Oracle® Integrated Lights Out Manager (ILOM) 3.0

Concepts Guide

Part No. 820-6410-12
October 2010, Revision A

Please
Recycle

Adobe PostScript™

Contents

Using This Documentation

This concepts guide describes the Oracle Integrated Lights Out Manager (ILOM) 3.0 features that are common to Oracle's Sun rack-mounted servers or server modules supporting Oracle ILOM 3.0.

You can access these ILOM features and perform ILOM tasks using different user interfaces, regardless of the Oracle Sun server platform that ILOM is managing. This guide is written for technicians, system administrators, authorized service providers, and users who have experience managing system hardware.

To fully understand the information that is presented in this guide, use the concepts guide in conjunction with other guides in the ILOM 3.0 Documentation Collection. For a description of the guides that comprise the ILOM 3.0 Documentation Collection, see "Related Documentation" on page xi.

This preface contains the following topics:

- "Related Documentation" on page xi
- "Documentation, Support and Training" on page xiii
- "Documentation Feedback" on page xiii
- "ILOM 3.0 Firmware Version Numbering Scheme" on page xiii

Related Documentation

The following table list the guides that comprise the ILOM 3.0 Documentation Collection. You can access or download these guides online at:

`http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`

Note – The documents comprising the ILOM 3.0 Documentation Collection were formerly referred to as Sun Integrated Lights Out Manager (ILOM) 3.0 guides.

Title	Content	Part Number	Format
Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide	Information that describes ILOM features and functionality	820-6410	PDF HTML
Oracle Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide	Information and procedures for network connection, logging in to ILOM for the first time, and configuring a user account or a directory service	820-5523	PDF HTML
Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide	Information and procedures for accessing ILOM functions using the ILOM web interface	820-6411	PDF HTML
Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide	Information and procedures for accessing ILOM functions using the ILOM CLI	820-6412	PDF HTML
Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide	Information and procedures for accessing ILOM functions using SNMP or IPMI management hosts	820-6413	PDF HTML
Oracle Integrated Lights Out Manager (ILOM) 3.0 CMM Administration Guide for Sun Blade 6000 and 6048 Modular Systems	Information and procedures for managing CMM functions in ILOM.	820-0052	PDF HTML
Oracle Integrated Lights Out Manager (ILOM) 3.0 Feature Updates and Release Notes	Late breaking information about new ILOM 3.0 features, as well as known problems and work arounds.	820-7329	PDF HTML

In addition to the ILOM 3.0 Documentation Collection, associated ILOM Supplement guides or platform Administration guides present ILOM features and tasks that are specific to the server platform you are using. Use the ILOM 3.0 Documentation Collection in conjunction with the ILOM Supplement or platform Administration guide that comes with your server platform.

Documentation, Support and Training

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

Documentation Feedback

Submit comments about this document by clicking the Feedback[+] link at http://docs.sun.com

Please include the title and part number of your document with your feedback:

Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide, part number 820-6410-12.

ILOM 3.0 Firmware Version Numbering Scheme

ILOM 3.0 provides a version numbering scheme to help you identify which version of ILOM you are running on your system. The numbering scheme includes a five-field string, for example, `a.b.c.d.e`, where:

- `a` – Represents the major version of ILOM.
- `b` – Represents a minor version of ILOM.
- `c` – Represents the update version of ILOM.
- `d` – Represents a micro version of ILOM. Micro versions are managed per platform or group of platforms. See your platform Product Notes for details.
- `e` – Represents a nano version of ILOM. Nano versions are incremental iterations of a micro version.

For example, ILOM 3.1.2.1.a would designate:

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

CHAPTER 1

ILOM Overview

Topics

Description	Links
Learn about ILOM features and functionality	• "What Is ILOM?" on page 2 • "What Does ILOM Do?" on page 2 • "ILOM Features and Functionality" on page 4 • "New Features in ILOM 3.0" on page 5 • "Roles for ILOM User Accounts" on page 6 • "ILOM Interfaces" on page 7 • "ILOM on the Server and CMM" on page 8 • "Access and Initial Login to ILOM" on page 9 • "`root` and `default` User Accounts" on page 9 • "`root` Factory Default Password Warning Message" on page 10 • "System Banner Messages" on page 12

Related Topics

For ILOM	Chapter or Section	Guide
• CLI	• CLI Overview • Logging In to and Out of ILOM	*Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* (820-6412)

Related Topics

For ILOM	Chapter or Section	Guide
• Web interface	• Web Interface Overview • Logging In to and Out of ILOM	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)
• SNMP and IPMI hosts	• SNMP Overview • IPMI Overview	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide* (820-6413)

The ILOM 3.0 Documentation Collection is available at:
`http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`

What Is ILOM?

Oracle's Integrated Lights Out Manager (ILOM) provides advanced service processor hardware and software that you can use to manage and monitor your Oracle Sun servers. ILOM's dedicated hardware and software is preinstalled on a variety of Oracle Sun server platforms, including x86-based Sun Fire servers, Sun Blade modular chassis systems, Sun Blade server modules, as well as on SPARC-based servers. ILOM is a vital management tool in the data center and can be used to integrate with other data center management tools already installed on your systems.

ILOM is supported on many Oracle systems enabling users to experience a single, consistent, and standards-based service processor (SP) across all Oracle Sun server product lines. This means you will have:

- Single, consistent system management interfaces for operators
- Rich protocol and standards support
- Broadening third-party management support
- System management functions integrated into Oracle's Sun servers at no extra cost

What Does ILOM Do?

ILOM enables you to actively manage and monitor the server independently of the operating system state, providing you with a reliable Lights Out Management (LOM) system. With ILOM, you can proactively:

- Learn about hardware errors and faults as they occur
- Remotely control the power state of your server
- View the graphical and non-graphical consoles for the host
- View the current status of sensors and indicators on the system
- Determine the hardware configuration of your system
- Receive generated alerts about system events in advance via IPMI PETs, SNMP traps, or email alerts.

The ILOM service processor (SP) runs its own embedded operating system and has a dedicated Ethernet port, which together provide out-of-band management capability. In addition, you can access ILOM from the server's host operating system (Solaris, Linux, and Windows). Using ILOM, you can remotely manage your server as if you were using a locally attached keyboard, monitor, and mouse.

ILOM automatically initializes as soon as power is applied to your 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.

You can easily integrate these management interfaces with other management tools and processes that you might have working already with your servers, such as Oracle Enterprise Ops Center. This easy-to-use system management platform for Solaris and Linux provides the tools that you need to efficiently manage systems on your network. Oracle Enterprise Ops Center can discover new and existing systems on your network, update firmware and BIOS configurations, provision the operating environment with off-the-shelf distributions or Solaris images, manage updates and configuration changes, and remotely control key aspects of the service processor such as boot control, power status, and indicator lights. For more information about Oracle Enterprise Ops Center, go to:

`http://www.oracle.com/us/products/enterprise-manager/opscenter/index.html`

In addition, you can integrate ILOM with these third-party management tools:

- Oracle Hardware Management Connector 1.2 for Altiris Deployment Solution
- BMC PATROL 6.9
- CA Unicenter Network and Systems Management (NSM)
- HP OpenView Operations for UNIX
- HP OpenView Operations for Windows
- HP Systems Insight Manager
- IBM Director
- IBM Tivoli Enterprise Console
- IBM Tivoli Monitoring (ITM)

- IBM Tivoli Netcool/OMNIbus
- IPMItool 1.8.10.3 for Microsoft Windows 2003
- Microsoft Operations Manager 2005
- Microsoft System Management
- Microsoft Systems Center Operations Manager 2007
- Sun Deployment Pack 1.0 for Microsoft System Center Configuration Manager 2007
- Sun Update Catalog for Microsoft System Center Configuration Manager 2007
- Sun IPMI System Management Driver for Server 2003 prior to R2
- Sun ILOM Common SNMP MIBs
- Service Processor Error Injector 1.0

A description of these third-party system management tools and their support for Oracle's Sun systems is available at:

`http://www.sun.com/system-management/tools.jsp`

ILOM Features and Functionality

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

TABLE 1-1 ILOM Features and Functionality

ILOM Feature	What You Can Do
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 ILOM initial configuration	• Manual SP configuration, including IP address, through BIOS interface, serial or Ethernet SP ports, or host OS
Downloadable firmware updates	• Download firmware updates via browser-based web interface
Remote hardware monitoring	• Monitor system status and event logs • Monitor customer-replaceable units (CRUs) and field-replaceable units (FRUs), including power supplies, fans, host bus adapters (HBAs), disks, CPUs, memory, and motherboard • Monitor environmentals (component temperatures) • Monitor sensors, including voltage and power • Monitor indicators (LEDs)

TABLE 1-1 ILOM Features and Functionality *(Continued)*

ILOM Feature	What You Can Do
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 Access	• Redirect the system serial console via 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 emergency shutdown or perform a graceful shutdown to shut down the host operating system before power off
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	• Monitor system BIOS, POST, and sensor messages • Log events in a consistent method for all "service" data • Monitor hardware and system-related errors, as well as ECC memory errors, reported into SP logs, syslog, and remote log-host
System alerts, including SNMP traps, IPMI PETs, remote syslog, and email alerts	• Monitor components using industry-standard SNMP commands and the IPMItool utility.

New Features in ILOM 3.0

ILOM 3.0 is enhanced with many new features and functions that were not available in ILOM 2.x, including improved security, improved usability, and easier integration into your data center environment. TABLE 1-2 lists new features for ILOM 3.0.

TABLE 1-2 ILOM 3.0 New Features

Category	Feature
General Functionality	
	DNS support
	Timezone support

TABLE 1-2 ILOM 3.0 New Features *(Continued)*

Category	Feature
	Configuration backup and restore
	Restore to factory defaults
	Enhanced LDAP and LDAP/SSL support
	Java-based remote storage CLI
	Power management capabilities
	Ability to generate new SSH keys
Scalability and Usability	
	User-configurable filtering of hardware monitoring information in CLI and web interface
	Use host name to access other services by name, such as LDAP, Active Directory, LDAP/SSL
Security	
	More granular user roles
	Predefined `root` and `default` accounts
	User SSH key authentication
	Ability to disable the network management port when you are using only the serial port
	Ability to disable individual services, such as IPMI, SSH, and KVMS, so that the port is closed
Serviceability	
	Data collection utility to diagnose system problems

Roles for ILOM User Accounts

For ILOM 3.0, user roles are implemented to control user privileges. However, for backward compatibility, ILOM 2.x style user accounts (which have either Administrator or Operator privileges) are still supported.

For more information about ILOM 3.0 user roles, see "ILOM 3.0 User Account Roles" on page 37.

Support for ILOM 2.x User Accounts

For backward compatibility, ILOM 3.0 supports ILOM 2.x user accounts such that users with ILOM 2.x Administrator or Operator privileges are granted ILOM 3.0 roles that match those privileges. TABLE 1-3 lists the roles assigned to users with Administrator and Operator privileges.

TABLE 1-3 ILOM 3.0 Roles Granted to ILOM 2.x User Accounts

2.x User Privileges	ILOM 3.0 User Roles Granted
Administrator	Admin (a), User Management (u), Console (c), Reset and Host Control (r), and Read Only (o)
Operator	Console (c), Reset and Host Control (r), and Read Only (o) **Note -** To make the level of authorization granted to users with Operator privileges consistent with 2.x capabilities, the Console (c) role granted in this case is modified to prohibit the user from accessing the ILOM Remote Console (JavaRConsole).

ILOM Interfaces

To access all of ILOM's features and functions, you can choose to use a browser-based web interface, a command-line interface, or industry-standard protocols. For more information on ILOM interfaces, see the Overview chapters in the ILOM 3.0 Procedures Guides.

ILOM supports multiple interfaces for accessing its features and functions. You can choose to use a browser-based web interface, a command-line interface, or industry-standard protocols.

- **Web interface** – The web interface provides an easy-to-use browser interface that enables you to log in to the SP, then to perform system management, monitoring, and ILOM configuration tasks.
- **Command-line interface (CLI)** – The command-line interface enables you to operate ILOM using keyboard commands and adheres to industry-standard DMTF-style CLI and scripting protocols. ILOM supports SSH v2.0 and v3.0 for secure access to the CLI. Using the CLI, you can reuse existing scripts with Oracle Sun systems, and automate tasks using familiar interfaces.
- **Remote Console** – The ILOM Remote Console (JavaRConsole) enables you to access your x64 or SPARC server's console remotely. It redirects the keyboard, mouse, and video screen, and can redirect input and output from the local machine's CD and diskette drives.

- **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.

  For more information about using IPMI to monitor or manage your Oracle Sun system, see the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide*.

- **WS-Management/CIM** – As of version 3.0.8, 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 ILOM enables developers to build and deploy network management applications to monitor and manage information about Oracle's Sun system hardware.

  For more information about WS-Management/CIM, see the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide*.

- **Simple Network Management Protocol (SNMP) interface** – ILOM also provides an SNMP v3.0 interface for third-party applications such as HP OpenView and IBM Tivoli. Some of the MIBs supported by ILOM 3.0 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)

For a complete list of SNMP MIBs supported and used by ILOM, see the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide.*

ILOM on the Server and CMM

ILOM supports two ways of managing a system: using the SP directly or using the chassis monitoring module (CMM), if you are using a modular chassis system.

- **Using the service processor directly** – Communicating directly with the rackmounted server SP or server module SP enables you to manage individual server operations. This approach might be useful when troubleshooting a server module or rackmounted server, or controlling access to specific servers in your data center.
- **Using the chassis monitoring module** – If you are using a modular chassis system, managing the system from the CMM enables you to use ILOM to set up and manage components throughout the entire modular chassis system, or to drill down to manage an individual server module.

Access and Initial Login to ILOM

You can access ILOM 3.0 from a browser interface or Secure Shell (SSH) client using either an IPv4 address, IPv6 address, or a DNS hostname. For detailed information on logging in to ILOM for the first time using the `root` user account, see the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

`root` and `default` User Accounts

ILOM 3.0 provides two preconfigured accounts: the `root` user account and the `default` user account. You will use the `root` account for initial login to ILOM. This `root` user account will be familiar to users who are migrating from ILOM 2.x to ILOM 3.0 and who know how to log in using the `root` user account. The `default` user account is a new feature in ILOM 3.0 that is used for password recovery.

`root` User Account

The `root` user account is persistent and is available on all interfaces (web interface, CLI, SSH, serial console, and IPMI) unless you choose to delete the `root` account. The `root` account provides built-in administrative privileges (read and write) for all ILOM features, functions, and commands.

To log in to ILOM, use the following `root` account user name and password:

User name: **`root`**

Password: **`changeme`**

To prevent unauthorized access to your system, you should change the root password (changeme) on each service processor (SP) or chassis monitoring module (CMM) installed in your system. Alternatively, you can delete the root account to secure access to your system. However, before you delete the root account, you must set up a new user account or configure a directory service so that you will be able to log in to ILOM.

default User Account

The default user account is used for password recovery. The default user account is available through the serial console only and you must prove physical presence at the server to use the default user account. The default user account cannot be changed or deleted.

If you delete the root account before you have configured another user account to log in to ILOM, you can use the default account as an alternative way to log in and re-create the root account. To re-create the root user account, use the normal ILOM user commands to create a new account. For information about how to create a user account, see the section about Add User Account and Assign Privileges in either the web interface or CLI section of the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide*.

For password recovery, use the following user name and password to log in using the default account:

User name: **default**

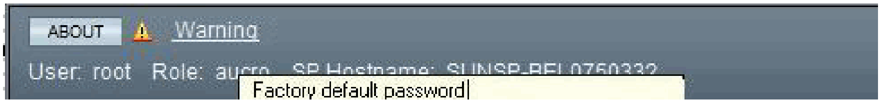
Password: **defaultpassword**

root Factory Default Password Warning Message

As of ILOM 3.0.6, when the root password in ILOM is set to the factory default, a warning will appear on the ILOM CLI and web interface.

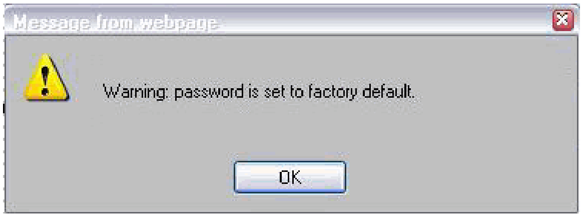
For example:

- In the ILOM web interface, a warning link will appear in the page header. Placing your mouse over the link will display the warning message or clicking the warning link will display the warning message in a dialog.



User: root Role: aucro SP Hostname: SUNSP-BEL0750332

Factory default password



Message from webpage

Warning: password is set to factory default.

- In the ILOM CLI, the following factory default warning message appears after logging in to ILOM.

```
Password:
Waiting for daemons to initialize...
Daemons ready
Oracle(TM) Integrated Lights Out Manager

Version 3.0.0.0 r46636
Copyright 2009 Sun Microsystems, Inc. All rights reserved.
Use is subject to license terms.

Warning: password is set to factory default.
```

System Banner Messages

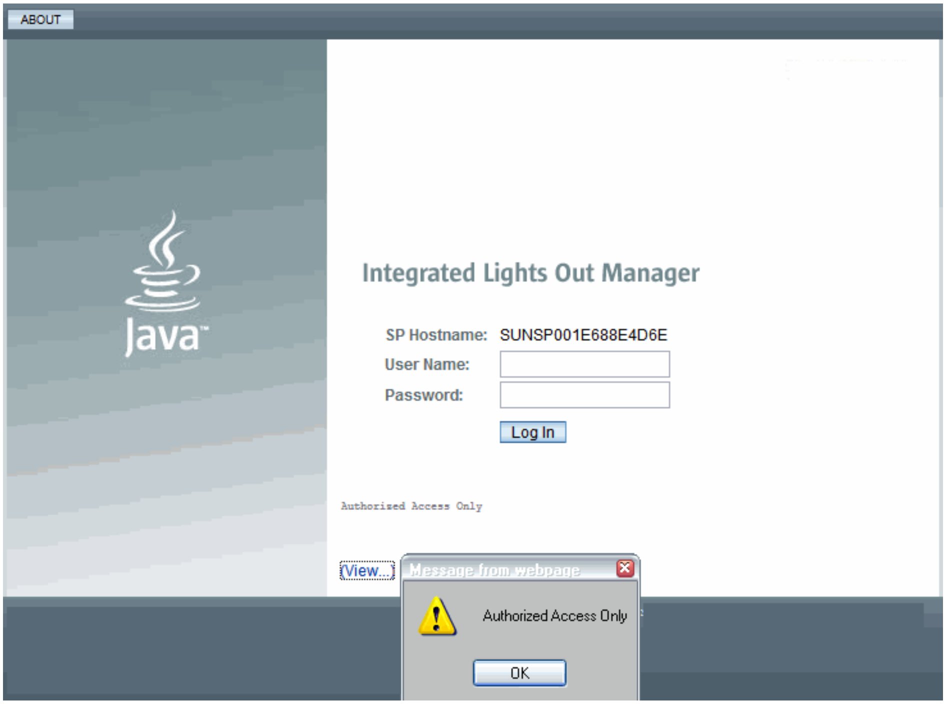
As of ILOM 3.0.8, system administrators can create banner messages and display them on the Login page or immediately after logging in to ILOM.

Creating and displaying banner messages in ILOM is optional. However, system administrators can use this capability whenever there is a need to share information about system updates, system policies, or other important announcements. Examples of where (Login page or after login) the banner message appear in ILOM after they have been created are shown in FIGURE 1-1, FIGURE 1-2, and FIGURE 1-3.

For instructions on how to create the banner messages in ILOM, see the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

FIGURE 1-1 Login Page – Connect Banner Example – Web Interface



Integrated Lights Out Manager

SP Hostname: SUNSP001E688E4D6E

User Name:

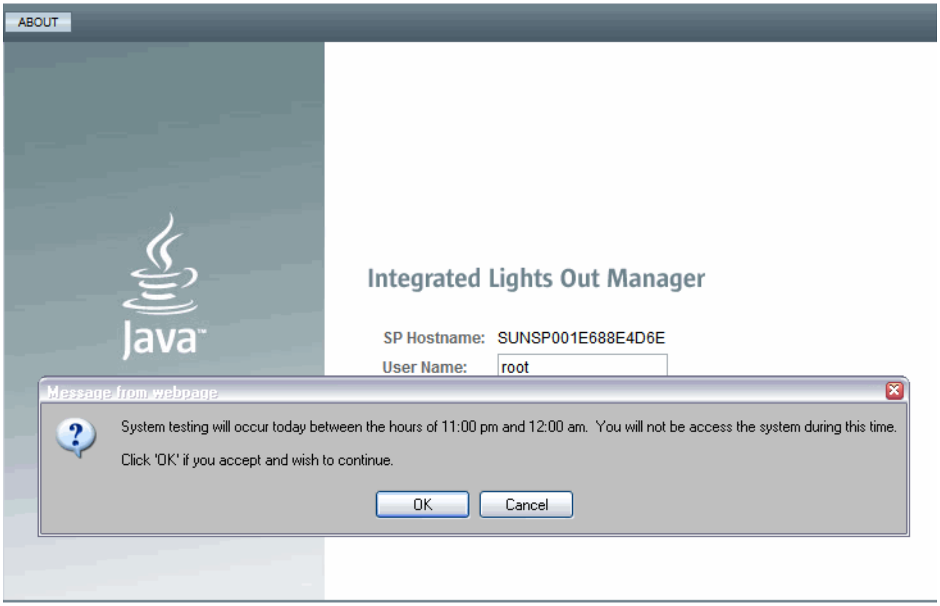
Password:

Authorized Access Only

Message from webpage

Authorized Access Only

FIGURE 1-2 After Logging In - Banner Message Example - Web Interface



SP Hostname: SUNSP001E688E4D6E

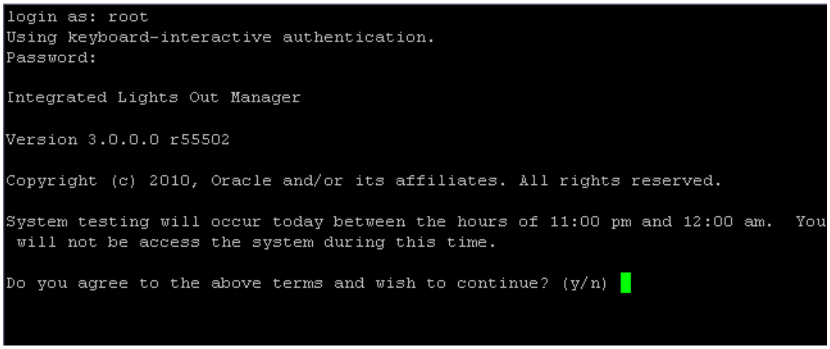
User Name: root

Message from webpage

System testing will occur today between the hours of 11:00 pm and 12:00 am. You will not be access the system during this time.

Click 'OK' if you accept and wish to continue.

FIGURE 1-3 Banner Message Example - CLI



```
login as: root
Using keyboard-interactive authentication.
Password:

Integrated Lights Out Manager

Version 3.0.0.0 r55502

Copyright (c) 2010, Oracle and/or its affiliates. All rights reserved.

System testing will occur today between the hours of 11:00 pm and 12:00 am.  You
 will not be access the system during this time.

Do you agree to the above terms and wish to continue? (y/n)
```

CHAPTER 2

ILOM Network Configurations

Topics

Description	Links
Learn about ILOM network management and connection methods	• "ILOM Network Management" on page 16
Learn about ILOM network communication settings and network port assignments	• "ILOM Communication Settings" on page 20 • "Network Port Assignments" on page 18 • "Switch Serial Port Output" on page 20 • "SP Management Port – Recommended Practice for Spanning Tree Parameters" on page 21
Learn about configuring ILOM in an IPv4 network environment	• "Network Configurations for IPv4" on page 21
Learn about configuring ILOM in a dual-stack IPv4/IPv6 network environment	• "Dual-Stack Network Configurations for IPv4 and IPv6 (ILOM 3.0.12)" on page 22
Learn about configuring the Local Interconnect Interface	• "Local Interconnect Interface: Local Connection to ILOM From Host OS" on page 26

Related Topics

For ILOM	Chapter or Section	Guide
• Getting started	• Connecting to ILOM • Initial ILOM Setup Procedures Using the Web Interface • Initial ILOM Setup Procedures Using the CLI	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide* (820-5523-10)

Related Topics

For ILOM	Chapter or Section	Guide
• CLI	• Logging In to and Out of ILOM • Configuring Communication Settings • Example Setup of Dynamic DNS • Configuring an IPv4 and IPv6 Network Environment	*Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* (820-6412)
• Web interface	• Logging In to and Out of ILOM • Configuring Communication Settings • Configuring an IPv4 and IPv6 Network Environment	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)
• IPMI and SNMP hosts	• Configuring ILOM Communication Settings	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide* (820-6413)

The ILOM 3.0 Documentation Collection is available at:
`http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`

ILOM Network Management

You can establish communication with ILOM through a console connection to the serial management port on the server or chassis monitoring module (CMM), or through an Ethernet connection to the network management port on the server or CMM.

A dedicated network management port will help you manage your server platform optimally with ILOM. Using the network management port, traffic destined for ILOM is kept separate from any data transfers made by the host operating system.

Refer to your platform documentation to determine how to connect to your network management port.

You can use Dynamic DNS to automatically assign a host name and IP address on new ILOM installations based on the system's serial number. See Appendix A for an overview of Dynamic DNS and configuration instructions.

ILOM Connection Methods

The way in which you connect to ILOM depends on your server platform. Refer to your platform documentation for details.

The following table lists the different methods you can use to connect to ILOM.

TABLE 2-1 ILOM Connection Methods

Connection Method	Rack-Mounted	Blade	Supported Interface	Description
Ethernet network management connection	Yes	Yes	CLI and web interface	Connect to the Ethernet network management port. You must know ILOM's host name or IP address.
Serial connection	Yes	Yes	CLI only	Connect directly to the serial management port.
Local Interconnect Interface (as of ILOM 3.0.12)	Verify support for this feature in your platform ILOM Supplement Guide or Administration Guide.			Enables you to connect to ILOM directly from the host operating system without the need of a physical network connection to the server SP. This feature is not supported on all Sun servers. For more information, see "Local Interconnect Interface: Local Connection to ILOM From Host OS" on page 26.

Note – ILOM supports a maximum of 10 active user sessions, including serial, Secure Shell (SSH), and web interface sessions per service processor (SP). Some SPARC systems support a maximum of only 5 active user sessions per SP.

Initial Setup Worksheet

The worksheet in TABLE 2-2 describes the information that you need to establish initial communication with ILOM

TABLE 2-2 Initial Setup Worksheet to Establish Communication With ILOM

Information for Setup	Requirement	Description
Management Connection–Serial	Mandatory - *if network environment does not support IPv4 DHCP or IPv6 stateless*	ILOM, by default, learns the IPv4 network address using DHCP and the IPv6 network address using IPv6 stateless. If your network environment does not support IPv4 DHCP or IPv6 stateless, you must establish a local serial console connection to ILOM via the serial management port on the server or Chassis Monitoring Module (CMM). If your network environment supports IPv4 DHCP or IPv6 stateless, see the setup information for Management Connection - Ethernet (below). For more information about how to attach a serial console to a server or CMM, refer to your platform documentation.
Management Connection–Ethernet	Optional	You can access ILOM remotely when using the IP address, host name, or local link address assigned to the server SP. This method requires a connection from your local area network to the Ethernet network management port (NET MGT) on the server or CMM. To establish a physical network connection to your server, refer to the installation documentation provided for your server or CMM.
SP Host Name Assignment	Optional	You can assign a meaningful host name to a server SP. For more information, see the *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* or the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*.
System Identifier Assignment	Optional	You can assign a system identifier (meaningful name) to a Sun server. For more information, see the *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* or the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*.
Dynamic DNS Configuration	Optional	You can configure Dynamic DNS to support the use of host names to access server SPs. For example information about setting up Dynamic DNS, see Appendix A. For Dynamic DNS configuration procedures, see *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*.

Network Port Assignments

TABLE 2-3 identifies the default network ports used by ILOM. Most of these network ports are configurable.

Note – TABLE 2-3 identifies default network ports as of ILOM 3.0.6. Some network ports might not be available if you are not using ILOM 3.0.6 or a later version of ILOM.

TABLE 2-3 ILOM Network Ports

Port	Protocol	Application
Common Network Ports		
22	SSH over TCP	SSH - Secure Shell
69	TFTP over UDP	TFTP - Trivial File Transfer Protocol (outgoing)
80	HTTP over TCP	Web (user-configurable)
123	NTP over UDP	NTP - Network Time Protocol (outgoing)
161	SNMP over UDP	SNMP - Simple Network Management Protocol (user-configurable)
162	IPMI over UDP	IPMI - Platform Event Trap (PET) (outgoing)
389	LDAP over UDP/TCP	LDAP - Lightweight Directory Access Protocol (outgoing; user-configurable)
443	HTTPS over TCP	Web (user-configurable))
514	Syslog over UDP	Syslog - (outgoing)
623	IPMI over UDP	IPMI - Intelligent Platform Management Interface
546	DHCP over UDP	DHCP - Dynamic Host Configuration Protocol (client)
1812	RADIUS over UDP	RADIUS - Remote Authentication Dial In User Service (outgoing; user-configurable)
SP Network Ports		
5120	TCP	ILOM Remote Console: CD
5121	TCP	ILOM Remote Console: Keyboard and Mouse
5123	TCP	ILOM Remote Console: Diskette
5555	TCP	ILOM Remote Console: Encryption
5556	TCP	ILOM Remote Console: Authentication
6481	TCP	ILOM Remote Console: Servicetag Daemon
7578	TCP	ILOM Remote Console: Video
7579	TCP	ILOM Remote Console: Serial
CMM Network Ports		
8000 - 8023	HTTP over TCP	ILOM drill-down to server modules (blades)

TABLE 2-3 ILOM Network Ports *(Continued)*

Port	Protocol	Application
8400 - 8423	HTTPS over TCP	ILOM drill-down to server modules (blades)
8200 - 8219	HTTP over TCP	ILOM drill-own to NEMs
8600 - 8619	HTTPS over TCP	ILOM drill-down to NEMs

Switch Serial Port Output

ILOM supports the ability on some Sun servers to switch the serial port output from the server between the SP console (SER MGT) and the host console (COM1). This is referred to as serial port sharing. By default, the SP console is connected to the system serial port. This feature is beneficial for Windows kernel debugging, as it enables you to view non-ASCII character traffic from the host console.

For more information and procedures for switching the serial port output, see the *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*

ILOM Communication Settings

You can use the ILOM CLI interface, web interface, or SNMP to manage ILOM's communication settings, including network, serial port, web, and Secure Shell (SSH) configurations. ILOM lets you view and configure system host names, IP addresses, DNS settings, and serial port settings. You also can enable or disable HTTP or HTTPS web access, and enable or disable SSH.

For more information and procedures for managing ILOM communication settings, see one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide*

SP Management Port – Recommended Practice for Spanning Tree Parameters

Since the SP network management port is not designed to behave like a switch port, the SP network management port does not support switch port features like spanning-tree portfast.

When configuring spanning tree parameters, consider these recommendations:

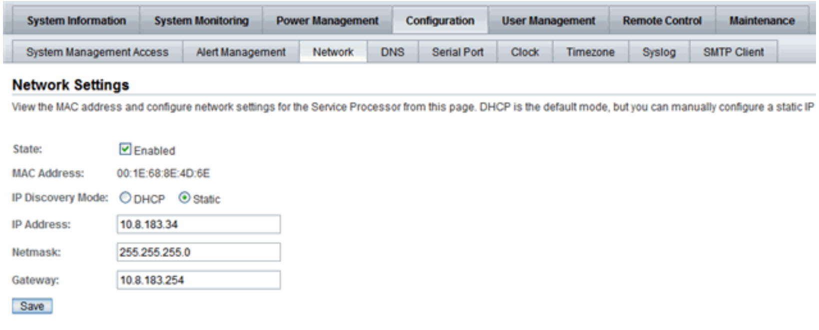
- The port used to connect the SP network management port to the adjacent network switch should always treat the SP network management port as a host port.
- The spanning tree option on the port connecting to the adjacent network switch should either be disabled entirely or at a minimum configured with the following parameters:

Spanning Tree Parameter	Recommended Setting
`portfast`	Enable this interface to immediately move to a forwarding state.
`bpdufilter`	Do not send or receive BPDUs on this interface.
`bpduguard`	Do not accept BPDUs on this interface.
`cdp`	Do not enable the discovery protocol on this interface.

Network Configurations for IPv4

ILOM, by default, uses IPv4 DHCP to learn the IPv4 address for the server SP. If DHCP is not supported in your network environment or if you prefer to set up a static IPv4 address, you can configure the IPv4 network settings in ILOM from the CLI or web interface. An example of the ILOM web interface settings is shown in FIGURE 2-1.

FIGURE 2-1 ILOM Network Settings for IPv4



Network Settings

View the MAC address and configure network settings for the Service Processor from this page. DHCP is the default mode, but you can manually configure a static IP

State: ☑ Enabled

MAC Address: 00:1E:68:8E:4D:6E

IP Discovery Mode: ○ DHCP ● Static

IP Address: 10.8.183.34

Netmask: 255.255.255.0

Gateway: 10.8.183.254

For instructions on how to configure the network settings in ILOM for IPv4, refer to one of the following ILOM procedure guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411), Chapter 4.
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* (820-6412), Chapter 4.

Dual-Stack Network Configurations for IPv4 and IPv6 (ILOM 3.0.12)

ILOM, by default, uses IPv6 stateless to learn the IPv6 address for the server SP. If IPv6 statesless is not supported in your network environment or if you prefer to use another IPv6 network setting to communicate with ILOM, you can modify the IPv6 network settings using the ILOM CLI or web interface.

Note – As of ILOM 3.0.12, dual-stack IPv4 and IPv6 network settings are supported on some servers. Verify support of the IPv6 settings in your platform ILOM Supplement Guide or Administration Guide.

ILOM IPv6 Enhancements

ILOM enhancements for IPv6 include:

- Support for a larger 128-bit IPv6 addressing space.

- Acceptance of IPv6 addresses in designated text entry fields and URLs throughout ILOM.

Note – IPv6 addresses are written with hexadecimal digits and colon separators like 2001:0db0:000:82a1:0000:0000:1234:abcd, as opposed to the dot-decimal notation of the 32-bit IPv4 addresses. IPv6 addresses are composed of two parts: a 64-bit subnet prefix, and a 64-bit host interface ID. To shorten the IPv6 address, you can: (1) omit all leading zeros and (2) replace one consecutive group of zeros with a double colon (::). For example: 2001:db0:0:82a1::1234:abcd

---

- Ability for ILOM to operate fully in a dual-stack IPv4 and IPv6 environment. Within a dual-stack network environment, ILOM is capable of responding to both IPv4 and IPv6 addresses that are concurrently configured for a device (server SP or CMM).
- Support for IPv6 protocols. As of ILOM 3.0.12, IPv6 protocol support includes: SSH, HTTP, HTTPS, Ping6, SNMP, JRC, NTP, KVMS, and all file transfer protocols (tftp, scp, ftp, and so on). Full support for all remaining IPv6 protocols is available as of ILOM 3.0.14.
- Support for the following IPv6 auto-configuration options are available for a device (server SP or CMM):

TABLE 2-4 IPv6 Address Auto-Configuration Options in ILOM

IPv6 Address Auto-Configurations	Description	Supported in ILOM Release:
`Stateless` (enabled by default)	When enabled, the IPv6 `Stateless` auto-configuration is run to learn the IPv6 address(es) for the device. **Note -** If you are running ILOM 3.0.12, this option appears as `stateless_only` in the CLI. If you are running ILOM 3.0.14 or later, this option appears as `stateless` in the CLI.	3.0.12
`DHCPv6 Stateless`	When enabled, the `DHCPv6 Stateless` auto-configuration is run to learn the DNS and domain information for the device.	3.0.14
`DHCPv6 Stateful`	When enabled, the `DHCPv6 Stateful` auto-configuration is run to learn the IPv6 address(es) and DNS information for the device.	3.0.14
`Disabled`	When enabled, the `Disabled` state will only set the Link Local address in ILOM. ILOM will not run any of the IPv6 auto-configuration options to configure an IPv6 address.	3.0.12

Note – As of ILOM 3.0.14, you can enable more than one IPv6 auto-configuration option to run at the same time with the exception of enabling these two auto-configuration options: to run at the same time: `DHCPv6 Stateless` and `DHCPv6 Stateful`.

- Ability to obtain routable IPv6 addresses from any of the following IPv6 network configurations:
  - `Stateless` auto-configuration (requires a network router configured for IPv6)
  - `DHCPv6 Stateful` auto-configuration
  - Manual configuration of single static IPv6 address.
- Support for reporting a Link-Local IPv6 address and up to 10 auto-configured IPv6 addresses per device.

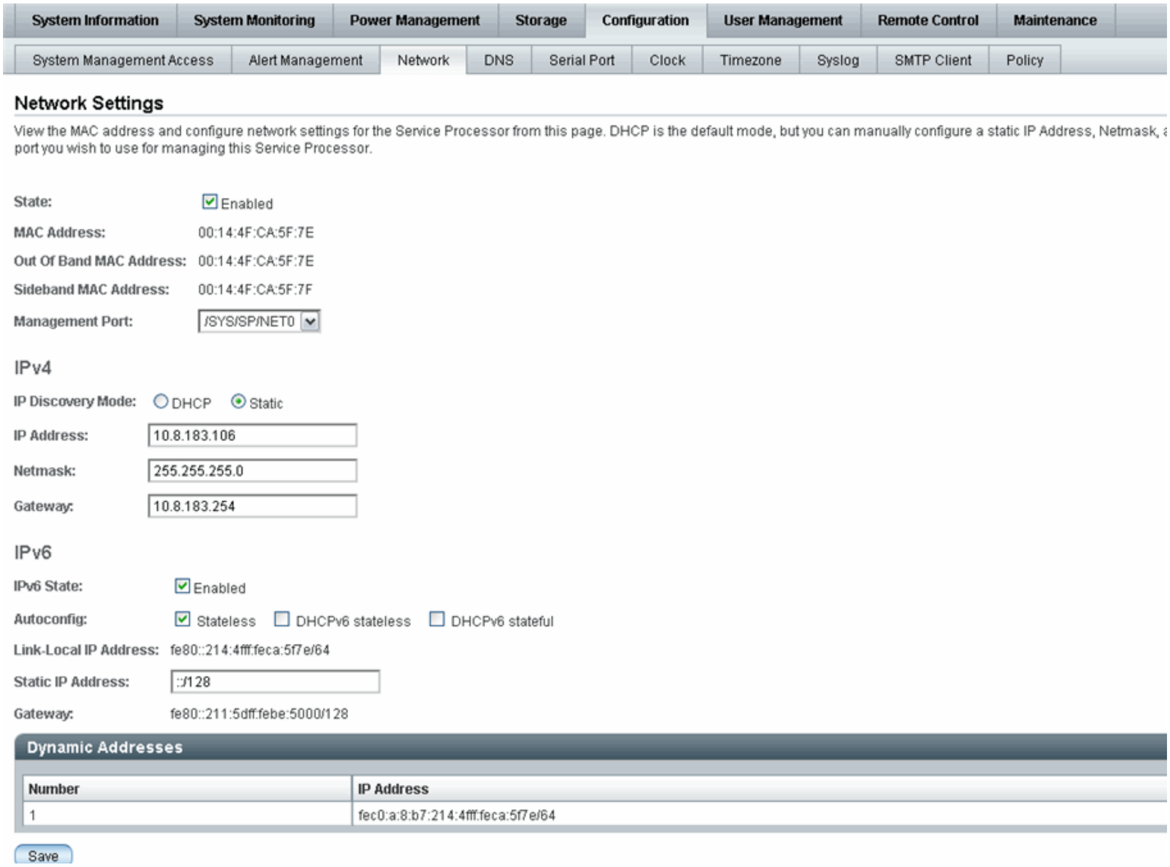
Note – The Link-Local IPv6 address is always shown in ILOM under the `/network/IPv6` target or on the Network Settings page. This address is a non-routable address that you can use to connect to the ILOM SP (or the CMM) from another IPv6 enabled node on the same network.

- Availability of a network configuration testing tool for IPv6 (Ping6).

Dual-Stack Network Options in ILOM CLI and Web Interface

The settings for configuring ILOM in a dual-stack IPv4 and IPv6 network environment are accessible for the server SP (web and CLI) or CMM (CLI only). See FIGURE 2-2 for an example of the dual-stack IPv4 and IPv6 web interface properties available for a server SP.

FIGURE 2-2 ILOM Server SP Web Interface – Network Settings for Dual-stack IPv4 and IPv6



Network Settings

View the MAC address and configure network settings for the Service Processor from this page. DHCP is the default mode, but you can manually configure a static IP Address, Netmask, a
port you wish to use for managing this Service Processor.

State: ☑ Enabled
MAC Address: 00:14:4F:CA:5F:7E
Out Of Band MAC Address: 00:14:4F:CA:5F:7E
Sideband MAC Address: 00:14:4F:CA:5F:7F
Management Port: /SYS/SP/NET0

IPv4

IP Discovery Mode: ○ DHCP ● Static
IP Address: 10.8.183.106
Netmask: 255.255.255.0
Gateway: 10.8.183.254

IPv6

IPv6 State: ☑ Enabled
Autoconfig: ☑ Stateless □ DHCPv6 stateless □ DHCPv6 stateful
Link-Local IP Address: fe80::214:4fff:feca:5f7e/64
Static IP Address: ::/128
Gateway: fe80::211:5dff:febe:5000/128

Dynamic Addresses

Number	IP Address
1	fec0:a:8:b7:214:4fff:feca:5f7e/64

Note – The dual-stack IPv4 and IPv6 properties for the CMM ar only accessible from the CLI. However, you can access the dual-stack IPv4 and IPv6 properties from CMM web interface for the individual server SPs.

For a brief description of the IPv6 configuration options shown in FIGURE 2-2, see TABLE 2-4 “IPv6 Address Auto-Configuration Options in ILOM” on page 23.

For instructions on how to configure the dual-stack network settings in ILOM for IPv4 and IPv6, refer to one of the following ILOM procedure guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411), Chapter 4.
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* (820-6412), Chapter 4.

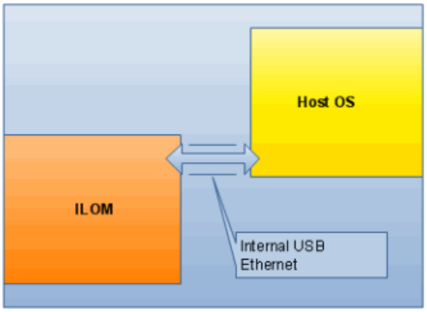
Local Interconnect Interface: Local Connection to ILOM From Host OS

As of ILOM 3.0.12, a communication channel known as the Local Interconnect Interface was added to ILOM to enable you to locally communicate with ILOM from the host operating system (OS) without the use of a network management (NET MGT) connection to the server. The local interconnect feature to ILOM is particularly useful when you want to locally perform these ILOM tasks from the host operating system:

- Server management functions in ILOM that you would have typically performed from the ILOM CLI, web interface, or IPMI interface through the network management (NET MGT) connection on the server.
- Data transfers, such as firmware upgrades, to ILOM that you would have typically performed from the host over a Keyboard Controller Style (KCS) interface using IPMI flash tools. In particular, the Local Interconnect Interface to ILOM can provide a more reliable and faster data transfer rate than traditional KCS interfaces.
- To enable future server monitoring and fault detection tools from Oracle.

Platform Server Support and ILOM Access Through the Local Interconnect Interface

Oracle servers supporting the Local Interconnect Interface between ILOM and the host operating system are shipped from the factory with an internal USB Ethernet device installed.



The internal USB Ethernet device provides two network connection points that are known as the ILOM SP connection point and the host OS connection point. In order to establish a local connection to ILOM from the host operating system, each connection point (ILOM SP and host OS) must be either automatically or manually assigned a unique non-routable IPv4 address on the same subnet.

Note – By default, Oracle provides non-routable IPv4 addresses for each connection point (ILOM SP and host OS). Oracle recommends not changing these addresses unless a conflict exists in your network environment with the provided non-routable IPv4 addresses.

Note – Non-routable IPv4 addresses are considered secured private addresses that prevent external Internet users from navigating to your system.

To verify whether your server supports the Local Interconnect Interface feature in ILOM, refer to the ILOM Supplement guide or Administration guide that is provided with your server.

Local Interconnect Interface Configuration Options

In ILOM you can choose to either have the Local Interconnect Interface automatically configured for you or manually configured. Details about both of these configuration options are provided below.

- **Automatic Configuration (Recommended)**

  Oracle automates the configuration of the Local Interconnect Interface feature when you install the Oracle Hardware Management Pack 2.1.0 or later software. No configuration is necessary from ILOM in this case.

  For more details about using the Oracle Hardware Management Pack 2.1.0 software to auto-configure the Local Interconnect Interface between the ILOM SP and the local host OS, see the *Oracle Server Hardware Management Pack User's Guide* (821-1609).

Note – If you choose to auto-configure the Local Interconnect Interface using the Oracle Hardware Management Pack software, you should accept the factory defaults provided in ILOM for Local Host Interconnect.

- **Manually Configured (Advanced Users Only)**

  If you are an advanced network administrator and prefer not to auto-configure the Local Interconnect Interface by installing the Oracle Hardware Management Pack 2.1.0 or later software, you can manually configure the connection points on the ILOM SP and host operating system.

  In order to manually configure the Local Interconnect Interface connection points, you must:

  a. On the host operating side, ensure that an Ethernet driver for your host OS was provided by the OS distribution and installed on the server. After you have confirmed that the appropriate Ethernet driver was installed on your server and your operating system recognizes the internal USB Ethernet device, you must manually configure an IPv4 address for the host OS connection point.

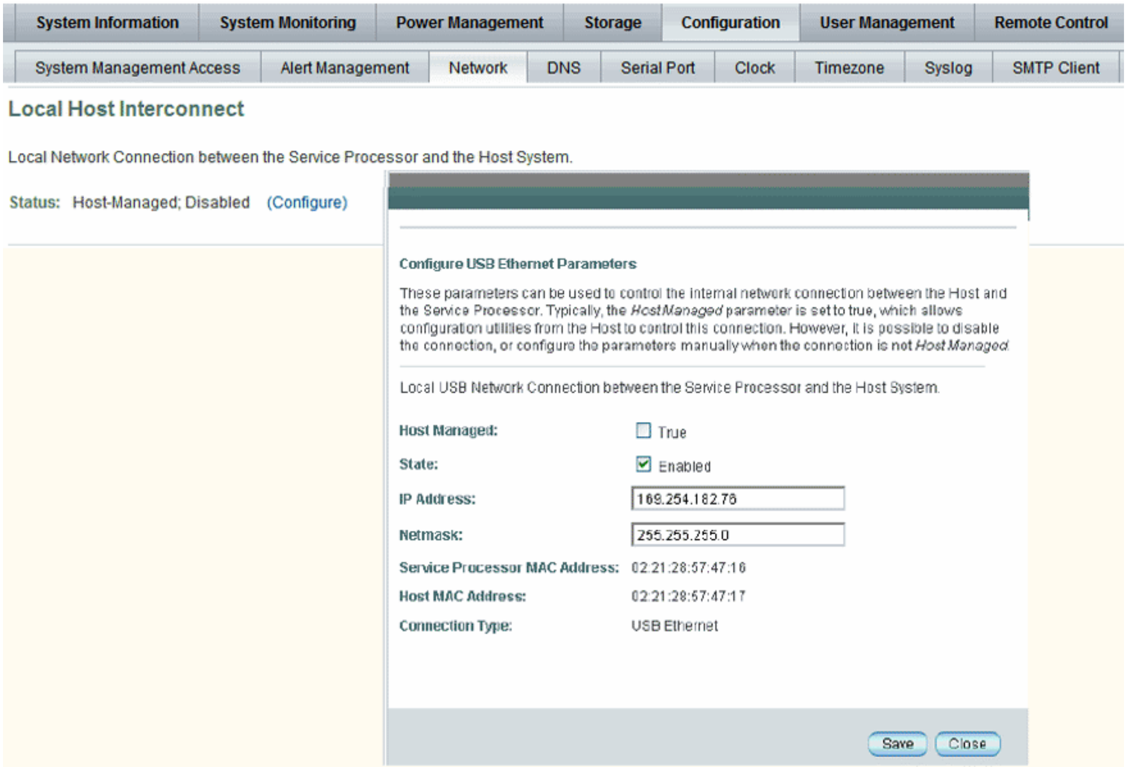
     For more details, see "Manual Host OS Configuration Guidelines for Local Interconnect Interface" on page 31.

  b. On the ILOM SP side, you must manually configure the Local Host Interconnect settings in ILOM. For more details about these settings, see "Local Host Interconnect Configuration Settings in ILOM" on page 28. For procedural information describing how to configure the Local Interconnect Interface, see Chapter 3 of the *Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* or the *Integrated Lights Out Manager (ILOM) Web Interface Procedures Guide*.

Local Host Interconnect Configuration Settings in ILOM

The Local Host Interconnect configuration settings in the ILOM web interface (or CLI) enable users with Administrator role privileges to control the Local Interconnect Interface between the host OS and the ILOM SP. See TABLE 2-5 for a brief description about the settings provided in ILOM for the Local Host Interconnect. For an example of the ILOM web interface settings for Local Host Interconnect, see FIGURE 2-3.

FIGURE 2-3 Local Host Interconnect Settings



Local Host Interconnect

Local Network Connection between the Service Processor and the Host System.

Status: Host-Managed; Disabled (Configure)

Configure USB Ethernet Parameters

These parameters can be used to control the internal network connection between the Host and the Service Processor. Typically, the *Host Managed* parameter is set to true, which allows configuration utilities from the Host to control this connection. However, it is possible to disable the connection, or configure the parameters manually when the connection is not *Host Managed*.

Local USB Network Connection between the Service Processor and the Host System.

Host Managed:	□ True
State:	☑ Enabled
IP Address:	169.254.182.76
Netmask:	255.255.255.0
Service Processor MAC Address:	02:21:28:57:47:16
Host MAC Address:	02:21:28:57:47:17
Connection Type:	USB Ethernet

TABLE 2-5 Local Host Interconnect Configuration Settings

Settings	Description
`Host Managed`	The `Host Managed` setting, by default, is set to `True`. When the `Host Managed` setting is set to `True` (enabled), ILOM permits the Oracle Hardware Management Pack configuration utility (known as ilomconfig) to auto-configure the connection points for the ILOM SP and the host OS on the Local Interconnect Interface. To prevent the Oracle Hardware Management Pack software from auto-configuring the connection points on the Local Interconnect Interface, the setting for `Host Managed` must be set to `False` (disabled).
`State`	The `State` setting, by default, is `disabled`. When the setting for `State` is `disabled`, the Local Interconnect Interface feature between the ILOM SP and the host OS is disabled. When the setting for `State` is `enabled`, the Local Interconnect Interface feature between the ILOM SP and host OS is enabled.

TABLE 2-5 Local Host Interconnect Configuration Settings *(Continued)*

Settings	Description
`IP Address`	ILOM, by default, provides a static non-routable IPv4 address (169.254.182.76) for the ILOM SP connection point on the Local Interconnect Interface. The IP address property is, by default, a read-only setting when the `Host Managed` setting is set to `True`. When the `Host Managed` setting is disabled (or property value is set to `False`), ILOM will allow you to modify the property value for the IPv4 address. **Note -** The default non-routable IPv4 address (169.254.182.76) should not be changed unless a conflict exists in your network environment with the default IPv4 address. When this address is left unchanged, this is the IP address you would use to locally connect to ILOM from the host operating system.
`Netmask`	ILOM, by default, provides a static `Netmask` address (255.255.255.0) for the ILOM SP connection point on the Local Interconnect Interface. The `Netmask` property is, by default, a read-only setting when the `Host Managed` setting is set to `True`. When the `Host Managed` setting is disabled (or property value is set to `False`), ILOM will allow you to modify the property value for the `Netmask` address. The default `Netmask` address (255.255.255.0) should not be changed unless a conflict exists in your network environment with the default `Netmask` address.
`Service Processor MAC Address`	The `Service Processor MAC Address` is a read-only setting. This setting displays the MAC address assigned to the ILOM SP.
`Host MAC Address`	The `Host MAC Address` is a read-only setting. This setting displays the MAC address assigned to the server and it represents how the host server sees the internal USB Ethernet device. **Note -** The internal USB Ethernet device is presented in the system as a traditional "Ethernet" interface. If you decide to manually configure the Local Interconnect Interface between the ILOM SP and the host OS, it might be necessary to use the host MAC address to determine which interface you will need to configure from the host OS side (like Solaris). For additional information about manually configuring the Local Interconnect Interface on the host OS connection point, see "Manual Host OS Configuration Guidelines for Local Interconnect Interface" on page 31.
`Connection Type`	The `Connection Type` is a read-only setting. This setting indicates a USB Ethernet connection.

Manual Host OS Configuration Guidelines for Local Interconnect Interface

If you chose to manually configure a non-routable IPv4 address for the ILOM SP connection point on the Local Interconnect Interface, you will also need to manually configure a non-routable IPv4 address for the host OS connection point on the Local Interconnect Interface. General guidelines, per operating system, for configuring a static non-routable IPv4 address for the host OS connection point are provided below. For additional information about configuring IP addresses on the host operating system, consult the vendor operating system documentation.

Note – ILOM will present the internal USB Ethernet device installed on your server as an USB Ethernet interface to the host operating system.

TABLE 2-6 General Guidelines for Configuring Internal USB Ethernet Device on Host OS

Operating System	General Guidelines
Windows Server 2008	After Windows discovers the internal USB Ethernet device, you will most likely be prompted to identify a device driver for this device. Since no driver is actually required, identifying the `.inf` file should satisfy the communication stack for the internal USB Ethernet device. The `.inf` file is available from the Oracle Hardware Management Pack 2.1.0 software distribution. You can download this management pack software from the Oracle software product download page (`www.oracle.com`) as well as extract the `.inf` file from the Management Pack software. For additional information about extracting the `.inf` file from the Management Pack software, see the *Oracle Server Hardware Management Pack User's Guide* (821-1609). After applying the `.inf` file from the Oracle Hardware Management Pack 2.1.0 software distribution, you can then proceed to configure a static IP address for the host OS connection point of the Local Interconnect Interface by using the Microsoft Windows Network configuration option located in the Control Panel (Start --> Control Panel). For more information about configuring an IPv4 address in Windows 2008, see the Microsoft Windows Operating System documentation or the Microsoft Tech Net site (`http://technet.microsoft.com/en-us/library/cc754203%28WS.10%29.aspx`).

TABLE 2-6 General Guidelines for Configuring Internal USB Ethernet Device on Host OS *(Continued)*

Operating System	General Guidelines

Linux	Most supported Linux operating system installations on an Oracle Sun platform server include the installation of the device driver for an internal Ethernet device.
	Typically, the internal USB Ethernet device is automatically discovered by the Linux operating system. The internal Ethernet device typically appears as `usb0`. However, the name for the internal Ethernet device might be different based on the distribution of the Linux operating system.
	The instructions below demonstrate how to configure a static IP address corresponding to `usb0`, which typically represents an internal USB Ethernet device found on the server:
	`\>lsusb usb0`
	  `\> ifconfig usb0 169.254.182.77`
	  `\> ifconfig usb0 netmask 255.255.255.0`
	  `\> ifconfig usb0 broadcast 169.254.182.255`
	  `\> ifconfig usb0`
	  `\> ip addr show usb0`
	Note - Rather than performing the typical `ifconfig` steps, it is possible to script the configuration of the interface. However, the exact network scripts vary among the Linux distributions. Typically, the operating version of Linux will have examples to model the network scripts.
	For more information about how to configure an IP address for device using a Linux operation system, see the Linux operating system documentation.

TABLE 2-6 General Guidelines for Configuring Internal USB Ethernet Device on Host OS *(Continued)*

Operating System	General Guidelines

Solaris	Most Solaris Operating System installations on a Oracle Sun platform server include the installation of the device driver for an internal USB Ethernet device. If this driver was not supported, you can extract this driver from the Oracle Hardware Management Pack 2.1.0 or later software. For information about how to extract the Solaris-specific OS driver for the Ethernet interface, see the *Oracle Server Hardware Management Pack User's Guide* (821-1609).
	Typically, the internal USB Ethernet device is automatically discovered by the Solaris operating system. The internal Ethernet device typically appears as `usbecm0`. However, the name for the internal Ethernet device might be different based on the distribution of the Solaris operating system.
	After the Solaris Operating System recognizes the local USB Ethernet device, the IP interface for the USB Ethernet device needs to be configured.
	The following instructions demonstrate how to configure a static IP address corresponding to `usbecm0`, which typically represents an internal USB Ethernet device found on the server.
	• Type the following command to `plumb` the IP interface or `unplumb` the IP interface:
	`ifconfig usbecm0 plumb`
	`ifconfig usbecm0 unplumb`
	• Type the following commands to set the address information:
	`ifconfig usbecm0 netmask 255.255.255.0 broadcast 169.254.182.255 169.254.182.77`
	• To set up the interface, type:
	`ifconfig usbecm0  up`
	• To bring the interface down, type:
	`ifconfig usbecm0  down`
	• To show the active interfaces, type:
	`ifconfig -a`
	• To test connectivity, ping the Solaris host or the SP internal USB Ethernet device.
	`ping` *<IPv4 address of Solaris Host>*
	`ping` <`I`*Pv4 address of SP-Ethernet USB>*
	Note - Rather than performing the typical `ifconfig` steps, it is possible to script the configuration of the interface. However, the exact network scripts can vary among the Solaris distributions. Typically, the operating version will have examples to model the network scripts.
	For more information about how to configure a static IP address for a device using the Solaris Operating System, see the Solaris Operating System documentation.

Note – If the internal USB Ethernet device driver was not included in your operating system installation, you can obtain the device driver for the Ethernet device from the Oracle Hardware Management Pack 2.1.0 or later software. For more information about extracting this file from the Management Pack, see the *Oracle Server Hardware Management Pack User's Guide* (821-1609).

CHAPTER 3

User Account Management

Topics

Description	Links
Learn about managing user accounts and roles	• "Guidelines for Managing User Accounts" on page 36 • "User Account Roles and Privileges" on page 37
Learn about Single Sign On	• "Single Sign On" on page 38
Learn about SSH authentication	• "SSH User Key-Based Authentication" on page 38
Learn about Active Directory	• "Active Directory" on page 39
Learn about LDAP	• "Lightweight Directory Access Protocol" on page 40 • "LDAP/SSL" on page 41
Learn about RADIUS	• "RADIUS" on page 41

Related Topics

For ILOM	Chapter or Section	Guide
• Getting started	• Initial ILOM Setup Procedures Using the Web Interface • Initial ILOM Setup Procedures Using the CLI	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide* (820-5523-10)
• CLI	• Managing User Accounts	*Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* (820-6412)
• Web interface	• Managing User Accounts	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)

Related Topics

For ILOM	Chapter or Section	Guide
• SNMP and IPMI hosts	• Managing User Accounts Using SNMP • SNMP Command Reference	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide* (820-6413)

The ILOM 3.0 Documentation Collection is available at:
http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic

Guidelines for Managing User Accounts

Apply the following general guidelines when you manage user accounts:

- ILOM supports a maximum of 10 active user sessions per service processor (SP). Some SPARC systems support a maximum of only 5 active user sessions per SP.
- The user name of an account must be at least four characters and no more than 16 characters. User names are case sensitive and must start with an alphabetical character. You can use alphabetical characters, numerals, hyphens, and underscores. Do not include spaces in user names.
- Each user account is assigned one or more advanced roles, which determine the privileges of the user account. Depending on the roles assigned to your user account, you can use the ILOM web interface, command-line interface (CLI), or SNMP to view account information and perform various administrative functions.
- You can either configure local accounts or you can have ILOM authenticate accounts against a remote user database, such as Active Directory, LDAP, LDAP/SSL, or RADIUS. With remote authentication, you can use a centralized user database rather than configuring local accounts on each ILOM instance.

For more information and procedures for managing user accounts, see one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide*

User Account Roles and Privileges

For ILOM 3.0, user roles are implemented to control user privileges. However, for backward compatibility, ILOM 2.x style user accounts (which have either Administrator or Operator privileges) are still supported.

ILOM 3.0 User Account Roles

ILOM 3.0 user accounts have defined roles that determine ILOM user access and rights. You can manage user accounts using the ILOM web interface or the CLI. The roles assigned to ILOM accounts are listed in TABLE 3-1.

TABLE 3-1 ILOM 3.0 User Account Roles

Roles	Definition	Privileges
`a`	Admin	A user who is assigned the Admin (`a`) role is authorized to view and change the state of ILOM configuration variables. With the exception of tasks that require Admin users to have User Management, Reset and Host Control and Console roles enabled.
`u`	User Management	A user who is assigned the User Management (`u`) role is authorized to create and delete user accounts, change user passwords, change roles assigned to other users, and enable/disable the physical-access requirement for the `default` user account. This role also includes authorization to set up LDAP, LDAP/SSL, RADIUS, and Active Directory.
`c`	Console	A user who is assigned the Console (`c`) role is authorized to access the ILOM Remote Console and the SP console and to view and change the state of the ILOM console configuration variables.
`r`	Reset and Host Control	A user who is assigned the Reset and Host Control (`r`) role is authorized to operate the system, which includes power control, reset, hot-plug, enabling and disabling components, and fault management. This role maps very closely to the ILOM 2.0 user with Operator privileges. For more information about backward compatibility of ILOM 2.0 user roles, see "Support for ILOM 2.x User Accounts" on page 7.
`o`	Read Only	A user who is assigned the Read Only (`o`) role is authorized to view the state of the ILOM configuration variables but cannot make any changes. Users assigned this role can also change the password and the Session Time-Out setting for their own user account.
`s`	Service	A user who is assigned the Service (`s`) role can assist Sun service engineers in the event that on-site service is required.

Single Sign On

Single Sign On (SSO) is a convenient authentication service that enables you to log in to ILOM once to establish your credentials, thus reducing the number of times you need to enter your password to gain access to ILOM. Single Sign On is enabled by default. As with any authentication service, authentication credentials are passed over the network. If this is not desirable, consider disabling the SSO authentication service.

SSH User Key-Based Authentication

Traditionally, automation of password authentication is made possible by SSH key-based authentication. Prior to the implementation of the SSH key-based authentication feature, users who logged in to the ILOM SP using SSH were required to supply a password interactively. An automatic mechanism for password authentication is most beneficial when you have multiple systems that require a similar update.

The primary capabilities afforded by SSH key-based authentication are as follows:

- Users are able to write scripts that automatically copy log files off of a service processor (SP) for archival and analysis.
- Users are able to write scripts that automatically and/or regularly execute SP commands over a network-based SSH connection from a remote system.

Thus, SSH key-based authentication enables you to accomplish both of the above activities through the use of scripts that execute without manual intervention and that do not include embedded passwords.

Regarding the use and handling of SSH keys, ILOM enables users to add generated keys to individual user accounts on the SP.

For more information and procedures for adding and deleting SSH keys, see one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Active Directory

ILOM supports Active Directory, the distributed directory service included with Microsoft Windows Server operating systems. Like an LDAP directory service implementation, Active Directory is used to authenticate user credentials.

Note – The service processor (SP) expects to communicate with the Active Directory server using a secure channel. To ensure security, the Active Directory server should be loaded with a certificate that can be presented during the SP user authentication process so that protocol negotiations can allow a private channel to be set up.

User Authentication and Authorization

Active Directory provides both authentication of user credentials and authorization of user access levels to networked resources. Active Directory uses authentication to verify the identity of a user before that user can access system resources. Active Directory uses authorization to grant specific access privileges to a user in order to control a user's rights to access networked resources. User access levels are configured or learned from the server based on the user's group membership in a network domain, which is a group of hosts identified by a specific Internet name. A user can belong to more than one group. Active Directory authenticates users in the order in which the user's domains were configured.

User Authorization Levels

Once authenticated, the user's authorization level can be determined in the following ways:

- In the simplest case, the user authorization of either Operator, Administrator, or Advanced Roles (see "User Account Roles and Privileges" on page 37) is learned directly through the Active Directory's configuration of the SP. Access and authorization levels are dictated by the `defaultrole` property. Setting up users in the Active Directory database requires only a password with no regard to group membership. On the SP, the `defaultrole` will be set to either Administrator, Operator, or the Advanced Role settings `a/u/c/r/o/s`. All users authenticated through Active Directory are assigned the privileges associated with the Administrator, Operator, or Advanced Roles based solely on this configuration.

- A more integrated approach is also available by querying the server. For configuration, the SP Administrator Group Tables, Operator Group Tables, or Custom Group Tables must be configured with the corresponding group names from the Active Directory server that will be used to determine access levels. Up to five Active Directory groups can be entered to designate an Administrator; another five can be used to assign Operator privileges; and up to five groups can be assigned to Custom Groups, which contain Advanced Roles (see "User Account Roles and Privileges" on page 37). Group membership of the user is used to identify the proper access level of either Administrator, Operator, or Advanced Roles by looking up each group name in the configured Active Directory tables on the SP. If the user's group list is not in either of the defined SP user groups, then access is denied. A user assigned to more than one group will receive the sum of all privileges.

For more information and procedures for configuring Active Directory settings, see one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide*

Lightweight Directory Access Protocol

ILOM supports Lightweight Directory Access Protocol (LDAP) authentication for users, based on the OpenLDAP software. LDAP is a general-purpose directory service. A directory service is a centralized database for distributed applications designed to manage the entries in a directory. Thus, multiple applications can share a single user database. For more detailed information about LDAP, go to:

`http://www.openldap.org/`

For more information and procedures for configuring LDAP settings, see one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide*

LDAP/SSL

LDAP/SSL offers enhanced security to LDAP users by way of Secure Socket Layer (SSL) technology. To configure LDAP/SSL in a SP, you need to enter basic data—such as primary server, port number, and certificate mode—and optional data such as alternate server or event or severity levels. You can enter this data using the LDAP/SSL configuration page of the ILOM web interface, the CLI, or SNMP.

For more information and procedures for configuring LDAP/SSL settings, see one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide*

RADIUS

ILOM supports Remote Authentication Dial-In User Service (RADIUS) authentication. RADIUS is an authentication protocol that facilitates centralized user administration. RADIUS provides many servers shared access to user data in a central database, providing better security and easier administration. A RADIUS server can work in conjunction with multiple RADIUS servers and other types of authentication servers.

RADIUS is based on a client-server model. The RADIUS server provides the user authentication data and can grant or deny access, and the clients send user data to the server and receive an “accept” or “deny” response. In the RADIUS client-server model, the client sends an Access-Request query to the RADIUS server. When the server receives an Access-Request message from a client, it searches the database for that user's authentication information. If the user's information is not found, the server sends an Access-Reject message and the user is denied access to the requested service. If the user's information is found, the server responds with an Access-Accept message. The Access-Accept message confirms the user's authentication data and grants the user access to the requested service.

All transactions between the RADIUS client and server are authenticated by the use of a specific text string password known as a shared secret. The client and server must each know the shared secret because it is never passed over the network. You must know the shared secret to configure RADIUS authentication for ILOM.

In order to use RADIUS authentication with ILOM, you must configure ILOM as a RADIUS client.

For more information and procedures for configuring RADIUS settings, see one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide*

CHAPTER 4

System Monitoring and Alert Management

Topics

Description	Links
Learn about system monitoring and management features in ILOM	• "System Monitoring" on page 44 • "Sensor Readings" on page 45 • "System Indicators" on page 45 • "Component Management" on page 46 • "Fault Management" on page 48 • "Clear Faults After Replacement of Faulted Components on Server or CMM" on page 49 • "ILOM Event Log" on page 50 • "Syslog Information" on page 51 • "Collect SP Data to Diagnose System Problems" on page 51
Learn about managing system alerts in ILOM	• "Alert Management" on page 52 • "Alert Management From the CLI" on page 55 • "Alert Management From the Web Interface" on page 56 • "Alert Management From an SNMP Host" on page 57

Related Topics

For ILOM	Section	Guide
• CLI	• Monitoring System Components • Managing System Components • Managing System Alerts	*Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* (820-6412)

Related Topics

For ILOM	Section	Guide
• Web interface	• Monitoring System Components • Managing System Components • Managing System Alerts	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)
• IPMI and SNMP hosts	• Monitoring System Components • Managing System Alerts	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide* (820-6413)

The ILOM 3.0 Documentation Collection is available at:
`http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`

System Monitoring

The system monitoring features in ILOM enable you to easily determine the health of the system and to detect errors, at a glance, when they occur. For instance, in ILOM you can:

- View instantaneous sensor readings about system component temperatures, current, voltage, speed, and presence. For more information, see "Sensor Readings" on page 45.
- Determine the state of indicators throughout the system. For more information, see "System Indicators" on page 45.
- Monitor the state of system components. For more information, see "Component Management" on page 46.
- Monitor the health of system components, as well as diagnose hardware failures, see "Fault Management" on page 48.
- Clear faults after replacement of faulty components, see "Clear Faults After Replacement of Faulted Components on Server or CMM" on page 49.
- Identify system errors and view event information in the ILOM event log. For more information, see "ILOM Event Log" on page 50.
- Combine and view events from multiple instances in ILOM by sending Syslog information. For more information, see "Syslog Information" on page 51.
- Collect data for use by Oracle Services personnel to diagnose system problems. For more information, see "Collect SP Data to Diagnose System Problems" on page 51.

Sensor Readings

All Oracle Sun server platforms are equipped with a number of sensors that measure voltages, temperatures, fan speeds, and other attributes about the system. Each sensor in ILOM contains nine properties describing various settings related to a sensor such as sensor type, sensor class, sensor value, as well as the sensor values for upper and lower thresholds.

ILOM regularly polls the sensors in the system and reports any events it encounters about sensor state changes or sensor threshold crossings to the ILOM event log. Additionally, if an alert rule was enabled in the system that matched the crossing threshold level, ILOM would automatically generate an alert message to the alert destination that you have defined.

You can view sensor readings from the ILOM web interface or CLI. For details, see "View Sensor Readings" in one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

System Indicators

System indicator LEDs are generally illuminated on the system by ILOM based on the server platform policy. Typically the system indicator LEDs are illuminated by ILOM when any of the following conditions occur:

- Fault or error is detected on a component.
- Field-replacement unit (FRU) requires service.
- Hot-plug module is ready for removal.
- Activity is occurring on FRU or system.

You can view the states of system indictors from the ILOM web interface or the CLI. Additionally, in some instances, you might be able to modify the state of a system indicator. For details, see the section about View and Manage System Indicators in one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Supported System Indicator States

ILOM supports the following system indicator states:

- **Off** – Normal operating status. Service is not required.
- **Steady On** – Component is ready for removal.

- **Slow Blink** – Component is changing state.
- **Fast Blink** – Helps locate a system in a data center.
- **Standby Blink** – Component is ready for activation, but is not operational at this time.

Types of System Indicator States

ILOM supports two types of system indicator states: *customer changeable* and *system assigned*.

- **Customer Changeable States** – Some system indicator LEDs in ILOM offer customer changeable states. Typically, these types of system indicators provide operational states of various system components. The type of states presented is determined by the system indicator. For example, depending on the system indicator, the following customer changeable states might be present:
  - **Off** – Normal operating status. Service is not required.
  - **Fast Blink** – Helps locate system in a data center.
- **System Assigned States** – System assigned indicators are *not* customer configurable. These types of system indicators provide read-only values about the operational state of a component. On most Oracle Sun server platforms, system assigned indicators are *Service Action Required LEDs*. These types of LEDs are typically illuminated when any of the following conditions are detected:
  - Fault or error is detected on a system component.
  - Hot-plug module is ready for removal.
  - Field-replacement unit (FRU) requires service.

Component Management

The Component Management features in ILOM enable you to monitor the state of various components that are installed on the server or managed by the Chassis Monitoring Module (CMM). For example, by using the Component Management features, you can:

- Identify the component name and type.
- Identify and change the component state (enabled or disabled).
- Identify the component’s fault status and, if necessary, clear the fault.
- Prepare to install or remove a component.

- Filter the component management display by Fault Status, Component State, Hardware Type, and Ready to Remove Status. Or, create a Custom Filter to filter the component management display by Component or FRU Name, Component or FRU part number, Ready to Remove Status (Ready or Not Ready), and Fault Status (OK or Faulted).

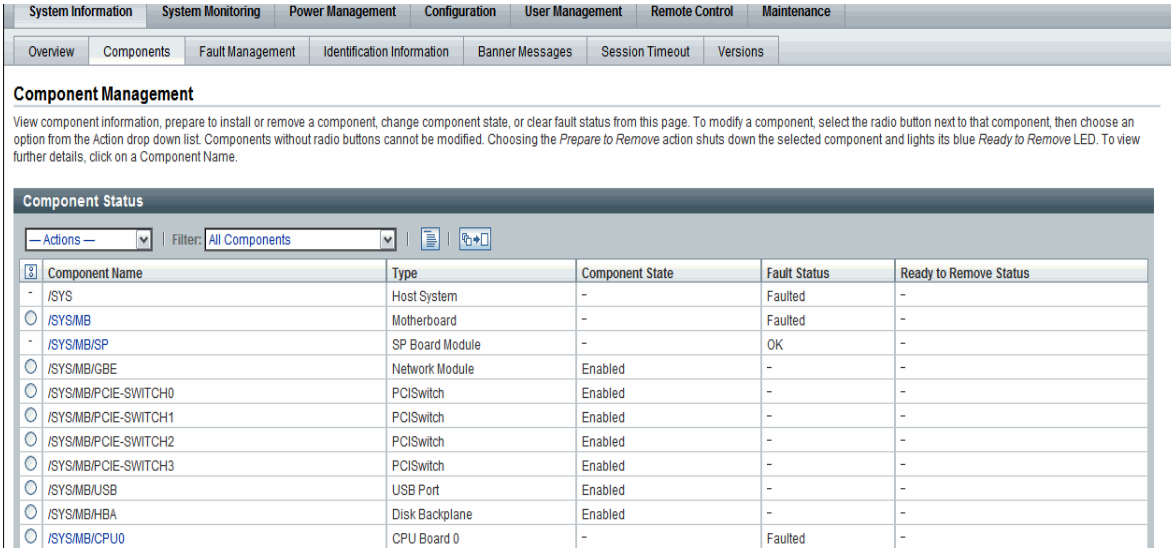
Depending on the component type, you can view the component information or you can view and modify the state of component.

The Component Management features are supported in both the ILOM Web Interface and command-line interface (CLI) for x86 systems server SPs, SPARC systems server SPs, and CMMs. For detailed instructions for managing system components from the ILOM web interface or the CLI, see the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

ILOM web interface examples of the Component Management features for a server SP and CMM are shown in the following figures.

FIGURE 4-1 Server SP Component Management Features in Web Interface



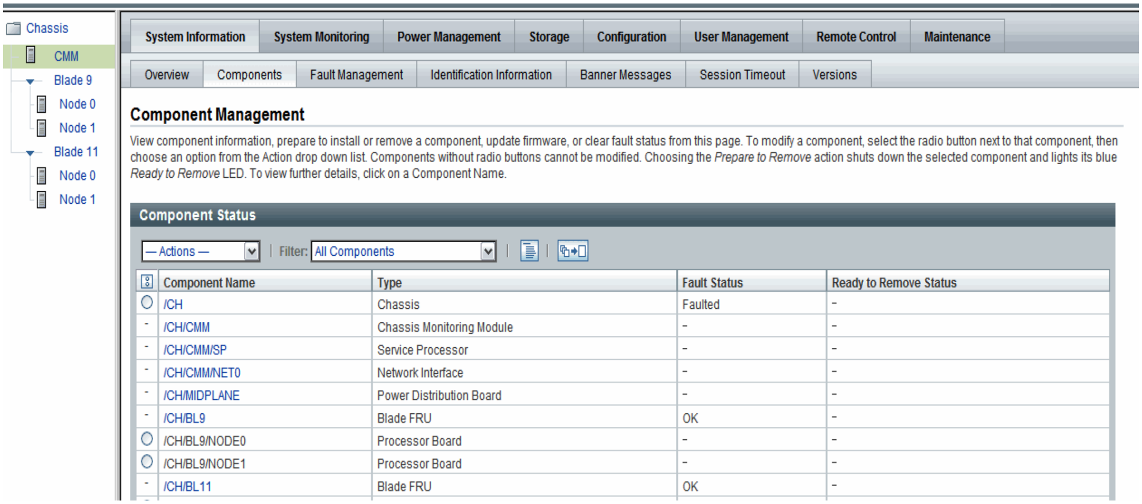
Component Management

View component information, prepare to install or remove a component, change component state, or clear fault status from this page. To modify a component, select the radio button next to that component, then choose an option from the Action drop down list. Components without radio buttons cannot be modified. Choosing the *Prepare to Remove* action shuts down the selected component and lights its blue *Ready to Remove* LED. To view further details, click on a Component Name.

Component Status

	Component Name	Type	Component State	Fault Status	Ready to Remove Status
-	/SYS	Host System	-	Faulted	-
○	/SYS/MB	Motherboard	-	Faulted	-
-	/SYS/MB/SP	SP Board Module	-	OK	-
○	/SYS/MB/GBE	Network Module	Enabled	-	-
○	/SYS/MB/PCIE-SWITCH0	PCISwitch	Enabled	-	-
○	/SYS/MB/PCIE-SWITCH1	PCISwitch	Enabled	-	-
○	/SYS/MB/PCIE-SWITCH2	PCISwitch	Enabled	-	-
○	/SYS/MB/PCIE-SWITCH3	PCISwitch	Enabled	-	-
○	/SYS/MB/USB	USB Port	Enabled	-	-
○	/SYS/MB/HBA	Disk Backplane	Enabled	-	-
○	/SYS/MB/CPU0	CPU Board 0	-	Faulted	-

FIGURE 4-2 CMM Component Management Features in Web Interface



Component Management

View component information, prepare to install or remove a component, update firmware, or clear fault status from this page. To modify a component, select the radio button next to that component, then choose an option from the Action drop down list. Components without radio buttons cannot be modified. Choosing the *Prepare to Remove* action shuts down the selected component and lights its blue *Ready to Remove* LED. To view further details, click on a Component Name.

Component Status

	Component Name	Type	Fault Status	Ready to Remove Status
○	/CH	Chassis	Faulted	-
-	/CH/CMM	Chassis Monitoring Module	-	-
-	/CH/CMM/SP	Service Processor	-	-
-	/CH/CMM/NET0	Network Interface	-	-
-	/CH/MIDPLANE	Power Distribution Board	-	-
-	/CH/BL9	Blade FRU	OK	-
○	/CH/BL9/NODE0	Processor Board	-	-
○	/CH/BL9/NODE1	Processor Board	-	-
-	/CH/BL11	Blade FRU	OK	-

Fault Management

Most Oracle Sun server platforms support the fault management software feature in ILOM. This feature enables you to proactively monitor the health of your system hardware, as well as diagnose hardware failures as they occur. In addition to monitoring the system hardware, the fault management software monitors environmental conditions and reports when the system's environment is outside acceptable parameters. Various sensors on the system components are continuously monitored. When a problem is detected, the fault management software automatically:

- Illuminates the Server Action Required LED on the faulted component.
- Updates the ILOM management interfaces to reflect the fault condition.
- Records information about the fault in the ILOM event log.

The type of system components and environmental conditions monitored by the fault management software are determined by the server platform. For more details about which components are monitored by the fault management software, consult your Sun server platform documentation.

Note – The ILOM fault management feature is currently available on all Sun server platforms, with the exception of the Sun Fire X4100 or X4200 series servers.

You can view the status of faulted components from the ILOM web interface or CLI. For details, see "View Fault Status" in one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Clear Faults After Replacement of Faulted Components on Server or CMM

The ILOM-based service processor (SP) receives error telemetry about error events that occur within the major system components on the host (CPU, memory, and I/O hub) and the environmental subsystem within the chassis (such as fans, power supplies, and temperature). The components and conditions are then diagnosed as fault events and captured in the ILOM event log.

As of ILOM 3.0.3, the steps that are necessary to clear a fault are largely dependent on the type of server platform you are using (server module versus rackmount server). For example:

- ILOM-based faults that occur on a server module are NOT persistent once the server module has been properly prepared for removal and is physically removed from the chassis. Therefore, no service actions are required to clear the fault after the component is physically replaced. The fault message is captured in the ILOM event log for historical purposes.
- ILOM-based faults that occur on a rackmount server ARE persistent and might require service actions to clear the fault after the component is physically replaced, unless the component is a hot-swappable component (such as a fan or power supply). Hot-swappable components are platform-specific; therefore, refer to the platform documentation for a list of the hot-swappable components. The fault message is captured in the ILOM event log for historical purposes. On a rackmount server, you must manually clear the following faults after physically replacing the components, which are not hot-swappable:
  - CPU fault
  - DIMM (memory module) fault
  - PCI card fault
  - Motherboard fault (if the motherboard is not being replaced)
- ILOM-based faults that occur on components installed in a chassis containing CMM(s) are automatically cleared by the ILOM CMM when the faulted component is replaced. However, if the chassis-level component is not hot-serviceable, then the fault needs to be manually cleared from the ILOM CMM.

In particular, the CMM automatically clears faults on the following chassis-level components after the faulted components are replaced:

- CMM fault
- Fan fault
- Power supply fault
- Network express module (NEM) fault
- PCI express module fault

Note – For more information about the ILOM fault management features offered on your system, refer to the procedures guides in the ILOM 3.0 Documentation Collection and the documentation provided with your Oracle server platform.

For instructions about clearing a fault using the ILOM CLI or web interface, see the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

ILOM Event Log

The ILOM event log enables you to view information about any event that occurred on the system. Some of these events include ILOM configuration changes, software events, warnings, alerts, component failure, as well as IPMI, PET, and SNMP events. The type of events recorded in the ILOM event log is determined by the server platform. For information about which events are recorded in the ILOM event log, consult your Sun server platform documentation.

Event Log Time Stamps and ILOM Clock Settings

ILOM captures time stamps in the event log based on the host server UTC/GMT timezone. However, if you view the event log from a client system that is located in a different timezone, the time stamps are automatically adjusted to the timezone of the client system. Therefore, a single event in the ILOM event log might appear with two timestamps.

In ILOM, you can choose to manually configure the ILOM clock based on the UTC/GMT timezone of the host server, or you can choose to synchronize the ILOM clock with other systems on your network by configuring the ILOM clock with an NTP server IP address.

Manage Event Log and Time Stamps From CLI, Web, or SNMP Host

You can view and manage the event log and time stamps in ILOM from the CLI, web interface, or an SNMP host. For details, see “Configure Clock Settings” and “Filter Event Log Output” in the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Syslog Information

Syslog is a standard logging utility used in many environments. Syslog defines a common set of features for logging events and also a protocol for transmitting events to a remote log host. You can use syslog to combine events from multiple instances of ILOM within a single place. The log entry contains all the same information that you would see in the local ILOM event log, including class, type, severity, and description.

For information about configuring ILOM to send syslog to one or two IP addresses, see “Configure Remote Syslog Receiver IP Addresses” in one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide*

Collect SP Data to Diagnose System Problems

The ILOM Service Snapshot utility enables you to produce a snapshot of the SP at any instant in time. You can run the utility from the ILOM CLI or the web interface. For more information about collecting SP data to diagnose system problems, see “Collect SP Data to Diagnose System Problems” on page 137.

Alert Management

ILOM supports alerts in the form of IPMI PET alerts, SNMP Trap alerts, and Email Notification alerts. Alerts provide advance warning of possible system failures. Alert configuration is available from the ILOM SP on your server.

Each Sun server platform is equipped with a number of sensors that measure voltages, temperatures, and other service-related attributes about the system. ILOM automatically polls these sensors and posts any events crossing a threshold to an ILOM event log, as well as generates alert message(s) to one or more customer-specified alert destinations. The alert destination specified must support the receipt of the alert message (IPMI PET or SNMP). If the alert destination does not support the receipt of the alert message, the alert recipient will be unable to decode the alert message.

Caution – ILOM tags all events or actions with LocalTime=GMT (or UTC). Browser clients show these events in LocalTime. This can cause apparent discrepancies in the event log. When an event occurs in ILOM, the event log shows it in UTC, but a client would show it in LocalTime. For more information about ILOM timestamps and clock settings, see "Event Log Time Stamps and ILOM Clock Settings" on page 50.

Alert Rule Configuration

In ILOM you can configure up to 15 alert rules using the ILOM web interface or CLI. For each alert rule you configure in ILOM, you must define three or more properties about the alert depending on the alert type.

The *alert type* defines the messaging format and the method for sending and receiving an alert message. ILOM supports these three alert types:

- IPMI PET alerts
- SNMP Trap alerts
- Email Notification alerts

All Sun server platforms support all three alert types.

Alert Rule Property Definitions

ILOM offers the following property values for defining an alert rule:

- Alert Type
- Alert Level
- Alert Destination
- Alert Destination Port
- Email Custom Sender
- Email Message Prefix
- Email Class Filter
- Email Type Filter
- SNMP Version (*SNMP Trap alerts only*)
- SNMP Community Name or User Name (*SNMP Trap alerts only*)

For information about each of these property values, see TABLE 4-1.

TABLE 4-1 Properties for Defining Alert Rules

Property Name	Requirement	Description
Alert Type	Mandatory	The alert type property specifies the message format and the delivery method that ILOM will use when creating and sending the alert message. You can choose to configure one of the following alert types: • **IPMI PET Alerts**. IPMI Platform Event Trap (PET) alerts are supported on all Sun server platforms and CMMs. For each IPMI PET alert you configure in ILOM, you must specify an IP address for an alert destination and one of four supported alert levels. Note that the alert destination specified must support the receipt of IPMI PET messages. If the alert destination does not support the receipt of IPMI PET messages, the alert recipient will not be able to decode the alert message. • **SNMP Trap Alerts**. ILOM supports the generation of SNMP Trap alerts to a customer-specified IP destination. All destinations specified must support the receipt of SNMP Trap messages. Note that SNMP Trap alerts are supported on rackmounted servers and blade server modules. • **Email Notification Alerts**. ILOM supports the generation of Email Notification alerts to a customer-specified email address. To enable the ILOM client to generate Email Notification alerts, ILOM initially requires you to configure the name of the outgoing SMTP email server that would be sending the Email alert messages.

TABLE 4-1 Properties for Defining Alert Rules *(Continued)*

Property Name	Requirement	Description
Alert Destination	Mandatory	The alert destination property specifies where to send the alert message. The alert type determines which destination you can choose to send an alert message. For example, IPMI PET and SNMP Trap alerts must specify an IP address destination. Email Notification alerts must specify an email address. If the proper format is not entered for an alert destination, ILOM will report an error.
Alert Destination Port	Optional	The alert destination port only applies when the alert type is an SNMP Trap. The destination port property specifies the UDP port to which SNMP Trap alerts are sent.
Alert Level	Mandatory	Alert levels act as a filter mechanism to ensure alert recipients only receive the alert messages that they are most interested in receiving. Each time you define an alert rule in ILOM, you must specify an alert level. The alert level determines which events generate an alert. The lowest level alert generates alerts for that level and for all alert levels above it. ILOM offers the following alert levels with Minor being the lowest alert offered: • **Minor**. This alert level generates alerts for informational events, lower and upper non-critical events, upper and lower critical events, and, upper and lower non-recoverable events. • **Major.** This alert level generates alerts for upper and lower non-critical events, upper and lower critical events, and, upper and lower non-recoverable events. • **Critical**. This alert level generates alerts for upper and lower critical events and upper and lower non-recoverable events. • **Down**. This alert level generates alerts for only upper non-recoverable and lower non-recoverable events. • **Disabled**. Disables the alert. ILOM will not generate an alert message. All the alert levels will enable the sending of a alert with the exception of *Disabled*. **Important -** ILOM supports alert level filtering for all IPMI traps and Email Notification traps. ILOM does not support alert level filtering for SNMP traps. To enable the sending of an SNMP trap (but not filter the SNMP trap by alert level) you can choose anyone of the following options: *Minor*, *Major*, *Critical*, or *Down*. To disable the sending of an SNMP trap, you must choose the *Disabled* option.
Email Custom Sender	Optional	The email custom sender property applies only when the alert type is an email alert. You can use the `email_custom_sender` property to override the format of the "from" address. You can use either one of these substitution strings: <*IPADDRESS*> or <*HOSTNAME*>; for example, alert@[<*IPADDRESS*>]. Once this property is set, this value will override any SMPT custom sender information.

TABLE 4-1 Properties for Defining Alert Rules *(Continued)*

Property Name	Requirement	Description
Email Message Prefix	Optional	The email message prefix property applies only when the alert type is an email alert. You can use the `email_message_prefix` property to prepend information to the message content.
Event Class Filter	Optional	The event class filter property applies only when the alert type is an email alert. The default setting is to send every ILOM event as an email alert. You can use the `event_class_filter` property to filter out all information except the selected event class. You can use "" (empty double quotes) to clear the filter and send information about all classes.
Event Type Filter	Optional	The event type filter property applies only when the alert type is an email alert. You can use the `event_type_filter` property to filter out all information except the event type. You can use "" (empty double quotes) to clear the filter and send information about all event types.
SNMP Version	Optional	The SNMP version property enables you to specify which version of an SNMP trap that you are sending. You can choose to specify: 1, 2c, or 3. This property value only applies to SNMP Trap alerts.
SNMP Community Name or User Name	Optional	The SNMP community name or user name property enables you to specify the community string or SNMP v3 user name used in the SNMP Trap alert. • For SNMP v1 or v2c, you can choose to specify a community name value for an SNMP alert. • For SNMP v3, you can choose to specify a user name value for an SNMP alert. **Note -** If you choose to specify an SNMP v3 user name value, you must define this user in ILOM as an SNMP user. If you do not define this user as an SNMP user, the trap receiver will not be able to decode the SNMP Trap alert. For more information about defining an SNMP user in ILOM, see the *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*, or the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*.

Alert Management From the CLI

You can enable, modify, or disable any alert rule configuration in ILOM from the command-line interface (CLI). All 15 alert rule configurations defined in ILOM are disabled by default. To enable alert rule configurations in ILOM, you must set values for the following properties: alert type, alert level, and alert destination.

You can also generate test alerts to any *enabled* alert rule configuration in ILOM from the CLI. This test alert feature enables you to verify that the alert recipient(s) specified in an *enabled* alert rule configuration receives the alert message.

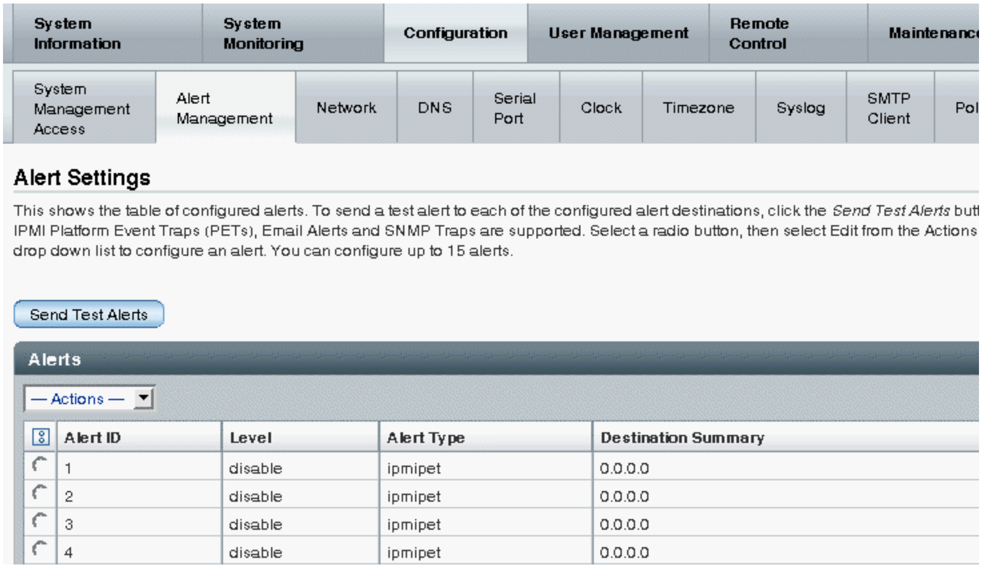
For additional information about how to manage alerts using the ILOM CLI, see “Managing System Alerts” in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*.

Alert Management From the Web Interface

You can enable, modify, or disable any alert rule configuration in ILOM from the Alert Settings web interface page. All 15 alert rule configurations presented on this page are disabled by default. The Actions drop-down list box on the page enables you to edit the properties associated with an alert rule. To enable an alert rule on this page, you must define an alert type, alert level, and a valid alert destination.

The Alert Settings page also presents a Send Test Alert button. This test alert feature enables you to verify that each alert recipient specified in an enabled alert rule receives an alert message.

FIGURE 4-3 Alert Settings Page



Alert Settings

This shows the table of configured alerts. To send a test alert to each of the configured alert destinations, click the *Send Test Alerts* butt IPMI Platform Event Traps (PETs), Email Alerts and SNMP Traps are supported. Select a radio button, then select Edit from the Actions drop down list to configure an alert. You can configure up to 15 alerts.

	Alert ID	Level	Alert Type	Destination Summary
○	1	disable	ipmipet	0.0.0.0
○	2	disable	ipmipet	0.0.0.0
○	3	disable	ipmipet	0.0.0.0
○	4	disable	ipmipet	0.0.0.0

For additional information about how to manage alerts using the ILOM web interface, see “Managing System Alerts” in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*.

Alert Management From an SNMP Host

You can use the `get` and `set` commands to view and configure alert rule configurations using an SNMP host.

Before you can use SNMP to view and configure ILOM settings, you must configure SNMP. For more information about how to use SNMP to manage system alerts, see "Managing System Alerts" in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide*.

CHAPTER 5

Storage Monitoring and Zone Management

Topics

Description	Links
Learn about storage monitoring for HDDs and RAID controllers	• "Storage Monitoring for HDDs and RAID Controllers" on page 60 • "CLI Storage Properties Shown for HDDs and RAID Controllers" on page 60 • "Monitoring Storage Components Using the CLI" on page 63 • "Monitoring Storage Components Using the Web Interface" on page 63
Learn about the CMM Zone Management feature	• "CMM Zone Management Feature" on page 68

Related Topics

For ILOM	Section	Guide
• CLI	• Monitoring Storage Components and Zone Manager	*Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* (820-6412)
• Web interface	• Monitoring Storage Components and Zone Manager	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)
• CLI and web interface	• Sun Blade Zone Manager	*Oracle Integrated Lights Out Manager (ILOM) CMM Administration Guide for Sun Blade 6000 and Sun Blade 6048 Modular Systems* (820-0052)

Related Topics

For ILOM	Section	Guide
The ILOM 3.0 Documentation Collection is available at: `http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`		

Storage Monitoring for HDDs and RAID Controllers

As of ILOM 3.0.6, ILOM supports additional storage monitoring functions for viewing and monitoring storage details that are associated with system hard disk drives (HDDs) and RAID controllers. These enhanced storage property details are available in ILOM from the CLI (as of ILOM 3.0.6) and the web interface (as of ILOM 3.0.8).

Note – Some Oracle Sun servers might not enable support for the storage monitoring functions that are described in this chapter. To determine whether storage monitoring support on your server has been enabled, see the ILOM Supplement guide for your server.

For Oracle Sun servers supporting the Storage Monitoring feature in ILOM, a system management pack must be installed to use the Storage Monitoring features. For information about how to download this management pack, see *Oracle Server Hardware Management Pack User's Guide* (821-1609).

Topics in this section include:

- "CLI Storage Properties Shown for HDDs and RAID Controllers" on page 60
- "Monitoring Storage Components Using the CLI" on page 63
- "Monitoring Storage Components Using the Web Interface" on page 63

CLI Storage Properties Shown for HDDs and RAID Controllers

Using the ILOM CLI, you can view the following properties (TABLE 5-1) that are associated with your system server HDDs and RAID controller options.

Note – The storage properties appearing in TABLE 5-1 might not be available for all storage configurations.

TABLE 5-1 Storage Properties Shown for HDDs and RAID Controllers

HDD Storage Properties (shown in ILOM CLI under /SYS)		
• Disk type (SATA or SAS)	• OK to remove status	• HBA ID for controller
• FRU type (hard disk)	• Service fault state	• HBA ID for disk
• FRU name	• Present device state	• RAID status (online, offline, failed, missing, and so on)
• FRU part number	• Disk capacity	• RAID dedicated hot-spare (for disk)
• FRU serial number	• Device name	• RAID global hot-spare (disk group)
• FRU manufacturer	• World Wide Name (WWN)	• RAID ID list that is applicable to the HDD
• FRU version	• FRU description	
RAID Controller Properties (shown in ILOM CLI under /STORAGE/raid)		
• FRU manufacturer	• PCI subdevice	• Maximum global hot spares (allowed number of global hot spares for controller)
• FRU model	• RAID levels supported	• Minimum stripe size (supported size in kilobytes)
• PCI vendor ID	• Maximum disks (allowed disks for controller)	• Maximum stripe size (supported size in kilobytes)
• PCI device ID	• Maximum RAIDs (allowed logical volumes for controller)	
• PCI subvendor ID	• Maximum hot spares (allowed dedicated hot spares for single RAID)	
RAID Controller Disk Properties (shown in ILOM CLI under /STORAGE/raid)		
• FRU name	• FRU version	• World Wide Name (WWN)
• FRU part number	• RAID status (offline, online, failed, missing, initializing)	• Dedicated hot spare (for disk)

TABLE 5-1 Storage Properties Shown for HDDs and RAID Controllers *(Continued)*

• FRU serial number	• Disk capacity (supported size in byte)	• Global hot spare (for disk group)
• FRU manufacturer	• Device name	• RAID IDs (list for this device)
• FRU description	• Disk type (SAS or SATA known by host operating system)	• System drive slot (corresponding internal hard drive NAC name for RAID)
RAID Controller Volume Properties (shown in ILOM CLI under /STORAGE/raid)		
• RAID level	• Mounted status	• Stripe size
• RAID volume status (OK, degraded, failed, missing)	• Device name, known by host operating system	• Targets for child member of RAID ID
• Disk capacity	• Resync status	

RAID Status Definitions for Physical and Logical Drives

When a physical disk is configured as part of a volume and is attached to a powered-on controller, ILOM reports one of the following status values for configured physical (TABLE 5-2) and logical (TABLE 5-3) drives.

TABLE 5-2 RAID Status Definitions for Physical RAID Disks

Physical RAID Disk ID Status	
OK	The disk is online.
Offline	The disk is offline per host request or for another reason such as disk is not compatible for use in volume.
Failed	The disk has failed.
Initializing	The disk is being initialized or rebuilt.
Missing	The disk is missing or not responding.
Unknown	The disk is not recognized.

TABLE 5-3 Status Definitions for Logical RAID Volumes

Logical RAID Volume Status	
OK	The volume is running at optimal level.
Degraded	The volume is running in degraded mode. An additional disk loss could result in permanent data loss.
Failed	The volume has too many failed disks and is not running.
Missing	The volume is not found or not available.
Unknown	The volume is not recognized or is not defined.

Monitoring Storage Components Using the CLI

To view and monitor storage details related to the HDDs and RAID controllers that are configured on your system, log in to the ILOM CLI and drill down the following target properties under:

- `/SYS/` to show details for HDDs

or

- `/STORAGE/raid` to show details for a RAID disk controller

For CLI procedures about how to view and monitor storage properties in ILOM, see the section about Viewing and Monitoring Storage Components in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*

Monitoring Storage Components Using the Web Interface

To view and monitor storage details related to the HDDs and RAID controllers that are configured on your system, log in to the ILOM web interface and drill-down to the web interface Storage --> RAID tabs. From the RAID tab, you can view and monitor details about:

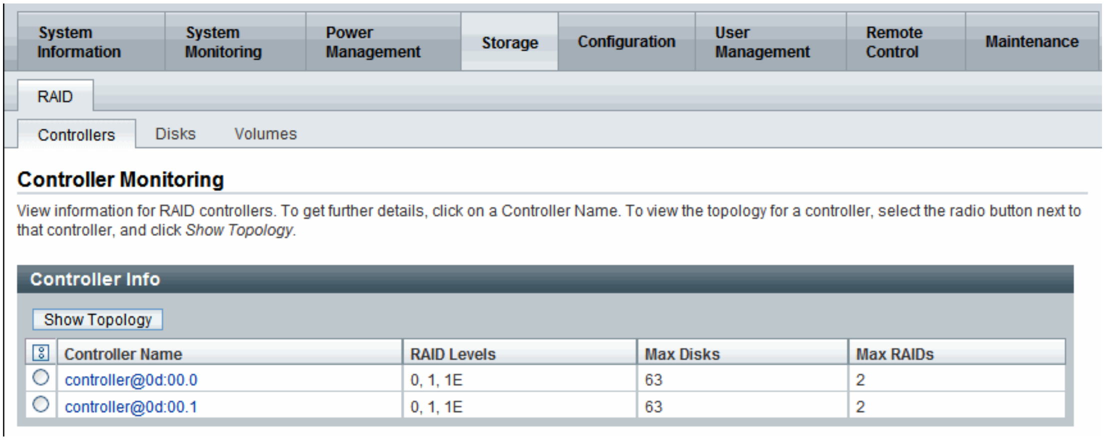
- Raid controllers (Controller tab) – see "RAID Controllers Tab Details" on page 64.
- Disks attached to RAID controllers (Disk tab) – see "Disks Attached to RAID Controllers Details" on page 65.
- RAID controller volume details (Volumes tab) – see "RAID Controller Volume Details" on page 67.

RAID Controllers Tab Details

From the Storage --> RAID --> Controller tab in ILOM, you can access configuration information about each RAID controller installed on your system. This information includes:

- RAID controller configuration details that describe the RAID levels, maximum number of disks, and the maximum number of RAIDs that can be configured on each installed RAID controller. For example, see FIGURE 5-1.
- RAID controller FRU properties and values for each installed RAID controller. For example, see FIGURE 5-2.
- RAID controller topology details that display information about attached disks, configured RAID volumes, and disks that are part of a RAID. For example, see FIGURE 5-3.

FIGURE 5-1 RAID Controller Configuration Details



Controller Monitoring

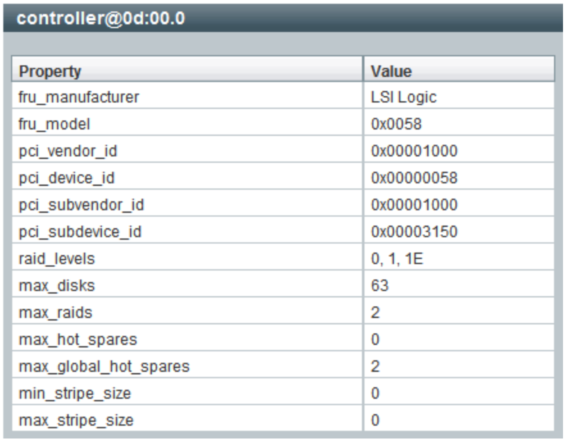
View information for RAID controllers. To get further details, click on a Controller Name. To view the topology for a controller, select the radio button next to that controller, and click *Show Topology*.

Controller Info

Show Topology

	Controller Name	RAID Levels	Max Disks	Max RAIDs
○	controller@0d:00.0	0, 1, 1E	63	2
○	controller@0d:00.1	0, 1, 1E	63	2

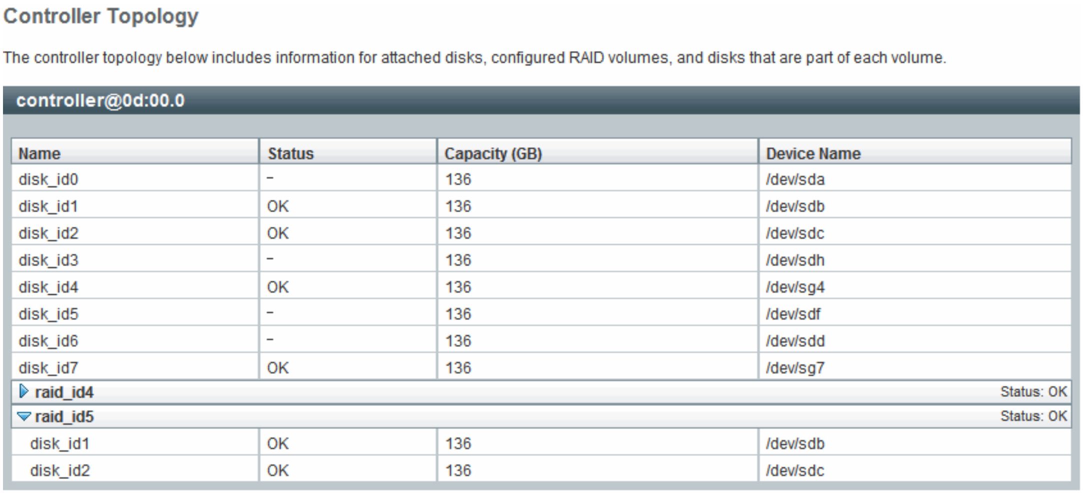
FIGURE 5-2 RAID Controller FRU Properties and Values



controller@0d:00.0

Property	Value
fru_manufacturer	LSI Logic
fru_model	0x0058
pci_vendor_id	0x00001000
pci_device_id	0x00000058
pci_subvendor_id	0x00001000
pci_subdevice_id	0x00003150
raid_levels	0, 1, 1E
max_disks	63
max_raids	2
max_hot_spares	0
max_global_hot_spares	2
min_stripe_size	0
max_stripe_size	0

FIGURE 5-3 RAID Controller Topology Details



Controller Topology

The controller topology below includes information for attached disks, configured RAID volumes, and disks that are part of each volume.

controller@0d:00.0

Name	Status	Capacity (GB)	Device Name
disk_id0	-	136	/dev/sda
disk_id1	OK	136	/dev/sdb
disk_id2	OK	136	/dev/sdc
disk_id3	-	136	/dev/sdh
disk_id4	OK	136	/dev/sg4
disk_id5	-	136	/dev/sdf
disk_id6	-	136	/dev/sdd
disk_id7	OK	136	/dev/sg7
▷ raid_id4			Status: OK
▽ raid_id5			Status: OK
disk_id1	OK	136	/dev/sdb
disk_id2	OK	136	/dev/sdc

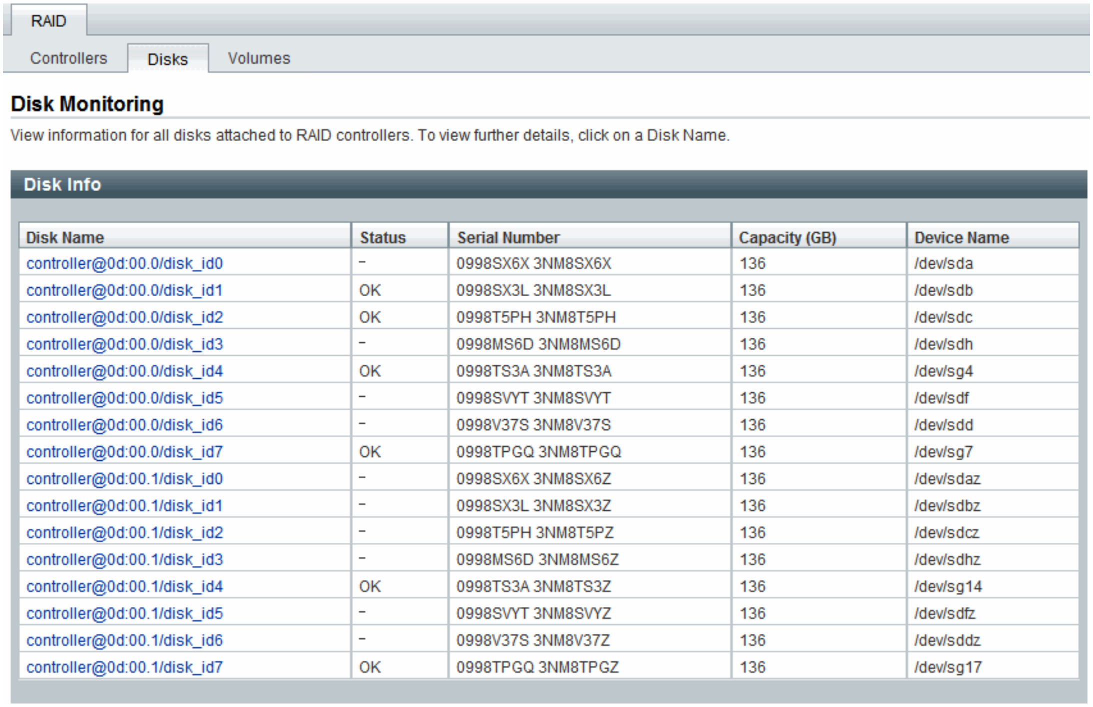
Disks Attached to RAID Controllers Details

From the Storage --> RAID --> Disks tab in ILOM, you can access configuration information about the disks that are attached to your RAID controllers. This information includes:

- Disk configuration details for each disk attached to a RAID controller. These details include the disk name, status, serial number, capacity, and device name. For example, see FIGURE 5-4.

- Disk FRU properties and values for each disk attached to a RAID controller. For example, see FIGURE 5-5.

FIGURE 5-4 Disk Details - Attached to RAID Controller



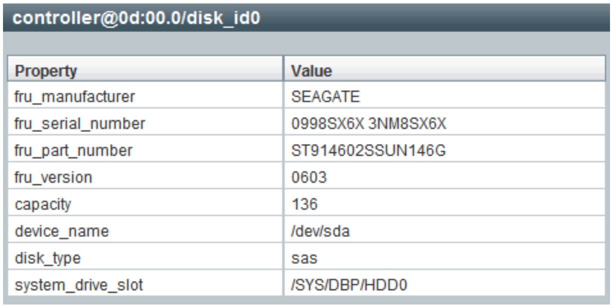
Disk Monitoring

View information for all disks attached to RAID controllers. To view further details, click on a Disk Name.

Disk Info

Disk Name	Status	Serial Number	Capacity (GB)	Device Name
controller@0d:00.0/disk_id0	–	0998SX6X 3NM8SX6X	136	/dev/sda
controller@0d:00.0/disk_id1	OK	0998SX3L 3NM8SX3L	136	/dev/sdb
controller@0d:00.0/disk_id2	OK	0998T5PH 3NM8T5PH	136	/dev/sdc
controller@0d:00.0/disk_id3	–	0998MS6D 3NM8MS6D	136	/dev/sdh
controller@0d:00.0/disk_id4	OK	0998TS3A 3NM8TS3A	136	/dev/sg4
controller@0d:00.0/disk_id5	–	0998SVYT 3NM8SVYT	136	/dev/sdf
controller@0d:00.0/disk_id6	–	0998V37S 3NM8V37S	136	/dev/sdd
controller@0d:00.0/disk_id7	OK	0998TPGQ 3NM8TPGQ	136	/dev/sg7
controller@0d:00.1/disk_id0	–	0998SX6X 3NM8SX6Z	136	/dev/sdaz
controller@0d:00.1/disk_id1	–	0998SX3L 3NM8SX3Z	136	/dev/sdbz
controller@0d:00.1/disk_id2	–	0998T5PH 3NM8T5PZ	136	/dev/sdcz
controller@0d:00.1/disk_id3	–	0998MS6D 3NM8MS6Z	136	/dev/sdhz
controller@0d:00.1/disk_id4	OK	0998TS3A 3NM8TS3Z	136	/dev/sg14
controller@0d:00.1/disk_id5	–	0998SVYT 3NM8SVYZ	136	/dev/sdfz
controller@0d:00.1/disk_id6	–	0998V37S 3NM8V37Z	136	/dev/sddz
controller@0d:00.1/disk_id7	OK	0998TPGQ 3NM8TPGZ	136	/dev/sg17

FIGURE 5-5 Disk FRU Properties and Values



controller@0d:00.0/disk_id0

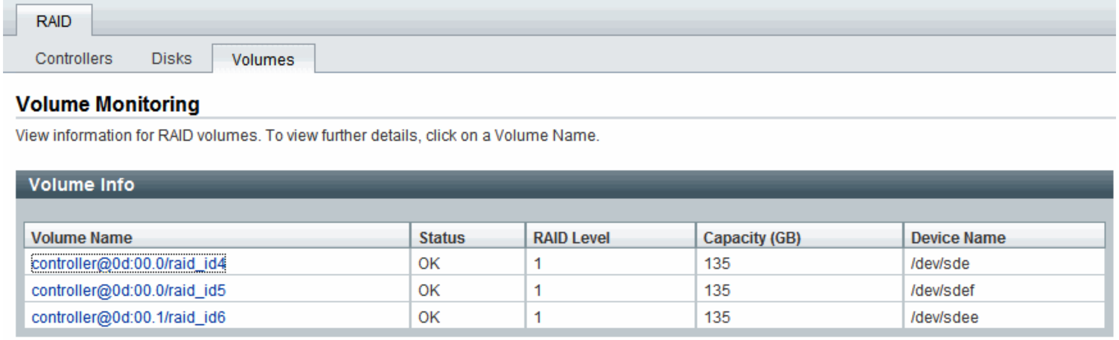
Property	Value
fru_manufacturer	SEAGATE
fru_serial_number	0998SX6X 3NM8SX6X
fru_part_number	ST914602SSUN146G
fru_version	0603
capacity	136
device_name	/dev/sda
disk_type	sas
system_drive_slot	/SYS/DBP/HDD0

RAID Controller Volume Details

From the Storage --> RAID --> Volume tab in ILOM, you can access configuration information about the RAID volumes that are configured on RAID controllers. This information includes:

- Volume configuration details for each volume configured on a RAID controller. These details include the volume name, status, RAID level, capacity, and device name. For example, see FIGURE 5-6.
- Volume properties and values for each volume configured on a RAID controller. For example, see FIGURE 5-7.

FIGURE 5-6 RAID Volume Configuration Details



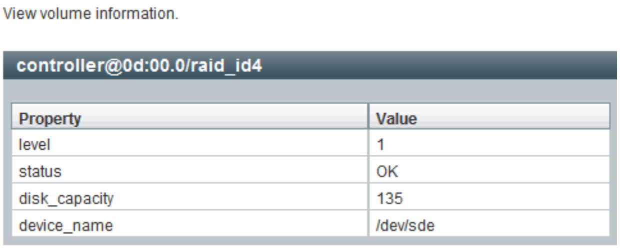
Volume Monitoring

View information for RAID volumes. To view further details, click on a Volume Name.

Volume Info

Volume Name	Status	RAID Level	Capacity (GB)	Device Name
controller@0d:00.0/raid_id4	OK	1	135	/dev/sde
controller@0d:00.0/raid_id5	OK	1	135	/dev/sdef
controller@0d:00.1/raid_id6	OK	1	135	/dev/sdee

FIGURE 5-7 RAID Volume Properties and Values



View volume information.

controller@0d:00.0/raid_id4

Property	Value
level	1
status	OK
disk_capacity	135
device_name	/dev/sde

For web procedures about how to view and monitor storage properties in ILOM, see the section about Viewing and Monitoring Storage Components in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

CMM Zone Management Feature

As of ILOM 3.0.10, a new zoning management feature is available on the CMM for SAS-2 storage devices that are installed in Oracle Sun Blade 6000 or Sun Blade 6048 Modular Systems.

For more information about how to manage SAS-2 chassis storage devices from ILOM, see the section about Zone management in the *Oracle Integrated Lights Out Manager (ILOM) CMM Administration Guide for Sun Blade 6000 and Sun Blade 6048 Modular Systems* (820-0052).

CHAPTER 6

Power Monitoring and Management of Hardware Interfaces

Topics

Description	Links
Identify Power Monitoring and Management feature updates per ILOM firmware point release	• "Summary of Power Management Feature Updates" on page 70
Become familiar with the power management terminology	• "Power Monitoring Terminology" on page 73
Learn about ILOM's real-time power monitoring and management features	• "System Power Consumption Metrics" on page 75 • "Power Policy Settings for Managing Server Power Usage" on page 82 • "Power Usage Statistics and History Metrics for Server SP and CMM" on page 86 • "Power Consumption Threshold Notifications as of ILOM 3.0.4" on page 91 • "Component Allocation Distribution as of ILOM 3.0.6 for Server SP and CMM" on page 91 • "Power Budget as of ILOM 3.0.6 for Server SPs" on page 6-101 • "Power Supply Redundancy for CMM Systems as of ILOM 3.0.6" on page 6-107 • "Platform-Specific CMM Power Metrics as of ILOM 3.0.6" on page 6-108

Related Topics

For ILOM	Chapter or Section	Guide
• CLI	• Monitoring Power Consumption	*Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* (820-6412)
• Web interface	• Monitoring Power Consumption	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)
• IPMI and SNMP hosts	• Monitoring Power Consumption	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference* (820-6413)

The ILOM 3.0 Documentation Collection is available at: `http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`

Summary of Power Management Feature Updates

TABLE 6-1 identifies the common power management feature enhancements and documentation updates made since ILOM 3.0.

TABLE 6-1 Power Management Feature Updates per ILOM Firmware Point Release

New or Enhanced Feature	Firmware Point Release	Documentation Updates	For Conceptual Information, See:
Monitor Power Consumption Metrics	ILOM 3.0	• New terms and definitions explained for Power Management Metrics. • New System Monitoring -->Power Management Consumption Metric properties. • New CLI and web procedures added for monitoring device power consumption.	• "Power Monitoring Terminology" on page 73 • "Web Interface Power Consumption Metrics as of ILOM 3.0" on page 76
Configure Power Policy Properties	ILOM 3.0	• New power policy properties explained. • New cli and web procedures added for configuring power policy settings.	• "Power Policy Settings in ILOM as of ILOM 3.0" on page 82
Monitor Power Consumption History	ILOM 3.0.3	• New power consumption history metrics explained. • New CLI and web procedures added for monitoring power consumption.	• "Power Usage Statistics and History Metrics for Server SP and CMM" on page 86

TABLE 6-1 Power Management Feature Updates per ILOM Firmware Point Release *(Continued)*

New or Enhanced Feature	Firmware Point Release	Documentation Updates	For Conceptual Information, See:
Web Interface Layout Update for Server Power Management	ILOM 3.0.4	• New top level tab added to ILOM web interface for Power Management -->Consumption page and History page • Updated procedures for Monitoring Power Consumption and History.	• "Web Interface Server and CMM Power Consumption Metrics As of ILOM 3.0.4" on page 78
Configure Power Consumption Notification Thresholds	ILOM 3.0.4	• New power consumption notification threshold settings explained. • New CLI and web procedures added for configuring the power consumption thresholds.	• "Power Consumption Threshold Notifications as of ILOM 3.0.4" on page 91
Monitor Allocation Power Distribution Metrics	ILOM 3.0.6	• New component allocation distribution metrics explained. • New CLI and web procedures added for monitoring power allocations. • New CLI and web procedures for configuring permitted power for blade slots.	• "Component Allocation Distribution as of ILOM 3.0.6 for Server SP and CMM" on page 91
Configure Power Budget Properties	ILOM 3.0.6	• New power budget properties explained. • New CLI and web procedures added for configuring power budget properties.	• "Power Budget as of ILOM 3.0.6 for Server SPs" on page 101
Configure Power Supply Redundancy Properties for CMM Systems	ILOM 3.0.6	• New power supply redundancy properties for CMM systems explained. • New CLI and web procedures added for configuring power supply redundancy properties on CMM systems.	• "Power Supply Redundancy for CMM Systems as of ILOM 3.0.6" on page 107
Monitor Advanced Power Metrics for Server Module from CMM	ILOM 3.0.6	• New CMM advanced power metrics explained for server modules.	• "Platform-Specific CMM Power Metrics as of ILOM 3.0.6" on page 108
Server Power Consumption Tab Properties Renamed	ILOM 3.0.8	• Revised ILOM web interface Power Consumption tab properties explained for server SPs.	• "Web Enhancements for Server SP Power Consumption Metrics As of 3.0.8" on page 79

TABLE 6-1 Power Management Feature Updates per ILOM Firmware Point Release *(Continued)*

New or Enhanced Feature	Firmware Point Release	Documentation Updates	For Conceptual Information, See:
Server Power Allocation Tab Replaces Distribution Tab	ILOM 3.0.8	• ILOM web Allocation tab replaces Distribution tab for server SPs. • New web procedure for viewing server power allocation properties	• "Power Management --> Distribution Tab Renamed to Allocation Tab as of ILOM 3.0.8 (Server SP)" on page 96
Server Limit Tab Replaces Budget Tab	ILOM 3.0.8	• ILOM web Limit tab replaces Budget tab for server SPs. • New web procedure for configuring power limit properties	• "Power Management --> Budget Tab Renamed to Limit Tab as of ILOM 3.0.8" on page 105
Web Interface Layout Update for CMM Power Management	ILOM 3.0.10	• New top level tab added to ILOM web interface for Power Management • Revised ILOM web Power Consumption tab properties for CMMs explained. • ILOM web Allocation tab replaces Distribution tab for CMMs. • Power Management Metrics tab removed from CMM ILOM web interface • Updated web procedure for configuring a grant limit for blade slots (previously known as allocatable power)	• "Web Enhancements for CMM Power Consumption Metrics As of 3.0.10" on page 81 • "Power Management --> Distribution Tab Renamed to Allocation Tab as of ILOM 3.0.10 (CMM)" on page 98 • "Platform-Specific CMM Power Metrics as of ILOM 3.0.6" on page 108
CLI Property Update for CMM Power Management	ILOM 3.0.10	• Revised CLI properties under the `blade slot` target explained. • Updated CLI procedure for configuring granted power or reserved power for blade slots • Updated CLI procedure for viewing power or grant limit for blade • Updated CLI procedure for configuring grant limit for blade	• "Revised CLI Power Allocation Properties as of ILOM 3.0.10" on page 100
Web Power Management Statistics tab	ILOM 3.0.14	• Power statistics previously available on the History tab have been moved to the Power Management -->Statistic tab.	• "Power Usage Statistics and Power History Web Enhancements as of ILOM 3.0.14" on page 88

Power Monitoring Terminology

TABLE 6-2 identifies the initial power monitoring terminology and definitions as of ILOM 3.0.3.

TABLE 6-2 Power Monitoring Terminology as of ILOM 3.0.3

Terms		Definition
Real-time power monitoring hardware interfaces		Power monitoring hardware interfaces enable real-time real time means that the service processor (SP) or individual power supply can be polled at any instance to retrieve and report “live” data to within one second accuracy
Power Consumption		Power consumption that is reported in ILOM includes input and output power.
	• Input Power	*Input power* is the power that is pulled into the system’s power supplies from an external source.
	• Output Power	*Output power* is the amount of power provided from the power supply to the system components.
Total Power Consumption		The *total power consumption* that is reported in ILOM is dependent on the hardware configuration: rackmount server, server module, or chassis monitoring module.
	• Rackmount Server Total Power Consumption	The *rackmount server total power consumption* is the input power consumed by the server.
	• Server Module Total Power Consumption	The *server module (blade) total power consumption* is the input power consumed only by the blade and not including any power consumed by shared components.
	• CMM Total Power Consumption	The *CMM total power consumption* is the input power consumed by the entire chassis or shelf.
Power Consumption Monitoring Properties		*Power consumption monitoring properties* include: maximum power, actual power, available power, and permitted power. **Note -** Some Oracle server platforms might not provide the power management metrics for maximum power, actual power, available power and permitted power.

TABLE 6-2 Power Monitoring Terminology as of ILOM 3.0.3 *(Continued)*

Terms	Definition
• Hardware Maximum Power Consumption Property	*Hardware maximum power* identifies the maximum input power that a system is capable of consuming at any instant given the hardware configuration of the system. Therefore, the hardware configuration maximum power is the sum of the maximum power that each processor, I/O module, memory module, fan, and so forth is capable of consuming. **Note -** The hardware maximum power consumption metric is not available from the ILOM web interface.
• Actual Power Property	*Actual Power* represents the consumed power for the rackmount server or chassis system. On a chassis monitoring module, this is the input power consumed by the entire chassis or shelf (all blades, NEMS, fans, and so forth). **Note -** .The Actual Power value is made available via the `/SYS/VPS` sensor.
• Available Power Property	*Available power* is the maximum power that the power supplies in the system can draw from an external source, for example: • For rackmount servers, the available power value represents the maximum input power that the power supplies are cable of consuming. • For chassis systems, this available power value represents the available amount of power guaranteed to the server module (blade) by the chassis.
• Permitted Power Property *or* • Peak Permitted Property	The *Permitted Power or Peak Permitted* (see note below) is the maximum power consumption guaranteed, for example: • For rackmount servers, the permitted power represents the maximum input power that the server guarantees it will consume at any instant. • For chassis systems, the permitted power represents the maximum power a server module guarantees it will consume at any instant. **Note -** The *Permitted Power* property on the server SP was renamed to *Peak Permitted* as of ILOM 3.0.8. The *Permitted Power* property on the CMM was renamed to *Peak Permitted* as of ILOM 3.0.10.
• Additional platform-specific power management metrics	Some servers might provide additional platform-specific power metrics under the `/SP/powermgmt/`advanced mode in the CLI or the Advanced Power Metrics table in the system Monitoring --> Power Management page in the web interface. Each advanced power metric includes a name, a unit, and a value. For additional information about platform-specific power management information, see the ILOM Supplement guide or the administrator guide that was provided with your server system.

For information about how to view the power management metrics in ILOM using the CLI or web interface, see the section about Monitoring the Power Consumption Interfaces in one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* (820-6412)

Real-Time Power Monitoring and Management Features

For details, about using ILOM's real-time power monitoring and management features see these topics:

- "System Power Consumption Metrics" on page 75
- "Power Policy Settings for Managing Server Power Usage" on page 82
- "Power Usage Statistics and History Metrics for Server SP and CMM" on page 86
- "Power Consumption Threshold Notifications as of ILOM 3.0.4" on page 91
- "Component Allocation Distribution as of ILOM 3.0.6 for Server SP and CMM" on page 91
- "Power Budget as of ILOM 3.0.6 for Server SPs" on page 101
- "Power Supply Redundancy for CMM Systems as of ILOM 3.0.6" on page 107
- "Platform-Specific CMM Power Metrics as of ILOM 3.0.6" on page 108

System Power Consumption Metrics

As of ILOM 3.0, you can view the server SP and CMM power consumption metrics using the ILOM CLI or web interface.

Since ILOM 3.0, web enhancements for the Power Consumption metrics have been made in ILOM 3.0.4, 3.0.8, and 3.0.10. The CLI power consumption metrics targets and properties have not changed since ILOM 3.0.

For information about how to access the power consumption metrics in ILOM, as well as updates made to the power consumption web interface since ILOM 3.0, see the following topics:

ILOM Interface	Platform Hardware	As of ILOM Firmware	Power Consumption Topic
Web	Server SP and CMM	ILOM 3.0	"Web Interface Power Consumption Metrics as of ILOM 3.0" on page 76

ILOM Interface	Platform Hardware	As of ILOM Firmware	Power Consumption Topic
CLI	Server SP and CMM	ILOM 3.0	"CLI Power Consumption Metrics as of ILOM 3.0" on page 77
Web	Server SP and CMM	ILOM 3.0.4	"Web Interface Server and CMM Power Consumption Metrics As of ILOM 3.0.4" on page 78
Web	Server SP	ILOM 3.0.8	"Web Enhancements for Server SP Power Consumption Metrics As of 3.0.8" on page 79
Web	CMM	ILOM 3.0.10	"Web Enhancements for CMM Power Consumption Metrics As of 3.0.10" on page 81
CLI	CMM	ILOM 3.0.10	"Revised CLI Power Allocation Properties as of ILOM 3.0.10" on page 100

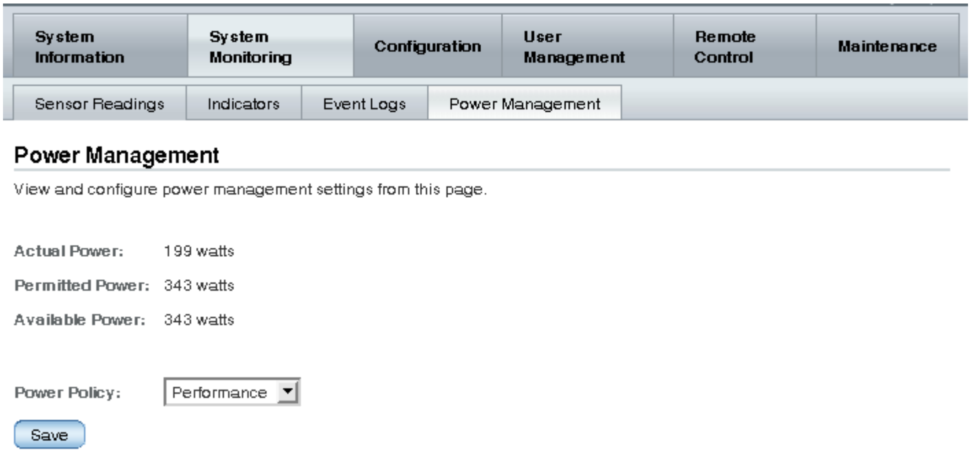
Note – The ability to monitor and provide the power consumption metrics in ILOM varies depending on the platform server implementation of this feature. For information about hardware platform-specific power consumption metrics provided for your server, see the ILOM Supplement Guide or administration guide provided with your system.

Web Interface Power Consumption Metrics as of ILOM 3.0

As of ILOM 3.0, you can control the power policy and view the power consumption metrics for a server SP or a CMM from the Power Management tab in the web interface.

The power consumption metrics (shown in FIGURE 6-1) for Actual Power, Permitted Power and Available Power are defined in "Power Monitoring Terminology as of ILOM 3.0.3" on page 73. For information describing the use of the Power Policy property, see "Power Policy Settings for Managing Server Power Usage" on page 82.

FIGURE 6-1 Power Management Web Interface Page as of ILOM 3.0.



Power Management

View and configure power management settings from this page.

Actual Power: 199 watts

Permitted Power: 343 watts

Available Power: 343 watts

Power Policy: Performance

CLI Power Consumption Metrics as of ILOM 3.0

TABLE 6-3 identifies the server SP and CMM power consumption metric properties available from the ILOM CLI as of ILOM 3.0.

TABLE 6-3 CLI Power Consumption Properties

Power Consumption Property	Use the `show` command to view the power consumption property value, for example:
Total System Power Consumption	`show /SYS/VPS`
Actual Power Consumption	`show /SP/powermangment actual_power` **Note -** The actual power value returned is the same as the value returned by /SYS/VPS sensor.
Power Supply Consumption	• For rackmount server power supply: show `/SYS/`*platform_path_to_powersupply*`/INPUT_POWER`|`OUTPUT POWER` • For CMM power supply: `show /CH/`*platform_path_to_powersupply*`/INPUT_POWER`|`OUTPUT POWER`

TABLE 6-3 CLI Power Consumption Properties *(Continued)*

Power Consumption Property	Use the `show` command to view the power consumption property value, for example:

Actual Power	• For rackmount servers:
	`show /SP/powermgmt available_power`
	• For CMMs:
	`show /CMM/powermgmt available_power`

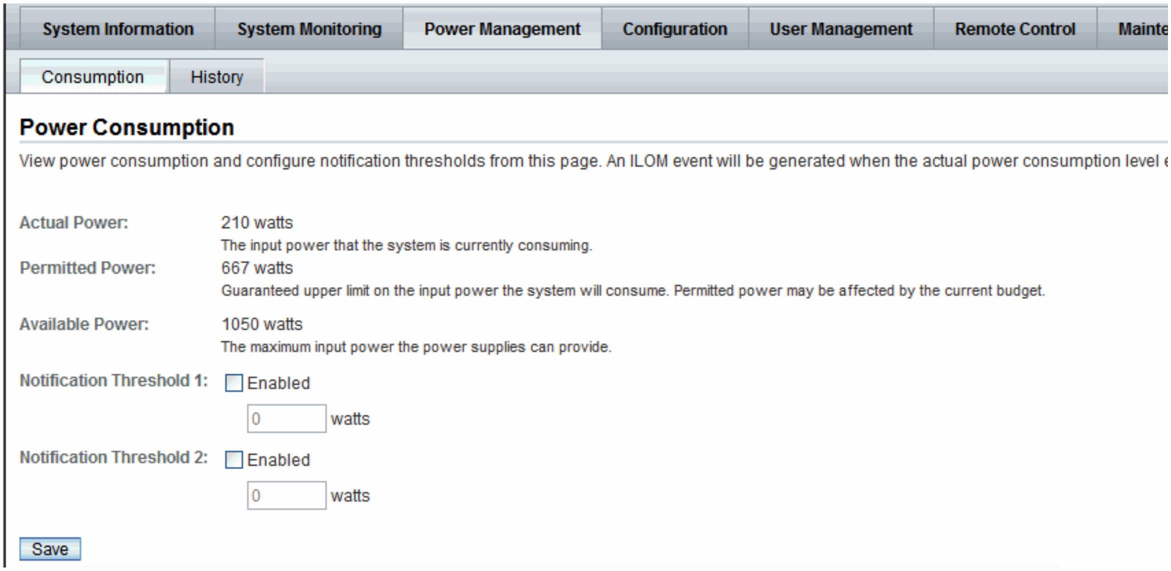
Maximum Hardware Power Consumption	`show /SP/powermgmt hwconfig_power`

Permitted Power Consumption	• For rackmount servers:
	`show /SP/powermgmt permitted_power`
	• For CMMs:
	`show /CMM/powermgmt permitted_power`

Web Interface Server and CMM Power Consumption Metrics As of ILOM 3.0.4

As of ILOM 3.0.4, the server SP and CMM power consumption metrics in the web interface have been moved to the Power Management --> Consumption page.

FIGURE 6-2 Power Consumption Page as of ILOM 3.0.4



Power Consumption

View power consumption and configure notification thresholds from this page. An ILOM event will be generated when the actual power consumption level e

Actual Power: 210 watts
The input power that the system is currently consuming.

Permitted Power: 667 watts
Guaranteed upper limit on the input power the system will consume. Permitted power may be affected by the current budget.

Available Power: 1050 watts
The maximum input power the power supplies can provide.

Notification Threshold 1: □ Enabled
0 watts

Notification Threshold 2: □ Enabled
0 watts

In this 3.0.4 web version of the Power Consumption page, the following changes were made for the Server SP and CMM:

- New properties for Notification Thresholds were added. For information about the Notification Threshold properties, see "Power Consumption Threshold Notifications as of ILOM 3.0.4" on page 91.
- The Power Policy property (shown in FIGURE 6-1) was removed from the earlier version of the Power Management page. For more information about using the power policy property after ILOM 3.0.4, see "Power Policy Settings for Managing Server Power Usage" on page 82.
- The properties for *Actual Power*, *Permitted Power*, and *Available Power* remained unchanged. For more information about these properties, see TABLE 6-2 "Power Monitoring Terminology as of ILOM 3.0.3" on page 73.

Web Enhancements for Server SP Power Consumption Metrics As of 3.0.8

As of ILOM 3.0.8, some of the power consumption properties on the web interface for the server SP have changed. For more information about these property changes, see TABLE 6-4. For an updated view of the Power Consumption page for the server SP as of ILOM 3.0.8 see FIGURE 6-3

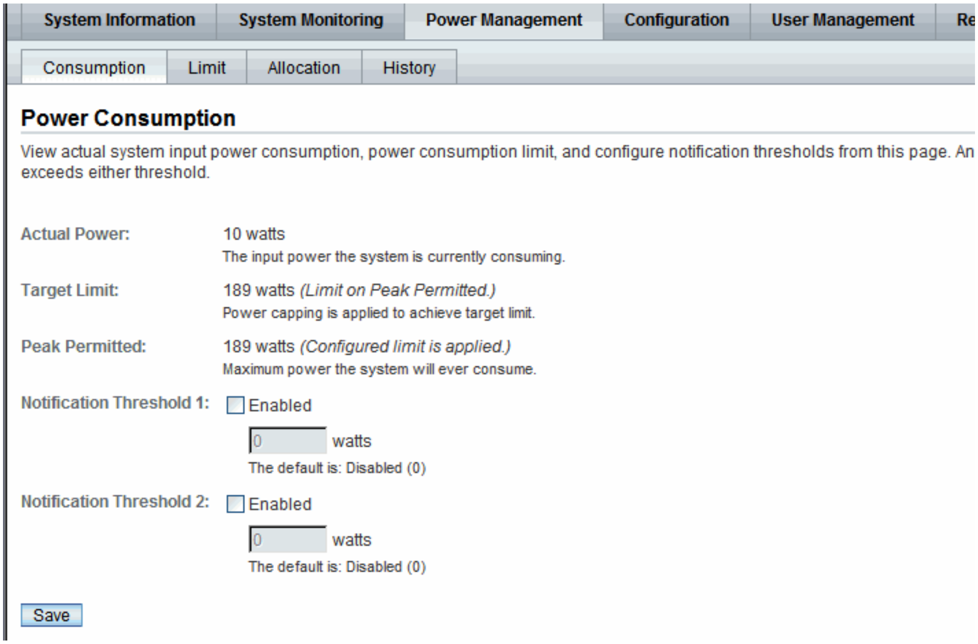
TABLE 6-4 Consumption Tab Server SP Settings Changes in ILOM 3.0.8

Consumption Tab Changes	Details
`Target Limit` (new property)	A new read-only property for `Target Limit` is available on the Power Management --> Consumption tab as of ILOM 3.0.8. The `Target Limit` (shown in FIGURE 6-3) property represents the power consumption limit value that was configured for the server. **Note -** The configuration options for the `Target Limit` property appear on the Power Management --> Limit tab. For more details about the `Target Limit` configuration options, see "Power Management --> Budget Tab Renamed to Limit Tab as of ILOM 3.0.8" on page 105.
`Peak Permitted` (renamed property)	The `Permitted Power` property on the Power Management --> Consumption tab in ILOM 3.0.4 (shown in FIGURE 6-2) was renamed to `Peak Permitted` in ILOM 3.0.8. The `Peak Permitted` read-only property (shown in FIGURE 6-3) represents the maximum power the system can consume. **Note -** For servers, the Peak Permitted value in ILOM is derived from the System Allocated power and the Target Limit. For more details, see "Advanced Server Power Budget Features as of ILOM 3.0.6" on page 103.

TABLE 6-4 Consumption Tab Server SP Settings Changes in ILOM 3.0.8 *(Continued)*

Consumption Tab Changes	Details
`Allocated Power` (removed)	The read-only property for `Allocated Power` (shown in FIGURE 6-2) was removed from the Power Management --> Consumption tab as of ILOM 3.0.8 (shown in FIGURE 6-3). **Note -** In ILOM 3.0.8, you can view Allocated Power values for the system and for each component on the Power Allocation Plan page. For more details, see "Power Management --> Distribution Tab Renamed to Allocation Tab as of ILOM 3.0.8 (Server SP)" on page 96.

FIGURE 6-3 Updated Power Management --> Consumption Tab - ILOM SP 3.0.8



Power Consumption

View actual system input power consumption, power consumption limit, and configure notification thresholds from this page. An
exceeds either threshold.

Actual Power: 10 watts
The input power the system is currently consuming.

Target Limit: 189 watts *(Limit on Peak Permitted.)*
Power capping is applied to achieve target limit.

Peak Permitted: 189 watts *(Configured limit is applied.)*
Maximum power the system will ever consume.

Notification Threshold 1: □ Enabled
0 watts
The default is: Disabled (0)

Notification Threshold 2: □ Enabled
0 watts
The default is: Disabled (0)

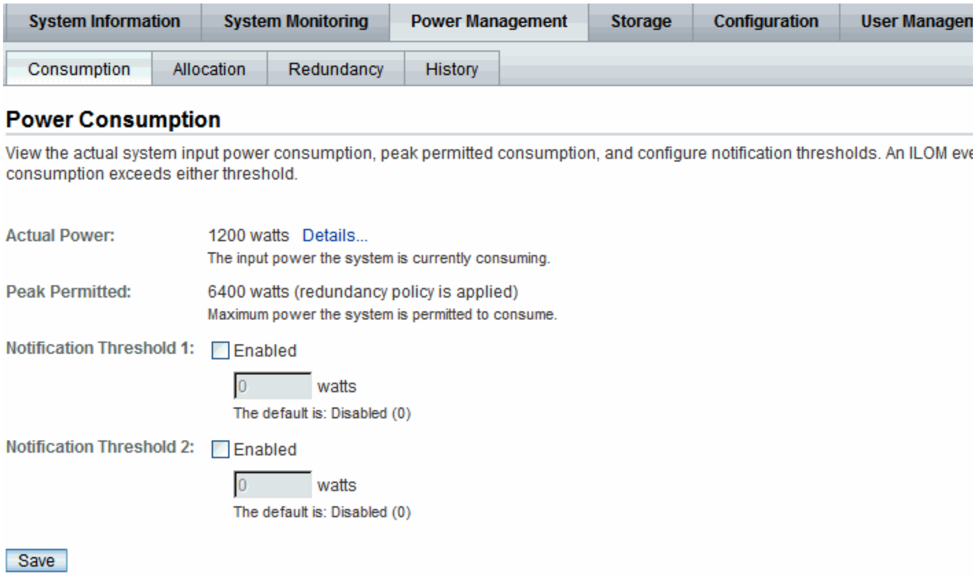
Web Enhancements for CMM Power Consumption Metrics As of 3.0.10

As of ILOM 3.0.10, some of the power consumption properties on the web interface for the CMM have changed. For more information about these property changes, see TABLE 6-5. For an updated view of the Power Consumption page for the server SP as of ILOM 3.0.8 see FIGURE 6-4.

TABLE 6-5 Consumption Tab CMM Settings Changes in ILOM 3.0.10

Consumption Tab Changes	Details
`Peak Permitted` (renamed property)	The `Permitted Power` property on the CMM Power Management --> Consumption tab was renamed to `Peak Permitted` in ILOM 3.0.10. The `Peak Permitted` read-only property (shown in FIGURE 6-4) represents the maximum power the system is permitted to use.
`Available Power` (renamed property and moved)	The read-only property for `Available Power` (previously available in ILOM 3.0.4) was removed from the CMM Power Management --> Consumption tab as of ILOM 3.0.10 (shown in FIGURE 6-4). The read-only property for `Available Power` was renamed to `Grantable Power` in ILOM 3.0.10 and moved to the Power Summary table on the Allocation tab. For more details, see "Power Management --> Distribution Tab Renamed to Allocation Tab as of ILOM 3.0.10 (CMM)" on page 98.

FIGURE 6-4 Updated Power Management --> Consumption Tab - ILOM CMM 3.0.10



Power Consumption

View the actual system input power consumption, peak permitted consumption, and configure notification thresholds. An ILOM eve consumption exceeds either threshold.

Actual Power: 1200 watts Details...
The input power the system is currently consuming.

Peak Permitted: 6400 watts (redundancy policy is applied)
Maximum power the system is permitted to consume.

Notification Threshold 1: □ Enabled
0 watts
The default is: Disabled (0)

Notification Threshold 2: □ Enabled
0 watts
The default is: Disabled (0)

Save

Power Policy Settings for Managing Server Power Usage

To help manage the power usage of your system, ILOM supports the following Power policies:

- "Power Policy Settings in ILOM as of ILOM 3.0" on page 82
- "Power Policy Settings in ILOM as of ILOM 3.0.4" on page 83
- "Power Capping Policy Settings in ILOM as of ILOM 3.0.8" on page 84

Power Policy Settings in ILOM as of ILOM 3.0

As of ILOM 3.0, two Power Policy settings (shown in FIGURE 6-1) are available from the ILOM CLI and web interface to help you manage the power usage on your system.

Note – The Power Policy feature was initially available on most x86 servers as of ILOM 3.0. As of ILOM 3.0.3, some SPARC platform servers supported this feature as well. To determine if your server supports a Power Policy feature, see the ILOM Supplement guide or administration guide provided for your server.

TABLE 6-6 defines the two Policy settings you can choose to configure from the ILOM CLI and web interface:

TABLE 6-6 Power Policy Properties Defined as of ILOM 3.0

Property	Description
Performance	The system is allowed to use all of the power that is available.
Elastic	The system power usage is adapted to the current utilization level. For example, the system will power up or down just enough system components to keep relative utilization at 70% at all times, even if workload fluctuates

For more details about how to access and configure the power policy settings in ILOM, see the section about Monitoring Power Consumption in one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

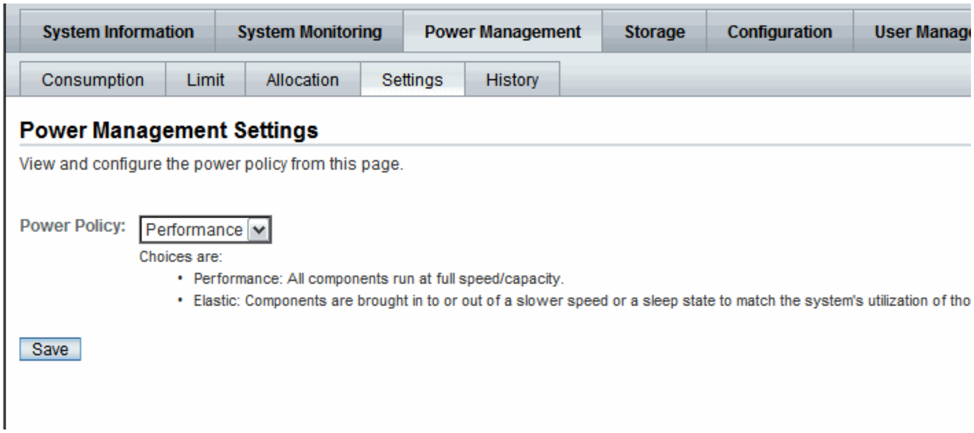
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide*

Power Policy Settings in ILOM as of ILOM 3.0.4

As of ILOM 3.0.4, the Power Policy settings in the ILOM interface have been changed as follows:

- The Power Management Power Policy properties available in the ILOM CLI or web interface (shown in FIGURE 6-1) were removed for x86 server SPs as of ILOM 3.0.4.
- The Power Management Power Policy properties available in the ILOM web interface (shown in FIGURE 6-1) for SPARC server supporting this feature have been moved to the Power Management -->Settings tab (shown in FIGURE 6-5). To verify if your SPARC system supports this feature, see the ILOM Supplement Guide or the administration guide supplied for your server.

FIGURE 6-5 Policy on Limit Tab for Some SPARC Servers as of ILOM 3.04.



Power Management Settings

View and configure the power policy from this page.

Power Policy: Performance

Choices are:

- Performance: All components run at full speed/capacity.
- Elastic: Components are brought in to or out of a slower speed or a sleep state to match the system's utilization of tho

Power Capping Policy Settings in ILOM as of ILOM 3.0.8

As of ILOM 3.0.8, advanced policy settings (shown in FIGURE 6-6) for power capping where added to the ILOM web interface for x86 servers and some SPARC servers.

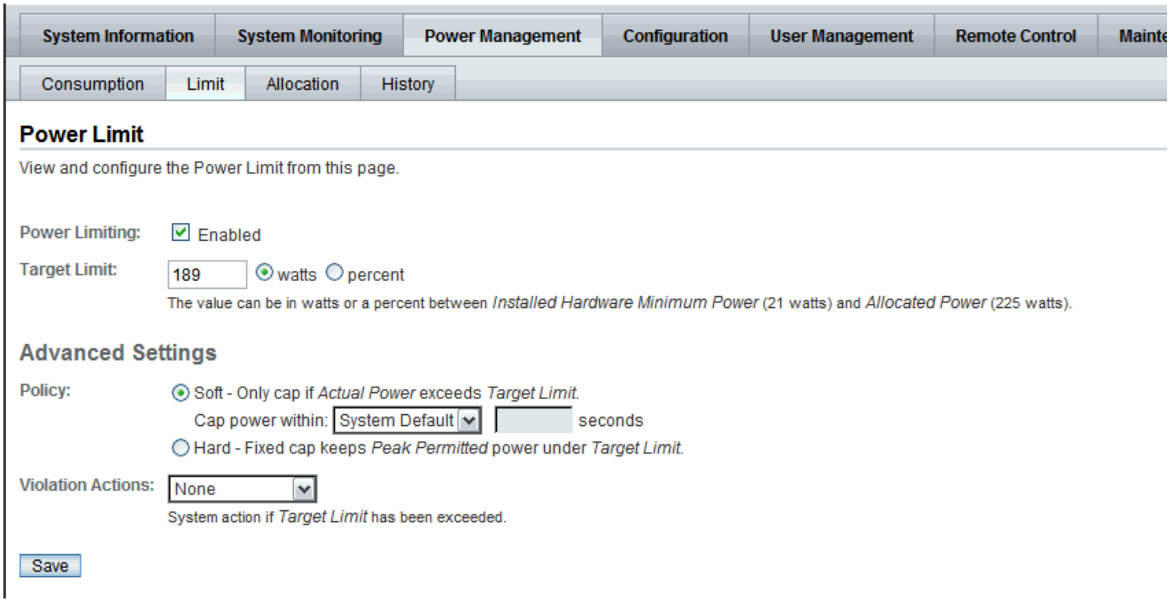
For detailed description of the power capping properties, see TABLE 6-7.

TABLE 6-7 Advanced Power Capping Policy Property Descriptions

Power Limit Property	Description
Policy	The Policy property enables you to configure the power capping policy. In the Policy property, specify which of the following types of power capping you want to apply: • **Soft** - `Only cap if actual power exceeds Target Limit.` – If you enabled the soft cap option, you can configure the grace period for capping `Actual Power` to within the `Target Limit`. - `System Default` – Platform selected optimum grace period. *or* - `Custom` – User-specified grace period. • **Hard** - `Fixed cap keeps Peak Permitted power under Target Limit.` – If you enable this option, power capping is permanently applied without a grace period.
Violation Actions	The Violation Actions property enables you to specify the settings you want ILOM to take if the power limit cannot be achieved within the set grace period. You can choose to specify one of the following actions: • `None` – If you enable this option and the power limit cannot be achieved, ILOM will display a `Status Error Message` to notify you that ILOM is unable to achieve the power capping limit specified. *or* • `Hard-Power-Off` – If this option is chosen and the power limit cannot be achieved, ILOM takes the following actions: * Display a `Status Error Message`. * Hard-power-off the server. **Note -** The default option for Violation Actions is `None`.

Note – The Advanced Power Capping Policy settings replaced the Time Limit properties originally available from the Power Management -> Budget tab in ILOM 3.0.6.

FIGURE 6-6 Advanced Power Policy Appear on Limit Tab as of ILOM 3.0.8



Power Limit

View and configure the Power Limit from this page.

Power Limiting: ☑ Enabled

Target Limit: 189 ● watts ○ percent

The value can be in watts or a percent between *Installed Hardware Minimum Power* (21 watts) and *Allocated Power* (225 watts).

Advanced Settings

Policy: ● Soft - Only cap if *Actual Power* exceeds *Target Limit.*

Cap power within: System Default seconds

○ Hard - Fixed cap keeps *Peak Permitted* power under *Target Limit.*

Violation Actions: None

System action if *Target Limit* has been exceeded.

For more information about configuring power limit properties using the ILOM web interface, see the section about Configure Server Power Limit Properties in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*.

Power Usage Statistics and History Metrics for Server SP and CMM

As of ILOM 3.0.3, a rolling average of power consumption in 15, 30, and 60 second intervals is available for the server SP and CMM. Specifically, these rolling averages displayed by the ILOM CLI or web interface are obtained by leveraging ILOM's sensor history capability.

Note – The power consumption history information presented in ILOM is retrieved at a rate determined by the individual platform server or CMM, which could range from 1 to 8 seconds, and typically could average between 3 to 5 seconds.

For more details about viewing the power usage and history information for a hardware device in ILOM, see the following topics:

- "Web Interface Power Usage Statistics and History Metrics" on page 86
- "CLI Power Consumption History Metrics" on page 90

Web Interface Power Usage Statistics and History Metrics

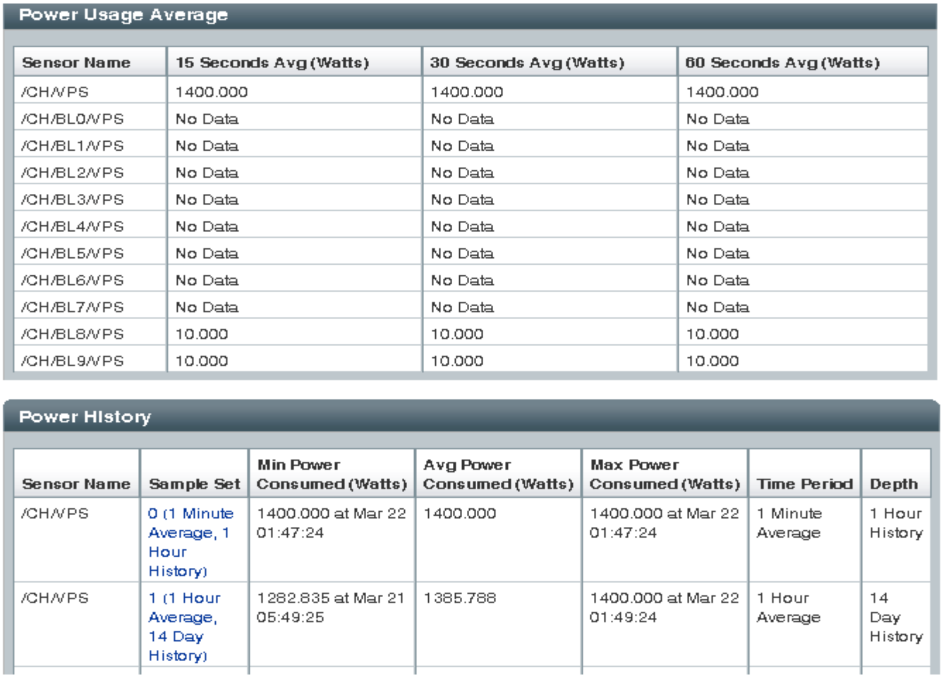
The Power Consumption History metrics for the server SP and CMM are available from the ILOM CLI and web interface.

- "Power Usage Statistics and History as of ILOM 3.0.3" on page 86
- "Power History - Data Set Sample of Power Consumed" on page 87
- "Power Usage Statistics and History Web Enhancements as of ILOM 3.0.4" on page 88
- "Power Usage Statistics and Power History Web Enhancements as of ILOM 3.0.14" on page 88

Power Usage Statistics and History as of ILOM 3.0.3

As of ILOM 3.0.3, you can access power metrics for system Power Usage Averages and History in the ILOM web interface from the System Monitoring -> Power Management page (click History link).

FIGURE 6-7 Web Power Usage and History Metrics for CMM as of ILOM 3.0.3



Power Usage Average

Sensor Name	15 Seconds Avg (Watts)	30 Seconds Avg (Watts)	60 Seconds Avg (Watts)
/CH/VPS	1400.000	1400.000	1400.000
/CH/BL0/VPS	No Data	No Data	No Data
/CH/BL1/VPS	No Data	No Data	No Data
/CH/BL2/VPS	No Data	No Data	No Data
/CH/BL3/VPS	No Data	No Data	No Data
/CH/BL4/VPS	No Data	No Data	No Data
/CH/BL5/VPS	No Data	No Data	No Data
/CH/BL6/VPS	No Data	No Data	No Data
/CH/BL7/VPS	No Data	No Data	No Data
/CH/BL8/VPS	10.000	10.000	10.000
/CH/BL9/VPS	10.000	10.000	10.000

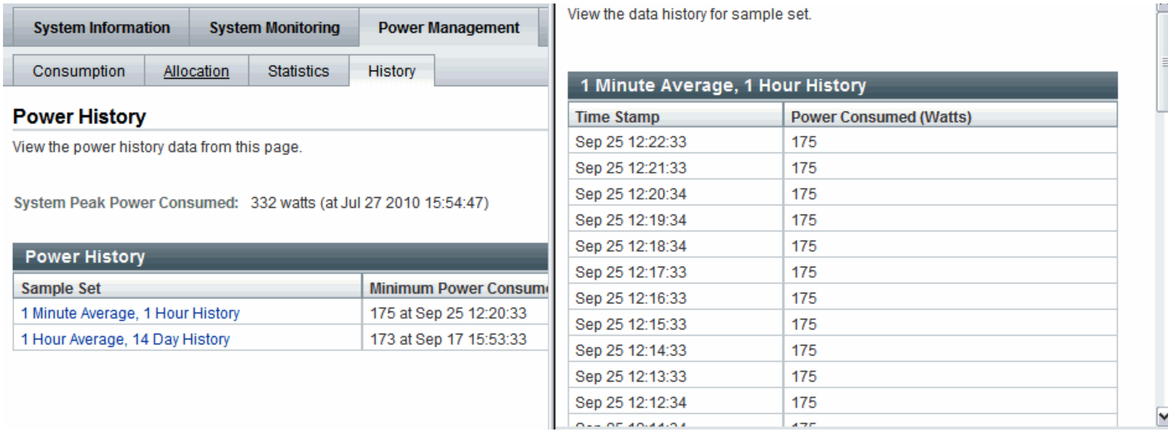
Power History

Sensor Name	Sample Set	Min Power Consumed (Watts)	Avg Power Consumed (Watts)	Max Power Consumed (Watts)	Time Period	Depth
/CH/VPS	0 (1 Minute Average, 1 Hour History)	1400.000 at Mar 22 01:47:24	1400.000	1400.000 at Mar 22 01:47:24	1 Minute Average	1 Hour History
/CH/VPS	1 (1 Hour Average, 14 Day History)	1282.835 at Mar 21 05:49:25	1385.788	1400.000 at Mar 22 01:49:24	1 Hour Average	14 Day History

Power History - Data Set Sample of Power Consumed

You can obtain a sample data set of the power consumed by the system for a specific duration by clicking the Sample Set link on the History page.

EXAMPLE 6-1 Data Set Sample of Power Consumed by System



Power History

View the power history data from this page.

System Peak Power Consumed: 332 watts (at Jul 27 2010 15:54:47)

Power History

Sample Set	Minimum Power Consum
1 Minute Average, 1 Hour History	175 at Sep 25 12:20:33
1 Hour Average, 14 Day History	173 at Sep 17 15:53:33

View the data history for sample set.

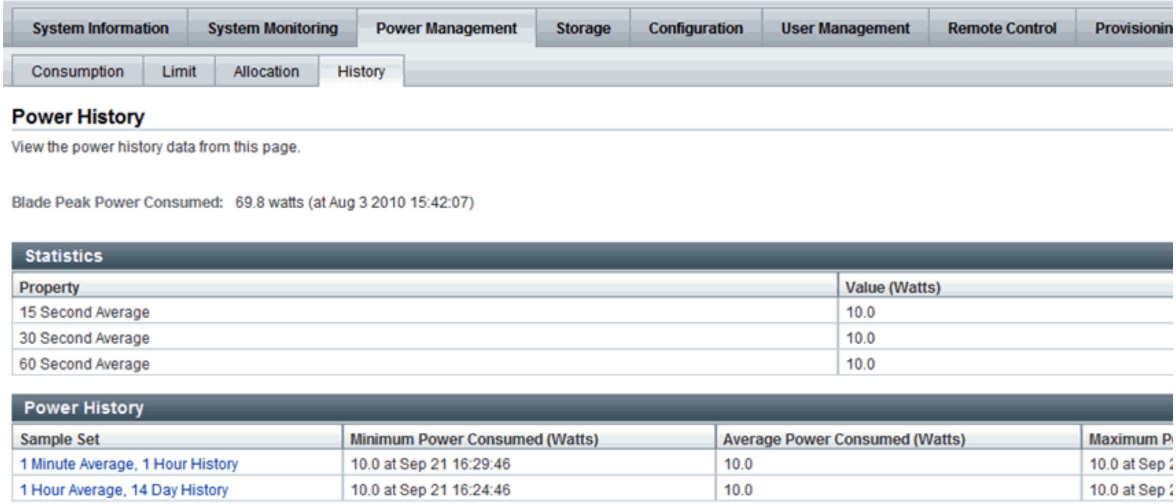
1 Minute Average, 1 Hour History

Time Stamp	Power Consumed (Watts)
Sep 25 12:22:33	175
Sep 25 12:21:33	175
Sep 25 12:20:34	175
Sep 25 12:19:34	175
Sep 25 12:18:34	175
Sep 25 12:17:33	175
Sep 25 12:16:33	175
Sep 25 12:15:33	175
Sep 25 12:14:33	175
Sep 25 12:13:33	175
Sep 25 12:12:34	175

Power Usage Statistics and History Web Enhancements as of ILOM 3.0.4

As of ILOM 3.0.4, the metrics for the power usage statistics and history was removed from the Power Management page (shown in FIGURE 6-7) to a separate Power Management --> History tab (shown in FIGURE 6-8).

FIGURE 6-8 Web Power Statistics and Power History for Server as of ILOM 3.0.4



Power History

View the power history data from this page.

Blade Peak Power Consumed: 69.8 watts (at Aug 3 2010 15:42:07)

Statistics

Property	Value (Watts)
15 Second Average	10.0
30 Second Average	10.0
60 Second Average	10.0

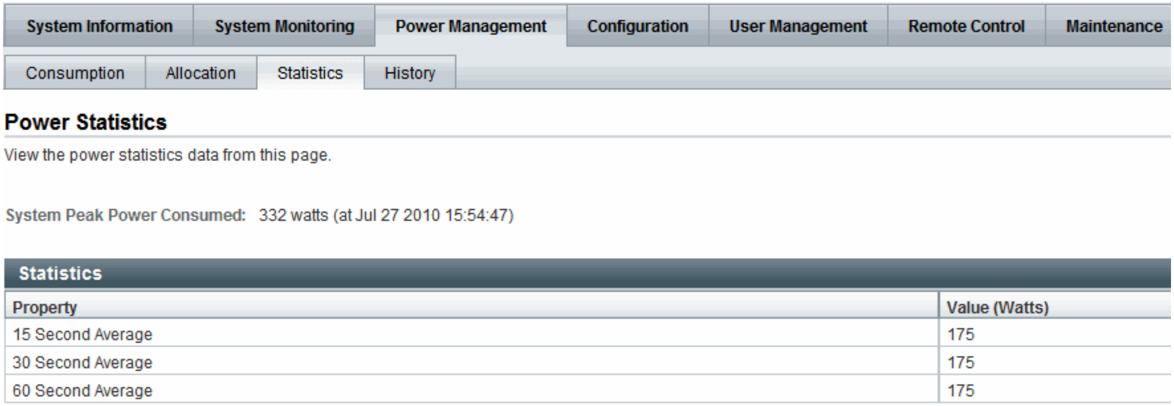
Power History

Sample Set	Minimum Power Consumed (Watts)	Average Power Consumed (Watts)	Maximum P
1 Minute Average, 1 Hour History	10.0 at Sep 21 16:29:46	10.0	10.0 at Sep 2
1 Hour Average, 14 Day History	10.0 at Sep 21 16:24:46	10.0	10.0 at Sep 2

Power Usage Statistics and Power History Web Enhancements as of ILOM 3.0.14

As of ILOM 3.0.14, the Statistics table appearing on the Power Management --> History tab in ILOM 3.0.4 (shown in FIGURE 6-8) was moved to a separate Statistic tab (shown in FIGURE 6-9 and FIGURE 6-10) in the ILOM web interface.

FIGURE 6-9 Power Statistics Tab for Server as of ILOM 3.0.14



Power Statistics

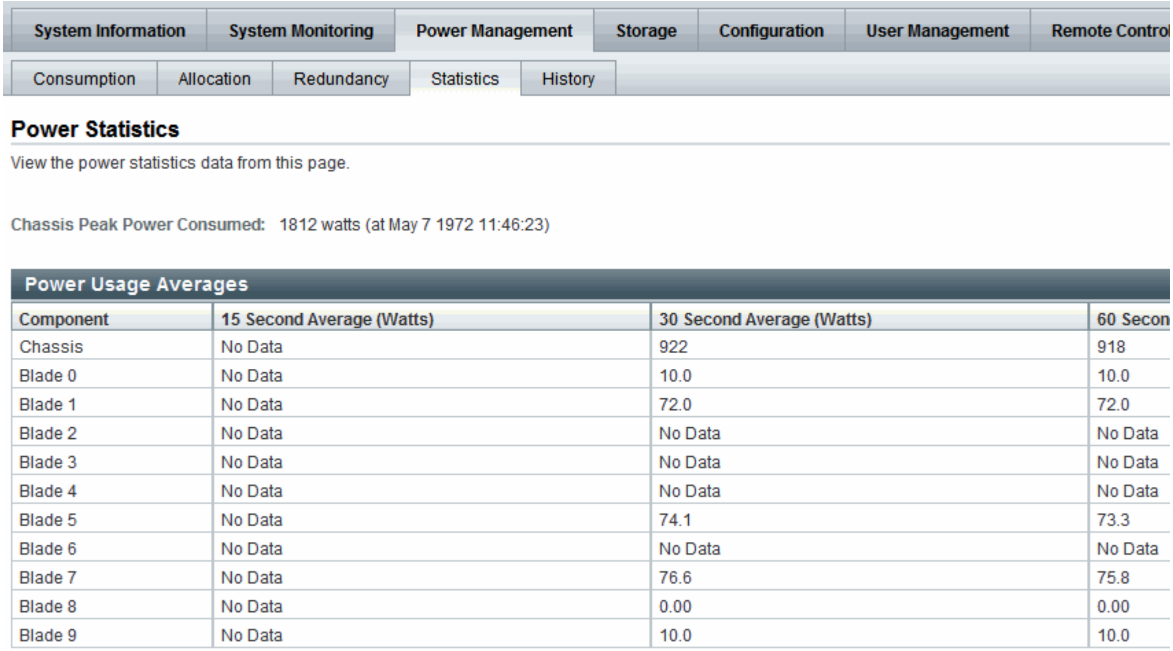
View the power statistics data from this page.

System Peak Power Consumed: 332 watts (at Jul 27 2010 15:54:47)

Statistics

Property	Value (Watts)
15 Second Average	175
30 Second Average	175
60 Second Average	175

FIGURE 6-10 Power Statistics Tab for CMM as of ILOM 3.0.14



Power Statistics

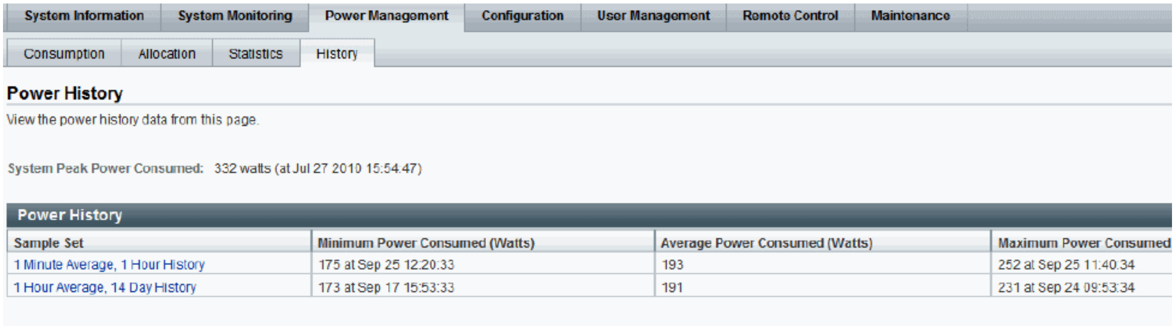
View the power statistics data from this page.

Chassis Peak Power Consumed: 1812 watts (at May 7 1972 11:46:23)

Power Usage Averages

Component	15 Second Average (Watts)	30 Second Average (Watts)	60 Secon
Chassis	No Data	922	918
Blade 0	No Data	10.0	10.0
Blade 1	No Data	72.0	72.0
Blade 2	No Data	No Data	No Data
Blade 3	No Data	No Data	No Data
Blade 4	No Data	No Data	No Data
Blade 5	No Data	74.1	73.3
Blade 6	No Data	No Data	No Data
Blade 7	No Data	76.6	75.8
Blade 8	No Data	0.00	0.00
Blade 9	No Data	10.0	10.0

FIGURE 6-11 Power History Tab for Server as of ILOM 3.0.14



Power History

View the power history data from this page.

System Peak Power Consumed: 332 watts (at Jul 27 2010 15:54:47)

Power History

Sample Set	Minimum Power Consumed (Watts)	Average Power Consumed (Watts)	Maximum Power Consumed
1 Minute Average, 1 Hour History	175 at Sep 25 12:20:33	193	252 at Sep 25 11:40:34
1 Hour Average, 14 Day History	173 at Sep 17 15:53:33	191	231 at Sep 24 09:53:34

CLI Power Consumption History Metrics

TABLE 6-8 identifies the power consumption history properties available from the ILOM CLI as of ILOM 3.0.3.

TABLE 6-8 CLI Power Consumption History Properties as of ILOM 3.0.3

Power Consumption History Property	Use the `show` command to view the power consumption history value, for example:

Rolling Power Usage Averages	• For server SPs:
	`show /SYS/VPS/history`
	• For CMMs:
	`show /CH/VPS/history`

Average Power Consumption	• For server SPs:
	`show /SYS/VPS/history/0`
	• For CMMs:
	`show /CH/VPS/history/0`

Sample set details for time stamp and power consumed in watts	• For server SPs:
	`show /SYS/VPS/history/0/list`
	• For CMMs:
	`show /CH/VPS/history/0/list`

Power Consumption Threshold Notifications as of ILOM 3.0.4

As of ILOM 3.0.4, two new Notification Threshold settings are available in the CLI and web interface (as shown in FIGURE 6-2). These Notification Threshold settings enable you to generate up two power consumption notifications when the specified power consumption value (in watts) exceeds the threshold. Each time the power consumption value exceeds the specified threshold (in watts) an ILOM event is generated and logged in the ILOM event log.

The power consumption notification generated by ILOM is dependent on the whether email alerts have been configured or if SNMP traps have been enabled. For more information, about email alerts and SNMP traps, see "System Monitoring and Alert Management" on page 43.

For more information about configuring the power consumption notification thresholds, see the section about View and Configure Notification Thresholds in one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide.*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*

Component Allocation Distribution as of ILOM 3.0.6 for Server SP and CMM

The Component Allocation Power Distribution feature in ILOM enables you to monitor, in real-time, the amount of power that is allocated to server components and, if applicable, CMM components.

Topics described in this section:

- "Monitoring Server Power Allocated Components" on page 92
- "Monitoring CMM Power Allocated Components" on page 93
- "Component Power Allocation Special Considerations" on page 95
- "Power Management --> Distribution Tab Renamed to Allocation Tab as of ILOM 3.0.8 (Server SP)" on page 96
- "Power Management --> Distribution Tab Renamed to Allocation Tab as of ILOM 3.0.10 (CMM)" on page 98
- "Revised CLI Power Allocation Properties as of ILOM 3.0.10" on page 100

Monitoring Server Power Allocated Components

TABLE 6-9 identifies the components that are allocated power in ILOM by your Oracle Sun server. For each component listed in TABLE 6-9, ILOM provides an allocated server power value in wattage that represents the sum of the maximum power consumed by either a single server component (such as a memory module), a category of server components (all memory modules), or all server power-consuming components.

TABLE 6-9 Server Power Allocated Components

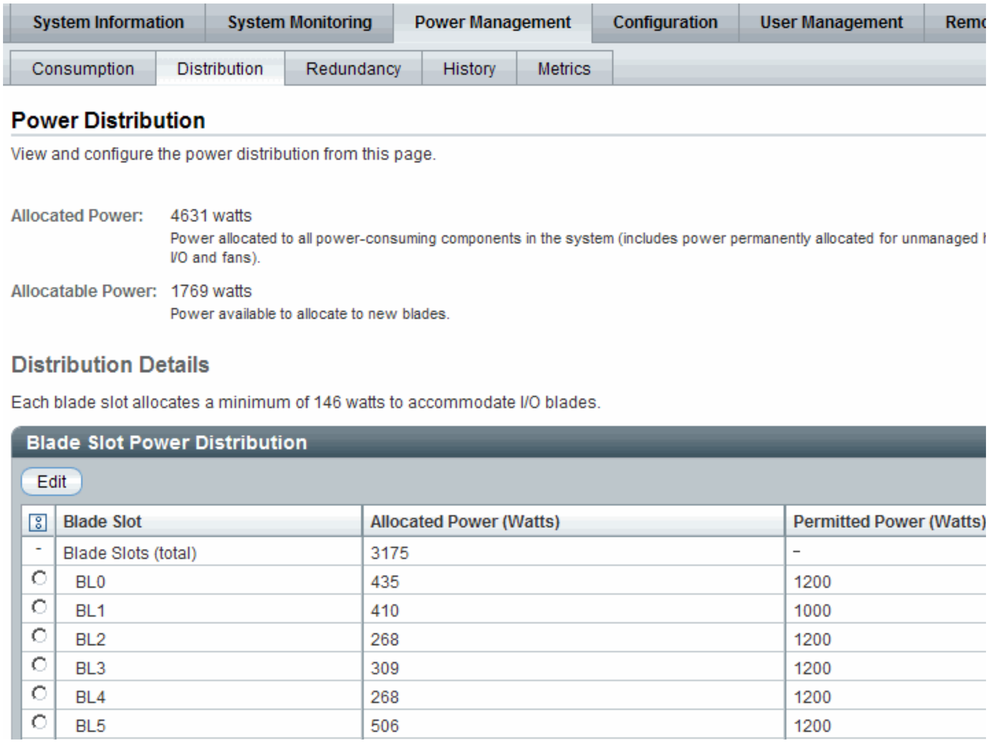
Server Power Allocated Component	Allocated Power (Watts)	Applicable to Rackmount Server	Applicable to Sun Blade Server Module
All server power-consuming components	X	X	X
CPUs	X	X	X
Memory modules, such as DIMMs	X	X	X
I/O modules, such as HDDs, PEMs, REMs*, RFEMs*	X	X	X
Motherboard (MB)	X	X	X
Power Supply Units (PSUs)	X	X	Does not apply**
Fans (FM)	X	X	Does not apply**

* These I/O modules apply only to Sun Blade server modules.

** These devices for server modules are allocated power by the CMM. See TABLE 6-10 for details.

You can monitor the server power allocated components from the Power Management --> Distribution page in the ILOM SP web interface or from the `SP/powermgmt/powerconf` CLI target in the ILOM SP CLI. An example of the Power Management --> Distribution page is shown FIGURE 6-12.

FIGURE 6-12 Power Management --> Distribution Tab - ILOM SP 3.0.6



Power Distribution

View and configure the power distribution from this page.

Allocated Power: 4631 watts
Power allocated to all power-consuming components in the system (includes power permanently allocated for unmanaged I/O and fans).

Allocatable Power: 1769 watts
Power available to allocate to new blades.

Distribution Details

Each blade slot allocates a minimum of 146 watts to accommodate I/O blades.

Blade Slot Power Distribution

	Blade Slot	Allocated Power (Watts)	Permitted Power (Watts)
-	Blade Slots (total)	3175	-
○	BL0	435	1200
○	BL1	410	1000
○	BL2	268	1200
○	BL3	309	1200
○	BL4	268	1200
○	BL5	506	1200

For more details about how to view the server or CMM power allocation, see the sections about View Server Component Power Allocation or View CMM Component Power Allocation in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*.

Update: As of ILOM 3.0.8 the Distribution tab is replaced by the Allocation tab. For more details, see "Power Management --> Distribution Tab Renamed to Allocation Tab as of ILOM 3.0.8 (Server SP)" on page 96 or "Power Management --> Distribution Tab Renamed to Allocation Tab as of ILOM 3.0.10 (CMM)" on page 98.

Monitoring CMM Power Allocated Components

TABLE 6-10 identifies the components that are allocated power in ILOM by the CMM in your Sun system chassis. For each component listed in TABLE 6-10, ILOM provides an allocated CMM power value in wattage that represents the sum of the maximum power consumed by either a single CMM component (a blade), a category of CMM components (all blades), or all CMM power-consuming components. It also provides a permitted CMM power value in wattage that represents the guaranteed maximum power the CMM component (or component category) can consume.

Note – The *Permitted Power* value in ILOM is derived from the *Power Supply Redundancy Policy* and the *Redundant Power* available (for details see,"Power Supply Redundancy for CMM Systems as of ILOM 3.0.6" on page 107). The CMM continuously monitors and tracks all the `Allocated Power` to the system, as well as the `Allocatable Power` remaining and it ensures that the sum for these numbers (allocated and allocatable) never exceeds the chassis *Permitted Power* value.

Note – Power to a Sun Blade server module is allocated by the CMM when a request for power is made by the server module. The server module requests power whenever it is powered on, and releases power back to the CMM whenever it is powered off. The CMM allocates power to the server module if the remaining allocatable power is sufficient to meet the server module's request. The CMM also checks whether there is a limit set to the amount of power that it is permitted to a server module (which is known as the *Blade Slot Permitted Power* in the web interface or `CMM/powermgmt/powerconf/bladeslots/BL`*n* `permitted_power` in the CLI). The CMM only allocates power to the server module if the requested power is less than or equal to this property.

TABLE 6-10 CMM Power Allocated Components

CMM Power Allocated Component	Allocated Power (Watts)	Permitted Power (Watts)	Allocatable 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)	X	Does not apply	Does not apply
Fans (FM)	X	Does not apply	Does not apply

* The `permitted power` allocated to blade slots is user configurable.

You can monitor the power allocated CMM components from the Power Management --> Distribution page in the ILOM CMM web interface or from the `CMM/powermgmt/powerconf` CLI target in the ILOM CMM CLI. For instructions, see the section about View CMM Component Power Allocation in one of the following guides.

- *Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*

- *Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

In addition to monitoring the power allocation for each CMM power allocated component, you can modify the permitted (maximum) power the CMM allocates to blade slots within the chassis. For instructions, see the section about Configure Permitted Power for Blade Slots in one of the following guides:

- *Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Component Power Allocation Special Considerations

When monitoring the server or CMM power allocated components, consider the following information:

- **Power allocation for component categories**. For component categories that include multiple components, such as fans, you will be able to monitor the total sum of power consumed by all components (fans), as well as the total sum of power consumed by an individual component (fan).
- **Hot-pluggable component power allocation**. ILOM automatically displays a pre-allocated maximum power value for any known component that can be placed in a hot-plug component location either on a server or on a system chassis. For example:
  - A hot-pluggable component location on an Oracle Sun server could include storage slots for hard disk drives (HDDs). In this case, ILOM will display a maximum power value for the HDD to be placed in the storage slot.
  - A hot-pluggable component location on a system chassis (with a CMM) can include blade slots for server modules or I/O server modules. In this case, ILOM will display a maximum power value for any I/O server module that could be placed in the blade slots. However, if I/O server modules are not supported in the system chassis, then ILOM will display a maximum power value for a server module (and not an I/O server module).

  For more information about which locations or components on your server or CMM chassis system are hot-pluggable, refer to the platform documentation shipped with your system.
- **Power supply power allocation**. ILOM automatically allocates power to the power supply to account for power losses between the wall outlet and the component.
- **Troubleshooting Sun Blade server module power-on issues.** If the Sun Blade server module is unable to power on, verify that the SP `permitted power` property value (`/SP/powermgmt permitted_power`) is not more than the CMM blade slot `permitted power` property value (`/CMM/powermmgt/powerconf/bladeslots/BL`*n* `permitted_power`).

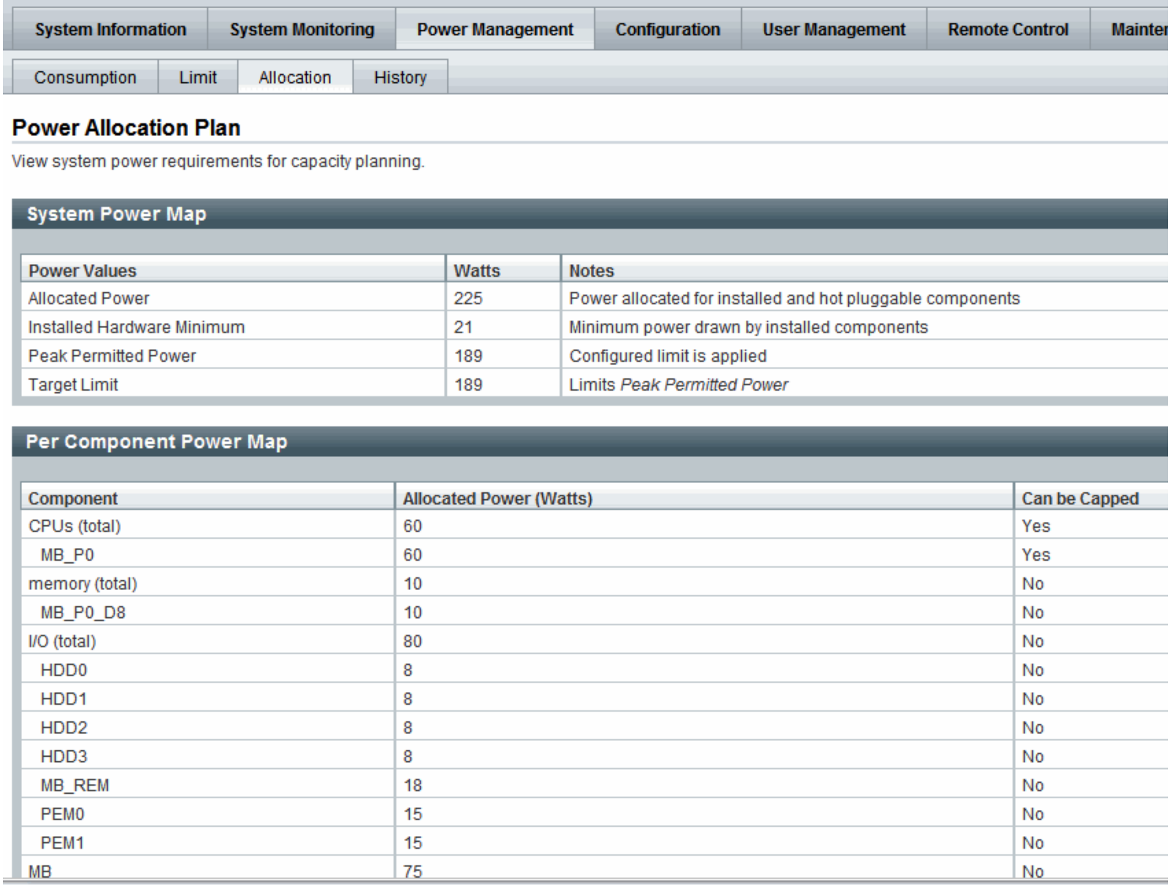
Note – ILOM 3.x server modules negotiate with the CMM and honor the permitted power restriction. Pre-3.x ILOM server modules will power on as long as there is enough allocatable power. Therefore, the permitted power constraint is only honored by server modules running ILOM 3.x or subsequent release.

Power Management --> Distribution Tab Renamed to Allocation Tab as of ILOM 3.0.8 (Server SP)

The Distribution tab that was previously available for the server SP in ILOM 3.0.6 (shown in FIGURE 6-12) was renamed in ILOM 3.0.8 to the Allocation tab (shown in FIGURE 6-13).

The Allocation tab, in ILOM 3.0.8, provides all the same power requirement information previously available on the Distribution tab in ILOM 3.0.6 (shown in FIGURE 6-12). However, the Allocation tab uses two tables to separate the system power requirements from the component power requirements (shown in FIGURE 6-13)

FIGURE 6-13 Power Management --> Allocation Tab - ILOM SP 3.0.8



Power Allocation Plan

View system power requirements for capacity planning.

System Power Map

Power Values	Watts	Notes
Allocated Power	225	Power allocated for installed and hot pluggable components
Installed Hardware Minimum	21	Minimum power drawn by installed components
Peak Permitted Power	189	Configured limit is applied
Target Limit	189	Limits *Peak Permitted Power*

Per Component Power Map

Component	Allocated Power (Watts)	Can be Capped
CPUs (total)	60	Yes
MB_P0	60	Yes
memory (total)	10	No
MB_P0_D8	10	No
I/O (total)	80	No
HDD0	8	No
HDD1	8	No
HDD2	8	No
HDD3	8	No
MB_REM	18	No
PEM0	15	No
PEM1	15	No
MB	75	No

Updated Server SP Power Allocation Web Procedure

For instructions for viewing the server power allocations in ILOM, see the section about View Server Power Allocation Plan in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*.

Power Management --> Distribution Tab Renamed to Allocation Tab as of ILOM 3.0.10 (CMM)

The Distribution tab that was previously available for the CMM in ILOM 3.0.6 (shown in FIGURE 6-12) was renamed in ILOM 3.0.10 to the Allocation tab (shown in FIGURE 6-14).

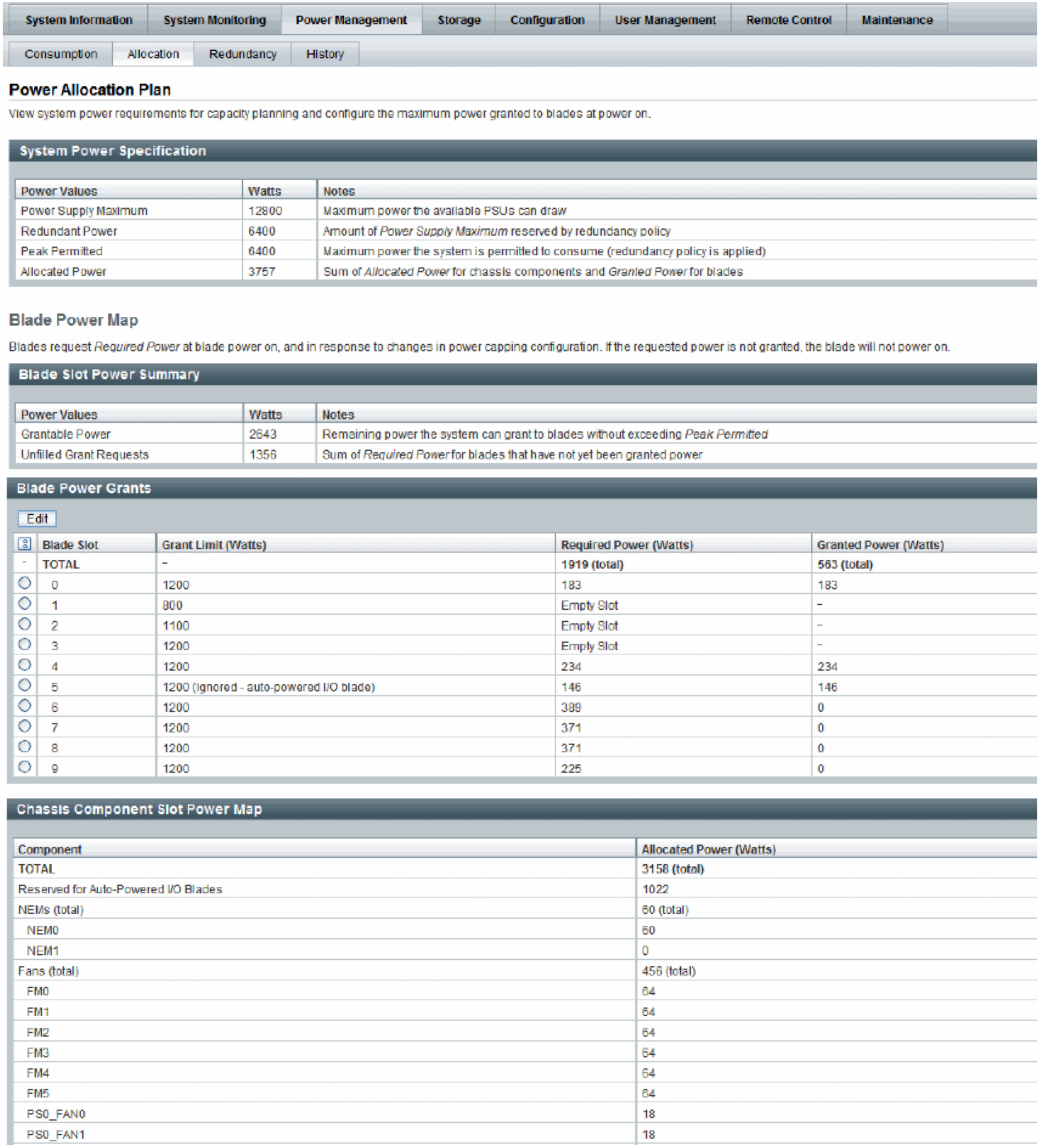
The Allocation tab, in ILOM 3.0.10, provides all the same power requirement information previously available on the CMM Power Distribution tab in ILOM 3.0.6. However, the new CMM Allocation tab in ILOM 3.0.10 provides two additional tables that identify the System Power Specifications and the Blade Power Grants (as shown in FIGURE 6-14).

TABLE 6-11 defines the property changes made on the CMM Allocation Tab as of 3.0.10.

TABLE 6-11 New or Revised Properties on CMM Allocation Tab

Updated Property Name	Details
Grantable Power (renamed property)	Allocatable Power in ILOM 3.0.6 was renamed to Grantable Power in ILOM 3.0.10. Grantable Power indicates the total remaining power (watts) available from the CMM to allocate to blade slots without exceeding grant limit.
Grant Limit (renamed property)	Permitted Power in ILOM 3.0.6 was renamed to Grant Limit in ILOM 3.0.10. Grant Limit represents the maximum power the system will grant to a blade slot. For instructions for setting the grant limit on a blade see, the procedure for Configure Grant Limit for Blade Slots in the *Oracle Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*.
Granted Power (renamed property)	Allocated Power in ILOM 3.0.6 was renamed to Granted Power in ILOM 3.0.10. Granted Power represents the sum of the maximum power consumed by either a single server component (such as a memory module), a category of server components (all memory modules), or all server power-consuming components.

FIGURE 6-14 Power Management -> Allocation Tab - ILOM CMM 3.0.10



Power Allocation Plan

View system power requirements for capacity planning and configure the maximum power granted to blades at power on.

System Power Specification

Power Values	Watts	Notes
Power Supply Maximum	12800	Maximum power the available PSUs can draw
Redundant Power	6400	Amount of *Power Supply Maximum* reserved by redundancy policy
Peak Permitted	6400	Maximum power the system is permitted to consume (redundancy policy is applied)
Allocated Power	3757	Sum of *Allocated Power* for chassis components and *Granted Power* for blades

Blade Power Map

Blades request *Required Power* at blade power on, and in response to changes in power capping configuration. If the requested power is not granted, the blade will not power on.

Blade Slot Power Summary

Power Values	Watts	Notes
Grantable Power	2643	Remaining power the system can grant to blades without exceeding *Peak Permitted*
Unfilled Grant Requests	1356	Sum of *Required Power* for blades that have not yet been granted power

Blade Power Grants

	Blade Slot	Grant Limit (Watts)	Required Power (Watts)	Granted Power (Watts)
-	TOTAL	-	1919 (total)	563 (total)
○	0	1200	183	183
○	1	800	Empty Slot	-
○	2	1100	Empty Slot	-
○	3	1200	Empty Slot	-
○	4	1200	234	234
○	5	1200 (ignored - auto-powered I/O blade)	146	146
○	6	1200	389	0
○	7	1200	371	0
○	8	1200	371	0
○	9	1200	225	0

Chassis Component Slot Power Map

Component	Allocated Power (Watts)
TOTAL	3158 (total)
Reserved for Auto-Powered I/O Blades	1022
NEMs (total)	60 (total)
NEM0	60
NEM1	0
Fans (total)	456 (total)
FM0	64
FM1	64
FM2	64
FM3	64
FM4	64
FM5	64
PS0_FAN0	18
PS0_FAN1	18

Revised CLI Power Allocation Properties as of ILOM 3.0.10

A summary of the CLI changes that were made in ILOM 3.0.10 to the CMM power configuration is provided in TABLE 6-12.

TABLE 6-12 New Power Management CLI Properties in ILOM 3.0.10

Renamed CLI Properties	Details

`allocated_power` renamed to `granted_power` for blade slots	The following CLI `allocated_power` property for all blade slots in ILOM 3.0.6:
	`/CMM/powermgmt/powerconf/bladeslot allocated_power`
	changed in ILOM 3.0.10 to `granted_power`:
	`/CMM/powermgmt/powerconf/bladeslot granted_power`

`allocated_power` renamed `granted_power` for blades	The following CLI `allocated_power` property for blades in ILOM 3.0.6:
	`/CMM/powermgmt/powerconf/bladeslot/BL`*n* `allocated_power -> granted_power`
	changed in ILOM 3.0.10 to `granted_power`:
	`/CMM/powermgmt/powerconf/bladeslot/BL`*n* `granted_power`

`permitted_power` renamed `grant_limit` for blades	The following CLI `permitted_power` property for blades in ILOM 3.0.6:
	`/CMM/powermgmt/powerconf/bladeslot/BL`*n* `permitted_power`
	changed in ILOM 3.0.10 to `grant_limit`:
	`/CMM/powermgmt/powerconf/bladeslot/BL`*n* `grant_limit`

For instructions for using these latest CLI properties to view granted power or grant limit per blade, see the procedures about View Granted Power or Grant Limit in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*.

Power Budget as of ILOM 3.0.6 for Server SPs

Note – The Power Budget properties described in this section are replaced in the web interface with the Limit tab properties as of ILOM 3.08. For updated details, see.

Some Oracle server platforms support a power budget. A power budget sets a limit on the system's power consumption. The system applies power capping when power consumption exceeds the power limit and guarantees that the maximum power consumption will not exceed the system's `Permitted Power`.

You can configure a power budget and then, at a later time, enable or disable the configuration properties that are set. After a power budget is enabled, the ILOM SP monitors the power consumption and applies power capping when needed. Power capping is achieved by limiting the maximum frequency at which the CPUs run. The ILOM SP coordinates this process with the operating system (OS) to ensure that the OS can continue applying its own power management policies within the set limit.

Power budget settings in ILOM are saved across all SP reboots and host power-off and power-on states. During an SP reboot, the applied power capping budget that is in effect will remain. After the SP completes the reboot process, power capping is then automatically adjusted, as needed, by the system.

ILOM's ability to achieve a power budget depends on the workload running on the system. For example, if the workload is causing the system to operate near the maximum power consumption, ILOM will be unable to achieve a budget that is close to the minimum power consumption. If ILOM is unable to achieve the set `Power Limit`, it will automatically generate a violation notification.

Power Budget topics described in this section include:

- "Why Use a Power Budget?" on page 102
- "Server Power Budget Properties as ILOM 3.0.6" on page 102
- "Advanced Server Power Budget Features as of ILOM 3.0.6" on page 103

For information about configuring Power Budget properties in the ILOM, see the section about Configure Server Power Budget Properties in one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Why Use a Power Budget?

The Power Budget feature in ILOM helps you to better plan and manage the power required for your data center. Typically the power allocated to a server is based on the nameplate power, as provided by the `/SP/powermgmt allocated_power` property.

The most effective way to use the Power Budget feature in ILOM is to:

1. Determine the workload that will operate on the Oracle server.
2. Set the `Power Limit` property in ILOM that is near (for example, at or slightly above) to the workload's normal operating power consumption.
3. Use the `Power Limit` property value to help plan the amount of power that will need to be allocated in your data center for this system.

Server Power Budget Properties as ILOM 3.0.6

TABLE 6-13 identifies the server power budget properties that you can view or configure from the CLI or web interface in ILOM.

TABLE 6-13 Server Power Budget Properties as of ILOM 3.0.6

Power Budget Property	Description
Activation State	Enable this property to enable the power budget configuration.
Status	The Status reports one of the following current power budget states: • **OK** – The OK status appears when the system is able to achieve the power limit, or when the power budget is not enabled. • **Violation** – The Violation status occurs when the system is not able to reduce power to the power limit. If the power consumption falls below the `Power Limit`, the violation is cleared and the status returns to `ok`. The budget status is also reported through a system sensor: `/SYS/PWRBS`. This is a discreet sensor which is set to `1` (deasserted) when the budget is `ok`, and to `2` (asserted) when the budget has been violated.

TABLE 6-13 Server Power Budget Properties as of ILOM 3.0.6 *(Continued)*

Power Budget Property	Description
Power Limit	Set a Power Limit in watts or as a percentage of the range between minimum and maximum system power. **Note -** The minimum system power is viewable in the CLI under the target /SP/powermgmt/budget min_powerlimit. The maximum system power is viewable from the Allocated Power property in the web interface or from the CLI under the target /SP/powermgmt allocated_power.

Advanced Server Power Budget Features as of ILOM 3.0.6

The advanced server power budget features in ILOM include properties for Time Limit and Violation Actions. These property settings (see TABLE 6-14) enable you to control the aggressiveness of power capping, and to configure a system action in response to a violated budget.

The server power budget is designed to ensure that power capping is not applied until the Power Limit is exceeded. The Time Limit property specifies the grace period for capping power to within the Power Limit, if exceeded. The system provides a default grace period that is set to achieve responsiveness at the least cost to the system performance. When the default grace period is enabled for the Time Limit property, anomalous spikes are ignored and power capping is applied only when power consumption remains above the Power Limit. If you specify a different grace period than the default grace period provided, the user-modified grace period could cause ILOM to increase or decrease the power cap severity in response to exceeding the Power Limit.

Server modules are allocated power by the chassis CMM, and must guarantee to not exceed this allocated amount. It might be necessary to reduce the server module's guaranteed maximum power to allow the server module to power on, or there might be some other administrative reason for requiring that the server power never exceeds a watts value. Setting the budget grace period to None instructs ILOM to permanently apply power capping to ensure that the Power Limit is never exceeded, at the cost of limited performance. If ILOM can guarantee the Power Limit with a grace period of None, it reduces the value of the Permitted Power property to reflect the new guaranteed maximum power. If the power limit or grace period is later increased, the Permitted Power value on a rackmount server is increased. However, the Permitted Power value for a Sun Blade server module will only increase if the chassis CMM is able to provide the server module with additional power.

TABLE 6-14 identifies the advanced server power budget property settings that you can view or configure from the ILOM CLI or web interface.

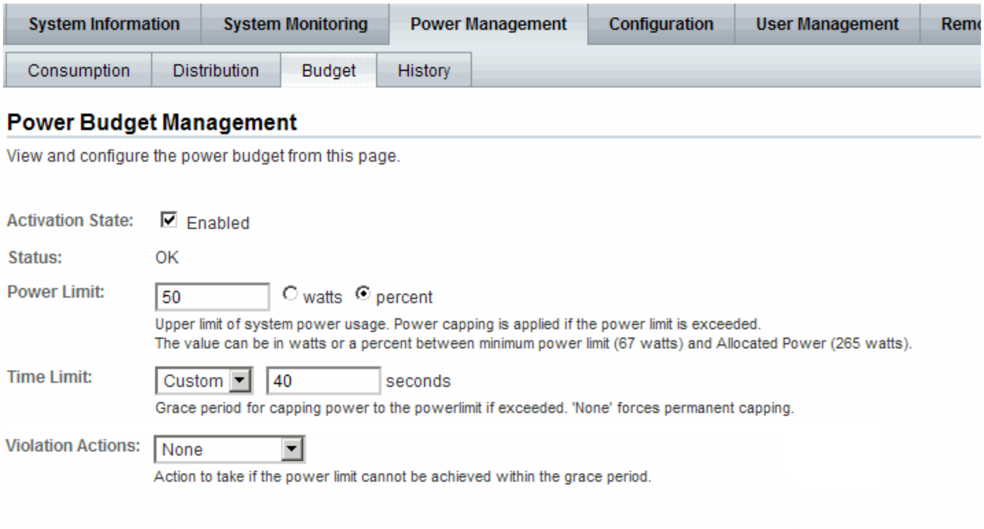
TABLE 6-14 Advanced Server Power Budget Properties as of ILOM 3.0.6

Power Budget Property	Description
Time Limit	Specify one of the following grace periods for capping the power usage to the limit: • **Default** – Platform selected optimum grace period. • **None** – No grace period. Power capping is permanently applied. • **Custom** – User-specified grace period.
Violation Actions	The actions that the system will take if the power limit cannot be achieved within the grace period. This option can be set to `None` or `Hard Power Off`. This setting, by default, is set to `None`.

Note – For best power capping performance, the default values are recommended for all advanced server power budget properties.

An example of the web interface Power Management --> Budget properties is shown in FIGURE 6-15.

FIGURE 6-15 SP - Power Management Budget Tab - ILOM 3.0.6



Power Budget Management

View and configure the power budget from this page.

Activation State: ☑ Enabled

Status: OK

Power Limit: 50 ○ watts ● percent

Upper limit of system power usage. Power capping is applied if the power limit is exceeded.
The value can be in watts or a percent between minimum power limit (67 watts) and Allocated Power (265 watts).

Time Limit: Custom 40 seconds

Grace period for capping power to the powerlimit if exceeded. 'None' forces permanent capping.

Violation Actions: None

Action to take if the power limit cannot be achieved within the grace period.

For instructions about how to view or configure the server and advanced server power budget properties in ILOM, see the section about Configure Server Power Budget Properties in one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Power Management --> Budget Tab Renamed to Limit Tab as of ILOM 3.0.8

The Budget tab that was previously available for server SPs in ILOM 3.0.6 was renamed in ILOM 3.0.8 to the Limit tab (shown in FIGURE 6-16).

The Limit tab in ILOM 3.0.8 provides all the same SP power capping information that was previously available on the Budget tab. However, some of the previous power capping properties have been renamed on the Power Management --> Limit tab in ILOM 3.0.8. For more details about the property changes made to the Limit tab, see TABLE 6-15.

TABLE 6-15 Limit Tab Server SP Setting Changes in ILOM 3.0.8

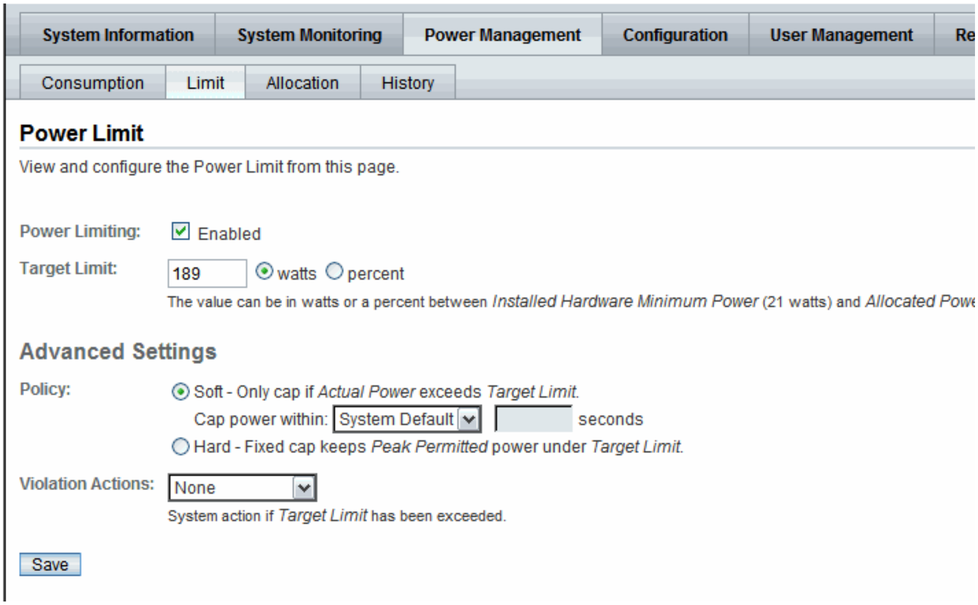
Limit Tab Property Changes	Details
`Power Limiting` (renamed property)	The `Activation State` property on the Budget tab in ILOM 3.0.6 (shown in FIGURE 6-15) was renamed to `Power Limiting` on the Power Management --> Limit tab in ILOM 3.0.8. The `Powering Limiting [] enable` property (shown in FIGURE 6-16) when selected enables the power limit configuration.
`Status Error Message` (replaces `Status` property)	The `Status` read-only property previously available on the Budget tab in ILOM 3.0.6 (shown in FIGURE 6-15) was replaced by a new `Status Error Message` on the Power Management --> Limit tab or Consumption tab in ILOM 3.0.8 (shown in FIGURE 6-16). The new `Status Error Message` only appears on your system when ILOM fails to achieve the power limit that was configured.
`Target Limit` (renamed property)	The `Power Limit` property on the Budget tab in ILOM 3.0.6 (shown in FIGURE 6-15) was renamed to `Target Limit` on the Power Management --> Limit tab in ILOM 3.0.8. The `Target Limit` property (shown in FIGURE 6-16) enables you to specify the a target limit value in watts or as a percentage. This value must be a range between the minimum and maximum system power.

TABLE 6-15 Limit Tab Server SP Setting Changes in ILOM 3.0.8 *(Continued)*

Limit Tab Property Changes	Details
`Policy` (renamed advanced property)	The `Time Limit` property on the Budget tab in ILOM 3.0.6 (shown in FIGURE 6-15) was renamed to `Policy` on the Power Management --> Limit tab in ILOM 3.0.8. The `Policy` property (shown in FIGURE 6-16) enables you to specify the type of power capping to apply: • **Soft** - `Only cap if actual power exceeds Target Limit` – If you enabled the soft cap option, you can configure the grace period for capping Actual Power to within the Target Limit. - `System Default` – Platform selected optimum grace period. *or* - `Custom` – User-specified grace period. • **Hard** - `Fixed cap keeps Peak Permitted power under Target Limit` – If you enabled this option, power capping is permanently applied without a grace period.

An example of the new Power Management --> Limit tab properties that are available for server SPs as of ILOM version 3.0.8 is shown in FIGURE 6-16.

FIGURE 6-16 Power Management --> Limit Tab - ILOM SP 3.0.8



Power Limit

View and configure the Power Limit from this page.

Power Limiting: ☑ Enabled

Target Limit: 189 ● watts ○ percent

The value can be in watts or a percent between *Installed Hardware Minimum Power* (21 watts) and *Allocated Powe*

Advanced Settings

Policy: ● Soft - Only cap if *Actual Power* exceeds *Target Limit*.

Cap power within: System Default seconds

○ Hard - Fixed cap keeps *Peak Permitted* power under *Target Limit*.

Violation Actions: None

System action if *Target Limit* has been exceeded.

Updated Power Limit Configuration Procedure

For information about configuring Power Limit properties in ILOM, see the section about Configure Server Power Limit Properties in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*.

Power Supply Redundancy for CMM Systems as of ILOM 3.0.6

From the ILOM CMM CLI or web interface you can view and configure the following power supply redundancy options:

- **Power Supply Redundancy Policy** – This policy controls the number of power supplies that are currently allocating power in addition to the number of power supplies that are reserved to handle power supply failures. Values for this redundancy policy property can be set to:
  - **None** – Reserves no power supplies.
  - **n+n** – Reserves half of the power supplies to handle power supply failures.
- **Redundant Power** – This value is provided by the system. It represents the available power that is not allocated.

To view or configure the CMM power supply redundancy options in the ILOM CLI or web interface, see the section about View or Configure CMM Power Supply Redundancy Properties in one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Platform-Specific CMM Power Metrics as of ILOM 3.0.6

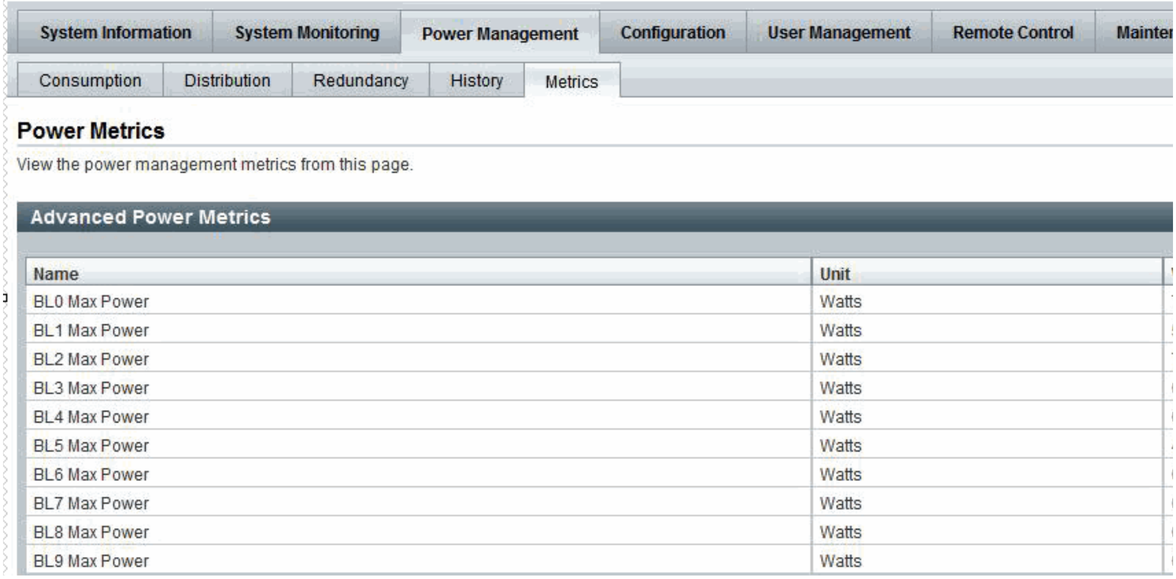
Note – As of ILOM 3.0.10, the CMM Power Metrics tab was removed from the ILOM CLI and web interface.

As of ILOM version 3.0.6, advanced power metrics are available in some Oracle systems from the ILOM CMM CLI or web interface. These metrics represent the maximum allocated power value for each blade slot. For empty slots or slots with I/O server modules, the value presented by ILOM represents the maximum power that an I/O server module could consume.

To determine whether your CMM system supports this ILOM 3.0.6 feature, refer to the platform ILOM Supplement for your server or CMM.

For Oracle systems supporting the CMM advanced power metrics, you can view the power metrics in the Power Management --> Metrics page of the ILOM web interface (FIGURE 6-17) or from the ILOM CLI under the target `/CMM/powermgmt/advanced/BL`*n*.

FIGURE 6-17 Sample Power Management Metrics Page



Power Metrics

View the power management metrics from this page.

Advanced Power Metrics

Name	Unit
BL0 Max Power	Watts
BL1 Max Power	Watts
BL2 Max Power	Watts
BL3 Max Power	Watts
BL4 Max Power	Watts
BL5 Max Power	Watts
BL6 Max Power	Watts
BL7 Max Power	Watts
BL8 Max Power	Watts
BL9 Max Power	Watts

CHAPTER 7

ILOM Back Up and Restore Operations

Topics

Description	Links
Learn about ILOM's configuration management features	• "ILOM Configuration Management Tasks" on page 110 • "Backup and Restore Operations" on page 111 • "Reset to Defaults Feature" on page 112

Related Topics

For ILOM	Chapter or Section	Guide
• CLI	• Backing Up and Restoring ILOM Configuration • Updating ILOM Firmware	*Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* (820-6412)
• Web interface	• Backing Up and Restoring ILOM Configuration • Updating ILOM Firmware	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)

The ILOM 3.0 Documentation Collection is available at: `http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`

ILOM Configuration Management Tasks

ILOM's configuration management tasks enable you to:

- Back up the ILOM configuration to a XML file on a remote system.
- Use the backup file to restore ILOM to the backed up configuration.
- Use the backup file to install the backed up configuration on other ILOM SPs.
- Reset the ILOM configuration to the default settings.

You can use the Backup and Restore and Reset to Defaults features together in the following ways:

- Save the ILOM configuration to a backup XML file, reset the ILOM configuration to the default settings, and use the command-line interface (CLI) or web interface to create a new ILOM configuration.
- Reset the ILOM configuration to the default settings and restore it using a known good ILOM configuration backup file.
- Use the CLI or web interface to create a new ILOM configuration, save the ILOM configuration to a backup XML file, edit the XML file to remove settings that are unique to a particular system, and perform restore operations to load the backup file to other systems.

Given the above capabilities, the following use cases describe how you might typically use these features:

- You changed your ILOM configuration but it no longer works and you want to recover ILOM by restoring it to a known good configuration. To do this, first reset the ILOM configuration to the default settings and then perform a Restore operation using the known good configuration.
- You want to use the Backup and Restore feature to replicate an ILOM configuration onto other systems. To do this, create a standard ILOM configuration, back up the configuration, edit the backed up XML file to remove settings that are unique to a particular system (for example, the IP address), then perform Restore operations to replicate the configuration onto the other systems.
- You created a minimum ILOM configuration but to make it complete you need to configure a number of users (ILOM supports a maximum of 10 active user sessions per service processor). If you have backed up a configuration previously that has the same users, you can edit the XML file so that it only includes the user information and then simply perform a Restore operation to overlay the minimum configuration with the configuration that has the user accounts. Reuse of large network configurations such as Active Directory is another use case for this approach.

You can use either the web interface or the CLI to perform configuration management tasks in ILOM. For more information about these tasks, see:

- "Backup and Restore Operations" on page 111
- "Reset to Defaults Feature" on page 112

Backup and Restore Operations

ILOM supports two separate operations for backup and restore.

- The Backup operation consists of gathering the current ILOM configuration data into an XML file and transferring that file to a remote system.
- The Restore operation consists of retrieving the XML backup file and using it to restore the ILOM SP to the backed up configuration.

Thus you can use Backup and Restore to save the ILOM configuration to a backup XML file, and later restore the backup file to the same system. Further, if you want to use the backup XML file on other systems, you can edit the XML file to remove or change settings that are unique, such as the IP address. The backup XML file is readable and can be edited manually.

Caution – If you are going to restore the edited backup XML file to the same system, you should reset the ILOM configuration to the default settings; otherwise, the restored configuration will simply overlay the current configuration. If you are going to restore the edited backup XML file to others systems that already contain an ILOM configuration, you should erase the ILOM configuration unless you want to overlay the current configuration. To erase the current ILOM configuration, you must reset the ILOM configuration to the default settings. For instructions, see "Reset the ILOM Configuration to Defaults" in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*, or in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*.

All of the information that can be configured on the system can be backed up. The privileges assigned to the user account that is used to execute the Backup operation determine how much of the configuration is included in the backup XML file. For security reasons, if the user account used to execute the Restore operation has fewer privileges than the account used to create the backup file, some of the configuration might not be restored. For each configuration property that is not restored due to lack of privileges, a log entry is created. Therefore, one way to verify that all the configuration properties were restored is to check the event log.

You can also limit the amount of information included in the backup XML file by using user accounts that have limited privileges. For example, an account assigned the Admin (a), User Management (u), Console (c), Reset and Host Control (r), and Read Only (o) roles would have full privileges and would create the most complete configuration backup file. For this reason, it is recommended that user accounts assigned the `a,u,c,r,o` roles be used whenever you perform Backup and Restore operations.

Configuration Backup and Restore operations do not change the power state of the host operating system. However, both operations cause all sessions on the ILOM SP to be momentarily suspended until the Backup or Restore operation completes. A Backup or Restore operation typically lasts two to three minutes, after which all logged in sessions resume normal operation.

For instructions on performing Backup and Restore operations and editing a backup XML file, see “Backing Up and Restoring ILOM Configuration” in the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Reset to Defaults Feature

With the Reset to Defaults feature in ILOM, you can reset the ILOM configuration settings to their default settings. When you use this feature you are given three options:

- **All** – Select this option if you want to erase the existing ILOM configuration file. When the ILOM SP reboots, the configuration file that was included in the SP firmware is used instead.
- **Factory** – Select this option if you want to erase the existing configuration file and the internal log files. When the ILOM SP reboots, the configuration file that was included in the SP firmware is used instead and the internal log files are erased.
- **None** – Select this option if you want to cancel the reset operation you initiated previously. To cancel a previously initiated reset operation you must initiate a reset operation with the None option before the ILOM SP reboots.

Note – When you execute an ILOM configuration reset, the reset configuration does not take effect until the ILOM SP reboots.

For instructions on resetting the ILOM configuration to the default settings, see “Reset the ILOM Configuration to Defaults” in the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

CHAPTER 8

ILOM Firmware Update Operations

Topics

Description	Links
Learn about ILOM's firmware update operations	• "ILOM Firmware Compatibility and Update Operations" on page 114 • "ILOM 3.0 Firmware on the Server SP" on page 114 • "ILOM 3.0 Firmware on the CMM" on page 114 • "ILOM Firmware Updates" on page 115 • "Process for Updating the Firmware" on page 116 • "ILOM Firmware Update - Preserve Configuration Option" on page 116 • "Troubleshoot the Firmware Update Session If Network Failure Occurs" on page 117

Related Topics

For ILOM	Chapter or Section	Guide
• IPMI and SNMP hosts	• Configuring ILOM Firmware Settings	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide* (820-6413)
• CLI and Web interface (CMM only)	• Firmware Update Procedures	*Oracle Integrated Lights Out Manager (ILOM) CMM Administration Guide for Sun Blade 6000 and Sun Blade 6048 Modular Systems* (820-0052)

The ILOM 3.0 Documentation Collection is available at:
`http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`

ILOM Firmware Compatibility and Update Operations

To download the latest version of ILOM or to determine the ILOM firmware compatibility for your server or chassis monitoring module (CMM), go to the following site:

`http://www.sun.com/systemmanagement/ilom_platforms.jsp`

For additional information about managing and updating ILOM firmware on the server SP or CMM, see these topics:

- "ILOM 3.0 Firmware on the Server SP" on page 114
- "ILOM 3.0 Firmware on the CMM" on page 114
- "ILOM Firmware Updates" on page 115
- "Process for Updating the Firmware" on page 116
- "ILOM Firmware Update - Preserve Configuration Option" on page 116
- "Troubleshoot the Firmware Update Session If Network Failure Occurs" on page 117

ILOM 3.0 Firmware on the Server SP

The ILOM 3.0 firmware on the SP provides administrators with full lights-out management for an Oracle server. This includes the ability to power cycle the server, set up a network connection, create and manage user accounts and roles, as well as monitor and maintain the server components locally or remotely.

ILOM 3.0 Firmware on the CMM

The ILOM 3.0 firmware on the CMM is the primary point of management for all chassis components and functions in a Sun Blade Modular System Chassis. It provides complete monitoring and management functionality for the components, including server module management, system power management, as well as hot-plug operations of infrastructure components such as power supply modules, fan modules, server modules, and network express modules.

Note – As of ILOM 3.0.10, a new feature is available to manage firmware updates for Oracle Sun Modular System Chassis components. For information and procedures for updating ILOM firmware on the CMM for chassis components, refer to the *Oracle Integrated Lights Out Manager (ILOM) CMM Administration Guide for Sun Blade 6000 and Sun Blade 6048 Modular Systems* (820-0052).

ILOM Firmware Updates

To ensure that your system has the latest features and product enhancements installed, it is highly recommended that you update the ILOM firmware on your system with the latest ILOM firmware release that is available.

Updating the firmware on your system to a prior release is *not* recommended. However, if you determine you need to run an earlier version of the firmware on your system, you can update the firmware to any prior firmware release that is available for download.

Prior to updating the ILOM firmware, you should identify the ILOM firmware version that is running on the server SP or CMM.

If you determine you are running ILOM 3.0 firmware on your server or CMM, refer to any of the following ILOM 3.0 guides for instructions for updating the ILOM firmware.

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) CMM Administration Guide for Sun Blade 6000 and Sun Blade 6048 Modular Systems*
- ILOM Supplement guide or platform Administration guide provided for your server

Note – For information about the firmware version numbering scheme used for ILOM 3.0, see "ILOM 3.0 Firmware Version Numbering Scheme" on page xiii.

If you determine that you have ILOM 2.x installed on your server or CMM and you are updating to a later ILOM 2.x version, you need to refer to the *Oracle Integrated Lights Out Manager 2.0 User's Guide* to find the firmware update procedures for ILOM 2.x.

Process for Updating the Firmware

The process for updating the firmware version installed on your Sun server or CMM involves:

1. Downloading the firmware image for your server or CMM from the Sun platform's product web site and place the image on your TFTP, FTP, or HTTP server.

2. If required by your platform, shut down the host operating system before changing the firmware on your server SP.

3. Logging in to ILOM using an Admin (a) role account.

4. Loading the firmware image on the server SP (or CMM) using the ILOM CLI or the web interface.

5. Optionally, preserve the current configuration in ILOM. For more information, see "ILOM Firmware Update - Preserve Configuration Option" on page 116

6. Verifying that the appropriate firmware version was installed after the system reboots.

ILOM Firmware Update - Preserve Configuration Option

When updating to a later firmware release, the Preserve Configuration option (when enabled) saves your existing configuration in ILOM and restores the configuration after the update process completes.

Note – The term *configuration* refers to the settings configured in ILOM by a user. These settings can include user management settings, SP network settings, serial port settings, alert management configurations, remote management configurations, and so on.

If you are updating to a prior firmware release and ILOM detects a preserved configuration for that release, the Preserve Configuration option (when enabled) reverts to the configuration for the prior release after the update process completes.

For example: If you update your system firmware from 3.0 to 2.0 and choose to enable Preserve Configuration during the update process, ILOM will:

- Determine whether a snapshot of the 2.0 configuration was previously preserved on the system.
- Restore the snapshot of the 2.0 configuration, if found, after the update process completes.

However, in this example, if ILOM is unable to locate the snapshot of the 2.0 configuration, the update process is stopped and the following error is reported:

```
The configuration matching the version cannot be restored.
Please retry without preserving config.

Firmware image update failed

load: Command Failed

->
```

To proceed, start the update process again and do not choose the Preserve Configuration option. When the update is complete and the system reboots, the ILOM default settings will be used.

Troubleshoot the Firmware Update Session If Network Failure Occurs

If you were performing the firmware update process using the ILOM web interface or CLI and a network failure occurs, ILOM will *not* reboot. You should *not* reboot the system. However, you should do the following:

1. Address and fix the network problem.
2. Reconnect to the ILOM SP.
3. Restart the update process.

CHAPTER 9

Remote Host Management Options

Topics

Description	Links
Identify the remote management options	• "Server SP Remote Management Options" on page 120
Learn about controlling the power state of a remote server	• "Remote Power Control" on page 120
Learn about redirecting storage media from the CLI on your local system to a remote host server	• "Storage Redirection CLI" on page 121 • "First Time Access" on page 121 • "Storage Redirection CLI Architecture" on page 122 • "Default Network Communication Port" on page 123
Learn about redirecting devices (keyboard, video display, mouse, storage) from the web interface on your local system to a remote host server	• "Oracle ILOM Remote Console" on page 123 • "Single or Multiple Remote Host Server Management Views" on page 124 • "Installation Requirements" on page 126 • "Network Communication Ports and Protocols" on page 127 • "Sign In Authentication Required" on page 127 • "CD and Diskette Redirection Operation Scenarios" on page 128
Learn about securing the ILOM Remote Console	• "ILOM Remote Console Computer Lock" on page 129
Learn how to control the host boot device on an x86 system SP	• "Host Control - Boot Device on x86 Systems" on page 131
Learn about Logical Domain (LDom) configurations on SPARC servers	• "ILOM Operations for LDom Configurations on SPARC Servers" on page 132

Related Topics

For ILOM	Chapter or Section	Guide
• CLI	• Managing Remote Hosts' Power States and Storage Redirection	*Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* (820-6412)
• Web interface	• Managing Remote Hosts' Power States and Redirection	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)

The ILOM 3.0 Documentation Collection is available at:
`http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`

Server SP Remote Management Options

As of ILOM 3.0, the remote management options in ILOM include:

- "Remote Power Control" on page 120
- "Storage Redirection CLI" on page 121
- "Oracle ILOM Remote Console" on page 123
- "ILOM Remote Console Computer Lock" on page 129
- "Host Control - Boot Device on x86 Systems" on page 131
- "ILOM Operations for LDom Configurations on SPARC Servers" on page 132

Information about each of these remote management options follows.

Remote Power Control

The remote power states in ILOM are available for all Oracle Sun servers from the ILOM CLI or web interface. These options enable you to control the power state of a remote host server or chassis.

For information about remotely managing the power states on a managed device, see the section about Managing Host Remote Power States in one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Storage Redirection CLI

The Storage Redirection CLI in ILOM is supported on all Oracle Sun x86 processor-based servers. This CLI is also supported on some SPARC processor-based servers. However, the Storage Redirection CLI is not supported on Sun server SPs or chassis monitoring modules (CMMs) running ILOM 2.0. It is also not supported on CMMs running ILOM 3.0; although, the CMM web interface still provides the download links to the Storage Redirection service and client CLI tools. Once the service and client tools are downloaded and running on your machine, they can be used for Storage redirection to a server module running ILOM 3.0.

The Storage Redirection CLI enables the storage devices (CD/DVD or ISO images) on your local client to behave as if they were directly attached to the remote host server. For instance, the redirection functionality enables you to locally perform these actions:

- Mount a storage device or image directly from your desktop to a remote SP host without launching the Oracle ILOM Remote Console application.
- Redirect media to use the `/SP/console` for text-based console interaction.
- Write scripts to start and stop storage redirection on multiple SP host servers.

Note – The Storage Redirection CLI is limited to remote media control. If you need to remotely manage other devices on a remote host server (such as the keyboard, video display, or mouse), you should use the Oracle ILOM Remote Console. For more information about the Oracle ILOM Remote Console, see "Oracle ILOM Remote Console" on page 123.

For instructions about how to launch and use the Storage Redirection CLI, see the section about "Managing Remote Host Storage Redirections" in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide.*

First Time Access

When you access the Storage Redirection CLI for the first time, you must sign in to the ILOM web interface to install the service and the client. After the service and client are installed on your system, you can subsequently start the service and launch the Storage Redirection CLI directly from a command window or terminal.

Note – You can, alternatively, choose to start the service directly from the ILOM web interface. If you choose to start the service from the ILOM web interface without installing it, you will need to subsequently access the ILOM web interface to start the service prior to launching the Storage Redirection CLI from a command window or terminal. For more information about how to install or start the service, see the section about "Managing Remote Hosts" in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*.

Storage Redirection CLI Architecture

The Storage Redirection CLI consists of a Java Web Start service and a scriptable, Java command-line client. You must start the service and initially install the client from the ILOM web interface. The Storage Redirection service runs in the background of your local client and establishes the connection between your local client and the remote host server. After a connection is established, you can locally launch the Storage Redirection CLI from a command window or terminal. The Storage Redirection CLI enables you to issue commands to the service for starting and stopping storage redirection.

FIGURE 9-1 Storage Redirection Service and Client

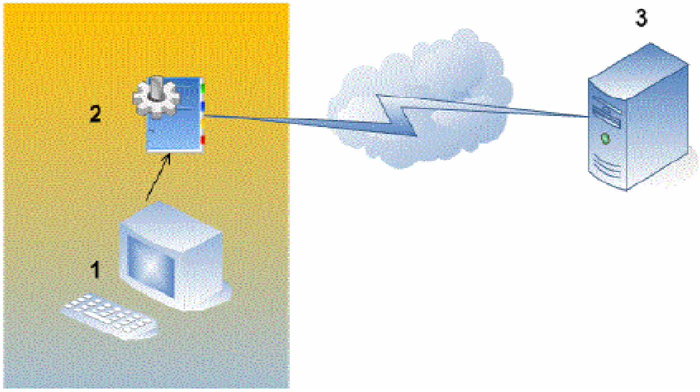


Figure Legend

1	Local client running Storage Redirection command-line client
2	Storage Redirection service running on local client
3	Remote host server

Note – You can only run one instance of the Storage Redirection service on your local system at one time. However, you can launch multiple Storage Redirection CLIs by issuing the Storage Redirection command (`-jar StorageRedir.jar`) from a local command window or terminal.

For instructions about how to launch and use the Storage Redirection feature in ILOM, see the section about Managing Remote Host Storage Redirections in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*

Default Network Communication Port

The default network communication port provided for Storage Redirection CLI is 2121. This default socket port enables the Storage Redirection CLI to communicate over the network with a remote host server SP. If you need to change the default network port, you must edit the `Jnlpgenerator-cli` file to manually override the default port number (2121).

For more information about how to edit the network port number that is referenced in the `Jnlpgenerator-cli` file, see "Change the Default Storage Redirect Port: 2121" in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*.

Oracle ILOM Remote Console

The Oracle ILOM Remote Console is supported on all Sun x86 processor-based servers. It is also supported on some SPARC processor-based servers. The Oracle ILOM Remote Console is a Java application that you can launch from the ILOM web interface. When you use the Oracle ILOM Remote Console, you can remotely redirect and control the following devices on a remote host server:

- Keyboard
- Mouse
- Video console display
- Storage devices or images (CD/DVD, floppy device, ISO image)

The Oracle ILOM Remote Console enables the devices on your local client to behave as if they were directly attached to the remote host server. For instance, the redirection functionality enables you to perform any of the following tasks:

- Install software from your local media drive to a remote host server.
- Run command-line utilities on a remote host server from a local client.

- Access and run GUI-based programs on a remote host server from a local client.
- Remotely configure server features from a local client.
- Remotely manage server policies from a local client.
- Remotely monitor server elements from a local client.
- Perform almost any software task from a local client that you normally could perform while sitting at a remote host server.

The Oracle ILOM Remote Console supports two methods of redirection: video and serial console. Video redirection is supported on all Sun x86 processor-based servers and some Sun SPARC processor-based servers. Serial console redirection is supported on all SPARC processor-based servers. Serial console redirection is not currently supported on x86 processor-based servers.

For instructions for redirecting host devices using the Oracle ILOM Remote Console, see “Managing Remote Hosts’ Power States and Redirection” in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide.*

International Keyboard Support for ILOM Remote Console

As of ILOM 3.0.9, the ILOM Remote Console fully supports the use of all characters on the following international keyboards.

- Swedish Keyboard
- Swiss-French Keyboard
- Finnish Keyboard

Note – Prior to ILOM 3.0.9, the ILOM Remote Console did not support the use of all the international characters on these keyboards.

Single or Multiple Remote Host Server Management Views

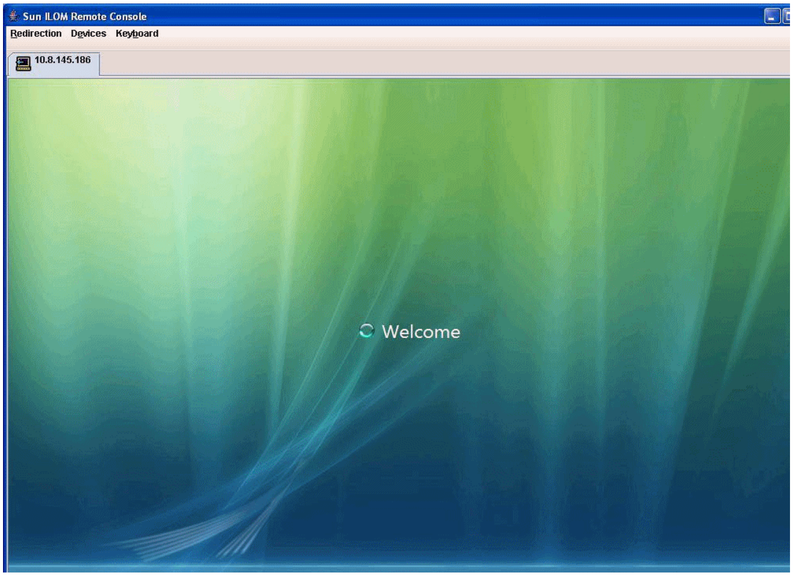
The Oracle ILOM Remote Console supports both single and multiple remote server management views.

Single and multiple server management views are currently supported on all x86 processor-based servers and some SPARC processor-based servers.

- **Single Remote Server Management View** – You can launch the Oracle ILOM Remote Console to manage a single remote host server from one window and utilize the remote Keyboard, Video, Mouse, Storage (KVMS) features.

  Single remote server management views are supported when you connect to the IP address of any server SP.

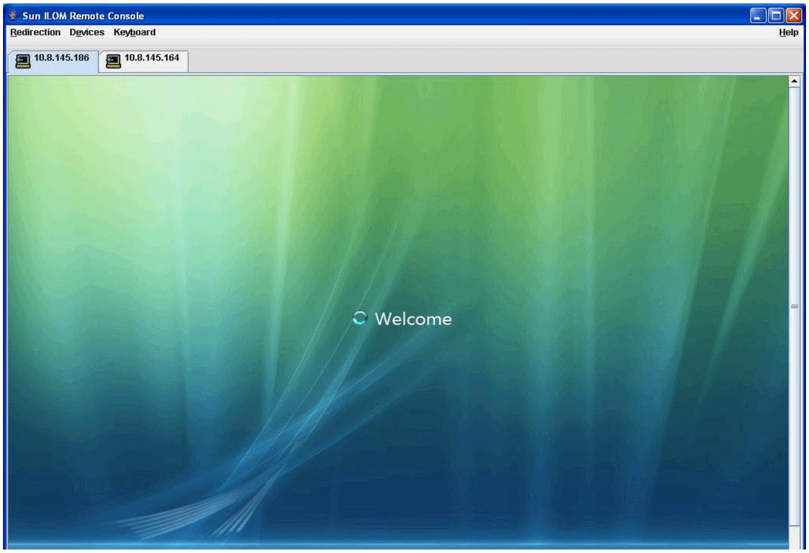
FIGURE 9-2 Single Server Management View



- **Multiple Remote Server Management Views** – You can launch the Oracle ILOM Remote Console to manage multiple remote host server views.

  Multiple remote server management views are supported when you either: (1) add a new Oracle ILOM Remote Control session to manage another remote host server; or (2) connect to the IP addresses that are associated with an x86 chassis monitoring module (CMM).

FIGURE 9-3 Multiple Server Management Views



Installation Requirements

The Oracle ILOM Remote Console does not require you to install any additional hardware or software. It is built into the ILOM software. However, to run the Oracle ILOM Remote Console, you must have the JRE 1.5 or higher (Java 5.0 or higher) software installed on your local client. To download the Java 1.5 runtime environment, go to: `http://java.com`

In addition, the Oracle ILOM Remote Console is supported on your local client with the operating systems, web browsers, and JVM listed in the following table.

TABLE 9-1 Supported Operating Systems, Web Browsers, and JVM

Operating System	Web Browser	Java Virtual Machine (JVM)
Oracle Solaris (9 and 10)	• Mozilla 1.7.5 and above • Firefox 1.0 and above	• 32-bit JDK
Linux (Red Hat, SuSE, Ubuntu, Oracle)	• Mozilla 1.7.5 and above • Firefox 1.0 and above • Opera 6.x and above	• 32-bit JDK
Microsoft Windows (98, 2000, XP, Vista)	• Internet Explorer 6.0 and above • Mozilla 1.7.5 and above • Firefox 1.0 and above • Opera 6.x and above	• 32-bit JDK

Network Communication Ports and Protocols

The Oracle ILOM Remote Console communicates to a remote host server SP using the following network ports and protocols.

TABLE 9-2 SP ILOM Remote Console Network Ports and Protocols

Port	Protocol	SP - ILOM Remote Console
5120	TCP	CD
5123	TCP	Diskette
5121	TCP	Keyboard and mouse
5556	TCP	Redirection authentication
7578	TCP	Video
7579	TCP	SPARC servers only

Sign In Authentication Required

When you launch the Oracle ILOM Remote Console from the ILOM web interface, you must sign in using an Admin (a) or Console (c) role account. The system will subsequently prompt you to reenter the Admin or Console role account each time you perform one of the following: start a redirection, stop a redirection, or restart a redirection.

Note – If the Single Sign On feature is disabled in ILOM, users with Admin (a) or Console (c) role privileges will be prompted to sign in to ILOM again using the Login dialog. For additional information about the Single Sign On feature, see "Single Sign On" on page 38.

CD and Diskette Redirection Operation Scenarios

Use the information in TABLE 9-3 to help identify different case scenarios in which the CD drive or diskette drive redirection functionality might behave during a Remote Console session.

TABLE 9-3 Remote Console Operation With DVD Drive and Diskette Drive

Case	Status	DVD as Seen by Remote Host	Diskette as Seen by Remote Host
1	Remote Console application not started, or Remote Console started but DVD/diskette redirection not started	DVD device present. No medium indication is sent to the host from ILOM when the hosts asks.	Diskette device present. No medium indication is sent to the host from ILOM when the host asks.
2	Remote Console application started with no medium present in the drive	DVD device present. When the host asks, which may be automatic or when you access the device on the host, the remote client sends a status message. In this case, since there is no medium, the status is no medium.	Diskette device present. When the host asks (for example, you double-click on a drive), the remote client sends a status message. In this case since there is no medium, the status is no medium.
3	Remote Console application started with no medium, then medium is inserted	DVD device present. When the hosts asks (automatic or manual), the remote client sends a status message as medium present and also indicates the medium change.	Diskette device present. When the host asks (manual), the remote client sends a status message as medium present and also indicates the medium change.
4	Remote Console application started with medium inserted	Same as case 3.	Same as case 3.
5	Remote Console application started with medium present, then medium is removed	Next command from the host will get a status message indicating medium not present.	Next command from the host will get a status message indicating medium not present.
6	Remote Console application started with image redirection	Same as case 3.	Same as case 3.

TABLE 9-3 Remote Console Operation With DVD Drive and Diskette Drive *(Continued)*

Case	Status	DVD as Seen by Remote Host	Diskette as Seen by Remote Host
7	Remote Console application started with image, but redirection is stopped (which is the only way to stop ISO redirection)	Driver knows DVD redirection stopped, so it sends a medium absent status on the next host query.	Driver knows DVD redirection stopped so it sends a medium absent status on the next diskette query.
8	Network failure	The software has a keep-alive mechanism. The software will detect keep-alive failure since there is no communication and will close the socket, assuming the client is unresponsive. Driver will send a no medium status to the host.	The software has a keep-alive mechanism. The software will detect unresponsive client and close the socket, as well as indicate to the driver that the remote connection went away. Driver will send a no medium status to the host.
9	Client crashes	Same as case 8.	Same as case 8.

For instructions about how to launch and use the ILOM Remote Console, see the section about Managing Remote Hosts in one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*

ILOM Remote Console Computer Lock

As of ILOM 3.0.4 or later, a Lock feature is available for the ILOM Remote Console that enhances your system security by enabling you to lock your computer when terminating a ILOM Remote Console session. Specifically, the lock behavior takes place either when you terminate an ILOM Remote Console session or when the managed network connection to the server is lost.

If you are running a Windows operating system on your host, you can enable the computer lock feature in ILOM by selecting Windows as your option. The Windows lock mode option works in conjunction with the standard Windows keyboard shortcut for locking the Windows operating system (CRTL+ALT+DEL K).

If you are running a Solaris or Linux operating system on your host, you can execute the computer lock behavior when the ILOM Remote Console terminates by implementing the custom lock mode feature in ILOM.

The custom lock mode feature in ILOM enables you to execute any system behavior that is tied to a predefined keyboard shortcut on your host operating system. To execute a custom keyboard shortcut behavior in ILOM, you must first define the behavior you want to take place on your host operating system with a keyboard shortcut. Then, to execute this behavior when the ILOM Remote Console terminates, you must specify the OS keyboard shortcut parameters in the custom KVMS lock mode feature in ILOM.

Special Considerations When Enabling the ILOM Remote Console Lock Option

Review the following special considerations in TABLE 9-1 prior to enabling the KVMS lock mode option in ILOM.

TABLE 9-1 Special Considerations When Enabling the Remote Console Lock Option

Special Consideration	Description
Console user role is required to set lock option.	To enable the ILOM Remote Console Lock option in ILOM, you must have Console (c) role privileges associated with your user account. For more information about setting up a user account in ILOM with Console privileges, see the User Management section in the ILOM 3.0 Documentation Collection.
A predefined keyboard shortcut on the OS is required to execute the custom lock mode feature.	Prior to enabling a custom keyboard shortcut in ILOM for when the ILOM Remote Console connection terminates, you must first define the keyboard shortcut behavior on your host operating system. For instructions for creating a keyboard shortcut on your host operating system, see the documentation supplied with your operating system.
The custom lock mode feature can be defined with up to four modifiers and one key.	When you specify the custom lock mode feature in ILOM, you can specify up to four modifiers and one key. A list of supported modifiers and keys that you can use to match your predefined OS keyboard shortcut appear in both the CLI KVMS help and the web interface KVMS page.
Lock behavior when running multiple ILOM Remote Console Sessions.	If more than one ILOM Remote Console session is opened to the same SP, the Windows lock or custom keyboard shortcut behavior configured in ILOM will only take place when you close the last SP ILOM Remote Console session.

For instructions about how to configure the remote console lock option in ILOM, see section about Managing Remote Hosts in one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*

Host Control - Boot Device on x86 Systems

As of ILOM 3.0.3, you can use the Host Control features in the CLI and web interface to select the host boot device settings that will override the boot device order in the BIOS. This ability gives the CLI and web interface parity with the existing IPMI interface.

The primary purpose of the boot device override feature is to enable the administrator to perform a one-time manual override of the server's BIOS boot order settings. This enables the administrator to quickly configure a machine or group of machines to boot from another device, such as the PXE boot environment.

The Host Control boot device settings are available in ILOM for Oracle Sun x86 systems SPs. This feature is not supported on the CMM. For Host Control settings in ILOM specific to SPARC system server SPs, consult the ILOM Supplement guide or platform Administration guide provided for that system.

For procedures on how to use the Host Control boot settings in ILOM on an x86 system SP, see the Remote Management Option procedures in the following ILOM guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

ILOM Operations for LDom Configurations on SPARC Servers

You can use ILOM to perform the following tasks on SPARC servers that have stored Logical Domain (LDom) configurations.

Task	Supported ILOM Point Release
View ILOM CLI targets and properties for stored LDom configurations from a host SPARC T3 Series server.	• 3.0.12 (CLI only) • 3.0.14 (CLI and web interface)
Specify which stored LDom configuration is used on the host SPARC server when the server is powered-on.	• 2.0.0 (CLI and web interface)
Enable (default) or disable the control domain boot property values from the host SPARC server.	• 2.0.0 (CLI and web interface)

For more information and procedures on how to view and configure LDom configurations on SPARC servers, see the following ILOM guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*, Chapter 12
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*, Chapter 12

CHAPTER **10**

Remote Hosts Diagnostics for x86 and SPARC Systems

Topics

Description	Links
Learn about diagnostic tests for x86 or SPARC systems	• "Diagnostics" on page 134
Collect data for use by Oracle Services personnel to diagnose system problems	• "Collect SP Data to Diagnose System Problems" on page 137

Related Topics

For ILOM	Chapter or Section	Guide
• CLI	• Diagnosing x86 Systems Hardware Issues • Diagnosing SPARC Systems Hardware Issues • Collect SP Data to Diagnose System Problems	*Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* (820-6412)
• Web interface	• Diagnosing x86 Systems Hardware Issues • Diagnosing SPARC Systems Hardware Issues • Collect SP Data to Diagnose System Problems	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)

The ILOM 3.0 Documentation Collection is available at:
`http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`

Diagnostics

All diagnostics have the same goals: stimulate some component or components, observe the behavior of the component(s) under test, and determine whether the behavior is expected. If the behavior is not expected, diagnostic tools can help to identify the likely cause of the error and send a clear message or notification to the user.

Diagnostic configuration options in ILOM are accessible from the Remote Control --> Diagnostics tab in the ILOM web interface or by using the CLI.

Refer to your platform ILOM Supplement guide or platform Administration guide for information about whether your server platform supports the following diagnostic options:

- “Pc-Check (x86 Systems)” on page 134
- “Generate NMI (x86 Systems)” on page 135
- “SPARC System Diagnostic Configuration Settings” on page 135

Information about each of these diagnostics options follows.

Pc-Check (x86 Systems)

Pc-Check is a DOS-based utility that is integrated into your system service processor (SP) firmware. This utility can be accessed from ILOM, or the utility can be accessed and executed from your server Tools and Drivers DVD. Pc-Check tests all motherboard components (CPU, memory, and I/O), ports, and slots. When enabled, this utility runs at host power-on. The Pc-Check utility is disabled by default in ILOM.

Pc-Check has four operating modes that you can run either through the ILOM web interface or through the ILOM CLI. These modes are as follows:

- **Enabled** – Select this mode if you want to run Pc-Check diagnostic tests upon start-up of the host. It is recommended that you run this mode prior to a mission-critical application to ensure the quality of the system. This mode runs a predefined test suite without user intervention and, upon completion, will continue to boot the next device based on the BIOS Boot Priority List. This mode is also recommended as a quick test for first-time field installation. These basic diagnostic tests typically take five minutes to complete.
- **Extended** – Select this mode if you want to run extended Pc-Check diagnostic tests upon start-up of the host. It is recommended that you run this mode for first-time installation of the system. This mode runs a comprehensive test suite to ensure that the system was transported without physical damage. This mode

should also be run any time you physically change the system configuration to ensure that newly added components are installed correctly prior to running production operating systems and applications. These extended diagnostic tests typically take 20 to 40 minutes to complete.

- **Manual** – Select this mode if you want to run select Pc-Check diagnostic tests upon start-up of the host. You can use this mode to select individual tests from the Pc-Check menus, or to select predefined test suites available through the Immediate Burn-in test menu.
- **Disabled** – Select this mode if you do not want to run Pc-Check diagnostic tests upon start-up of the host. This is the default mode when your system arrives. You should set up Pc-Check to Disabled mode when you have concluded running the diagnostic tests.

For more information on specific test suites and in-depth instructions for running the Pc-Check diagnostics utility, see the *Oracle x86 Servers Diagnostics Guide* (820-6750).

Generate NMI (x86 Systems)

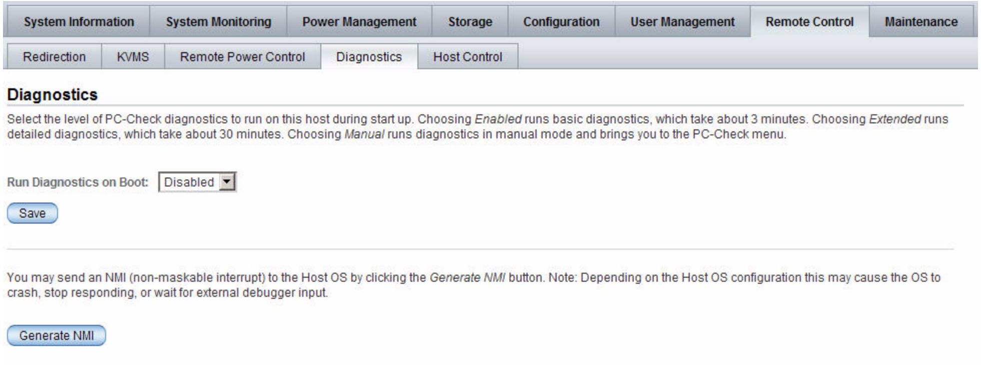
You can send a non-maskable interrupt (NMI) to the host operating system using either the CLI or the web interface. Note that sending an NMI to the host could cause the host to stop responding and wait for input from an external debugger.

SPARC System Diagnostic Configuration Settings

On a Sun SPARC system using 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.

ILOM web interface examples of x86 server and SPARC server Diagnostics pages are displayed below.

FIGURE 10-1 Diagnostic Page for x86 Systems



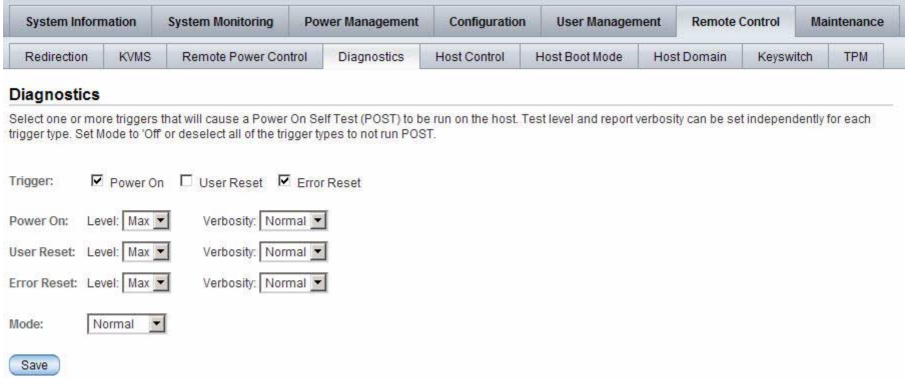
Diagnostics

Select the level of PC-Check diagnostics to run on this host during start up. Choosing *Enabled* runs basic diagnostics, which take about 3 minutes. Choosing *Extended* runs detailed diagnostics, which take about 30 minutes. Choosing *Manual* runs diagnostics in manual mode and brings you to the PC-Check menu.

Run Diagnostics on Boot: Disabled

You may send an NMI (non-maskable interrupt) to the Host OS by clicking the *Generate NMI* button. Note: Depending on the Host OS configuration this may cause the OS to crash, stop responding, or wait for external debugger input.

FIGURE 10-2 Diagnostics Page for SPARC Servers



Diagnostics

Select one or more triggers that will cause a Power On Self Test (POST) to be run on the host. Test level and report verbosity can be set independently for each trigger type. Set Mode to 'Off' or deselect all of the trigger types to not run POST.

Trigger: ☑ Power On ☐ User Reset ☑ Error Reset

Power On: Level: Max Verbosity: Normal

User Reset: Level: Max Verbosity: Normal

Error Reset: Level: Max Verbosity: Normal

Mode: Normal

Collect SP Data to Diagnose System Problems

The ILOM Service Snapshot utility enables you to produce a snapshot of the server processor at any instant in time. You can run the utility from the ILOM CLI or the web interface.

Caution – The purpose of the 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 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.

As of ILOM 3.0.3, a FRUID data set option is available from the Snapshot utility. Specifically, this option enables 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 Services representative instructs a customer to use the option.

APPENDIX A

Example Setup of Dynamic DNS

This appendix describes how to configure the Dynamic Domain Name Service (DDNS) on a typical customer's infrastructure. The instructions and example configuration provided here do not affect ILOM or the service processor (SP).

The following topics are covered in this appendix:

Dynamic DNS Overview

Once DDNS is configured, new ILOM systems will be automatically assigned a host name and an IP address at install time. Thus, once you have configured DDNS, clients can use either host names or IP addresses to access any ILOM SPs that have been added to the network.

By default, ILOM systems are shipped with Dynamic Host Configuration Protocol (DHCP) enabled so that you can use DHCP to configure the SP's network interface. With DDNS, you can further leverage DHCP to automatically make the DNS server aware of the host names of ILOM systems that have been added to the network and configured using DHCP.

Note – Domain Name Service (DNS) support, which was added to ILOM in the 3.0 release, allows hosts such as NTP servers, logging servers, and firmware upgrade servers, to be referred to within the ILOM command-line interface (CLI) and other user interfaces by host name or IP address. DDNS support, as described in this appendix, allows SPs to be referred to by their host names without being manually configured.

ILOM systems are assigned well-known host names consisting of a prefix followed by a hyphen and the ILOM SP product serial number. For rackmounted systems and server modules, the host name will consist of the prefix SUNSP and the product serial number. For a server chassis with multiple chassis monitoring modules (CMMs), the host name for each CMM will consist of the prefix SUNCMM*n* and the product serial number, where *n* is 0 or 1. For example, given a product serial number of 0641AMA007, the host name for a rackmounted system or a server module would be SUNSP-0641AMA007. For a server chassis with two CMMs, the host names for the CMMs would be SUNCMM0-0641AMA007 and SUNCMM1-0641AMA007.

Once DDNS has been configured, SP/DHCP/DNS transactions are automatically executed to add new host names and associated IP addresses to the DNS database. Each transaction comprises the following steps:

1. ILOM creates the SP host name using the appropriate prefix and the product serial number and the ILOM SP sends the host name to the DHCP server as part of the DHCP request.
2. When the DHCP server receives the request, it assigns an IP address to the ILOM SP from an available pool of addresses.
3. The DHCP server then sends an update to the DNS server to notify it of the newly configured ILOM SP's host name and IP address.
4. The DNS server updates its database with the new information, thus completing the SP/DHCP/DNS transaction.

Once an SP/DHCP/DNS transaction is completed for a given host name, clients can make a DNS request using that host name and DNS will return the assigned IP address.

To determine the host name of a particular ILOM SP, simply check the product serial number on the outside of the SP itself and combine the product serial number with the appropriate prefix as described above. You can also determine host names by checking the server logs for DNS zone update messages.

Note – You can use the CLI to change the SP host name to something other than the default. However, if you change the host name to a non-default name, clients must use that host name to refer to the SP using DNS.

The DNS information is updated when a DHCP lease renewal causes an IP address change, and the DNS information is deleted when the DHCP lease is released.

Note – For all ILOM SPs that have been assigned host names prior to DDNS support or that may have been configured using DDNS and MAC address-based host names, the previously configured host names will remain in effect.

Example Dynamic DNS Configuration

This section describes how to set up an example DDNS configuration. You can use the procedures and sample files provided here, with site-specific modifications, to set up your own DDNS configuration.

Note – How you set up DDNS depends on the infrastructure in use at your site. Solaris, Linux, and Windows operating systems all support server solutions that offer DDNS functionality. This example configuration uses Debian r4.0 as the server operating system environment.

This following topics are covered in this section:

- "Assumptions" on page 141
- "Configure and Start the DHCP and DNS Servers" on page 141
- "References" on page 143

Assumptions

This example configuration is based on the following assumptions:

- There is a single server that handles both DNS and DHCP for the network the SP resides on.
- The SP network address is 192.168.1.0.
- The DHCP/DNS server address is 192.168.1.2
- The IP addresses from 192.168.1.100 to 192.168.1.199 are used as a pool to provide addresses to the SP and other clients.
- The domain name is `example.com`.
- There is no existing DNS or DHCP configuration in place. If there is, use the following files as a guideline to update the existing configuration.

▼ Configure and Start the DHCP and DNS Servers

To configure the servers, follow these steps:

1. **Install the `bind9` and `dhcp3-server` packages from the Debian distribution.**

   Installing the `dnsutils` package provides access to `dig`, `nslookup` and other useful tools as well.

2. **Using** `dnssec-keygen`**, generate a key to be shared between the DHCP and DNS servers to control access to the DNS data.**

3. **Create a DNS configuration file named** `/etc/bind/named.conf` **that contains the following:**

```
options {
  directory "/var/cache/bind";
  auth-nxdomain no;    # conform to RFC1035
  listen-on-v6 { any; };
};
// prime the server with knowledge of the root servers
zone "." {
  type hint;
  file "/etc/bind/db.root";
};
// be authoritative for the localhost forward and reverse zones,
// and for broadcast zones as per RFC 1912
zone "localhost" {
  type master;
  file "/etc/bind/db.local";
};
zone "127.in-addr.arpa" {
  type master;
  file "/etc/bind/db.127";
};
zone "0.in-addr.arpa" {
  type master;
  file "/etc/bind/db.0";
};
zone "255.in-addr.arpa" {
  type master;
  file "/etc/bind/db.255";
};
// additions to named.conf to support DDNS updates from dhcp server
key server.example.com {
  algorithm HMAC-MD5;
  secret "your-key-from-step-2-here"
};
zone "example.com" {
  type master;
  file "/etc/bind/db.example.com";
  allow-update { key server.example.com; };
};
zone "1.168.192.in-addr.arpa" {
  type master;
  file "/etc/bind/db.example.rev";
  allow-update { key server.example.com; };
};
```

4. **Add empty zone files for the local network.**

   Empty zone files should be named `/etc/bind/db.example.com` and `/etc/bind/db.example.rev`.

   Copying the distribution supplied `db.empty` files is sufficient; they will be updated automatically by the DNS server.

5. **Create a `/etc/dhcp3/dhcpd.conf` file that contains the following:**

```
ddns-update-style interim;
ddns-updates      on;
server-identifier server;
ddns-domainname   "example.com.";
ignore client-updates;
key server.example.com {
  algorithm hmac-md5;
  secret your-key-from-step-2-here;
}
zone example.com. {
  primary 127.0.0.1;
  key server.example.com;
}
zone 1.168.192.in-addr.arpa. {
  primary 127.0.0.1;
  key server.example.com;
}
default-lease-time 600;
max-lease-time 7200;
authoritative;
log-facility local7;
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.100 192.168.1.199;
  option domain-name-servers 192.168.1.2;
}
```

6. **After completing steps 1 through 5 above, run the `/etc/init.d` script to start the DNS and DHCP servers.**

   Once the servers are running, any new ILOM SPs configured for DHCP will be automatically accessible using their host name when they are powered on. Use log files, `dig`, `nslookup`, and other utilities for debugging, if necessary.

References

For more information on the Linux DHCP and DNS servers used in this example, see the Internet Systems Consortium web site at: `http://www.isc.org/`

APPENDIX **B**

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 The amount of power consumed by all power supplies in the system.

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).

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.

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.

command-line interface (CLI) A text-based interface that enables users to type executable instructions at a command prompt.

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 which 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.

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 in order to reach the console prompt. A 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 Management Architecture (FMA) An architecture that ensures a computer can continue to function despite a hardware or software failure.

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 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. A 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.

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

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.

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 Replacable Unit (FRU) inventory reporting, system monitoring, logging, system recovery (including local and remote system resets and power on and off capabilities), and alerting.

internal serial port The connection between the host server and ILOM that enables an ILOM user to access the host serial console. The 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 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 "192.168.255.256," which specifies the actual location of a machine on an intranet or the Internet.

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(TM) Web Start application A web application launcher. With Java Web Start, applications are launched by clicking on 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 via 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.

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.

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(TM) 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).

Operator A user with limited privileges to the managed host system.

out-of-band (OOB) system management Server management capability that is enabled when the operating system network drivers or the server are not functioning properly.

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.

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 The maximum power that the server will permit 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 cycling The process of turning the power to a system off then on again.

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 minute 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

real-time clock (RTC) A battery-backed component that maintains the time and date for a system, even when the system is powered off.

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.

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.

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.

S

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 Socket 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 A working scheme that divides 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 Sun Blade server modules.

Sun Blade server module A server module (blade) that can be plugged into a chassis, also known as a modular system

Sun 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.

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

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 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

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, via 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.

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