations to defaults • Reset the zoning password (when not using Sun Blade Zone Manager) **Note -** Zoning configurations are saved as part of the CMM configurations.	`/STORAGE/sas_zoning`	Admin (a)

Related Information

- "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22

- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "SAS Zoning Chassis Blade Storage Resources" on page 231

CMM Blade Management Tasks and Applicable CLI Target

Use the following table to help identify the applicable CLI namespace target for monitoring and managing blade servers from the CMM.

Task	Description	Targets Containing the Necessary Properties	User Role Required to Configure Properties
Manage chassis blades through the CMM.	• Monitor and manage blades in the chassis as you would if you were logged into the blade service processor **Note -** Standard targets are shown (such as HOST, System, and SP). Legacy targets will be shown for server blades that have CLI legacy targets enabled or have pre-ILOM 3.1 firmware on their service processor.	`/Servers/Blades` `Blade_`*n*	Role depends on the management task

Related Information

- "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22
- *Oracle ILOM 3.1 Configuration and Maintenance Guide*, "Configuring Host Server Management Actions" on page 147

CLI Legacy Service State Tasks and Applicable CLI Targets

Use the following table to help identify the legacy Oracle ILOM 3.0 CLI namespace targets.

Note – Depending on your system, and if you have upgraded to Oracle ILOM 3.1 from an earlier ILOM 3.0 version, the legacy targets are enabled by default.

Note – The /STORAGE target is only considered legacy in the CMM when there is no chassis SAS-2 storage available for management. If SAS-2 storage exists in the chassis, the /STORAGE target will be visible.

Task	Description	Targets Containing the Necessary Properties	User Role Required to Configure Properties

Show server legacy CLI targets.	• Show (`enable`) system legacy targets (`/SYS` and `/STORAGE`) that were available for Oracle ILOM 3.0
	Note - The `/SYS` and /STORAGE targets are similar to `/System` targets. Refer to the Oracle ILOM 3.0 documentation for details.
		`/SP/cli`
		`legacy_targets=`
		enable | *disabled*
			Admin (`a`)

Show blade chassis legacy targets.	• Show (`enable`) chassis legacy targets (`/CH`) that were available for Oracle ILOM 3.0
	Note - The `/CH` targets are similar to `/System` targets. Refer to the Oracle ILOM 3.0 documentation for details.
		`/CMM/cli`
		`legacy_targets=`
		enable | *disabled*
			Admin (`a`)

Glossary

A

access control list (ACL) A software authorization mechanism that enables you to control which users have access to a server. Users can define ACL rules that are specific to a particular file or directory, granting or denying access to one or more users or groups.

Active Directory A distributed directory service included with Microsoft Windows Server operating systems. It provides both authentication of user credentials and authorization of user access levels to networked resources.

actual power consumption The amount of power wattage used by the managed device (blade chassis, rackmount server, or blade server).

address In networking, a unique code that identifies a node in the network. Names such as "host1.companyname.com" are translated to dotted-quad addresses, such as "168.124.3.4" by the domain name service (DNS).

address resolution A means for mapping Internet addresses into physical media access control (MAC) addresses or domain addresses.

Address Resolution Protocol (ARP) A protocol used to associate an Internet Protocol (IP) address with a network hardware address (MAC address).

Administrator The person with full access (root) privileges to the managed host system.

agent A software process, usually corresponding to a particular local managed host, that carries out manager requests and makes local system and application information available to remote users.

alert A message or log generated by the collection and analysis of error events. An alert indicates that there is a need to perform some hardware or software corrective action.

Alert Standard Format (ASF) A preboot or out-of-band platform management specification that enables a device, such as an intelligent Ethernet controller, to autonomously scan ASF-compliant sensors on the motherboard for voltage, temperature, or

other excursions and to send Remote Management and Control Protocol (RMCP) alerts according to the Platform Event Trap (PET) specification. ASF was intended primarily for out-of-band management functions for client desktops. ASF is defined by the Distributed Management Task Force (DMTF).

allocated power The maximum input power wattage assigned to a managed device.

audit log A log that tracks all interface-related user actions, such as user logins, logouts, configuration changes, and password changes. The user interfaces monitored for user actions include: Oracle ILOM web interface, CLI, Fault Management Shell (captive shell), Restricted Shell, as well as SNMP and IPMI client interfaces.

authentication The process that verifies the identity of a user in a communication session, or a device or other entity in a computer system, before that user, device, or other entity can access system resources. Session authentication can work in two directions. A server authenticates a client to make access-control decisions. The client can authenticate the server as well. With Secure Sockets Layer (SSL), the client always authenticates the server.

authenticated user A user that has successfully undergone the process of authentication and has subsequently been granted access privileges to particular system resources.

authorization The process of granting specific access privileges to a user. Authorization is based on authentication and access control.

available power On a rackmounted server, available power is the sum of all the power that the power supplies can provide. On a server module, available power is the amount of power the chassis is willing to provide to the server module.

B

bandwidth A measure of the volume of information that can be transmitted over a communication link. Often used to describe the number of bits per second a network can deliver.

baseboard management controller (BMC) A device used to manage chassis environmental, configuration, and service functions, and receive event data from other parts of the system. It receives data through sensor interfaces and interprets this data by using the sensor data record (SDR) to which it provides an interface. The BMC provides another interface to the system event log (SEL). Typical functions of the BMC are to measure processor temperature, power supply values, and cooling fan status. The BMC can take autonomous action to preserve system integrity.

baud rate The rate at which information is transmitted between devices, for example, between a terminal and a server.

bind In the Lightweight Directory Access Protocol (LDAP), this refers to the authentication process that LDAP requires when users access the LDAP directory. Authentication occurs when the LDAP client binds to the LDAP server.

BIOS (Basic Input/Output System) System software that controls the loading of the operating system and testing of hardware at system power-on. BIOS is stored in read-only memory (ROM).

bits per second (bps) The unit of measurement for data transmission speed.

blade server power consumption The sum of power being consumed by its local components.

boot loader A program contained in read-only memory (ROM) that automatically runs at system power-on to control the first stage of system initialization and hardware tests. The boot loader then transfers control to a more complex program that loads the operating system.

C

cache A copy of original data that is stored locally, often with instructions or the most frequently accessed information. Cached data does not have to be retrieved from a remote server again when requested. A cache increases effective memory transfer rates and processor speed.

certificate Public key data assigned by a trusted Certificate Authority (CA) to provide verification of an entity's identity. This is a digitally signed document. Both clients and servers can have certificates. Also called a "public key certificate."

Certificate Authority (CA) A trusted organization that issues public key certificates and provides identification to the owner of the certificate. A public key Certificate Authority issues certificates that state a relationship between an entity named in the certificate, and a public key that belongs to that entity, which is also present in the certificate.

chassis monitoring module (CMM) A typically redundant, hot-pluggable module that works with the service processor (SP) on each blade to form a complete chassis management system.

client In the client-server model, a system or software on a network that remotely accesses resources of a server on a network.

CMM power consumption The sum of input power being consumed by the blade chassis power supplies.

command-line interface (CLI) A text-based interface that enables users to type executable instructions at a command prompt.

Common Information Model (CIM) The Common Information Model (CIM) is a computer industry standard for defining device and application characteristics so that system administrators and management programs can control devices and applications from different manufacturers or sources in the same way.

console A terminal, or dedicated window on a screen, where system messages are displayed. The console window enables you to configure, monitor, maintain, and troubleshoot many server software components.

Coordinated Universal Time (UTC) The international standard for time. UTC was formerly called Greenwich Meridian Time (GMT). UTC is used by Network Time Protocol (NTP) servers to synchronize systems and devices on a network.

core file A file created by the Solaris or Linux operating system when a program malfunctions and terminates. The core file holds a snapshot of memory, taken at the time the fault occurred. Also called a "crash dump file."

critical event A system event that seriously impairs service and requires immediate attention.

customer-replaceable unit (CRU) A system component that the user can replace without special training or tools.

D

Data Encryption Standard (DES) A common algorithm for encrypting and decrypting data.

Desktop Management Interface (DMI) A specification that sets standards for accessing technical support information about computer hardware and software. DMI is hardware and operating system (OS) independent, and can manage workstations, servers, or other computing systems. DMI is defined by the Distributed Management Task Force (DMTF).

digital signature A certification of the source of digital data. A digital signature is a number derived from a public key cryptographic process. If the data is modified after the signature was created, the signature becomes invalid. For this reason, a digital signature can ensure data integrity and detection of data modification.

Digital Signature Algorithm (DSA) A cryptographic algorithm specified by the Digital Signature Standard (DSS). DSA is a standard algorithm used to create digital signatures.

direct memory access (DMA) The transfer of data directly into memory without supervision of the processor.

directory server In the Lightweight Directory Access Protocol (LDAP), a server that stores and provides information about people and resources within an organization from a logically centralized location.

Distinguished Name (DN) In the Lightweight Directory Access Protocol (LDAP), a unique text string that identifies an entry's name and location within the directory. A DN can be a fully qualified domain name (FQDN) that includes the complete path from the root of the tree.

Distributed Management Task Force (DMTF) A consortium of over 200 companies that authors and promotes standards for the purpose of furthering the ability to remotely manage computer systems. Specifications from the DTMF include the Desktop Management Interface (DMI), the Common Information Model (CIM), and the Alert Standard Format (ASF).

domain A grouping of hosts that is identified by a name. The hosts usually belong to the same Internet Protocol (IP) network address. The domain also refers to the last part of a fully qualified domain name (FQDN) that identifies the company or organization that owns the domain. For example, "oracle.com" identifies Oracle Corporation as the owner of the domain.

domain name The unique name assigned to a system or group of systems on the Internet. The host names of all the systems in the group have the same domain name suffix, such as "oracle.com." Domain names are interpreted from right to left. For example, "oracle.com" is both the domain name of Oracle Corporation, and a subdomain of the top-level ".com" domain.

domain name server (DNS) The server that typically manages host names in a domain. DNS servers translate host names, such as "www.example.com," into Internet Protocol (IP) addresses, such as "030.120.000.168."

domain name system (DNS) A distributed name resolution system that enables computers to locate other computers on a network or the Internet by domain name. The system associates standard Internet Protocol (IP) addresses, such as "00.120.000.168," with host names, such as "www.oracle.com." Machines typically get this information from a DNS server.

dynamic domain name service (DDNS) A service that ensures that a Domain Name Server (DNS) always knows the dynamic or static IP address associated with a domain name.

Dynamic Host Configuration Protocol (DHCP) A protocol that enables a DHCP server to assign Internet Protocol (IP) addresses dynamically to systems on a Transmission Control Protocol/Internet Protocol (TCP/IP) network.

E

enhanced parallel port (EPP) A hardware and software standard that enables systems to transmit data at twice the speed of standard parallel ports.

Ethernet An industry-standard type of local area network (LAN) that enables real-time communication between systems connected directly through cables. Ethernet uses a Carrier Sense Multiple Access/Collision Detection (CSMA/CD) algorithm as its access method, wherein all nodes listen for, and any node can begin transmitting data. If multiple nodes attempt to transmit at the same time (a collision), the transmitting nodes wait for a random time before attempting to transmit again.

event A change in the state of a managed object. The event-handling subsystem can provide a notification to which a software system must respond when it occurs, but which the software did not solicit or control.

event log A log that tracks informational, warning, or error messages about a managed device, such as the addition or removal of a component or the failure of a component. The properties of the events recorded in the log can include: the severity of the event, the event provider (class), and the date and time the event was logged.

exhaust temperature The temperature of air exiting the back of the server or chassis.

external serial port The RJ-45 serial port on the server.

externally initiated reset (XIR) A signal that sends a "soft" reset to the processor in a domain. XIR does not reboot the domain. An XIR is generally used to escape from a hung system so a user can reach the console prompt. The user can then generate a core dump file, which can be useful in diagnosing the cause of the hung system.

F

failover The automatic transfer of a computer service from one system, or more often a subsystem, to another to provide redundant capability.

Fast Ethernet Ethernet technology that transfers data up to 100M bits per second. Fast Ethernet is backward-compatible with 10M-bit per second Ethernet installations.

fault A detected error condition in the hardware or software.

Fault Management Architecture (FMA) An architecture that ensures that a computer can continue to function despite a hardware or software failure.

Fault Manager An Oracle ILOM feature that enables you to proactively monitor the health of your system hardware, as well as diagnose hardware failures as they occur. When a component is in a faulty state, fault events are captured in the Oracle ILOM Open Problems table and the event log.

Fault Manager shell A user interface that enables Oracle Services personnel to diagnose system problems. Users can run commands in this shell only if requested to do so by Oracle Services.

faulted state An indicator of a component that is present but is unusable or degraded because one or more problems have been diagnosed by Oracle ILOM. Oracle ILOM automatically disables the component to prevent further damage to the system.

field-replaceable unit (FRU) A system component that is replaceable at the customer site.

file system A consistent method by which information is organized and stored on physical media. Different operating systems typically have different file systems. File systems are often a tree-structured network of files and directories, with a root directory at the top and parent and child directories below the root.

File Transfer Protocol (FTP) A basic Internet protocol based on Transmission Control Protocol/Internet Protocol (TCP/IP) that enables the retrieving and storing of files between systems on the Internet without regard for the operating systems or architectures of the systems involved in the file transfer.

firewall A network configuration, usually both hardware and software, that protects networked computers within an organization from outside access. A firewall can monitor or prohibit connections to and from specified services or hosts.

firmware Software that is typically used to help with the initial booting stage of a system and with system management. Firmware is embedded in read-only memory (ROM) or programmable ROM (PROM).

fully qualified domain name (FQDN) The complete and unique Internet name of a system, such as "www.oracle.com." The FQDN includes a host server name (www) and its top-level (.com) and second-level (.oracle) domain names. An FQDN can be mapped to a system's Internet Protocol (IP) address.

G

gateway A computer or program that interconnects two networks and then passes data packets between the networks. A gateway has more than one network interface.

Gigabit Ethernet Ethernet technology that transfers data up to 1000M bits per second.

grant limit The maximum sum of power wattage the CMM can grant to a blade slot.

grantable power The total sum of remaining power wattage that the CMM can allocate to the Oracle blade chassis slots without exceeding the grant limit.

granted power The maximum sum of power wattage the CMM has granted to all blade slots requesting power or to an individual blade slot requesting power.

graphical user interface (GUI) An interface that uses graphics, along with a keyboard and mouse, to provide easy-to-use access to an application.

H

health status states Indicators that specify the health of the managed device. Possible status states are: OK, Service Required, Not Available, and Offline.

host A system, such as a backend server, with an assigned Internet Protocol (IP) address and host name. The host is accessed by other remote systems on the network.

host ID Part of the 32-bit Internet Protocol (IP) address used to identify a host on a network.

host name The name of a particular machine within a domain. Host names always map to a specific Internet Protocol (IP) address.

hot-plug Describes a component that is safe to remove or add while the system is running. However, before removing the component, the system administrator must prepare the system for the hot-plug operation. After the new component is inserted, the system administrator must instruct the system to reconfigure the device into the system.

hot-swap Describes a component that can be installed or removed by simply pulling the component out and putting a new component into a running system. The system either automatically recognizes the component change and configures it or requires user interaction to configure the system. However, in neither case is a reboot required. All hot-swappable components are hot pluggable, but not all hot-pluggable components are hot-swappable.

Hypertext Transfer Protocol (HTTP) The Internet protocol that retrieves hypertext objects from remote hosts. HTTP messages consist of requests from client to server and responses from server to client. HTTP is based on Transmission Control Protocol/Internet Protocol (TCP/IP).

Hypertext Transfer Protocol Secure (HTTPS) An extension of HTTP that uses Secure Sockets Layer (SSL) to enable secure transmissions over a Transmission Control Protocol/Internet Protocol (TCP/IP) network.

I

in-band system management — Server management capability that is enabled only when the operating system is initialized and the server is functioning properly.

inlet air temperature — The temperature entering into the front of the server or chassis.

installed hardware minimum — The smallest amount of input power wattage consumed by the hardware components installed on the server.

Integrated Lights Out Manager (ILOM) — An integrated hardware, firmware, and software solution for in-chassis or in-blade system management.

Intelligent Platform Management Interface (IPMI) — A hardware-level interface specification that was designed primarily for out-of-band management of server systems over a number of different physical interconnects. The IPMI specification describes extensive abstractions regarding sensors. This enables a management application running on the operating system (OS) or in a remote system to comprehend the environmental makeup of the system and to register with the system's IPMI subsystem to receive events. IPMI is compatible with management software from heterogeneous vendors. IPMI functionality includes field-replaceable unit (FRU) inventory reporting, system monitoring, logging, system recovery (including local and remote system resets and power-on and power-off capabilities), and alerting.

internal serial port — The connection between the host server and Oracle ILOM that enables an Oracle ILOM user to access the host serial console. The Oracle ILOM internal serial port speed must match the speed of the serial console port on the host server, often referred to as serial port 0, COM1, or /dev/ttyS0. Normally, the host serial console settings match Oracle ILOM's default settings (9600 baud, 8N1 [eight data bits, no parity, one stop bit], no flow control).

Internet Control Message Protocol (ICMP) — An extension to the Internet Protocol (IP) that provides for routing, reliability, flow control, and sequencing of data. ICMP specifies error and control messages used with the IP.

Internet Protocol (IP) — The basic network layer protocol of the Internet. IP enables the unreliable delivery of individual packets from one host to another. IP does not guarantee that the packet will be delivered, how long it will take, or if multiple packets will be delivered in the order they were sent. Protocols layered on top of IP add connection reliability.

Internet Protocol (IP) address — In Transmission Control Protocol/Internet Protocol (TCP/IP), a unique 32-bit number that identifies each host or other hardware system on a network. The IP address is a set of numbers separated by dots, such as "192.0.2.1" which specifies the actual location of a machine on an intranet or the Internet.

input power Power that is pulled into the chassis power supply units from an external power source.

IPMItool A utility used to manage IPMI-enabled devices. IPMItool can manage IPMI functions of either the local system or a remote system. Functions include managing field-replaceable unit (FRU) information, local area network (LAN) configurations, sensor readings, and remote system power control.

J

Java Remote Console A console written in Java that allows a user to access an application while it is running.

Java Web Start application A web application launcher. With Java Web Start, you launch applications by clicking the web link. If the application is not present on your system, Java Web Start downloads it and caches it onto your system. Once an application is downloaded to its cache, it can be launched from a desktop icon or browser.

K

kernel The core of the operating system (OS) that manages the hardware and provides fundamental services, such as filing and resource allocation, that the hardware does not provide.

Keyboard Controller Style (KCS) interface A type of interface implemented in legacy personal computer (PC) keyboard controllers. Data is transferred across the KCS interface using a per-byte handshake.

keyboard, video, mouse, storage (KVMS) A series of interfaces that enables a system to respond to keyboard, video, mouse, and storage events.

L

lights out management (LOM) Technology that provides the capability for out-of-band communication with the server even if the operating system is not running. This enables the system administrator to switch the server on and off; view system temperatures, fan speeds, and so forth; and restart the system from a remote location.

Lightweight Directory Access Protocol (LDAP) A directory service protocol used for the storage, retrieval, and distribution of information, including user profiles, distribution lists, and configuration data. LDAP runs over Transmission Control Protocol/Internet Protocol (TCP/IP) and across multiple platforms.

Lightweight Directory Access Protocol (LDAP) server A software server that maintains an LDAP directory and service queries to the directory. The Oracle Sun Directory Services and the Netscape Directory Services are implementations of an LDAP server.

local area network (LAN) A group of systems in close proximity that can communicate through connecting hardware and software. Ethernet is the most widely used LAN technology.

local host The processor or system on which a software application is running.

M

major event A system event that impairs service, but not seriously.

managed system When used in the documentation, refers to any of the following Oracle hardware systems: Oracle rackmount server, Oracle blade server, or chassis monitoring module (CMM).

Management Information Base (MIB) A tree-like, hierarchical system for classifying information about resources in a network. The MIB defines the variables that the master Simple Network Management Protocol (SNMP) agent can access. The MIB provides access to the server's network configuration, status, and statistics. Using SNMP, you can view this information from a network management station (NMS). By industry agreement, individual developers are assigned portions of the tree structure to which they may attach descriptions that are specific to their own devices.

man pages Online UNIX documentation.

media access control (MAC) address Worldwide unique, 48-bit, hardware address number that is programmed in to each local area network interface card (NIC) at the time of manufacture.

Message Digest 5 (MD5) A secure hashing function that converts an arbitrarily long data string into a short digest of data that is unique and of fixed size.

minor event A system event that does not currently impair service, but which needs correction before it becomes more severe.

N

namespace In the tree structure of a Lightweight Directory Access Protocol (LDAP) directory, a set of unique names from which an object name is derived and understood. For example, files are named within the file namespace, and printers are named within the printer namespace.

Network File System (NFS) A protocol that enables disparate hardware configurations to function together transparently.

Network Information Service (NIS) A system of programs and data files that UNIX systems use to collect, collate, and share specific information about machines, users, file systems, and network parameters throughout a network of computer systems.

network interface card (NIC) An internal circuit board or card that connects a workstation or server to a networked device.

network management station (NMS) A powerful workstation with one or more network management applications installed. The NMS is used to remotely manage a network.

network mask A number used by software to separate the local subnet address from the rest of a given Internet Protocol (IP) address.

Network Time Protocol (NTP) An Internet standard for Transmission Control Protocol/Internet Protocol (TCP/IP) networks. NTP synchronizes the clock times of networked devices with NTP servers to the millisecond using Coordinated Universal Time (UTC).

node An addressable point or device on a network. A node can connect a computing system, a terminal, or various peripheral devices to the network.

nonvolatile memory A type of memory that ensures that data is not lost when system power is off.

notification threshold A value that defines the amount of power wattage consumed that will trigger an alert notification.

O

object identifier (OID) A number that identifies an object's position in a global object registration tree. Each node of the tree is assigned a number, so that an OID is a sequence of numbers. In Internet usage the OID numbers are delimited by dots, for example, "0.128.45.12." In the Lightweight Directory Access Protocol (LDAP), OIDs are used to uniquely identify schema elements, including object classes and attribute types.

OpenBoot PROM A layer of software that takes control of an initialized system after the power-on self-test (POST) successfully tests components. OpenBoot PROM builds data structures in memory and boots the operating system.

OpenIPMI An operating system-independent, event-driven library for simplifying access to the Intelligent Platform Management Interface (IPMI).

open problem An indicator that a problem, or fault condition, is detected on a managed device. Oracle ILOM identifies the problem on the Open Problems web page or the Open Problems tabular CLI output.

Operator A user with limited privileges to the managed host system.

Oracle ILOM Remote Console A graphical user interface that enables a user to redirect devices (keyboard, mouse, video display, storage media) from a desktop to a remote host server.

out-of-band (OOB) system management Server management capability that is enabled when the operating system network drivers or the server is not functioning properly.

output power The amount of power provided from the power supply units to the chassis components.

P

parity A method used by a computer for checking that data received matches data sent. Also refers to information stored with data on a disk that enables the controller to rebuild data after a drive failure.

Pc-Check An application made by Eurosoft (UK) Ltd. that runs diagnostic tests on computer hardware.

peak permitted The maximum power wattage a managed device can consume.

permissions A set of privileges granted or denied to a user or group that specify read, write, or execution access to a file or directory. For access control, permissions state whether access to the directory information is granted or denied, and the level of access that is granted or denied.

permitted power consumption The maximum power wattage that the server will allow to be used at any given time.

physical address An actual hardware address that matches a memory location. Programs that refer to virtual addresses are subsequently mapped to physical addresses.

Platform Event Filtering (PEF) A mechanism that configures the service processor to take selected actions when it receives event messages, for example, powering off or resetting the system or triggering an alert.

Platform Event Trap (PET) A configured alert triggered by a hardware or firmware (BIOS) event. A PET is an Intelligent Platform Management Interface (IPMI)–specific, Simple Network Management Protocol (SNMP) trap, which operates independently of the operating system.

port The location (socket) to which Transmission Control Protocol/Internet Protocol (TCP/IP) connections are made. Web servers traditionally use port 80, the File Transfer Protocol (FTP) uses port 21, and Telnet uses port 23. A port enables a client program to specify a particular server program in a computer on a network. When a server program is started initially, it binds to its designated port number. Any client that wants to use that server must send a request to bind to the designated port number.

port number A number that specifies an individual Transmission Control Protocol/Internet Protocol (TCP/IP) application on a host machine, providing a destination for transmitted data.

power allocation plan A feature that enables a user to effectively monitor and acquire the precise power metrics allocated to a single managed device, or to the individual components installed on a managed device. This aids in planning an energy-efficient data center.

power consumption A value that shows either the input power consumed by the managed device or the output power provided by the power supply units (PSUs).

power cycling The process of turning the power to a system off then on again.

power supply maximum The largest amount of input power wattage that the power supplies are capable of consuming.

Power Monitoring interface An interface that enables a user to monitor real-time power consumption, including available power, actual power, and permitted power, for the service processor (SP) or an individual power supply with accuracy to within one second of the time the power usage occurred.

power-on self-test (POST) A program that takes uninitialized system hardware and probes and tests its components at system startup. POST configures useful components into a coherent, initialized system and hands it over to the OpenBoot PROM. POST passes to OpenBoot PROM a list of only those components that have been successfully tested.

Preboot Execution Environment (PXE) An industry-standard client-server interface that enables a server to boot an operating system (OS) over a Transmission Control Protocol/Internet Protocol (TCP/IP) network using Dynamic Host Configuration Protocol (DHCP). The PXE specification describes how the network adapter card and BIOS work together to provide basic networking capabilities for the primary bootstrap program, enabling it to perform a secondary bootstrap over the network, such as a TFTP load of an OS image. Thus, the primary bootstrap program, if coded to PXE standards, does not need knowledge of the system's networking hardware.

Privacy Enhanced Mail (PEM) A standard for Internet electronic mail that encrypts data to ensure privacy and data integrity.

protocol A set of rules that describes how systems or devices on a network exchange information.

proxy A mechanism whereby one system acts on behalf of another system in responding to protocol requests.

public key encryption A cryptographic method that uses a two-part key (code) that is made up of public and private components. To encrypt messages, the published public keys of the recipients are used. To decrypt messages, the recipients use their unpublished private keys, which are known only to them. Knowing the public key does not enable users to deduce the corresponding private key.

R

rackmount server power consumption The sum of input power being consumed by the rackmount chassis power supplies.

real-time clock (RTC) A battery-backed component that maintains the time and date for a system, even when the system is powered off.

real-time power monitoring A feature that, through polling hardware interfaces (CMM, SP, PSUs, and so on), provides continuously updated power consumption metrics, within one second of accuracy.

reboot An operating system–level operation that performs a system shutdown followed by a system boot. Power is a prerequisite.

redirection The channeling of input or output to a file or device rather than to the standard input or output of a system. The result of redirection sends input or output that a system would normally display to the display of another system.

redundant power The available power wattage currently not allocated to the blade chassis power supplies.

required power The maximum sum of power wattage required for all blade slots or for an individual blade slot.

Remote Authentication Dial-In User Service (RADIUS) A protocol that authenticates users against information in a database on a server and grants authorized users access to a resource.

Remote Management and Control Protocol (RMCP) A networking protocol that enables an administrator to respond to an alert remotely by powering the system on or off or forcing a reboot.

remote procedure call (RPC) A method of network programming that enables a client system to call functions on a remote server. The client starts a procedure at the server, and the result is transmitted back to the client.

remote system A system other than the one on which the user is working.

reset A hardware-level operation that performs a system power-off, followed by a system power-on.

role An attribute of user accounts that determines user access rights.

root In UNIX operating systems, the name of the superuser (root). The root user has permissions to access any file and carry out other operations not permitted to ordinary users. Roughly equivalent to the Administrator user name on Windows Server operating systems.

root directory The base directory from which all other directories stem, either directly or indirectly.

router A system that assigns a path over which to send network packets or other Internet traffic. Although both hosts and gateways do routing, the term "router" commonly refers to a device that connects two networks.

RSA algorithm A cryptographic algorithm developed by RSA Data Security, Inc. It can be used for both encryption and digital signatures.

S

schema Definitions that describe what type of information can be stored as entries in the directory. When information that does not match the schema is stored in the directory, clients attempting to access the directory might be unable to display the proper results.

Secure Shell (SSH) A UNIX shell program and network protocol that enables secure and encrypted log in and execution of commands on a remote system over an insecure network.

Secure Sockets Layer (SSL) A protocol that enables client-to-server communication on a network to be encrypted for privacy. SSL uses a key exchange method to establish an environment in which all data exchanged is encrypted with a cipher and hashed to protect it from eavesdropping and alteration. SSL creates a secure connection between a web server and a web client. Hypertext Transfer Protocol Secure (HTTPS) uses SSL.

sensor data record (SDR) To facilitate dynamic discovery of features, the Intelligent Platform Management Interface (IPMI) includes this set of records. They include software information, such as how many sensors are present, what type they

	are, their events, threshold information, and so on. The sensor data records enable software to interpret and present sensor data without any prior knowledge about the platform.
serial console	A terminal or a tip line connected to the serial port on the service processor. A serial console is used to configure the system to perform other administrative tasks.
serial port	A port that provides access to the command-line interface (CLI) and the system console stream using serial port redirection.
server certificate	A certificate used with Hypertext Transfer Protocol Secure (HTTPS) to authenticate web applications. The certificate can be self-signed or issued by a Certificate Authority (CA).
Server Message Block (SMB) protocol	A network protocol that enables files and printers to be shared across a network. The SMB protocol provides a method for client applications to read and write to files on and request services from server programs in the network. The SMB protocol enables you to mount file systems between Windows and UNIX systems. The SMB protocol was designed by IBM and subsequently modified by Microsoft Corp. Microsoft renamed the protocol the Common Internet File System (CIFS).
service processor (SP)	A device used to manage chassis environmental, configuration, and service functions, and receive event data from other parts of the system. It receives data through sensor interfaces and interprets this data by using the sensor data record (SDR) to which it provides an interface. The SP provides another interface to the system event log (SEL). Typical functions of the SP are to measure processor temperature, power supply values, and cooling fan status. The SP can take autonomous action to preserve system integrity.
session time-out	A specified duration after which a server can invalidate a user session.
Simple Mail Transfer Protocol (SMTP)	A Transmission Control Protocol/Internet Protocol (TCP/IP) used for sending and receiving email.
Simple Network Management Protocol (SNMP)	A simple protocol used to exchange data about network activity. With SNMP, data travels between a managed device and a network management station (NMS). A managed device can be any device that runs SNMP, such as hosts, routers, web servers, or other servers on the network.
Single Sign On (SSO)	A form of authentication in which a user enters credentials once to access multiple applications.
Snapshot utility	An application that collects data about the state of the server processor (SP). Oracle Services uses this data for diagnostic purposes.
subnet	An identifiably separate part of an organization's network. A subnet can divide a single logical network into smaller physical networks to simplify routing. The subnet is the portion of an Internet Protocol (IP) address that identifies a block of host IDs.

subnet mask A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address and one or more bits of the local portion. Also called an "address mask."

Sun Blade Modular System A chassis that holds multiple Oracle blade server modules.

Sun blade server module A server module (blade) that can be plugged into a chassis, also known as a modular system.

superuser A special user who has privileges to perform all administrative functions on a UNIX system. Also called "root."

syslog A protocol over which log messages can be sent to a server.

system event log (SEL) A log that provides nonvolatile storage for system events that are logged autonomously by the service processor or directly with event messages sent from the host.

system identifier A text string that helps identify the host system. This string is included as a varbind in SNMP traps generated from the SUN-HW-TRAP-MIB. While the system identifier can be set to any string, it is most commonly used to help identify the host system. The host system can be identified by a description of its location or by referencing the host name used by the operating system on the host.

T

target In the Oracle ILOM command-line interface, every object in the CLI namespace.

target limit A value, set on the Oracle server, that determines (by wattage or percentage) the power budgeting parameters allowed on the server.

target namespace In the Oracle ILOM command-line interface, a hierarchical, predefined tree that contains every managed object in the system. For more details, see *namespace*.

Telnet The virtual terminal program that enables the user of one host to log in to a remote host. A Telnet user of one host who is logged in to a remote host can interact as a normal terminal user of the remote host.

threshold Minimum and maximum values within a range that sensors use when monitoring temperature, voltage, current, and fan speed.

time-out A specified time after which the server should stop trying to finish a service routine that appears to be hung.

transmission control block (TCB) Part of the Transmission Control Protocol/Internet Protocol (TCP/IP) that records and maintains information about the state of a connection.

Transmission Control Protocol/Internet Protocol (TCP/IP) An Internet protocol that provides for the reliable delivery of data streams from one host to another. TCP/IP transfers data between different types of networked systems, such as systems running Oracle Solaris, Microsoft Windows, or Linux software. TCP guarantees delivery of data and that packets will be delivered in the same sequence in which they were sent.

trap Event notification made by Simple Network Management Protocol (SNMP) agents by their own initiative when certain conditions are detected. SNMP formally defines seven types of traps and permits subtypes to be defined.

Trivial File Transport Protocol (TFTP) A simple transport protocol that transfers files to systems. TFTP uses User Datagram Protocol (UDP).

U

unfilled grant requests The total sum of ungranted power wattage that the chassis monitoring module has been requested to grant to the chassis blade slots.

uniform resource identifier (URI) A unique string that identifies a resource on the Internet or an intranet.

Universal Serial Bus (USB) An external bus standard that supports data transfer rates of 450M bits per second (USB 2.0). A USB port connects devices, such as mouse pointers.

user account A record of essential user information that is stored on the system. Each user who accesses a system has a user account.

User Datagram Protocol (UDP) A connectionless transport layer protocol that adds some reliability and multiplexing to the Internet Protocol (IP). UDP enables one application program to deliver, through IP, datagrams to another application program on another machine. The Simple Network Management Protocol (SNMP) is usually implemented over UDP.

user privilege levels An attribute of a user that designates the operations a user can perform and the resources a user can access.

user identification (userid) A unique string identifying a user to a system.

user identification number (UID number) The number assigned to each user accessing a UNIX system. The system uses UID numbers to identify, by number, the owners of files and directories.

user name A combination of letters, and possibly numbers, that identifies a user to the system.

W

web server Software that provides services to access the Internet or an intranet. A web server hosts web sites, provides support for HTTP-HTTPS and other protocols, and executes server-side programs.

Web Services for Management (WS-Management) protocol and Common Information Model (CIM) Distributed Management Task Force (DMTF) standards, implemented in Oracle ILOM, that enable developers to build and deploy network management applications to monitor and manage information about Oracle system hardware.

wide area network (WAN) A network consisting of many systems that provides file transfer services. A WAN can cover a large physical area, sometimes worldwide.

X

X.509 certificate The most common certificate standard. X.509 certificates are documents containing a public key and associated identity information, digitally signed by a Certificate Authority (CA).

X Window System A common UNIX window system that enables a workstation or terminal to control multiple sessions simultaneously.

Index

D

M

N

O

P

R

S

T

U

V

W

X

Z