



Guía del usuario de Sun™ Integrated Lights Out Manager 2.0

Sun Microsystems, Inc.
www.sun.com

Nº de referencia: 820-2697-10
Julio de 2007, revisión A

Envíe sus comentarios sobre este documento a través de: <http://www.sun.com/hwdocs/feedback>

Copyright 2007 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, EE.UU. Todos los derechos reservados.

Sun Microsystems, Inc. tiene derechos de propiedad intelectual sobre la tecnología que se describe en este documento. En concreto, pero sin limitarse a lo citado a continuación, dichos derechos de propiedad intelectual incluyen una o más patentes estadounidenses de las mostradas en <http://www.sun.com/patents> y una o más patentes adicionales o solicitudes de patente pendientes en los EE.UU. y otros países.

El presente documento y el producto al que hace referencia se distribuyen en virtud de licencias que restringen su utilización, copia, distribución y descompilación. Queda prohibida la reproducción total o parcial del producto o del presente documento, en cualquier forma y por cualquier medio, sin la autorización previa por escrito de Sun o sus distribuidores autorizados, si los hubiese.

El software de otros fabricantes, incluida la tecnología de tipos de letra, está protegido por copyright y los distribuidores de Sun otorgan la licencia correspondiente.

Algunas partes de este producto pueden derivarse de sistemas Berkeley BSD, cuya licencia otorga la Universidad de California. UNIX es una marca registrada en los EE.UU. y otros países, con licencia exclusiva de X/Open Company, Ltd.

Sun, Sun Microsystems, el logotipo de Sun, Java, docs.sun.com y Solaris son marcas comerciales o marcas registradas de Sun Microsystems, Inc. en los EE.UU. y en otros países.

Todas las marcas comerciales SPARC se utilizan en virtud de una licencia y son marcas comerciales o marcas registradas de SPARC International, Inc. en los EE.UU. y otros países. Los productos con marcas comerciales SPARC se basan en una arquitectura desarrollada por Sun Microsystems, Inc.

La interfaz gráfica de usuario OPEN LOOK y Sun™ ha sido desarrollada por Sun Microsystems, Inc. para sus usuarios y titulares de licencia. Sun reconoce el trabajo de Xerox como pionera en la investigación y el desarrollo del concepto de interfaces de usuario visuales o gráficas para la industria informática. Sun dispone de una licencia no exclusiva de Xerox para la utilización de Xerox Graphical User Interface; esta licencia cubre también a los titulares de licencias de Sun que utilizan las interfaces gráficas de usuario OPEN LOOK y cumplen los contratos de licencia por escrito de Sun.

Derechos del Gobierno de los EE.UU.: uso comercial. Los usuarios gubernamentales deben cumplir lo establecido en el contrato de licencia estándar de Sun Microsystems, Inc., así como las provisiones aplicables de la FAR y sus suplementos.

LA DOCUMENTACIÓN SE PROPORCIONA "TAL CUAL" SIN NINGUNA GARANTÍA, REPRESENTACIÓN NI CONDICIÓN EXPRESA O IMPLÍCITA, INCLUIDA CUALQUIER GARANTÍA DE COMERCIALIZACIÓN, IDONEIDAD PARA FINES ESPECÍFICOS O CONTRAVENCIÓN DEL PRESENTE CONTRATO, EXCEPTO EN LOS CASOS EN QUE DICHA RENUNCIA SEA JURÍDICAMENTE NULA Y SIN VALOR.



Para
reciclar



Adobe PostScript

Contenido

Prólogo xvii

1. Introducción a ILOM 1

Qué es ILOM 1

ILOM en el SP y el CMM 2

Interfaces de ILOM 3

Red de administración de ILOM 4

Métodos de conexión con ILOM 5

Funciones de las cuentas de usuario de ILOM 6

Cuenta de administrador de ILOM preconfigurada 6

Características de ILOM 7

Nuevas funciones de ILOM 2.0 9

Otras herramientas de administración 9

2. Establecimiento de la comunicación inicial con ILOM 11

Configuración inicial de ILOM 12

Hoja de configuración inicial 12

Consideraciones sobre la asignación de direcciones IP mediante DHCP 14

Difusión de paquetes DHCPDISCOVER en la plataforma de servidor
Sun 15

Requisitos para la asignación mediante DHCP 15

Dirección MAC de la interfaz de red del SP	15
Requisitos posteriores a la asignación mediante DHCP	17
Consideraciones sobre la asignación de direcciones IP estáticas	18
Requisitos para la asignación de direcciones IP estáticas	18
Configuración del dispositivo serie o el emulador de terminal	19
Requisitos posteriores a la asignación de direcciones IP estáticas	19
Configuración de direcciones IP de la red de administración	20
Asignación de los puertos de red de ILOM	20
Identificación del SP y el CMM del servidor mediante un nombre de sistema	22
Texto de identificación del sistema de los servidores Sun	22
Asignación de direcciones IP a las interfaces de los SP en las plataformas de servidor Sun	23
▼ Asignación de direcciones IP con DHCP utilizando una conexión de administración Ethernet	23
▼ Asignación de una dirección IP estática al SP del servidor mediante una conexión serie	25
▼ Asignación de una dirección IP estática al CMM mediante una conexión serie	27
Edición de las direcciones IP asignadas mediante una conexión de administración Ethernet	29
▼ Edición de las direcciones IP existentes en ILOM mediante la interfaz web	29
▼ Edición de las direcciones IP existentes en ILOM mediante la línea de comandos	31
Asignación del nombre o el identificador del sistema	33
▼ Asignación del nombre y el identificador del sistema mediante la interfaz web	33
▼ Asignación del nombre y el identificador del sistema mediante la línea de comandos	34

3. Interfaz de la línea de comandos e inicio de la sesión de ILOM	37
Descripción general de la interfaz de la línea de comandos	38
Arquitectura jerárquica de la interfaz de la línea de comandos	39
Sintaxis de los comandos de la CLI	40
Comandos de la CLI	41
Opciones de los comandos	41
Destinos de los comandos	42
Propiedades de los comandos	42
Ejecución de los comandos	42
▼ Ejecución de comandos por separado	42
▼ Ejecución de comandos combinados	43
Conexión con ILOM mediante la línea de comandos	44
▼ Inicio de la sesión de ILOM	44
▼ Cierre de la sesión de ILOM	45
4. Interfaz web e inicio de la sesión de ILOM	47
Descripción de la interfaz web	47
Requisitos del navegador y el software	48
Componentes de la interfaz web	49
Componentes de las fichas de navegación	50
Ficha System Information	50
Ficha Versions	51
Ficha Session Time-Out	51
Ficha Components	51
Ficha Identification Information	51
Ficha System Monitoring	52
Ficha Sensor Readings	52
Ficha Indicators	52
Ficha Event Logs	52

Ficha Configuration	53
Ficha System Management Access	53
Ficha Alert Management	54
Ficha Network	54
Ficha Serial Port	54
Ficha Clock Settings	54
Ficha Syslog	55
Ficha SMTP Client	55
Ficha User Management	55
Ficha User Accounts	55
Ficha Active Sessions	56
Ficha LDAP	56
Ficha RADIUS	56
Ficha Active Directory	56
Ficha Remote Control	56
Ficha Redirection	57
Remote Power Control	57
Mouse Mode Settings	57
Ficha Maintenance	57
Ficha Firmware Upgrade	58
Ficha Reset SP	58
Conexión con ILOM mediante la interfaz web	58
▼ Inicio de la sesión de ILOM	58
▼ Carga del certificado SSL	61
▼ Establecimiento del tiempo de espera para finalizar la sesión	62
▼ Cierre de la sesión de ILOM	63

5. Administración de cuentas de usuario 65

Directrices para administrar las cuentas de usuario 67

Funciones y privilegios de las cuentas de usuario 67

Cuentas de administrador de ILOM preconfiguradas 68

- ▼ Cambio de contraseña de la cuenta root de ILOM mediante la interfaz web 68
- ▼ Cambio de contraseña de la cuenta root de ILOM mediante la línea de comandos 70

Single Sign On 71

- ▼ Habilitación o inhabilitación de Single Sign On mediante la línea de comandos 71
- ▼ Habilitación o inhabilitación de Single Sign On mediante la interfaz web 71

Administración de cuentas de usuario mediante la línea de comandos 72

- ▼ Adición de una cuenta de usuario mediante la línea de comandos 72
- ▼ Modificación de una cuenta de usuario mediante la línea de comandos 73
- ▼ Supresión de una cuenta de usuario mediante la línea de comandos 73
- ▼ Visualización de la lista de cuentas de usuario mediante la línea de comandos 73
- ▼ Visualización de una cuenta de usuario específica mediante la línea de comandos 73
- ▼ Configuración de una cuenta de usuario mediante la línea de comandos 74

Destinos, propiedades y valores 74

- ▼ Visualización de la lista de sesiones de usuario mediante la línea de comandos 75
- ▼ Visualización de una sesión de usuario específica mediante la línea de comandos 75

Administración de cuentas de usuario mediante la interfaz web	76
▼ Adición de cuentas de usuario y establecimiento de privilegios mediante la interfaz web	76
▼ Modificación de una cuenta de usuario mediante la interfaz web	79
▼ Supresión de una cuenta de usuario mediante la interfaz web	82
▼ Visualización de las sesiones de usuario mediante la interfaz web	83
Active Directory	84
Introducción a Active Directory	84
Configuración de Active Directory	85
▼ Configuración de Active Directory mediante la interfaz web	85
Propiedades de la página de configuración de Active Directory	86
Tablas de destinos de Active Directory	88
Propiedades de las tablas de destinos de Active Directory	89
▼ Edición de las tablas de Active Directory mediante la interfaz web	90
Determinación de los niveles de autorización de los usuarios	91
Seguridad de la conexión de Active Directory	92
Establecimiento de la seguridad en la conexión de Active Directory mediante la línea de comandos	92
▼ Acciones con <code>getcertfile</code> desde la línea de comandos	92
▼ Habilitación de <code>strictcertmode</code> mediante la línea de comandos	93
▼ Comprobación de <code>certfilestatus</code> mediante la línea de comandos	93
Establecimiento de la seguridad en la conexión de Active Directory mediante la interfaz web	94
▼ Carga de un certificado mediante la interfaz web	94
▼ Comprobación del estado del archivo de certificado mediante la interfaz web	95
▼ Habilitación del modo de certificado estricto mediante la interfaz web	95
LDAP (Lightweight Directory Access Protocol)	96
Introducción a LDAP	96
Clientes y servidores LDAP	96

Organización del directorio en los servidores LDAP	97
Configuración de LDAP	98
▼ Configuración del servidor LDAP	99
▼ Configuración de ILOM para LDAP mediante la línea de comandos	100
▼ Configuración de ILOM para LDAP mediante la interfaz web	100
Autenticación RADIUS	102
Clientes y servidores RADIUS	102
Parámetros de RADIUS	103
Configuración de RADIUS	103
▼ Configuración de RADIUS mediante la línea de comandos	103
▼ Configuración de RADIUS mediante la interfaz web	104
Comandos de RADIUS	104
show /SP/clients/radius	104
set /SP/clients/radius	106
show /SP/clients	107
6. Administración del inventario y los componentes	109
Visualización de la información de los componentes y administración del inventario	110
▼ Visualización de la información de los componentes mediante la línea de comandos	110
▼ Visualización de la información de los componentes mediante la interfaz web	111
Realización de acciones con los componentes	113
Retirada y sustitución de los componentes	113
▼ Preparación para retirar un componente mediante la línea de comandos	113
▼ Forma de saber si un componente está listo para su retirada mediante la línea de comandos	114
▼ Puesta en servicio de un componente mediante la línea de comandos	114
▼ Preparación para retirar un componente mediante la interfaz web	115

▼	Puesta de un componente en servicio mediante la interfaz web	115
	Habilitación e inhabilitación de componentes	116
▼	Habilitación e inhabilitación de los componentes mediante la línea de comandos	116
▼	Habilitación e inhabilitación de los componentes mediante la interfaz web	116
	Configuración de normas	117
▼	Configuración de las normas mediante la línea de comandos	117
▼	Configuración de las normas mediante la interfaz web	118
7.	Supervisión del sistema y administración de alertas	119
	Descripción de la supervisión del sistema	121
	Lecturas de los sensores	121
	Obtención de lecturas de los sensores mediante la interfaz web	122
	Obtención de lecturas de los sensores mediante la línea de comandos	123
	Indicadores del sistema	125
	Posibles estados de los indicadores del sistema	125
	Visualización y administración de los indicadores mediante la interfaz web	126
	Visualización y administración de los indicadores mediante la línea de comandos	127
	Registro de eventos de ILOM	128
	Marcas de tiempo del registro de eventos y configuración del reloj de ILOM	129
	Configuraciones admitidas para el reloj	129
	Visualización o configuración del reloj mediante la interfaz web	129
	Visualización y configuración del reloj mediante la línea de comandos	130
	Información de Syslog	130
	Administración de errores	131
	Visualización de los estados de error mediante la interfaz web	132

Visualización de los estados de error mediante la línea de comandos	133
Supervisión de los sensores del sistema, los indicadores y el registro de eventos de ILOM	134
▼ Identificación del estado de los indicadores mediante la interfaz web	134
▼ Obtención de las lecturas de los sensores mediante la interfaz web	135
▼ Visualización o borrado del registro de eventos de ILOM mediante la interfaz web	136
▼ Visualización o borrado del registro de eventos de ILOM mediante la línea de comandos	138
▼ Visualización y configuración del reloj mediante la interfaz web	140
▼ Configuración de las direcciones IP de un destinatario de Syslog remoto mediante la interfaz web	141
▼ Configuración de las direcciones IP de un destinatario de Syslog remoto mediante la línea de comandos	142
Introducción a la administración de alertas	143
Configuración de las reglas de alertas	144
Definición de propiedades para las reglas de alertas	144
Administración de las reglas de alertas mediante la interfaz web de ILOM	147
Requisitos previos	148
▼ Modificación de una regla de alerta mediante la interfaz web	149
▼ Inhabilitación de una regla de alerta mediante la interfaz web	150
▼ Generación de pruebas de alertas mediante la interfaz web	150
Administración de las reglas de alertas mediante la línea de comandos de ILOM	151
Comandos para administrar las reglas de alertas desde la línea de comandos	152
Requisitos previos	154
▼ Modificación de las reglas de alertas mediante la línea de comandos	154
▼ Inhabilitación de una regla de alerta mediante la línea de comandos	155
▼ Generación de pruebas de alertas mediante la línea de comandos	156

- Configuración de un cliente SMTP para alertas de notificación por correo electrónico 157
 - ▼ Habilitación del cliente SMTP mediante la interfaz web 158
 - ▼ Habilitación de un cliente SMTP mediante la línea de comandos 158

8. Configuración de la comunicación en ILOM 161

Administración de la configuración de red de ILOM mediante la línea de comandos 162

Introducción a la configuración de red 163

- ▼ Visualización de la configuración de red mediante la línea de comandos 163
- ▼ Configuración de los valores de red mediante la línea de comandos 163
 - Destinos, propiedades y valores 164

Configuración del puerto serie 165

- ▼ Visualización de la configuración del puerto serie mediante la línea de comandos 165
- ▼ Configuración del puerto serie mediante la línea de comandos 166
 - Destinos, propiedades y valores 166
- ▼ Habilitación del acceso HTTP o HTTPS a la web mediante la línea de comandos 167
 - Destinos, propiedades y valores 167

Configuración de Secure Shell 168

- ▼ Establecimiento de una conexión remota segura para ejecutar los comandos de la línea de comandos 168
- ▼ Visualización de la clave actual mediante la línea de comandos 169
- ▼ Habilitación o inhabilitación de SSH mediante la línea de comandos 170
- ▼ Habilitación o inhabilitación de SSH mediante la interfaz web 170
- ▼ Generación de una clave nueva mediante la línea de comandos 171
- ▼ Generación de una clave nueva mediante la interfaz web 172
- ▼ Reinicio del servidor SSH mediante la línea de comandos 172
- ▼ Reinicio del servidor SSH mediante la interfaz web 172

Administración de la configuración de red de ILOM mediante la interfaz web 173

- ▼ Visualización de la configuración de red mediante la interfaz web 173
- ▼ Configuración de los valores de red mediante la interfaz web 173
- ▼ Visualización de la configuración del puerto serie mediante la interfaz web 175
- ▼ Configuración de los valores del puerto serie mediante la interfaz web 176
- ▼ Habilitación del acceso HTTP o HTTPS a la web mediante la interfaz web 176

9. IPMI (Intelligent Platform Management Interface) 179

Descripción de IPMI 179

ILOM e IPMI 180

Uso de IPMITool 180

Alertas de IPMI 181

Ejemplos de IPMITool 182

- ▼ Visualización de la lista de sensores y sus valores 182
- ▼ Visualización de los datos de un sensor 183
- ▼ Encendido del host 183
- ▼ Apagado del host 183
- ▼ Apagado y encendido del host 183
- ▼ Cierre normal del host 183
- ▼ Visualización de la información de fabricación de las unidades FRU 184
- ▼ Visualización del registro de eventos del sistema de IPMI 185

10. SNMP (Simple Network Management Protocol) 187

Descripción de SNMP 188

Funcionamiento de SNMP 189

Archivos MIB de SNMP 190

Alertas y capturas de eventos de SNMP 191

- Administración de usuarios de SNMP mediante la línea de comandos 192
 - ▼ Adición de una cuenta de usuario de SNMP mediante la línea de comandos 192
 - ▼ Edición de una cuenta de usuario de SNMP mediante la línea de comandos 192
 - ▼ Supresión de una cuenta de usuario de SNMP mediante la línea de comandos 193
 - ▼ Adición o edición de una comunidad SNMP mediante la línea de comandos 193
 - ▼ Supresión de una comunidad SNMP mediante la línea de comandos 193
- Destinos, propiedades y valores 194
 - ▼ Configuración de los destinos de capturas de eventos de SNMP mediante la línea de comandos 195
- Administración de cuentas de usuario de SNMP mediante la interfaz web 196
 - ▼ Configuración de SNMP mediante la interfaz web 196
 - ▼ Adición o edición de una cuenta de usuario de SNMP mediante la interfaz web 197
 - ▼ Supresión de una cuenta de usuario de SNMP mediante la interfaz web 199
 - ▼ Adición o edición de una comunidad SNMP mediante la interfaz web 200
 - ▼ Supresión de una comunidad SNMP mediante la interfaz web 200
 - ▼ Configuración de los destinos de capturas de eventos de SNMP mediante la interfaz web 201
- Ejemplos de SNMP 202
 - ▼ Visualización y configuración de los valores de SNMP 202
 - ▼ Obtención de información mediante los comandos `snmpget` o `snmpwalk net-snmp` 204
 - ▼ Configuración de la información mediante `snmpset` 204
 - ▼ Recepción de capturas de eventos mediante `snmptrapd` 205

11. Actualización del firmware de ILOM 207

Proceso de actualización del firmware 207

Descripción de la actualización del firmware de ILOM 208

- ▼ Visualización de la información de versión de ILOM mediante la línea de comandos 208
- ▼ Actualización del firmware de ILOM mediante la línea de comandos 209
- ▼ Visualización de la información de versión de ILOM mediante la interfaz web 209
- ▼ Actualización del firmware de ILOM mediante la interfaz web 210
- ▼ Reinicio del SP de ILOM 211

12. Administración remota de los servidores x64 mediante Sun ILOM Remote Console 213

Descripción de Remote Console 214

Vistas de administración de uno o varios servidores host remotos 215

Requisitos de instalación 216

Puertos y protocolos de comunicación en red 217

Cuenta de usuario con función de administrador: autenticación de sesión obligatoria 217

Ejecución y configuración de ILOM para administración remota 218

- ▼ Conexión con la interfaz web de ILOM 218
- ▼ Configuración de las opciones de control remoto de ILOM mediante la interfaz web 219

Ejecución y configuración de Sun ILOM Remote Console para administrar servidores x64 remotos 222

- ▼ Ejecución de Remote Console mediante la interfaz web de ILOM 222
- ▼ Adición de una sesión de servidor 224
- ▼ Inicio, detención o reinicio de la redirección de dispositivos 224
- ▼ Redirección del teclado y el ratón 225
- ▼ Control de los modos de teclado y el envío de funciones de teclas 226
- ▼ Redirección de dispositivos de almacenamiento 227

▼ Salida de Sun ILOM Remote Console	228
Situaciones de uso de la redirección de CD y disquetes	229
A. Información de referencia de la interfaz de la línea de comandos de ILOM	231
Referencia abreviada de los comandos de la CLI	231
Información de referencia de los comandos de la CLI	237
B. Glosario	253
Índice	273

Prólogo

La *Guía del usuario de Sun Integrated Lights Out Manager 2.0* presenta las características y tareas de ILOM comunes a todos los servidores blade o servidores de bastidor Sun compatibles con este firmware. La forma de acceder a estas tareas y utilizarlas es similar en todos los casos, sea cual sea la plataforma de servidor Sun que ILOM esté administrando. Otros documentos dirigidos a los usuarios presentan las características y tareas de ILOM específicas de la plataforma utilizada. Encontrará la información de ILOM específica de cada plataforma en el juego de documentación entregado con su sistema.

Antes de leer este documento

Esta guía proporciona información detallada sobre las características y funciones de ILOM que son comunes a todas las plataformas de servidor administradas por este firmware. Para comprender adecuadamente toda la información y realizar las tareas explicadas en la guía, debería utilizar este documento en combinación con la documentación de ILOM entregada con el servidor.

Organización del documento

Este documento incluye la información siguiente:

El [Capítulo 1](#) contiene una descripción general de las características y funciones de ILOM.

En el [Capítulo 2](#) se explica la forma de establecer la comunicación inicial con ILOM y los tipos de tareas que pueden realizarse con diferentes conexiones.

En el [Capítulo 3](#) se explica la forma de usar la interfaz de la línea de comandos de ILOM y el modo de iniciar la sesión de ILOM utilizando esta interfaz.

En el [Capítulo 4](#) se explica la forma de usar la interfaz web de ILOM y el modo de iniciar la sesión de ILOM utilizando esta interfaz.

En el [Capítulo 5](#) se explica la forma de administrar las cuentas de usuario utilizando la interfaz de la línea de comandos o la interfaz web de ILOM, así como la manera de configurar Active Directory, LDAP y RADIUS.

El [Capítulo 6](#) contiene los procedimientos para ver y modificar la información de los componentes, así como para preparar componentes, desinstalarlos y volverlos a poner en servicio, y configurar normas de uso.

En el [Capítulo 7](#) se explica cómo administrar las alertas y supervisar el sistema mediante el uso de sensores, indicadores y registros de eventos.

El [Capítulo 8](#) contiene una descripción general de los parámetros de configuración de red de ILOM y las tareas que es preciso realizar para configurarlos mediante la interfaz de la línea de comandos o la interfaz web de ILOM.

En el [Capítulo 9](#) se describe la interfaz de administración inteligente de plataformas IPMI (Intelligent Platform Management Interface) e IPMItool.

En el [Capítulo 10](#) se explica el funcionamiento de SNMP y la forma de administrar los usuarios de SNMP mediante la interfaz de la línea de comandos o la interfaz web.

En el [Capítulo 11](#) se explica cómo actualizar y reiniciar el firmware de ILOM mediante la interfaz de la línea de comandos o la interfaz web de ILOM.

En el [Capítulo 12](#) se describe la aplicación Remote Console de ILOM y la forma de ejecutarla y configurarla para administrar una plataforma de servidor de forma remota.

El [Apéndice A](#) contiene una lista de comandos ejecutables desde la interfaz de la línea de comandos de ILOM y la explicación de su uso.

El [Apéndice B](#) contiene un glosario con la definición de algunas palabras y expresiones utilizadas en esta guía.

Convenciones tipográficas

Tipo de letra*	Significado	Ejemplos
AaBbCc123	Se utiliza para indicar nombres de comandos, archivos y directorios, y mensajes del sistema que aparecen en la pantalla.	Edite el archivo <code>.login</code> . Utilice <code>ls -a</code> para ver la lista de todos los archivos. <code>% Tiene correo.</code>
AaBbCc123	Lo que escribe el usuario, a diferencia de lo que aparece en la pantalla.	<code>% su</code> Password:
<i>AaBbCc123</i>	Títulos de libros, palabras o términos nuevos y palabras que deben enfatizarse. Variables de la línea de comandos que deben sustituirse por nombres o valores reales.	Consulte el capítulo 6 del <i>Manual del usuario</i> . Se conocen como opciones de <i>clase</i> . Para efectuar esta operación, <i>debe</i> estar conectado como superusuario. Para borrar un archivo, escriba <code>rm nombre de archivo</code> .

* Los valores de configuración de su navegador podrían diferir de los que figuran en esta tabla.

Documentación relacionada

Debería utilizar este documento en combinación con la documentación de ILOM entregada con la plataforma en uso.

Documentación, asistencia técnica y formación

Servicio de Sun	Dirección
Documentación	http://www.sun.com/documentation/
Asistencia técnica	http://www.sun.com/support/
Formación	http://www.sun.com/training/

Sitios web de terceros

Sun no se hace responsable de la disponibilidad de los sitios web de terceros que se mencionan en este documento. Sun no avala ni se hace responsable del contenido, la publicidad, los productos ni otros materiales disponibles en dichos sitios o recursos, o a través de ellos. Sun tampoco se hace responsable de los daños o pérdidas, supuestos o reales, provocados por el uso o la confianza puesta en el contenido, los bienes o los servicios disponibles en dichos sitios o recursos, o a través de ellos.

Sun agradece sus comentarios

Sun tiene interés en mejorar la calidad de su documentación por lo que agradece sus comentarios y sugerencias. Puede enviar sus comentarios desde la siguiente dirección:

<http://www.sun.com/hwdocs/feedback>

Los comentarios deben incluir el título y el número de referencia del documento:

Guía del usuario de Sun Integrated Lights Out Manager 2.0, referencia 820-2697-10.

Introducción a ILOM

Sun™ Integrated Lights Out Manager (ILOM) 2.0 es un firmware de administración de sistemas que puede utilizarse para supervisar, controlar y configurar una serie de plataformas de servidor Sun.

Este capítulo contiene las secciones siguientes:

- “Qué es ILOM” en la página 1
- “ILOM en el SP y el CMM” en la página 2
- “Interfaces de ILOM” en la página 3
- “Red de administración de ILOM” en la página 4
- “Métodos de conexión con ILOM” en la página 5
- “Funciones de las cuentas de usuario de ILOM” en la página 6
- “Cuenta de administrador de ILOM preconfigurada” en la página 6
- “Características de ILOM” en la página 7
- “Nuevas funciones de ILOM 2.0” en la página 9
- “Otras herramientas de administración” en la página 9

Qué es ILOM

Integrated Lights Out Manager (ILOM) es un firmware de administración de sistemas que se entrega preinstalado en algunas plataformas de servidor Sun. Su presencia permite administrar y supervisar de forma activa los componentes instalados en el servidor. Mediante ILOM, es posible ver la configuración del hardware, supervisar la información del sistema, manejar las alertas y realizar otras actividades para tener un control proactivo sobre el sistema. Para ello, proporciona una interfaz web basada en navegador y una interfaz de línea de comandos, así como sendas interfaces de usuario de SNMP e IPMI. ILOM se inicializa

automáticamente tan pronto como el sistema recibe energía y sigue ejecutándose con independencia del estado del sistema operativo host, lo que lo convierte en un sistema de administración remota que no requiere la presencia física del operador.

Entre las principales características de ILOM se incluyen:

- Utiliza su propio procesador y sus propios recursos para la ejecución.
- Permite administrar el servidor sin consumir recursos del sistema.
- Sigue posibilitando la administración mediante la alimentación de modo de espera incluso cuando se ha apagado el servidor.
- Proporciona una red de administración independiente de la red de datos.
- Suministra una vista concisa del inventario de hardware y los datos del entorno.
- Proporciona capacidad para controlar la alimentación del sistema, administrar componentes y acceder a la consola del host.
- Sirve como punto de integración para otras herramientas de administración tales como Sun N1™ System Manager y aplicaciones de otros fabricantes.
- Permite descargar los cambios de la BIOS y el firmware del procesador de servicios (SP).
- Administra el inventario de los componentes conectables en marcha.

ILOM en el SP y el CMM

ILOM funciona con una gran variedad de plataformas de servidor Sun, entre ellas, servidores para montaje en bastidor y servidores blade. Se preinstala en el procesador de servicios (SP) del servidor blade o de bastidor, o bien en el módulo de supervisión del chasis (CMM), según corresponda a la plataforma utilizada.

ILOM admite dos formas de administrar un sistema: mediante el uso del SP directamente o, si procede, mediante el CMM.

- **Uso del procesador de servicios:** la posibilidad de administrar los SP de los servidores del bastidor estableciendo comunicación directa con el SP o los blades permite controlar cada operación del sistema o los blades de forma independiente. Este método puede resultar útil para resolver problemas en un determinado procesador de servicios o acceder a sistemas o blades específicos de instalaciones compartidas por varios propietarios.
- **Uso del módulo de supervisión del chasis:** si el sistema incluye un CMM, éste puede utilizarse para configurar y administrar los componentes de todo el sistema o administrar el SP de un módulo blade específico.

Interfaces de ILOM

ILOM puede utilizarse mediante una serie de interfaces.

- **Interfaz web:** proporciona una interfaz de navegador muy fácil de utilizar que permite iniciar la sesión en el SP y realizar tareas de IPMI, supervisión y administración del sistema. Encontrará más información sobre la interfaz web de ILOM en el [Capítulo 4](#).
- **Interfaz de la línea de comandos (CLI):** permite manejar ILOM introduciendo comandos con el teclado y es conforme con las interfaces CLI y los protocolos de generación de secuencias de comandos estándar: CLP “SMASH” del DMTF. Es posible conectar un terminal o un PC que ejecute un emulador de terminales directamente al puerto serie del sistema, o bien conectarlo al puerto de administración de red Ethernet utilizando el protocolo SSH (Secure Shell). Para obtener información sobre la interfaz de la línea de comandos, consulte el [Capítulo 3](#).
- **Remote Console:** esta aplicación de ILOM permite acceder a la consola del servidor de forma remota. Redirige el teclado, el ratón y la pantalla de vídeo, y puede redirigir las entradas y salidas procedentes de las unidades de CD y disquete de la máquina local. Si precisa información sobre Remote Console, consulte el [Capítulo 12](#).
- **IPMI (Intelligent Platform Management Interface):** mediante el uso de IPMI v1.5 y v2.0 con la utilidad IPMItool, puede administrar y configurar dispositivos utilizando una interfaz de línea de comandos para recuperar la información del controlador de administración de la placa base (BMC) del sistema. Con IPMItool, puede supervisar el estado de los componentes de hardware de forma remota, examinar los registros del sistema, recibir informes sobre componentes sustituibles y redirigir la consola del servidor. Encontrará más información sobre IPMI en el [Capítulo 9](#).
- **Interfaz SNMP (Simple Network Management Protocol):** ILOM también proporciona una interfaz SNMP v3.0 (con compatibilidad limitada con SNMP v1 y SNMP v2c) para aplicaciones de administración de centros de procesamiento de datos (CPD) externas tales como Sun N1™ System Manager y otras aplicaciones de terceros como Hewlett-Packard OpenView® y IBM Tivoli®. Encontrará más información sobre SNMP en el [Capítulo 10](#).

Red de administración de ILOM

La plataforma del servidor Sun se entrega con un puerto de administración de red y un puerto de datos. Estas conexiones Ethernet físicas son independientes y están destinadas a ILOM y los sistemas operativos que se ejecutan en el hardware del host. Si lo desea, puede administrar la plataforma con ILOM estableciendo conexión con el puerto dedicado a la administración de red. Si decide conectarse a ILOM mediante este puerto, el tráfico destinado a ILOM se separará de cualquier otra transferencia de datos efectuada por el host del sistema operativo. No pasa ningún paquete de datos a través del puerto de administración de red. Esto permite aislar el tráfico de administración en una red independiente si es necesario.

La ubicación y la etiqueta que designa el puerto de administración de red son específicas de cada sistema. Asimismo, el tipo de plataforma del servidor determina cómo se establece la comunicación de administración interna. Por ejemplo, en un servidor blade, el puerto de red proporciona una conexión con todos los CMM y SP del chasis. Consulte la documentación de su plataforma para averiguar la forma en que el sistema establece sus comunicaciones para la administración.

Si decide no utilizar ILOM ni el puerto de administración de red para administrar el servidor, no podrá disponer de muchas de las funciones avanzadas de ILOM, entre ellas, la supervisión del entorno, la administración con IPMI y la interfaz web. Puede usar el puerto de datos del sistema operativo host para acceder a aplicaciones de administración de red, herramientas de SNMP o utilidades del sistema operativo de terceros, aunque estas soluciones sólo proporcionan una vista limitada de la plataforma. Asimismo, tiene la posibilidad de administrar el servidor de forma local estableciendo la conexión a través del puerto serie del servidor mediante un terminal o un PC que ejecute un software de emulación de terminales. Tenga presente que, si no dispone de ninguna forma de conexión directa con ILOM, no podrá administrar la plataforma del servidor Sun de forma remota.

Métodos de conexión con ILOM

La forma de establecer conexión con ILOM depende de la plataforma de servidor utilizada.

En la tabla siguiente, figuran los métodos disponibles para efectuar la conexión con ILOM.

TABLA 1-1 Métodos de conexión con ILOM

Método de conexión	Servidor de bastidor	Blade	Interfaz admitida	Descripción
Conexión de administración de red Ethernet	Sí	Sí	CLI e interfaz web	Conexión con el puerto de administración de red Ethernet. Es preciso conocer la dirección IP de ILOM. Este método puede utilizarse mediante la interfaz web y la línea de comandos.
Conexión serie, a través de servidor o blade	Sí	No	Sólo CLI	Conexión directa con el puerto serie de administración del servidor o el blade. Si es preciso, utilice un cable adaptador serie para efectuar la conexión con el puerto serie. Este método sólo puede utilizarse mediante la interfaz de la línea de comandos.
Conexión serie, a través del CMM	No	Sí	Sólo CLI	Conexión con el puerto serie del CMM. Este método sólo puede utilizarse mediante la interfaz de la línea de comandos.

Nota – ILOM admite un máximo de 10 sesiones activas, lo que incluye sesiones de comunicación serie, SSH (Secure Shell) e interfaz web.

Para realizar la administración de red utilizando la interfaz web o la línea de comandos de ILOM, necesita conocer la dirección IP del CMM o el SP que desee administrar. Cada CMM y SP recibe una dirección IP exclusiva durante la configuración inicial del sistema. Para asignar direcciones IP iniciales a los SP y CMM, consulte el [Capítulo 2](#).

Funciones de las cuentas de usuario de ILOM

Las cuentas de usuario de ILOM tienen funciones definidas que determinan el tipo de acceso y los derechos de los usuarios de ILOM. Los administradores pueden manejar estas cuentas utilizando la interfaz web o la línea de comandos de ILOM. Las funciones asignadas a las cuentas de ILOM son:

- **Administrador:** permite acceder a todos los componentes, funciones y comandos de ILOM.
- **Operador:** proporciona acceso completo para administrar y supervisar el sistema host y acceso de sólo lectura a la configuración de ILOM.

Cuenta de administrador de ILOM preconfigurada

ILOM tiene preinstalada una cuenta de administrador preconfigurada:

- Nombre de usuario: `root`
- Contraseña: `changeme`

Esta cuenta, conocida como `root`, no puede borrarse ni modificarse, salvo en lo que concierne a la contraseña predeterminada (`changeme`), que puede sustituirse por otra. Esta cuenta incorpora privilegios administrativos (acceso de lectura y escritura) sobre todos los componentes, funciones y comandos de ILOM.

La primera vez que se accede a ILOM, en el nivel del SP o el CMM, es preciso iniciar la sesión como usuario `root` con la contraseña predeterminada, `changeme`. Una vez iniciada la sesión y establecida la conexión de red con el sistema, es conveniente cambiar la contraseña `changeme` asociada a la cuenta `root` de ILOM. Cambie esta contraseña en cada SP y CMM del sistema para impedir el acceso no autorizado. Para obtener más información sobre el cambio de contraseña de la cuenta `root` de ILOM, consulte [“Reinicio del SP de ILOM” en la página 211](#).

Características de ILOM

En la Tabla 1-1 figuran las características y tareas de ILOM que son comunes a todos los sistemas Sun compatibles con este software de administración. Para saber si una función puede utilizarse en su sistema, consulte la documentación de usuario suministrada con el servidor.

TABLA 1-2 Características de ILOM

Característica	Ventaja para el usuario
INTERFACES	
Interfaz web	<ul style="list-style-type: none">• Proporciona una interfaz de usuario de navegador basada en la interfaz estándar de Sun.
Interfaz de la línea de comandos	<ul style="list-style-type: none">• Es compatible con las interfaces de línea de comandos y las herramientas de secuencias de comandos estándar: CLP “SMASH” del DMTF.• Reutiliza secuencias de comandos existentes con los sistemas Sun, automatiza las tareas utilizando interfaces conocidas.
Interfaces de administración de sistemas	<ul style="list-style-type: none">• Es compatible con los protocolos estándar SNMP v1, v2c, v3 e IPMI v1.5 y v2.0. La MIB de plataforma permite administrar la plataforma utilizando SNMP además de IPMI. La MIB de control permite integrar en ILOM aplicaciones de administración personalizadas o de terceros.• Proporciona acceso a sistemas remotos mediante la aplicación Remote Console de ILOM.
SEGURIDAD	
Funcionalidad SSH 2.0	<ul style="list-style-type: none">• Proporciona acceso seguro a la interfaz de la línea de comandos.
LDAP, MSFT Active Directory, RADIUS	<ul style="list-style-type: none">• Permite utilizar los protocolos estándar de autenticación y autorización para facilitar la integración en entornos existentes.
Administración de usuarios	<ul style="list-style-type: none">• Incorpora las funciones de administrador y operador con niveles de acceso configurables para añadir más seguridad y control sobre los sistemas.
Posibilidad de cambiar la contraseña de root	<ul style="list-style-type: none">• Impide el acceso no autorizado al sistema. La contraseña predeterminada se cambia utilizando un botón de comando o un puente.
Certificado SSL	<ul style="list-style-type: none">• Permite establecer comunicaciones seguras utilizando la certificación SSL predeterminada y una clave autofirmada para el acceso mediante HTTPS.

TABLA 1-2 Características de ILOM (*continuación*)

Característica	Ventaja para el usuario
ACCESO LOCAL Y REMOTO	
Acceso al SP mientras el host está apagado.	<ul style="list-style-type: none"> • Permite a ILOM seguir funcionando con independencia del estado del sistema operativo host.
Puerto dedicado a la administración de red	<ul style="list-style-type: none"> • Separa el tráfico de administración de red del tráfico de datos.
Remote Console	<ul style="list-style-type: none"> • Proporciona una interfaz web sencilla para acceder a sistemas remotos. No es preciso entrar en el SP para iniciar Remote Console.
Campo de nombre del sistema editable	<ul style="list-style-type: none"> • Permite al administrador utilizar el campo de nombre del sistema host, además de la dirección IP, para identificar el sistema.
Activación y desactivación de la interfaz web	<ul style="list-style-type: none"> • Restringe el acceso a ILOM para permitir sólo la entrada a través de la interfaz de la línea de comandos.
SUPERVISIÓN Y REGISTRO DE EVENTOS	
Supervisión y control mediante SNMP e IPMI	<ul style="list-style-type: none"> • Supervisa los componentes utilizando comandos de SNMP estándar y la utilidad IPMItool de IPMI.
Registro de eventos	<ul style="list-style-type: none"> • Proporciona un método homogéneo para registrar todos los datos de "servicios".
Umbral de alerta configurables	<ul style="list-style-type: none"> • Permite a los usuarios configurar el SP para enviar una alerta PET de IPMI cuando se superan los umbrales.
Notificación de eventos por correo electrónico	<ul style="list-style-type: none"> • Proporciona una forma rápida y cómoda de notificar los eventos.
Notificación de los errores del hardware y el sistema, y los errores de memoria ECC mediante los registros del SP, el registro del sistema y el host de registros remoto	<ul style="list-style-type: none"> • Facilita y agiliza la identificación y el diagnóstico de errores, con la consiguiente reducción de caídas del sistema.
CONTROL DE LA ALIMENTACIÓN	
Apagado forzoso	<ul style="list-style-type: none"> • Permite efectuar el apagado de urgencia del sistema.
Cierre normal y ciclo de apagado y encendido	<ul style="list-style-type: none"> • Permite al usuario cerrar el sistema operativo antes de apagar el sistema.
Encendido y apagado remotos	<ul style="list-style-type: none"> • Permite al usuario controlar el encendido y apagado del sistema de forma remota.
FIRMWARE	
Identificación de las versiones del firmware desde la interfaz web o la línea de comandos	<ul style="list-style-type: none"> • Proporciona una forma sencilla de identificar las versiones del firmware.
Actualizaciones del firmware desde la interfaz web o la línea de comandos	<ul style="list-style-type: none"> • Proporciona procedimientos sencillos para actualizar el firmware.

TABLA 1-2 Características de ILOM (continuación)

Característica	Ventaja para el usuario
CONFIGURACIÓN	
Configuración manual del SP, incluida la dirección IP, a través de la interfaz de la BIOS, los puertos serie o Ethernet del SP o el SO host	• Simplifica la configuración inicial.
Dirección IP del SP programable desde el teclado y el monitor locales	• Facilita la configuración IP manual de los sistemas de un centro de procesamiento de datos.

Nuevas funciones de ILOM 2.0

- Active Directory
- Alertas por correo electrónico
- Nuevas MIB actualizadas específicas de Sun
- Captura de eventos SNMP
- Versiones internacionales de Remote Console

Otras herramientas de administración

Los servidores Sun admiten una serie de herramientas de administración de sistemas que pueden utilizarse para controlar el sistema. Entre estas herramientas se incluyen, además de ILOM:

- **Sun N1 System Manager:** herramienta de administración de sistemas completa que puede adquirirse por separado. Ofrece funciones flexibles que simplifican el manejo de la infraestructura de los servidores Sun Fire x64, SPARC y los módulos de servidor Sun Blade. Con Sun N1 System Manager, los administradores de TI pueden supervisar, mantener y provisionar múltiples sistemas de forma remota desde cualquier estación de administración Sun N1. Para obtener más información sobre Sun N1 System Manager, visite el sitio siguiente:

http://www.sun.com/software/products/system_manager

- **Herramientas de administración de sistemas de terceros:** los sistemas Sun permiten utilizar SNMP (v1, v2c, v3) e IPMI (v1.5 y v2.0) para integrar herramientas de administración de otras marcas tales como HP Systems Insight Manager y IBM Tivoli. La lista de algunas de las herramientas de terceros más importantes y su compatibilidad con los sistemas Sun x64 se encuentra en:

<http://www.sun.com/x64/system-management/tools.jsp>

Establecimiento de la comunicación inicial con ILOM

Es posible establecer comunicación con ILOM conectando la consola al puerto serie de administración del servidor o el CMM, o bien a través de una conexión Ethernet con el puerto de administración de red del servidor o el CMM.

El tipo de conexión que se establezca determinará el tipo de tareas que se podrán realizar. Por ejemplo, para poder acceder de forma remota a todas las funciones de administración de ILOM, será preciso establecer una conexión Ethernet y asignar una dirección IP al SP del servidor y, si procede, al CMM.

Este capítulo contiene las secciones siguientes:

- “Configuración inicial de ILOM” en la página 12
 - “Hoja de configuración inicial” en la página 12
 - “Consideraciones sobre la asignación de direcciones IP mediante DHCP” en la página 14
 - “Consideraciones sobre la asignación de direcciones IP estáticas” en la página 18
 - “Configuración de direcciones IP de la red de administración” en la página 20
 - “Asignación de los puertos de red de ILOM” en la página 20
 - “Identificación del SP y el CMM del servidor mediante un nombre de sistema” en la página 22
 - “Texto de identificación del sistema de los servidores Sun” en la página 22
- “Asignación de direcciones IP a las interfaces de los SP en las plataformas de servidor Sun” en la página 23
 - “Asignación de direcciones IP con DHCP utilizando una conexión de administración Ethernet” en la página 23
 - “Asignación de una dirección IP estática al SP del servidor mediante una conexión serie” en la página 25
 - “Asignación de una dirección IP estática al CMM mediante una conexión serie” en la página 27

- “Edición de las direcciones IP asignadas mediante una conexión de administración Ethernet” en la página 29
 - “Edición de las direcciones IP existentes en ILOM mediante la interfaz web” en la página 29
 - “Edición de las direcciones IP existentes en ILOM mediante la línea de comandos” en la página 31
 - “Asignación del nombre o el identificador del sistema” en la página 33
-

Configuración inicial de ILOM

Antes de establecer la comunicación con ILOM, debería consultar los temas siguientes:

- “Hoja de configuración inicial” en la página 12
- “Consideraciones sobre la asignación de direcciones IP mediante DHCP” en la página 14
- “Consideraciones sobre la asignación de direcciones IP estáticas” en la página 18
- “Configuración de direcciones IP de la red de administración” en la página 20
- “Asignación de los puertos de red de ILOM” en la página 20
- “Identificación del SP y el CMM del servidor mediante un nombre de sistema” en la página 22
- “Texto de identificación del sistema de los servidores Sun” en la página 22

Hoja de configuración inicial

Use la hoja de la [TABLA 2-1](#) a fin de recopilar la información necesaria para establecer la comunicación inicial con ILOM.

TABLA 2-1 Hoja de configuración inicial para establecer la comunicación con ILOM

Información de configuración	Requisito	Descripción
Conexión de la consola serie local	<p>Opcional: <i>si se utiliza DHCP para asignar la dirección IP inicial.</i></p> <p>Obligatoria: <i>si no se utiliza el servidor DHCP para asignar la dirección IP inicial.</i></p>	<p>Si no utiliza un servidor DHCP para asignar las direcciones IP al SP o el CMM, debe establecer una conexión de la consola serie local con ILOM a través del puerto serie de administración del servidor o el módulo de supervisión del chasis (CMM).</p> <p>Para obtener más información sobre la forma de conectar una consola serie al servidor o el CMM, consulte la documentación de usuario suministrada con la plataforma de servidor Sun.</p>
Conexión Ethernet de administración remota	Opcional	<p>Conecte un cable de red (Ethernet) al puerto de administración de red del servidor o el CMM. La etiqueta que aparece sobre el puerto de administración de red puede variar en función de la plataforma de servidor utilizada. Algunos de estos puertos aparecen etiquetados como NET MGT o MGT. Si tiene alguna duda sobre la etiqueta del puerto de administración de red o la forma de conectarle un cable Ethernet, consulte la documentación de usuario suministrada con la plataforma.</p> <p>Para acceder a toda la gama de funciones de administración de ILOM, es preciso conectar la red de área local al puerto de administración de red de un servidor o un CMM.</p> <p>Recuerde que todos los servidores Sun destinados a montaje en bastidor incorporan un puerto de administración de red, pero no así los módulos de los servidores Sun Blade. La comunicación Ethernet con los módulos de servidores blade se realiza a través del puerto de administración de red del CMM.</p>
Asignación de direcciones IP al SP	Obligatorio	<p>Decida si asignará direcciones IP estáticas o DHCP a cada SP o CMM del servidor. Toda la comunicación de administración de sistemas remotos con ILOM se realiza a través de la red de administración del CMM o el SP del servidor.</p> <p>Para obtener más información, consulte los temas siguientes:</p> <ul style="list-style-type: none"> • “Consideraciones sobre la asignación de direcciones IP mediante DHCP” en la página 14 • “Consideraciones sobre la asignación de direcciones IP estáticas” en la página 18 • “Asignación de direcciones IP a las interfaces de los SP en las plataformas de servidor Sun” en la página 23

TABLA 2-1 Hoja de configuración inicial para establecer la comunicación con ILOM (*continuación*)

Información de configuración	Requisito	Descripción
Interfaz de ILOM	Obligatorio	<p>Al establecer (o modificar) una dirección IP en el CMM o el SP de un servidor, se utiliza una de las siguientes interfaces:</p> <ul style="list-style-type: none"> • Interfaz de la línea de comandos (CLI): se utiliza para establecer la dirección IP inicial. Si no se ha asignado ninguna dirección IP al CMM o el SP del servidor, puede conectarse a ILOM para asignarla a través de una consola serie local. La interfaz de la línea de comandos se utiliza normalmente para todas las tareas que se realizan en ILOM a través de una conexión serie (consola serie local, emulador de terminal o conexión SSH remota). • Interfaz web: se utiliza para modificar una dirección IP existente. Si se ha asignado una dirección IP al CMM o el SP del servidor y se ha establecido una conexión LAN con el puerto MGT, puede conectarse con ILOM para cambiar la dirección (o direcciones) IP existente utilizando la interfaz web. Esta interfaz se utiliza normalmente para todas las tareas que se realizan en ILOM a través de una conexión Ethernet de administración. <p>Para obtener más información sobre las interfaces de ILOM, consulte el Capítulo 3 y el Capítulo 4.</p>
Acceso a ILOM con un servidor de seguridad	Opcional	<p>Consulte el uso de los puertos de red de ILOM para redes Ethernet que precisen acceso a través de un servidor de seguridad. Para obtener más información, consulte “Asignación de los puertos de red de ILOM” en la página 20.</p>
Asignación del nombre de sistema al SP	Opcional	<p>Si lo desea, puede asignar un nombre de sistema host significativo a un SP del servidor. Para obtener más información, consulte “Identificación del SP y el CMM del servidor mediante un nombre de sistema” en la página 22 o “Asignación del nombre o el identificador del sistema” en la página 33.</p>
Asignación de un identificador del sistema	Opcional	<p>Si lo desea, puede asignar un identificador del sistema (nombre significativo) a un servidor Sun. Para obtener más información, consulte “Identificación del SP y el CMM del servidor mediante un nombre de sistema” en la página 22 o “Asignación del nombre o el identificador del sistema” en la página 33.</p>

Consideraciones sobre la asignación de direcciones IP mediante DHCP

Si tiene previsto utilizar un servidor DHCP (Dynamic Host Configuration Protocol) para asignar la dirección IP a un CMM o un SP del servidor, consulte los temas siguientes:

- [“Difusión de paquetes DHCPDISCOVER en la plataforma de servidor Sun”](#) en la [página 15](#)
- [“Requisitos para la asignación mediante DHCP”](#) en la [página 15](#)
- [“Dirección MAC de la interfaz de red del SP”](#) en la [página 15](#)
- [“Requisitos posteriores a la asignación mediante DHCP”](#) en la [página 17](#)

Difusión de paquetes DHCPDISCOVER en la plataforma de servidor Sun

El CMM o el SP de los servidores Sun transmite automáticamente un paquete DHCPDISCOVER cuando la plataforma empieza a recibir corriente. Si tiene instalado un servidor DHCP en la red, éste devuelve automáticamente a cada SP o CMM que haya enviado la petición un paquete DHCPOFFER que contiene la dirección (o direcciones) IP y cualquier otra información de configuración de red.

Nota – Puede dejar que el servidor DHCP asigne las direcciones IP de Ethernet por usted o configurar dicho servidor para que asigne direcciones IP específicas suministrando la dirección MAC de los SP. Para obtener más información, consulte la documentación de usuario del servidor DHCP. Si precisa más información sobre la forma de obtener la dirección MAC del CMM o el SP del servidor, consulte [“Dirección MAC de la interfaz de red del SP” en la página 15](#).

Requisitos para la asignación mediante DHCP

Deben darse las siguientes condiciones para poder asignar direcciones IP a las interfaces de SP del servidor Sun utilizando un servidor DHCP:

- Debe haber un cable Ethernet conectado al puerto de administración del servidor o el CMM.
- Tiene que haber un servidor DHCP conectado a la misma subred que la plataforma de servidor Sun.
- El servidor DHCP tiene que estar configurado para aceptar nuevas direcciones MAC (Media Access Control).
- ILOM tiene que tener habilitada la opción de configuración con DHCP. Esta opción está habilitada de forma predeterminada.

Dirección MAC de la interfaz de red del SP

Si tiene previsto usar un servidor DHCP para asignar la dirección (o direcciones) IP a la interfaz de red de cada SP, puede que necesite conocer la dirección MAC del CMM o el SP del servidor.

Puede obtener la dirección MAC del procesador de servicios mediante uno de los métodos descritos en la [TABLA 2-2](#).

TABLA 2-2 Métodos para obtener la dirección MAC del SP

Categoría de ILOM	Método	Descripción
SP de servidor montado en bastidor	Ver la etiqueta interna.	Normalmente, la dirección MAC del SP de la red de administración se encuentra en un adhesivo pegado al servidor. Si la dirección no aparece en dicho adhesivo, consulte la documentación de usuario suministrada con la plataforma de servidor Sun.
SP de servidor blade		
CMM	Ver la etiqueta interna.	Normalmente, la dirección MAC del CMM de la red de administración se encuentra en un adhesivo pegado al CMM. Si la dirección no aparece en dicho adhesivo, consulte la documentación de usuario suministrada con la plataforma de servidor Sun.
Todos	Hoja de información del cliente	Consulte la hoja de información del cliente (Customer Information Sheet) suministrada con la plataforma.

Requisitos posteriores a la asignación mediante DHCP

Una vez que el servidor DHCP ha asignado la dirección (o direcciones) IP a cada interfaz de red del SP, puede identificar las direcciones asignadas utilizando uno de los métodos especificados en la [TABLA 2-3](#).

TABLA 2-3 Métodos para identificar las direcciones IP asignadas por el servidor DHCP

Método	Descripción
Archivo de registro de DHCP (Tenga presente que este archivo no forma parte de ILOM, sino que es el archivo de registro del servidor DHCP.)	Abra el archivo de registro de DHCP y haga lo siguiente: <ol style="list-style-type: none">1. Localice la dirección MAC del procesador de servicios en el campo de dirección MAC.2. Identifique el valor del campo de dirección IP que corresponda al valor contenido en el campo de dirección MAC.3. Utilice la dirección IP identificada en el paso 2 para establecer la comunicación remota con ILOM utilizando la interfaz web. <p>Sugerencia: normalmente, las entradas del registro DHCP son líneas independientes compuestas por los siguientes campos separados por comas: ID, fecha, hora, descripción, dirección IP, nombre del sistema, dirección MAC.</p>
Conexión de la consola serie	Establezca una conexión de la consola serie con el puerto serie del servidor o el CMM. Inicie la sesión de ILOM como usuario root utilizando la interfaz de la línea de comandos y escriba uno de los siguientes comandos: <ul style="list-style-type: none">• Para servidores independientes montados en bastidor: <code>show /SP/network</code>• Para módulos de servidor blade en un chasis: <code>show /CH/BLn/SP network</code>• Para un CMM situado en la ranura 0 de un chasis: <code>show /CMM/network/CMM0</code>• Para un CMM situado en la ranura 1 de un chasis: <code>show /CMM/network/CMM1</code>

Consideraciones sobre la asignación de direcciones IP estáticas

Si tiene previsto asignar direcciones IP estáticas al CMM o el SP de un servidor, consulte los temas siguientes:

- [“Requisitos para la asignación de direcciones IP estáticas”](#) en la página 18
- [“Configuración del dispositivo serie o el emulador de terminal”](#) en la página 19
- [“Requisitos posteriores a la asignación de direcciones IP estáticas”](#) en la página 19

Requisitos para la asignación de direcciones IP estáticas

Para asignar inicialmente una dirección IP estática al CMM o el SP de un servidor, es preciso cumplir los requisitos descritos en la [TABLA 2-4](#).

TABLA 2-4 Requisitos para la asignación de direcciones IP estáticas

Requisitos	Paso	Descripción
Establecer una conexión de consola serie.	1	<p>Establezca una conexión serie entre la consola y el CMM o el SP del servidor conectando un terminal, o un PC que ejecute un emulador de terminal, al puerto serie del servidor o el CMM.</p> <p>Para obtener más información sobre la forma de conectar un PC o un terminal serie al puerto serie del servidor o el CMM, consulte la documentación de usuario suministrada con la plataforma de servidor Sun.</p> <p>Recuerde que, en el caso de plataformas de servidor Sun que tienen CMM, puede configurar la dirección IP estática de los SP del blade utilizando la interfaz de la línea de comandos de ILOM en el CMM.</p>
Configurar los valores del puerto serie.	2	<p>Configure los valores serie necesarios para el dispositivo terminal o el software de emulación de terminal.</p> <p>Para obtener más información, consulte “Configuración del dispositivo serie o el emulador de terminal” en la página 19.</p>
Asignar la dirección IP estática utilizando la línea de comandos de ILOM.	3	<p>Asigne la dirección IP estática utilizando la interfaz de la línea de comandos de ILOM.</p> <p>Para obtener más información, consulte los temas siguientes que sean aplicables a la configuración de su sistema:</p> <ul style="list-style-type: none">• “Asignación de una dirección IP estática al SP del servidor mediante una conexión serie” en la página 25. <p>o</p> <ul style="list-style-type: none">• “Asignación de una dirección IP estática al CMM mediante una conexión serie” en la página 27.

Configuración del dispositivo serie o el emulador de terminal

Al establecer la conexión con ILOM mediante una consola serie, es necesario configurar el dispositivo terminal o el software de emulación de terminal para que utilicen los valores siguientes:

- 8N1: ocho bits de datos, sin paridad, un bit de parada
- 9600 baudios
- Control de flujo de hardware inhabilitado (CTS/RTS)
- Control de flujo de software inhabilitado (XON/XOFF)

Los siguientes comandos `show` de la línea de comandos permiten ver las propiedades y los valores asociados al puerto serie externo de un servidor o un CMM:

```
show <destino>
```

Ejemplos:

- Para un CMM: `show /CMM/serial/external`
- Para un servidor montado en un bastidor: `show /SP/serial/external`
- Para un módulo de servidor blade: `show /CH/BLn/SP/serial/external`

Requisitos posteriores a la asignación de direcciones IP estáticas

Es posible administrar direcciones IP de forma remota mediante la interfaz web o la línea de comandos de ILOM si se cumplen estos requisitos:

- Asignación de una dirección IP al CMM o el SP del servidor.
- Establecimiento de una conexión Ethernet con el puerto de administración de red del servidor o el CMM.

Para obtener más información sobre la forma de realizar la asignación de direcciones IP mediante una conexión de administración de red Ethernet, consulte [“Edición de las direcciones IP asignadas mediante una conexión de administración Ethernet” en la página 29](#).

Configuración de direcciones IP de la red de administración

Las conexiones IP de ILOM normalmente se configuran en la interfaz de red del SP, que permite separar el tráfico de administración del tráfico de datos. Las direcciones IP DHCP o estáticas asignadas al CMM o el SP de un servidor se conocen como *direcciones IP de la red de administración* y no deben confundirse con las direcciones IP de la red de datos.

Recuerde que las direcciones IP de la red de datos se configuran después de haber instalado un sistema operativo host en un servidor. Es importante diferenciar estas direcciones IP de las direcciones IP de la red de administración, ya que tienen distintas finalidades.

Todas las referencias futuras a las direcciones IP de la red de administración que se hagan en esta guía se citarán como “dirección IP del SP del servidor” o “dirección IP del CMM”. Normalmente, estas referencias aparecen al suministrar instrucciones para establecer una conexión con la interfaz web o la interfaz de la línea de comandos de ILOM.

Para obtener más información sobre la red de administración de ILOM, consulte [“Red de administración de ILOM” en la página 4](#).

Si precisa información sobre la forma de asignar las direcciones IP de la red de datos a un servidor, consulte la documentación de usuario suministrada con el sistema operativo host.

Asignación de los puertos de red de ILOM

En la [TABLA 2-5](#) y la [TABLA 2-6](#) se indican los puertos de red utilizados por ILOM de forma predeterminada. La mayoría de ellos son configurables. Si va a configurar un acceso seguro a ILOM mediante un servidor de seguridad, deberá configurar estos puertos de acuerdo con los que utilice el servidor de seguridad.

TABLA 2-5 Asignación directa de los puertos de ILOM en el SP del servidor

Puertos	Protocolos	Aplicaciones
80	HTTP sobre TCP	SP: puerto configurable por el usuario de ILOM
443	HTTPS sobre TCP	SP: puerto configurable por el usuario de ILOM
5120	TCP	SP: Remote Console de ILOM (CD)
5123	TCP	SP: Remote Console de ILOM (disquete)
5121	TCP	SP: Remote Console de ILOM (teclado y ratón)

TABLA 2-5 Asignación directa de los puertos de ILOM en el SP del servidor (*continuación*)

7578	TCP	SP: Remote Console de ILOM (vídeo)
22	SSH sobre TCP	SSH (Secure Shell)
69	TFTP sobre UDP	TFTP (Trivial File Transport Protocol)
123	NTP sobre UDP	NTP (Network Time Protocol)
161	SNMP sobre UDP	SNMP (Simple Network Management Protocol)
162	IPMI sobre UDP	IPMI: captura de eventos de plataforma PET (puerto de salida)
389	LDAP sobre UDP/TCP	LDAP: Lightweight Directory Access Protocol (puerto configurable por el usuario)
514	Syslog sobre UDP	Syslog (puerto de salida)
546	DHCP sobre UDP	DHCP (Dynamic Host Configuration Protocol) (cliente)
623	IPMI sobre UDP	IPMI (Intelligent Platform Management Interface)
1812	RADIUS sobre UDP	RADIUS (Remote Authentication Dial In User Service)

TABLA 2-6 Asignación directa de los puertos de red de ILOM en el CMM

Puertos	Protocolos	Aplicaciones
80	HTTP sobre TCP	CMM: ILOM (puerto configurable por el usuario)
443	HTTPS sobre TCP	CMM: ILOM (puerto configurable por el usuario)
8000 - 8009	HTTP sobre TCP	CMM: ILOM en cada módulo (BL0-BL9)
8400 - 8409	HTTPS sobre TCP	CMM: ILOM en cada módulo (BL0-BL9)
22	SSH sobre TCP	SSH (Secure Shell)
69	TFTP sobre UDP	TFTP (Trivial File Transport Protocol)
123	NTP sobre UDP	NTP (Network Time Protocol)
161	SNMP sobre UDP	SNMP (Simple Network Management Protocol)
389	LDAP sobre UDP/TCP	LDAP: Lightweight Directory Access Protocol (puerto configurable por el usuario)
514	Syslog sobre UDP	Syslog (puerto de salida)
546	DHCP sobre UDP	DHCP (Dynamic Host Configuration Protocol) (cliente)
1812	RADIUS sobre UDP	RADIUS (Remote Authentication Dial In User Service)

Identificación del SP y el CMM del servidor mediante un nombre de sistema

Como alternativa a la dirección IP, es posible utilizar un nombre de sistema para identificar un determinado CMM o SP del servidor en la red. También se puede utilizar el nombre de sistema para establecer la conexión con ILOM en el CMM o el SP. Normalmente, este tipo de identificación del sistema y de conexión requiere la asociación del nombre del sistema a la dirección IP del SP (o el CMM) en el servicio de nombres (por ejemplo, DNS, NIS o SMB). Si utiliza nombres de sistema para identificar los CMM o los SP del servidor en el entorno de red, puede aplicar el mismo método para identificar el SP o el CMM en ILOM. Para ello, tiene que introducir el nombre de sistema del SP o el CMM en la página System Identification (identificación del sistema). Para obtener más información, consulte [“Asignación del nombre y el identificador del sistema mediante la interfaz web”](#) en la página 33.

Texto de identificación del sistema de los servidores Sun

El identificador del sistema es una cadena de texto que el usuario puede definir para facilitar la identificación de los componentes de un sistema Sun. Por ejemplo, es posible crear un identificador del sistema que indique la ubicación de un dispositivo, la identidad de un determinado servidor en un bastidor o la finalidad de un sistema.

Estos identificadores también se incluyen en las capturas de eventos SNMP y pueden ayudar a asociar la captura a la instancia de ILOM que se esté ejecutando en el sistema.

Para definir un identificador del sistema en ILOM, puede utilizar cualquier texto que describa el sistema o componente. El texto puede estar formado por todo tipo de caracteres a excepción de las comillas. Para obtener más información sobre la forma de especificar identificadores del sistema en ILOM, consulte [“Asignación del nombre o el identificador del sistema”](#) en la página 33.

Asignación de direcciones IP a las interfaces de los SP en las plataformas de servidor Sun

Utilice los procedimientos siguientes para asignar direcciones IP a las interfaces de red de los SP en las plataformas de servidor Sun.

- “Asignación de direcciones IP con DHCP utilizando una conexión de administración Ethernet” en la página 23
- “Asignación de una dirección IP estática al SP del servidor mediante una conexión serie” en la página 25
- “Asignación de una dirección IP estática al CMM mediante una conexión serie” en la página 27
- “Asignación del nombre y el identificador del sistema mediante la interfaz web” en la página 33
- “Asignación del nombre y el identificador del sistema mediante la línea de comandos” en la página 34

▼ Asignación de direcciones IP con DHCP utilizando una conexión de administración Ethernet

Siga estos pasos para asignar direcciones IP mediante DHCP:

1. **Asegúrese de que el servidor DHCP esté configurado para aceptar nuevas direcciones MAC (Media Access Control).**
Consulte la documentación suministrada con el software del servidor DHCP.
2. **Cerciórese de que haya un cable Ethernet conectado a uno de los puertos siguientes:**
 - Puerto Ethernet (NET MGT) del CMM, si procede.
 - Puerto Ethernet (MGT) de un servidor autónomo montado en un bastidor, si procede.

Nota – Si ILOM no se ha configurado previamente con una dirección IP estática, emite automáticamente un paquete DHCPDISCOVER con el ID de la dirección MAC de cada una de las interfaces de red de su SP. Si ILOM ya tiene configurada una dirección IP estática, deberá inhabilitarla en la ficha Network Settings (configuración de red). Para obtener más información sobre la modificación de direcciones IP, consulte [“Edición de las direcciones IP asignadas mediante una conexión de administración Ethernet” en la página 29.](#)

3. El servidor DHCP de la red devuelve un paquete DHCPPOFFER con la dirección IP y otra información. A continuación, el procesador de servicios administra las direcciones IP asignadas por el servidor DHCP.
4. Utilice uno de los métodos siguientes para obtener las direcciones IP asignadas por DHCP a las interfaces de red de los SP:
 - **ILOM y CMM con una conexión serie**

Inicie la sesión de ILOM como administrador utilizando una consola serie conectada al panel posterior del CMM. Por ejemplo, en el indicador de inicio de sesión, puede escribir el nombre de usuario preconfigurado para el administrador, root, y su contraseña predeterminada, changeme, y presionar Intro.
 - Para establecer el directorio de trabajo del CMM activo, escriba:
cd /CMM/network/CMM0
 - Para ver la dirección IP del CMM activo, escriba: **show**
 - Para descender en el nivel de detalle y ver las direcciones IP de cada blade, escriba:
show /CH/BL0/SP/network

Nota – CMM0 representa el CMM instalado en la ranura CMM0. BL0 representa el blade instalado en la ranura BL0. Para especificar el CMM o blade de destino, debe especificar el número de la ranura en la que se encuentre instalado el módulo. Las ranuras de blades pueden estar numeradas de 0 a 9. Las de los CMM pueden llevar los números 0 o 1.

- **ILOM y SP del servidor con una conexión serie**

Inicie la sesión de ILOM como administrador utilizando una consola serie conectada al panel posterior de un blade. Por ejemplo, en el indicador de inicio de sesión, puede escribir el nombre de usuario preconfigurado para el administrador, root, y su contraseña predeterminada, changeme, y presionar Intro.

Para ver la dirección IP del SP del blade, escriba:
show /SP/network
- **Registros del servidor DHCP**

Para ampliar la información, consulte [“Requisitos posteriores a la asignación mediante DHCP” en la página 17](#), o lea la documentación del servidor DHCP para obtener más detalles.

▼ Asignación de una dirección IP estática al SP del servidor mediante una conexión serie

Siga estos pasos para asignar una dirección IP estática al SP del servidor utilizando una conexión serie:

- 1. Establezca una conexión de la consola serie local con el SP del servidor.**
Conecte una consola serie al puerto serie del servidor o el CMM. Para obtener más información, consulte la documentación de usuario suministrada con la plataforma de servidor Sun.
- 2. Configure los valores siguientes en la ventana de terminal que aparece en la consola serie conectada:**
 - 8N1: ocho bits de datos, sin paridad, un bit de parada
 - 9600 baudios
 - Control de flujo de hardware inhabilitado (CTS/RTS)
 - Control de flujo de software inhabilitado (XON/XOFF)
- 3. Pulse Intro para establecer la conexión entre la consola serie y la interfaz del SP.**
Aparecerá el indicador de inicio de sesión de ILOM.
Por ejemplo: *nombre del sistema* Login:
- 4. Inicie la sesión de ILOM como administrador introduciendo un nombre de usuario y una contraseña de administrador, y pulse Intro.**

Nota – Puede iniciar la sesión de ILOM utilizando la cuenta de administrador que se entrega preconfigurada en ILOM: `root/changeme`. Para obtener más información, consulte [“Cuenta de administrador de ILOM preconfigurada” en la página 6](#).

Aparece el indicador predeterminado (->). El sistema está listo para recibir comandos de la interfaz de la línea de comandos para establecer los valores de configuración de red.

- 5. Escriba el comando siguiente para establecer el directorio de trabajo:**
`cd /SP/network`

6. Utilice los siguientes comandos en la línea de comandos para especificar la dirección IP, la máscara de red y la puerta de enlace.

Comando	Descripción y ejemplo
<code>set pendingipaddress=</code>	<p>Escriba este comando seguido de la dirección IP estática que quiera asignar al SP del servidor.</p> <p>Por ejemplo, si escribe: <code>set pendingipaddress=129.144.82.26</code> está indicando a ILOM que asigne 129.144.82.26 como dirección IP del SP del servidor.</p>
<code>set pendingipnetmask=</code>	<p>Escriba este comando seguido de la dirección de máscara de red estática que quiera asignar al SP del servidor.</p> <p>Por ejemplo, si escribe: <code>set pendingipnetmask=255.255.255.0</code> está indicando a ILOM que asigne 255.255.255.0 como máscara de red del SP del servidor.</p>
<code>set pendingipgateway=</code>	<p>Escriba este comando seguido de la dirección de puerta de enlace estática que quiera asignar al SP del servidor.</p> <p>Por ejemplo, si escribe: <code>set pendingipgateway=129.144.82.254</code> está indicando a ILOM que asigne 129.144.82.254 como dirección de puerta de enlace del SP del servidor.</p>
<code>setpendingipdiscovery=</code>	<p>Escriba este comando para que ILOM establezca una dirección IP estática en el SP del servidor.</p> <p><code>set pendingipdiscovery=static</code></p>
<code>set commitpending=true</code>	<p>Escriba este comando (<code>true</code>) para asignar los valores de red especificados.</p> <p>Por ejemplo: <code>set pendingipaddress=129.144.82.26</code> <code>set pendingipnetmask=255.255.255.0</code> <code>set pendingipnetmask=129.144.82.254</code> <code>set commitpending=true</code></p>

Normalmente, después de asignar (o cambiar) una dirección IP, finalizará la conexión con ILOM establecida utilizando la dirección IP anterior. Utilice la nueva dirección IP asignada para conectarse a ILOM.

▼ Asignación de una dirección IP estática al CMM mediante una conexión serie

Siga estos pasos para asignar una dirección IP estática al CMM utilizando una conexión serie:

1. **Compruebe si la conexión serie con el CMM activo está operativa.**

Para obtener más información sobre la forma de conectar una consola serie a un CMM, consulte la documentación de usuario suministrada con la plataforma de servidor Sun.

2. **Inicie la sesión de ILOM como administrador introduciendo un nombre de usuario y una contraseña de administrador, y pulse Intro.**

Nota – Puede iniciar la sesión de ILOM utilizando la cuenta de administrador que se entrega preconfigurada en ILOM: `root/changeme`. Para obtener más información, consulte [“Cuenta de administrador de ILOM preconfigurada” en la página 6](#).

Aparece el indicador predeterminado (->) y el sistema está listo para ejecutar los comandos de la línea de comandos con los que se establecerán los valores de configuración de red.

3. **Antes de definir una dirección IP estática en el CMM a través de la línea de comandos de ILOM, escriba el comando siguiente para establecer el directorio de trabajo:**

```
cd /CMM/network/CMM0
```

Nota – CMM0 se refiere al CMM instalado en la ranura CMM0. El CMM de destino se especifica haciendo referencia al número de ranura del CMM.

4. Utilice los siguientes comandos para especificar la dirección IP, la máscara de red y la puerta de enlace.

Comando	Descripción y ejemplo
<code>set pendingipaddress=</code>	<p>Escriba este comando seguido de la dirección IP estática que quiera asignar al CMM.</p> <p>Por ejemplo, si escribe: <code>set pendingipaddress=129.144.82.26</code> está indicando a ILOM que asigne <code>129.144.82.26</code> como dirección IP del CMM.</p>
<code>set pendingipnetmask=</code>	<p>Escriba este comando seguido de la dirección de máscara de red estática que quiera asignar al CMM.</p> <p>Por ejemplo, si escribe: <code>set pendingipnetmask=255.255.255.0</code> está indicando a ILOM que asigne la dirección <code>255.255.255.0</code> como máscara de red del CMM.</p>
<code>set pendingipgateway=</code>	<p>Escriba este comando seguido de la dirección de puerta de enlace estática que quiera asignar al CMM.</p> <p>Por ejemplo, si escribe:</p> <pre>set pendingipgateway=129.144.82.254</pre> <p>está indicando a ILOM que asigne la dirección <code>129.144.82.254</code> como puerta de enlace del CMM.</p>
<code>set pendingipdiscovery=</code>	<p>Escriba el comando siguiente para indicar a ILOM que desea establecer una dirección IP estática.</p> <pre>set pendingipdiscovery=static</pre>
<code>set commitpending=true</code>	<p>Escriba este comando (<code>true</code>) para asignar los valores de red especificados.</p> <p>Ejemplo:</p> <pre>set pendingipaddress=129.144.82.26 set pendingipnetmask=255.255.255.0 set pendingipgateway=129.144.82.254 set comitpending=true</pre>

Si se ha conectado a ILOM a través de una conexión SSH remota, la conexión realizada con la dirección IP anterior finalizará. Utilice la nueva dirección IP asignada para conectarse a ILOM.

Edición de las direcciones IP asignadas mediante una conexión de administración Ethernet

Utilice los procedimientos siguientes para modificar las asignaciones de direcciones IP del procesador de servicios a través de una conexión de administración Ethernet:

- “Edición de las direcciones IP existentes en ILOM mediante la interfaz web” en la página 29
- “Edición de las direcciones IP existentes en ILOM mediante la línea de comandos” en la página 31

▼ Edición de las direcciones IP existentes en ILOM mediante la interfaz web

Siga estos pasos si quiere editar las direcciones IP previamente asignadas al CMM o el SP del servidor utilizando la interfaz web de ILOM:

1. **Utilice un cliente basado en navegador para escribir la dirección IP del CMM o el SP en el cuadro de dirección del navegador y pulse Intro.**
Aparece la pantalla de acceso a ILOM.
2. **En esta pantalla, inicie la sesión como administrador introduciendo el nombre de usuario y la contraseña de administrador.**

Sugerencia – Puede iniciar la sesión de ILOM utilizando la cuenta de administrador que se entrega preconfigurada en ILOM: `root/changeme`. Para obtener más información, consulte “[Cuenta de administrador de ILOM preconfigurada](#)” en la página 6.

Aparece la interfaz de ILOM.

3. **En el panel derecho de la interfaz, haga clic en Configuration (configuración) --> Network (red).**
Se abre la página Network Settings (configuración de red) del servidor o el CMM.

FIGURA 2-1 ILOM en el SP del servidor: página de configuración de red

FIGURA 2-2 ILOM en el CMM: página de configuración de red

Name	MAC	Mode	IP Address	Gateway	Netmask
/CHIMASTERCMM	00:03:BA:84:CB:2A	DHCP	0.0.0.0	0.0.0.0	0.0.0.0
/CHICMM0	00:03:BA:F1:3B:88	Static	10.8.145.160	10.8.145.254	255.255.255.0
/CHIBL1	00:03:BA:F1:32:86	Static	10.8.145.162	10.8.145.254	255.255.255.0
/CHIBL3	00:03:BA:F1:2C:42	Static	10.8.145.164	10.8.145.254	255.255.255.0

4. Para editar las direcciones IP asignadas a las interfaces del SP, haga lo siguiente:
 - a. Seleccione el botón de la opción Use the Following IP Address (usar la siguiente dirección IP).
 - b. Introduzca los valores de IP Address, Subnet Mask y Gateway (dirección IP, máscara de subred y puerta de enlace, respectivamente) en los cuadros de texto.
 - c. Haga clic en Save (guardar) para que la nueva configuración tenga efecto. Normalmente, después de asignar (o cambiar) una dirección IP, finalizará la conexión con ILOM establecida utilizando la dirección IP anterior. Utilice la nueva dirección IP asignada para conectarse a ILOM.

▼ Edición de las direcciones IP existentes en ILOM mediante la línea de comandos

Siga estos pasos si quiere editar las direcciones IP previamente asignadas al CMM o el SP del servidor utilizando la interfaz de la línea de comandos de ILOM:

1. Establezca una conexión de consola serie o una conexión SSH con el CMM o el SP del servidor:

■ Conexión de la consola serie local

Conecte una consola serie al puerto serie del servidor o el CMM.

Para obtener más información, consulte la documentación de usuario suministrada con la plataforma de servidor Sun.

o

■ Conexión Secure Shell (SSH) remota

Establezca una conexión Secure Shell con el CMM o el SP del servidor.

Desde el cliente remoto, y como usuario root, establezca una conexión segura con el CMM o el SP del servidor. Por ejemplo, puede establecer una conexión segura con el SP del servidor desde un cliente SSH remoto escribiendo lo siguiente:

```
ssh -l root dirección_ip_servidor
```

```
Password: changeme
```

Aparece el indicador predeterminado (->) y el sistema está listo para ejecutar los comandos de la línea de comandos con los que se establecerán los valores de configuración de red.

2. Escriba uno de los comandos siguientes para establecer el directorio de trabajo del SP:

- Para un servidor independiente montado en un bastidor: `cd /SP/network`
- Para un módulo de servidor blade integrado en un chasis: `cd /SP/network`
- Para un CMM situado en la ranura 0 de un chasis: `cd /CMM/network/CMM0`
- Para un CMM situado en la ranura 1 de un chasis: `cd /CMM/network/CMM1`

3. Escriba el comando `show` para ver la dirección (o direcciones) IP asignada, por ejemplo:

- Para un servidor independiente montado en un bastidor: `show /SP/network`
- Para módulos de servidor blade en un chasis: `show /CH/BLn/SP network`
- Para un CMM situado en la ranura 0 de un chasis: `show /CMM/network/CMM0`
- Para un CMM situado en la ranura 1 de un chasis: `show /CMM/network/CMM1`

4. Escriba los comandos siguientes para cambiar la dirección IP existente.

Comando	Descripción y ejemplo
<code>set pendingipaddress=</code>	<p>Escriba este comando seguido de la dirección IP estática que quiera asignar al CMM o al SP del servidor.</p> <p>Por ejemplo, si escribe: <code>set pendingipaddress=129.144.82.26</code> está indicando a ILOM que asigne 129.144.82.26 como dirección IP del SP del servidor.</p>
<code>set pendingipnetmask=</code>	<p>Escriba este comando seguido de la dirección de máscara de red que quiera asignar al CMM o al SP del servidor.</p> <p>Por ejemplo, si escribe: <code>set pendingipnetmask=255.255.255.0</code> está indicando a ILOM que asigne la dirección 255.255.255.0 como máscara de red del SP del servidor (o el CMM).</p>
<code>set pendingipgateway=</code>	<p>Escriba este comando seguido de la dirección de puerta de enlace que quiera asignar al CMM o al SP del servidor.</p> <p>Por ejemplo, si escribe: <code>set pendingipgateway=129.144.82.254</code> está indicando a ILOM que asigne la dirección 129.144.82.254 como puerta de enlace del SP del servidor (o el CMM).</p>
<code>setpendingipdiscovery=</code>	<p>Escriba el comando siguiente para indicar a ILOM que desea establecer una dirección IP estática en el SP o el CMM.</p> <p><code>set pendingipdiscovery=static</code></p>
<code>set commitpending=true</code>	<p>Escriba este comando (<code>true</code>) para asignar los valores de red especificados.</p> <p>Por ejemplo: <code>set pendingipaddress=129.144.82.26</code> <code>set pendingipnetmask=255.255.255.0</code> <code>set pendingipnetmask=129.144.82.254</code> <code>set commitpending=true</code></p>

Si se ha conectado a ILOM a través de una conexión SSH remota, la conexión realizada con la dirección IP anterior finalizará. Utilice la nueva dirección IP asignada para conectarse a ILOM.

Asignación del nombre o el identificador del sistema

Si utiliza nombres de sistema para identificar los CMM o los SP del servidor Sun en la red, puede configurar ILOM para presentar esa misma identificación (nombre del sistema) en la página inicial del SP o el CMM. Asimismo, puede configurar ILOM con una cadena de texto explicativa que le ayudará a identificar el sistema en la red. Para obtener instrucciones detalladas sobre la forma de asignar un nombre de sistema o una cadena de texto de identificación del sistema en ILOM, consulte:

- [“Asignación del nombre y el identificador del sistema mediante la interfaz web” en la página 33](#)
- [“Asignación del nombre y el identificador del sistema mediante la línea de comandos” en la página 34](#)

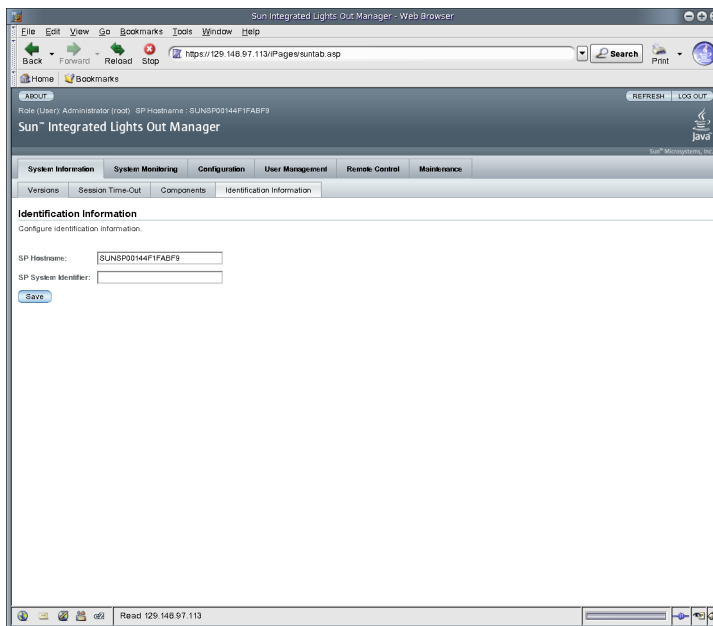
Si precisa más información sobre la asignación del nombre de sistema o ejemplos de cadenas de texto de identificación, consulte [“Identificación del SP y el CMM del servidor mediante un nombre de sistema” en la página 22](#) o [“Texto de identificación del sistema de los servidores Sun” en la página 22](#).

▼ Asignación del nombre y el identificador del sistema mediante la interfaz web

Siga estos pasos para asignar un nombre o un identificador del sistema en ILOM utilizando la interfaz web:

- 1. Utilice un cliente basado en navegador para escribir la dirección IP del SP del servidor en el cuadro de dirección del navegador y pulse Intro.**
Aparece el cuadro de diálogo de acceso a ILOM.
- 2. En este cuadro de diálogo, inicie la sesión como administrador introduciendo el nombre de usuario y la contraseña de administrador.**
Aparece la interfaz de ILOM.
- 3. Seleccione System Information (información del sistema) --> Identification Information (datos de identificación).**
Se abre la página Identification Information (datos de identificación).

FIGURA 2-3 Página de datos de identificación



4. **Escriba el nombre de sistema del SP en el campo SP Hostname.**
El nombre se compone de caracteres alfanuméricos y puede incluir guiones.
5. **En el campo SP System Identifier (identificador del sistema del SP), escriba el texto que utilizará para identificar el sistema.**
El identificador del sistema puede estar compuesto por una cadena de texto formada mediante cualquier combinación de teclas de un teclado estándar excepto las comillas.
6. **Haga clic en Save (guardar) para que la configuración tenga efecto.**

▼ Asignación del nombre y el identificador del sistema mediante la línea de comandos

Siga estos pasos para asignar un nombre o un identificador del sistema en ILOM utilizando la interfaz de la línea de comandos:

1. **Establezca una conexión de consola serie o una conexión SSH con el CMM o el SP del servidor:**
 - **Conexión de la consola serie local**
Conecte una consola serie al puerto serie del servidor o el CMM.

Para obtener más información, consulte la documentación de usuario suministrada con la plataforma de servidor Sun.

o

■ **Conexión Secure Shell (SSH) remota**

Establezca una conexión Secure Shell con el CMM o el SP del servidor.

Desde el cliente remoto, y como usuario root, establezca una conexión segura con el CMM o el SP del servidor. Por ejemplo, puede establecer una conexión segura con el SP del servidor desde un cliente SSH remoto escribiendo lo siguiente:

```
ssh -l root dirección_ip_servidor
```

```
Password: changeme
```

Aparece el indicador predeterminado (->) y el sistema está listo para ejecutar los comandos de la línea de comandos con los que se establecerán los valores de configuración de red.

2. **Para establecer el nombre y el texto de identificación del sistema del SP, escriba lo siguiente en la línea de comandos:**

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

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

El nombre se compone de caracteres alfanuméricos y puede incluir guiones. El identificador del sistema puede estar compuesto por una cadena de texto formada mediante cualquier combinación de teclas de un teclado estándar excepto las comillas.

Interfaz de la línea de comandos e inicio de la sesión de ILOM

La interfaz de la línea de comandos de ILOM (CLI) permite utilizar el teclado para introducir comandos con los que configurar y administrar muchos de los componentes y funciones de ILOM. Cualquier tarea que pueda realizar utilizando la interfaz web de ILOM tiene su equivalente como comando de la CLI.

Este capítulo contiene las secciones siguientes:

- “Descripción general de la interfaz de la línea de comandos” en la página 38
- “Arquitectura jerárquica de la interfaz de la línea de comandos” en la página 39
- “Sintaxis de los comandos de la CLI” en la página 40
- “Ejecución de los comandos” en la página 42
 - “Ejecución de comandos por separado” en la página 42
 - “Ejecución de comandos combinados” en la página 43
- “Conexión con ILOM mediante la línea de comandos” en la página 44
 - “Inicio de la sesión de ILOM” en la página 44
 - “Cierre de la sesión de ILOM” en la página 45

Nota – Los ejemplos de sintaxis de este capítulo utilizan el destino que empieza por `/SP/`, aunque podría cambiarse por el destino que empieza por `/CMM/` en función de la plataforma de servidor Sun utilizada. Los destinos subordinados son comunes para todas las plataformas de servidor Sun.

Descripción general de la interfaz de la línea de comandos

La interfaz de la línea de comandos (CLI) de ILOM se basa en la especificación CLP (*Command-Line Protocol, versión 11.0a.8 Draft*) para administración de servidores elaborada por la DMTF (Distributed Management Task Force). Puede ver la especificación completa en el sitio siguiente:

http://www.dmtf.org/standards/published_documents/DSP0214.pdf

El CLP de la DMTF proporciona una interfaz de administración para uno o varios servidores que es independiente del estado del servidor, el método de acceso o el sistema operativo instalado.

La arquitectura de este CLP establece un modelo de espacio de nombres jerárquico, un árbol predefinido que contiene cada objeto administrado del sistema. En este modelo, un pequeño número de comandos opera sobre un gran espacio de nombres de destinos que pueden ser modificados por opciones y propiedades. El espacio de nombres define los destinos correspondientes a los verbos de los comandos.

Arquitectura jerárquica de la interfaz de la línea de comandos

En la tabla siguiente figuran los distintos métodos jerárquicos que pueden emplearse con la interfaz de la línea de comandos de ILOM en función de la plataforma de servidor Sun que se utilice.

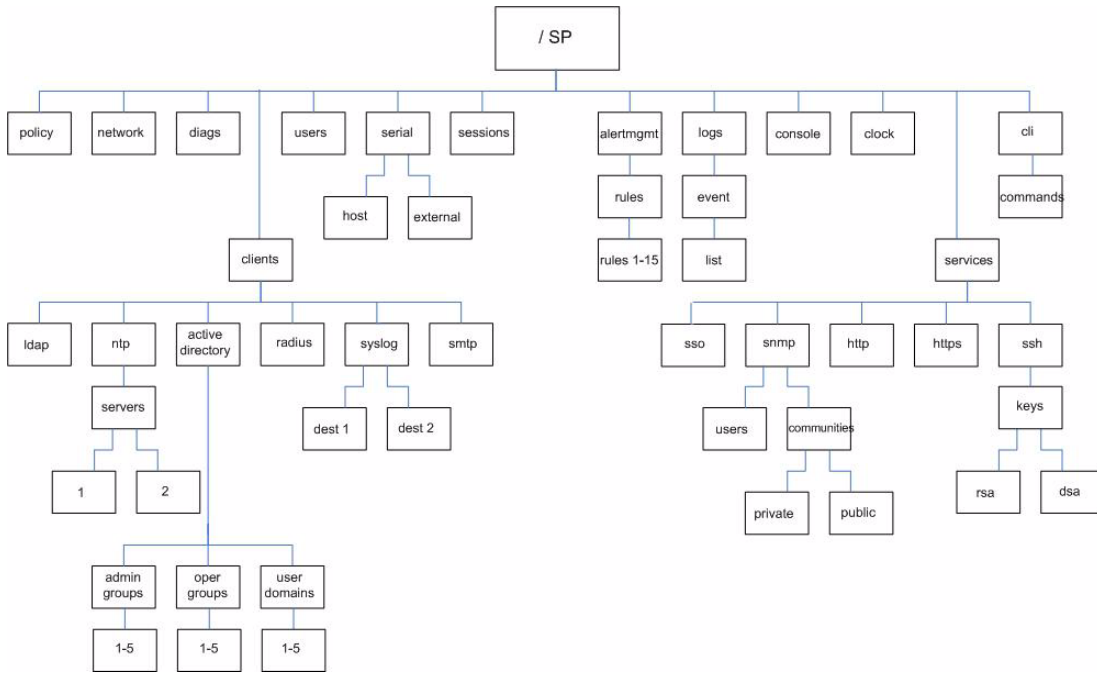
TABLA 3-1 Tipos de destinos de ILOM

Tipo de destino	Descripción
* /SP	Los destinos y propiedades situados por debajo de este tipo de destino se utilizan para configurar el procesador de servicios (SP) de ILOM y ver los registros y consolas.
* /CMM	En las plataformas blade, este destino sustituye a /SP y se utiliza para configurar el módulo de supervisión del chasis (CMM) de ILOM.
* /SYS	Los destinos y propiedades situados debajo de este tipo de destino proporcionan funciones de administración del hardware, el inventario y el entorno. Los destinos corresponden directamente a la nomenclatura de todos los componentes de hardware, algunos de los cuales aparecen impresos en el hardware físico.
* /CH	En las plataformas blade, este tipo de destino sustituye a /SYS y proporciona funciones de administración del hardware, el inventario y el entorno en el nivel del chasis. El destino corresponde directamente a la nomenclatura de todos los componentes de hardware, algunos de los cuales aparecen impresos en el hardware físico.
* /HOST	Los destinos y propiedades situados debajo de este tipo de destino se utilizan para supervisar y administrar el sistema operativo host. Sólo puede utilizarse con sistemas SPARC.

Nota – El acceso a algunos de los árboles subordinados dentro de la jerarquía depende de la plataforma de servidor Sun que se esté utilizando.

Los procesadores de servicios pueden acceder a dos espacios de nombres: el espacio de nombres /SP y el espacio de nombres del sistema global /SYS. En el espacio de nombres /SP, puede administrar y configurar el procesador de servicios. En el espacio de nombres /SYS puede acceder a la información de los sensores y a otros datos relativos al hardware del sistema administrado.

FIGURA 3-1 Ejemplo de árbol de destinos de la CLI de ILOM para /SP



Para obtener más información sobre los privilegios de los usuarios, consulte [“Funciones de las cuentas de usuario de ILOM”](#) en la página 6.

Sintaxis de los comandos de la CLI

Al utilizar la interfaz de la línea de comandos de ILOM, la información se introduce en el orden siguiente:

Sintaxis de los comandos: <comando> <opciones> <destino> <propiedades>

En las secciones siguientes se incluye más información sobre cada parte de la sintaxis.

Comandos de la CLI

La interfaz de la línea de comandos de ILOM permite utilizar los comandos que figuran en la tabla siguiente de acuerdo con la especificación CLP de la DMTF.

En los comandos de la CLI existe diferencia entre mayúsculas y minúsculas.

TABLA 3-2 Comandos de la CLI

Comando	Descripción
cd	Permite el desplazamiento por el espacio de nombres de objetos.
create	Introduce un objeto en el espacio de nombres.
delete	Suprime un objeto del espacio de nombres.
exit	Finaliza la sesión de la interfaz de la línea de comandos.
help	Presenta información de ayuda sobre los comandos y destinos.
load	Transfiere un archivo desde un origen dado a un destino dado.
reinicio	Restablece el estado del destino.
set	Establece las propiedades del destino según el valor especificado.
show	Presenta información sobre los destinos y las propiedades.
start	Inicia el destino.
stop	Detiene el destino.
version	Presenta la versión del procesador de servicios que se está ejecutando.

Opciones de los comandos

La interfaz de la línea de comandos de ILOM permite utilizar las opciones siguientes, pero tenga presente que no todos los comandos admiten todas las opciones. Las opciones `help` y `examine` pueden utilizarse con cualquiera de los comandos.

TABLA 3-3 Opciones de la CLI

Forma completa de la opción	Forma abreviada	Descripción
-default		Con esta opción, el comando ejecuta sólo sus funciones predeterminadas.
-destination		Especifica el destino de los datos.
-display	-d	Presenta en pantalla los datos elegidos por el usuario.

TABLA 3-3 Opciones de la CLI (*continuación*)

Forma completa de la opción	Forma abreviada	Descripción
-help	-h	Presenta información de ayuda.
-level	-l	Ejecuta el comando para el destino actual y todos los destinos que contenga, hasta el nivel especificado.
-output	-o	Especifica el contenido y el formato de la salida del comando. ILOM sólo admite el formato <code>-o table</code> , que presenta los destinos y propiedades en forma de tabla.
-script		Omite las advertencias o mensajes normalmente asociados al comando.
-source		Indica la ubicación de una imagen de origen.

Destinos de los comandos

Cada objeto del espacio de nombres es un destino.

Propiedades de los comandos

Las propiedades son los atributos configurables específicos de cada objeto.

Ejecución de los comandos

La mayoría de los comandos se ejecutan especificando la ubicación del destino e introduciendo el comando. Puede ejecutar cada una de estas acciones por separado o combinarlas en la misma línea de comandos.

▼ Ejecución de comandos por separado

1. **Sitúese en el espacio de nombres utilizando el comando `cd`.**

Por ejemplo:

```
cd /SP/services/http
```

2. Introducción del comando, el destino y el valor.

Por ejemplo:

```
set port=80
o
set prop1=x
set prop2=y
```

▼ Ejecución de comandos combinados

- **Introduzca el comando en una misma línea utilizando la sintaxis**
`<comando><destino>=valor`.

Por ejemplo:

```
set /SP/services/http port=80
o
set /SP/services/http prop1=x prop2=y
```

La tabla siguiente contiene un ejemplo, con su correspondiente descripción, de los métodos de ejecución de comandos combinados y por separado.

TABLA 3-4 Ejecución de un comando combinado y por separado

Sintaxis del comando	Descripción del comando
Ejecución del comando por separado	Desplazamiento al espacio de nombres
> cd /SP/services/http	/SP/services/http
> set port=80	Introducción del comando, el destino y el valor: define el "puerto" con el valor "80".
Ejecución del comando combinado:	En el espacio de nombres /SP/services/http,
> cd /SP/services/http port=80	define el "puerto" con el valor "80".

Conexión con ILOM mediante la línea de comandos

En esta sección se explica cómo iniciar y cerrar las sesiones de ILOM. Antes de iniciar la sesión en la interfaz de la línea de comandos de ILOM, debería consultar [“Asignación de direcciones IP a las interfaces de los SP en las plataformas de servidor Sun”](#) en la página 23 para configurar ILOM.

ILOM admite un máximo de 10 sesiones activas, lo que incluye sesiones de comunicación serie, SSH e interfaz web. No es posible realizar conexiones Telnet con ILOM.

▼ Inicio de la sesión de ILOM

Puede acceder a la interfaz de la línea de comandos de ILOM de forma remota a través de una conexión SSH (Secure Shell) o una conexión serie. Las conexiones Secure Shell están habilitadas de forma predeterminada.

El procedimiento siguiente representa un ejemplo de uso de un cliente SSH en un sistema UNIX: utilice el cliente SSH adecuado para su sistema operativo. El nombre de usuario predeterminado es `root` y la contraseña predeterminada es `changeme`.

Siga estos pasos para iniciar la sesión de ILOM utilizando la conexión SSH habilitada:

1. Escriba este comando para iniciar la sesión de ILOM:

```
$ ssh root@direcciónip
```

donde *direcciónip* es la dirección IP del SP del servidor.

2. Cuando aparezca el mensaje solicitándolo, escriba esta contraseña:

```
Password: changeme
```

Después de acceder con el nombre de usuario y la contraseña predeterminados, debería cambiar la contraseña predeterminada de la cuenta `root` de ILOM (`changeme`). Para obtener más información sobre la forma de cambiar la contraseña de la cuenta `root`, consulte [“Cambio de contraseña de la cuenta root de ILOM mediante la línea de comandos”](#) en la página 70.

▼ Cierre de la sesión de ILOM

Siga este procedimiento para finalizar la sesión de ILOM:

- **Escriba este comando para salir de ILOM:**
-> **exit**

Interfaz web e inicio de la sesión de ILOM

ILOM incorpora una sencilla interfaz web que se ejecuta con numerosos navegadores. Esta interfaz puede utilizarse para acceder a todos los componentes y funciones proporcionados por ILOM.

Este capítulo contiene las secciones siguientes:

- “Descripción de la interfaz web” en la página 47
 - “Requisitos del navegador y el software” en la página 48
 - “Componentes de la interfaz web” en la página 49
 - “Componentes de las fichas de navegación” en la página 50
 - “Conexión con ILOM mediante la interfaz web” en la página 58
 - “Inicio de la sesión de ILOM” en la página 59
 - “Carga del certificado SSL” en la página 61
 - “Establecimiento del tiempo de espera para finalizar la sesión” en la página 62
 - “Cierre de la sesión de ILOM” en la página 63
-

Descripción de la interfaz web

La interfaz web de ILOM es accesible a través de un navegador y utiliza una interfaz estándar de Sun. A través de ella, es posible supervisar y administrar sistemas locales y remotos. Una de las ventajas más importantes de ILOM es la posibilidad de redirigir la consola gráfica del servidor a una estación de trabajo local o un sistema portátil. Cuando se redirige la consola del host, es posible configurar el teclado y el ratón del sistema local para que actúen como ratón y teclado del servidor. También es posible configurar la unidad de disquete o de CD-ROM del sistema remoto como dispositivo conectado de forma virtual al sistema Sun. El acceso a todas estas funciones se realiza utilizando la aplicación Remote Console de ILOM. Si precisa

más información sobre Remote Console, consulte el [Capítulo 12](#). La interfaz web proporciona cuentas de usuario que tienen definidas ciertas funciones y privilegios. Para obtener más información sobre los niveles de privilegios, consulte “[Funciones de las cuentas de usuario de ILOM](#)” en la [página 6](#).

Requisitos del navegador y el software

La interfaz web se ha probado con los últimos navegadores de web Mozilla™, Firefox e Internet Explorer publicados y puede ser compatible con otros navegadores.

Sólo es posible ejecutar una instancia de la interfaz web de ILOM en un mismo navegador. Si intenta ejecutar varias instancias de la interfaz en el mismo navegador, sólo se verá en pantalla la primera instancia.

Se ha comprobado la compatibilidad de ILOM con los siguientes sistemas operativos y navegadores:

- Solaris (9 y 10)
 - Mozilla 1.4 y 1.7
 - Firefox 1.x y superiores
- Linux (Red Hat, SuSE, Ubuntu)
 - Mozilla 1.x y superiores
 - Firefox 1.x y superiores
 - Opera 6.x y superiores
- Microsoft Windows (98, 2000, XP, Vista)
 - Internet Explorer 5.5, 6.x, 7.x
 - Mozilla 1.x y superiores
 - Firefox 1.x y superiores
 - Opera 6.x y superiores
- Macintosh (OSX v10.1 y superiores)
 - Internet Explorer 5.2
 - Mozilla 1.x y superiores
 - Firefox 1.x y superiores
 - Safari (todas)

Nota – ILOM se entrega preinstalado en el sistema Sun e incluye la aplicación Remote Console. Para ejecutar Remote Console, es preciso tener el entorno de ejecución JRE 1.5 (Java 1.5 runtime environment), o una versión posterior, instalado en el cliente local. Para descargar el software JRE, entre en <http://java.com>. Si precisa más información sobre Remote Console, consulte el [Capítulo 12](#).

Componentes de la interfaz web

A continuación se ilustra la página principal de la interfaz web de ILOM.

FIGURA 4-1 Página principal de la interfaz web de ILOM



Cada página de la interfaz web tiene tres secciones fundamentales: la cabecera, las fichas de navegación y la zona de contenido.

Nota – Si utiliza la interfaz web de ILOM con un módulo de supervisión del chasis (CMM), existe otro componente en la interfaz denominado panel de navegación.

La cabecera contiene los botones siguientes e información sobre cada página de la interfaz:

- **Botón About (acerca de):** haga clic en él para ver la información sobre el producto y los derechos de propiedad intelectual.
- **Campo User (usuario):** muestra el nombre de usuario de la persona que haya abierto la sesión de la interfaz web y la función de ese usuario.

- **Campo Server (servidor):** muestra el nombre de sistema del SP o el CMM de ILOM.
- **Botón Refresh (actualizar):** haga clic en este botón para renovar los datos incluidos en la zona de contenido de la página. Este botón no guarda los datos nuevos que haya introducido o seleccionado en la página.
- **Botón Log Out (cerrar sesión):** se utiliza para finalizar la sesión de la interfaz web.

Nota – No utilice el botón de actualización del navegador cuando esté utilizando la interfaz web.

La estructura de navegación por la interfaz web de ILOM incluye fichas y fichas secundarias en las que se hace clic para abrir una página específica. Cuando se hace clic en una ficha principal, aparecen las fichas secundarias con más opciones para seleccionar. Para obtener más información, consulte [“Componentes de las fichas de navegación” en la página 50](#).

En la zona de contenido encontrará información sobre un tema específico o la operación que quiera realizar.

Componentes de las fichas de navegación

En la sección siguiente se describen las fichas principales y secundarias que se encuentran entre los componentes más comunes de la interfaz web de ILOM. Encontrará más información sobre cada una de estas fichas en los capítulos correspondientes de esta guía.

Ficha System Information

Al abrir ILOM, la primera pantalla que aparece de forma predeterminada es la ficha System Information (información del sistema) con sus fichas secundarias, tal y como se ilustra en la siguiente figura. Dentro de la ficha System Information, tiene acceso a las siguientes fichas secundarias:

- Ficha Versions
- Ficha Session Time-Out
- Ficha Components
- Ficha Identification Information

FIGURA 4-2 Ficha System Information



Ficha Versions

En la sección Versions (versiones), puede ver la versión de ILOM que se está ejecutando. Para obtener más información, consulte [“Visualización de la información de versión de ILOM mediante la interfaz web”](#) en la página 209.

Ficha Session Time-Out

En la sección Session Time-Out (tiempo de espera para fin de sesión), puede establecer la cantidad de tiempo que la sesión de ILOM puede permanecer inactiva antes de cerrarse. Para obtener más información, consulte [“Establecimiento del tiempo de espera para finalizar la sesión”](#) en la página 62.

Ficha Components

En la sección Components (componentes), puede ver el nombre, el tipo y el estado de los componentes que ILOM está supervisando. Para obtener más información, consulte [“Visualización de la información de los componentes mediante la interfaz web”](#) en la página 111.

Ficha Identification Information

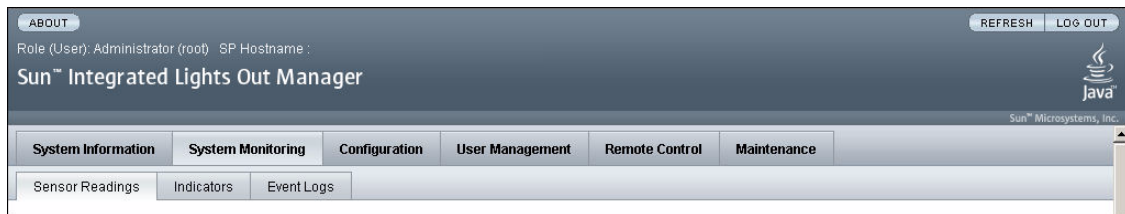
En la sección Identification Information (datos de identificación), puede introducir o cambiar la información de identificación del SP. Para obtener más información, consulte [“Asignación del nombre y el identificador del sistema mediante la interfaz web”](#) en la página 33.

Ficha System Monitoring

Al hacer clic en System Monitoring (supervisión del sistema), la imagen de la ficha y sus fichas secundarias es similar a la de la siguiente figura. Dentro de la ficha System Monitoring, tiene acceso a las siguientes fichas secundarias:

- Ficha Sensor Readings
- Ficha Indicators
- Ficha Event Logs

FIGURA 4-3 Ficha System Monitoring



Ficha Sensor Readings

En la sección Sensor Readings (lecturas de los sensores), puede ver el nombre y el tipo de los sensores y la lectura que indican. Para obtener más información, consulte [“Lecturas de los sensores” en la página 121](#).

Ficha Indicators

En la sección Indicators (indicadores), puede ver el nombre y estado de los indicadores y los LED. Para obtener más información, consulte [“Indicadores del sistema” en la página 125](#).

Ficha Event Logs

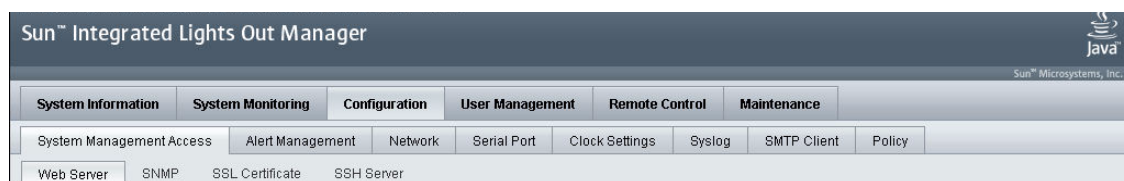
En la sección Event Logs (registros de eventos) puede ver diversa información sobre cada evento en particular, lo que incluye el ID, la clase, el tipo, la gravedad, la fecha y hora, y la descripción del evento. Para obtener más información, consulte [“Registro de eventos de ILOM” en la página 128](#).

Ficha Configuration

Al hacer clic en Configuration (configuración), la imagen de la ficha y sus fichas secundarias es similar a la de la siguiente figura. La ficha Configuration da acceso a las siguientes fichas secundarias:

- Ficha System Management Access
- Ficha Alert Management
- Ficha Network
- Ficha Serial Port
- Ficha Clock Settings
- Ficha Syslog
- Ficha SMTP Client
- Ficha Policy

FIGURA 4-4 Ficha Configuration



Ficha System Management Access

La sección System Management Access (acceso a la administración del sistema) permite acceder a las funciones Web Server, SNMP y SSL Certificate.

Ficha Web Server

En la sección Web Server (servidor web), puede editar o actualizar valores de configuración del servidor web tales como el servidor HTTP o el puerto HTTP. Para obtener más información, consulte [“Habilitación del acceso HTTP o HTTPS a la web mediante la interfaz web” en la página 176.](#)

Ficha SNMP

En esta sección, puede editar o actualizar los datos de configuración de SNMP. Para obtener más información, consulte [“Configuración de SNMP mediante la interfaz web” en la página 196.](#)

Ficha SSL Certificate

En la sección SSL Certificate (certificado SSL), puede ver información sobre el certificado SSL predeterminado. También tiene la opción de buscar e introducir un certificado SSL nuevo. Para obtener más información, consulte [“Carga del certificado SSL” en la página 61](#).

SSH Server

En la sección SSH Server (servidor SSH), puede configurar el acceso y la generación de claves para el servidor Secure Shell (SSH). Para obtener más información, consulte [“Habilitación o inhabilitación de SSH mediante la interfaz web” en la página 170](#).

Ficha Alert Management

En la sección Alert Management (administración de alertas), puede ver datos sobre cada alerta y cambiar la lista de alertas configuradas. Para obtener más información, consulte [“Administración de las reglas de alertas mediante la interfaz web de ILOM” en la página 147](#).

Ficha Network

En la sección Network (red), puede ver y editar la configuración de red de ILOM. Para obtener más información, consulte [“Visualización de la configuración de red mediante la interfaz web” en la página 173](#).

Ficha Serial Port

En la sección Serial Port (puerto serie), puede ver y editar la velocidad de baudios del puerto serie interno y externo. Para obtener más información, consulte [“Visualización de la configuración del puerto serie mediante la interfaz web” en la página 175](#).

Ficha Clock Settings

En la sección Clock Settings (configuración del reloj), puede ver y editar la hora y la configuración de NTP. Para obtener más información, consulte [“Marcas de tiempo del registro de eventos y configuración del reloj de ILOM” en la página 129](#).

Ficha Syslog

En esta sección, puede configurar las direcciones de los servidores a los que se enviarán los mensajes de Syslog. Para obtener más información, consulte [“Configuración de las direcciones IP de un destinatario de Syslog remoto mediante la interfaz web”](#) en la página 141.

Ficha SMTP Client

En la sección SMTP puede configurar el estado del cliente SMTP que se utiliza para enviar las notificaciones de alerta por correo electrónico. Para obtener más información, consulte [“Habilitación del cliente SMTP mediante la interfaz web”](#) en la página 158.

Ficha Policy

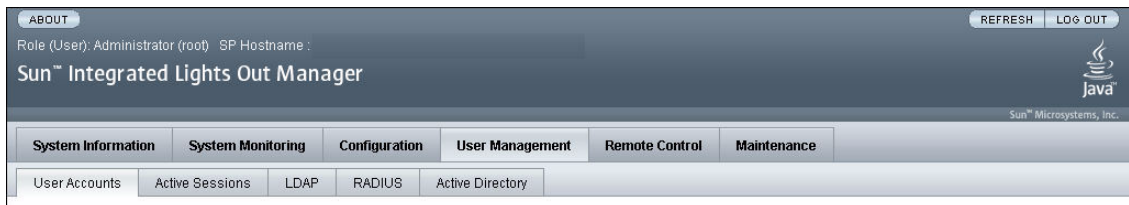
En esta sección, puede habilitar o inhabilitar las opciones que controlan el comportamiento del sistema, entre ellas, las normas de encendido y apagado. Para obtener más información, consulte [“Configuración de normas”](#) en la página 117.

Ficha User Management

Al hacer clic en User Management (administración de usuarios), la imagen de la ficha y sus fichas secundarias es similar a la de la siguiente figura. La ficha User Management da acceso a las siguientes fichas secundarias:

- Ficha User Accounts
- Ficha Active Sessions
- Ficha LDAP
- Ficha RADIUS
- Ficha Active Directory

FIGURA 4-5 Ficha User Management



Ficha User Accounts

En la sección User Accounts (cuentas de usuario), puede agregar, borrar o modificar las cuentas de usuario locales de ILOM. Para obtener más información, consulte [“Adición de cuentas de usuario y establecimiento de privilegios mediante la interfaz web” en la página 76.](#)

Ficha Active Sessions

En la sección Active Sessions (sesiones activas), puede ver los usuarios que han abierto una sesión en ILOM y el tipo de sesión que han abierto. Para obtener más información, consulte [“Visualización de las sesiones de usuario mediante la interfaz web” en la página 83.](#)

Ficha LDAP

En esta sección, puede configurar el acceso a ILOM de los usuarios de LDAP. Para obtener más información, consulte [“Configuración de ILOM para LDAP mediante la interfaz web” en la página 100.](#)

Ficha RADIUS

En esta sección, puede configurar el acceso a ILOM de los usuarios de RADIUS. Para obtener más información, consulte [“Configuración de RADIUS mediante la interfaz web” en la página 104.](#)

Ficha Active Directory

En esta sección, puede configurar los valores de Active Directory. Para obtener más información, consulte [“Configuración de Active Directory mediante la interfaz web” en la página 85.](#)

Ficha Remote Control

Al hacer clic en la ficha Remote Control (control remoto), la imagen de la ficha y sus fichas secundarias es similar a la de la siguiente figura. La ficha Remote Control da acceso a las siguientes fichas secundarias:

- Ficha Redirection
- Ficha Remote Power Control
- Ficha Mouse Mode Settings

FIGURA 4-6 Ficha Remote Control



Ficha Redirection

En la sección Redirection (redirección), puede administrar el host de forma remota redirigiendo la consola del sistema a una máquina local. Para obtener más información, consulte [“Configuración de las opciones de control remoto de ILOM mediante la interfaz web”](#) en la página 219.

Remote Power Control

En la sección Remote Power Control (control remoto de la alimentación), puede controlar el encendido y apagado del sistema. Para obtener más información, consulte [“Configuración de las opciones de control remoto de ILOM mediante la interfaz web”](#) en la página 219.

Mouse Mode Settings

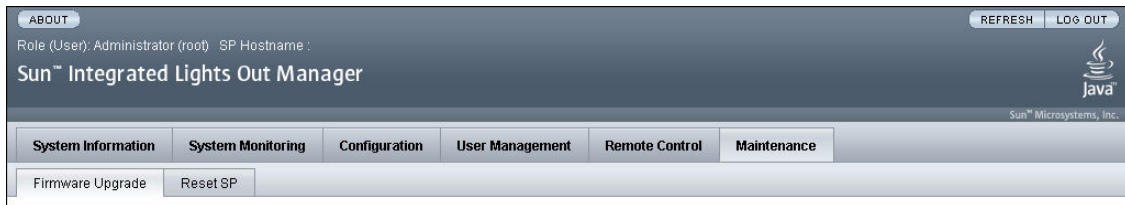
En la sección Mouse Mode Settings (configuración del modo de ratón), puede elegir el modo de funcionamiento que utilizará para el ratón local mientras administra el host de forma remota. Para obtener más información, consulte [“Configuración de las opciones de control remoto de ILOM mediante la interfaz web”](#) en la página 219.

Ficha Maintenance

Al hacer clic en la ficha Maintenance (mantenimiento), la imagen que aparece de la ficha y sus fichas secundarias es similar a la de la siguiente figura. La ficha Maintenance da acceso a las siguientes fichas secundarias:

- Ficha Firmware Upgrade
- Ficha Reset SP

FIGURA 4-7 Ficha Maintenance



Ficha Firmware Upgrade

En la sección Firmware Upgrade (actualización del firmware), puede iniciar el proceso para obtener la actualización del firmware de ILOM. Para obtener más información, consulte [“Actualización del firmware de ILOM mediante la interfaz web” en la página 210.](#)

Ficha Reset SP

En la sección Reset SP (reinicio del SP), puede iniciar el proceso de restablecer el procesador de servicios (SP). Para obtener más información, consulte [“Reinicio del SP de ILOM” en la página 211.](#)

Conexión con ILOM mediante la interfaz web

En esta sección se explica cómo iniciar y cerrar la sesión de la interfaz web, así como la forma de cargar un certificado SSL y establecer el tiempo de espera para que finalice la sesión.

▼ Inicio de la sesión de ILOM

En esta sección se explica cómo iniciar la sesión de la interfaz web de ILOM.

Nota – ILOM arranca automáticamente cuando un sistema Sun se conecta a una toma de corriente de CA o cuando un módulo de servidor se introduce en un chasis que recibe energía. Si el puerto de administración Ethernet no está conectado o el proceso DHCP (Dynamic Host Configuration Protocol) de ILOM falla por la ausencia de un servidor DHCP en la red de administración, ILOM podría tardar más en iniciarse.

Si se inhabilita el uso del servidor proxy del navegador (en caso de que se utilice) para acceder a la red de administración, se puede acelerar el tiempo de respuesta de la interfaz web.

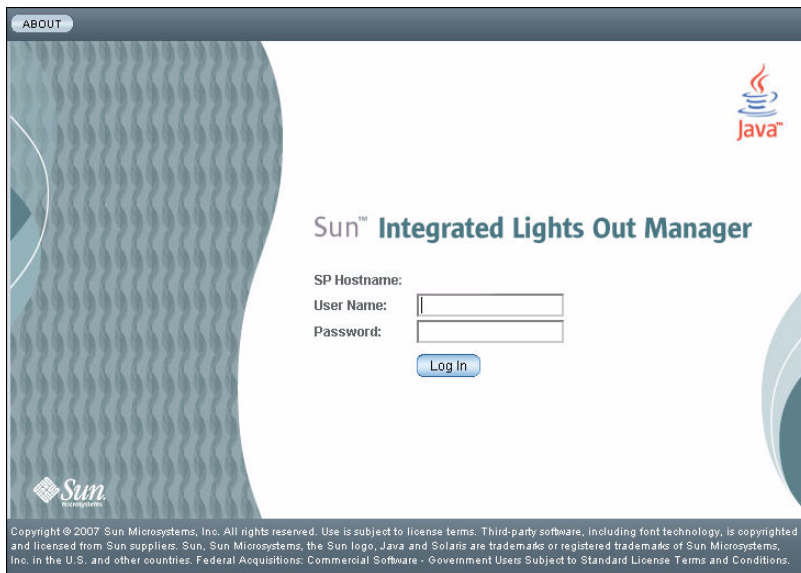
Necesita conocer la dirección IP de ILOM. Para obtener información sobre la forma de ver y configurar la dirección IP, consulte [“Asignación de direcciones IP a las interfaces de los SP en las plataformas de servidor Sun” en la página 23.](#)

Siga este procedimiento para iniciar la sesión de la interfaz web de ILOM:

1. **Para entrar en la interfaz web, escriba la dirección IP de ILOM en el navegador de web.**

Se abre la página de inicio de sesión de la interfaz web.

FIGURA 4-8 Página de inicio de sesión



2. Escriba el nombre de usuario y la contraseña.

Puede utilizar el nombre y la contraseña predeterminados.

- Nombre de usuario predeterminado: root
- Contraseña predeterminada: changeme

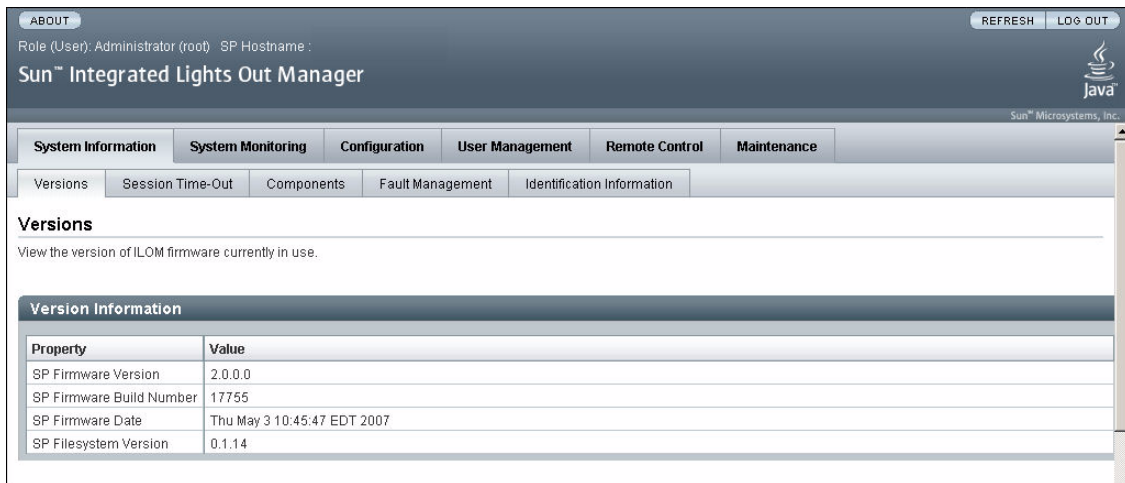
Tanto el nombre de usuario como la contraseña se escriben en minúsculas.

ILOM se entrega con un ID de usuario predefinido que tiene asignado el nombre root y la función de administrador (Administrator). No puede borrar este ID de usuario ni cambiar sus atributos de función. También se suministra una contraseña predeterminada, changeme. Esta contraseña es necesaria para iniciar la sesión en la interfaz de la línea de comandos (CLI), en Secure Shell (SSH) y en la interfaz web.

3. Haga clic en Log In (iniciar sesión).

Se abre la página Versions (versiones) de la interfaz web.

FIGURA 4-9 Página de versiones



The screenshot shows the Sun Integrated Lights Out Manager (ILOM) web interface. At the top, there is a navigation bar with tabs for System Information, System Monitoring, Configuration, User Management, Remote Control, and Maintenance. Below this, there are sub-tabs for Versions, Session Time-Out, Components, Fault Management, and Identification Information. The main content area is titled "Versions" and contains a table with the following data:

Property	Value
SP Firmware Version	2.0.0.0
SP Firmware Build Number	17755
SP Firmware Date	Thu May 3 10:45:47 EDT 2007
SP Filesystem Version	0.1.14

Después de iniciar la sesión de ILOM y establecer la conexión de red con el sistema, debería considerar la posibilidad de cambiar la contraseña predeterminada (changeme) asociada a la cuenta root de ILOM a fin de proteger el sistema contra accesos no autorizados. Para obtener más información sobre el cambio de contraseña de la cuenta root de ILOM, consulte [“Cambio de contraseña de la cuenta root de ILOM mediante la interfaz web”](#) en la página 68.

▼ Carga del certificado SSL

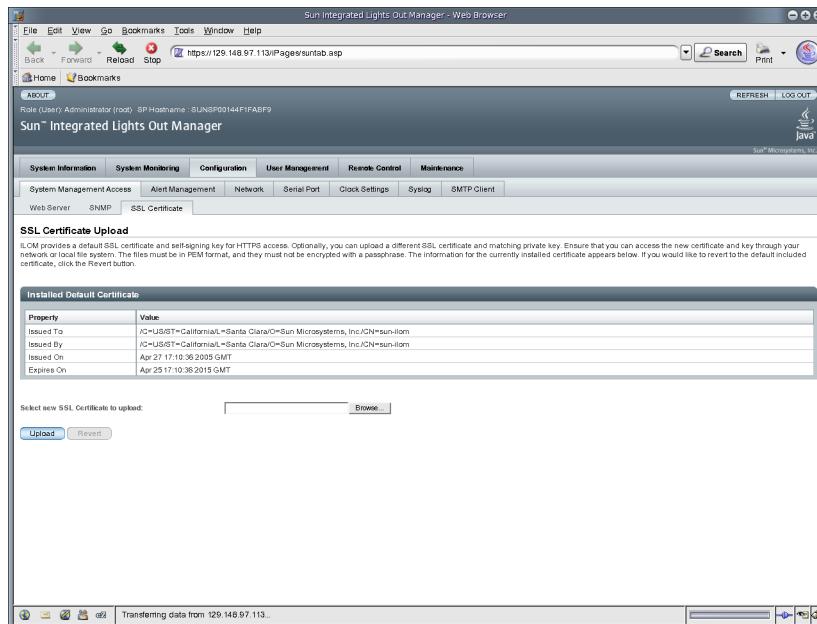
ILOM proporciona un certificado SSL predeterminado y una clave autofirmada para el acceso mediante HTTPS.

No obstante, tiene la opción de cargar otro certificado SSL y su clave privada correspondiente. Asegúrese de poder acceder al nuevo certificado y su clave a través de la red o el sistema de archivos local.

Siga este procedimiento para cargar el certificado SSL:

1. **Inicie la sesión de ILOM.**
2. **Seleccione Configuration (configuración) --> System Management Access (acceso a la administración del sistema) --> SSL Certificate (certificado SSL).**
Se abre la página SSL Certificate Upload (carga del certificado SSL).

FIGURA 4-10 Página de carga del certificado SSL



3. **Escriba el nombre de archivo del nuevo certificado SSL o haga clic en el botón Browse (examinar) para buscarlo en el sistema.**

El nombre del archivo tiene la extensión `.pem`. El procesador de servicios no admite certificados cifrados con frase de contraseña.

4. Haga clic en el botón **Upload (cargar)** para obtener el certificado SSL seleccionado. Se abre el cuadro de diálogo SSL Certificate Upload Status (estado de la carga del certificado SSL).

5. Una vez cargados el certificado y la clave privada, haga clic en el botón **OK (aceptar)** para reiniciar el servidor web de ILOM y empezar a utilizar el nuevo certificado SSL.

Es preciso reiniciar el servidor web de ILOM para que el certificado entre en efecto.

▼ Establecimiento del tiempo de espera para finalizar la sesión

El valor de tiempo de espera para el fin de sesión no se conserva después de cerrar la sesión de ILOM. Es preciso volver a definirlo cada vez que se inicia la sesión en la interfaz web de la aplicación.

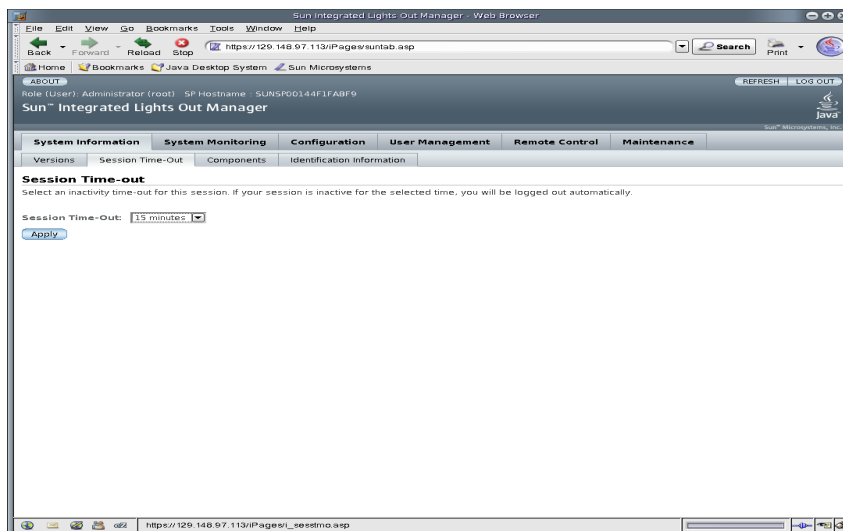
Siga este procedimiento para establecer el tiempo que una sesión de ILOM puede permanecer inactiva antes de cerrarse.

1. **Inicie la sesión de ILOM.**

2. **Seleccione System Information (información del sistema) -> Session Time-Out (tiempo de espera para fin de sesión).**

Se abre la página Session Time-Out (tiempo de espera para fin de sesión).

FIGURA 4-11 Página Session Time-Out



3. En la lista desplegable **Session Time-Out**, seleccione el tiempo que la sesión puede permanecer inactiva antes de cerrarse.

Si no se realiza ninguna actividad en la sesión durante la cantidad de tiempo seleccionada, la sesión de ILOM se cerrará automáticamente.

▼ Cierre de la sesión de ILOM

- Para cerrar la sesión de la interfaz web, haga clic en el botón **Log Out (cerrar sesión)**.

Este botón está situado en el extremo superior derecho de la interfaz.

Administración de cuentas de usuario

ILOM admite un total de 10 cuentas de usuario. Una de ellas, la de administrador, está preconfigurada y proporciona acceso de lectura y escritura a todos los componentes, funciones y comandos de ILOM. Mediante la interfaz web o la interfaz de la línea de comandos (CLI) de ILOM, es posible agregar, modificar y borrar cuentas de usuario.

Este capítulo contiene las secciones siguientes:

- “Directrices para administrar las cuentas de usuario” en la página 67
- “Funciones y privilegios de las cuentas de usuario” en la página 67
- “Cuentas de administrador de ILOM preconfiguradas” en la página 68
 - “Cambio de contraseña de la cuenta root de ILOM mediante la interfaz web” en la página 68
 - “Cambio de contraseña de la cuenta root de ILOM mediante la línea de comandos” en la página 70
- “Single Sign On” en la página 71
 - “Habilitación o inhabilitación de Single Sign On mediante la línea de comandos” en la página 71
 - “Habilitación o inhabilitación de Single Sign On mediante la interfaz web” en la página 71
- “Administración de cuentas de usuario mediante la línea de comandos” en la página 72
 - “Adición de una cuenta de usuario mediante la línea de comandos” en la página 72
 - “Modificación de una cuenta de usuario mediante la línea de comandos” en la página 73
 - “Supresión de una cuenta de usuario mediante la línea de comandos” en la página 73
 - “Visualización de la lista de cuentas de usuario mediante la línea de comandos” en la página 73

- “Visualización de una cuenta de usuario específica mediante la línea de comandos” en la página 73
- “Configuración de una cuenta de usuario mediante la línea de comandos” en la página 74
- “Visualización de la lista de sesiones de usuario mediante la línea de comandos” en la página 75
- “Visualización de una sesión de usuario específica mediante la línea de comandos” en la página 75
- “Administración de cuentas de usuario mediante la interfaz web” en la página 76
 - “Adición de cuentas de usuario y establecimiento de privilegios mediante la interfaz web” en la página 76
 - “Modificación de una cuenta de usuario mediante la interfaz web” en la página 79
 - “Supresión de una cuenta de usuario mediante la interfaz web” en la página 82
 - “Visualización de las sesiones de usuario mediante la interfaz web” en la página 83
- “Active Directory” en la página 84
 - “Configuración de Active Directory mediante la interfaz web” en la página 85
 - “Edición de las tablas de Active Directory mediante la interfaz web” en la página 90
 - “Determinación de los niveles de autorización de los usuarios” en la página 91
 - “Seguridad de la conexión de Active Directory” en la página 92
- “LDAP (Lightweight Directory Access Protocol)” en la página 96
 - “Configuración del servidor LDAP” en la página 99
 - “Configuración de ILOM para LDAP mediante la línea de comandos” en la página 100
 - “Configuración de ILOM para LDAP mediante la interfaz web” en la página 100
- “Autenticación RADIUS” en la página 102
 - “Clientes y servidores RADIUS” en la página 102
 - “Parámetros de RADIUS” en la página 103
 - “Configuración de RADIUS mediante la línea de comandos” en la página 103
 - “Configuración de RADIUS mediante la interfaz web” en la página 104
 - “Comandos de RADIUS” en la página 104

Nota – Los ejemplos de sintaxis de este capítulo utilizan el destino que empieza por /SP/, pero podría cambiarse por el destino que empieza por /CMM/, en función de la plataforma de servidor Sun utilizada. Los destinos subordinados son comunes para todas las plataformas de servidor Sun.

Directrices para administrar las cuentas de usuario

Utilice las siguientes directrices generales cuando administre cuentas de usuario.

- ILOM admite un total de 10 cuentas de usuario, una de las cuales, la de administrador, está preconfigurada. No es posible borrar la cuenta de administrador. Si se han configurado las 10 cuentas de usuario, es preciso borrar una de ellas para poder agregar otra.
- Sólo las cuentas con privilegios de administrador pueden agregar, modificar o borrar cuentas de usuario. No obstante, los usuarios con privilegios de operador pueden modificar su propia contraseña.
- Los nombres de las cuentas de usuario deben tener entre 4 y 16 caracteres. Existe diferencia entre mayúsculas y minúsculas a la hora de escribirlos y deben comenzar por un carácter alfabético. Es posible utilizar caracteres alfabéticos, números, guiones y el carácter de subrayado. No incluya espacios en los nombres de usuario.
- Puede configurar cuentas locales o dejar que ILOM las autentique utilizando como referencia una base de datos de usuario remota como Active Directory, LDAP o RADIUS. Con la autenticación remota, puede utilizar una base de datos de usuario centralizada en lugar de tener que configurar cuentas locales en cada instancia de ILOM. Asimismo, la autenticación remota permite cambiar una sola vez la contraseña de un usuario en el servidor.

Funciones y privilegios de las cuentas de usuario

Las cuentas de usuario tienen dos posibles funciones y cada una de ellas otorga ciertos privilegios al usuario de ILOM. Las funciones y privilegios de los usuarios incluyen:

- **Administrador:** permite acceder a todos los componentes, funciones y comandos de ILOM.
- **Operador:** proporciona acceso restringido a los componentes, funciones y comandos de ILOM. En general, los operadores no pueden cambiar las opciones de configuración.

Cuentas de administrador de ILOM preconfiguradas

Las cuentas de administrador de ILOM preconfiguradas, también conocidas como cuentas de usuario fijas, incluyen:

Nombre de usuario: root

Contraseña: changeme

El nombre de usuario, `root`, no puede borrarse ni modificarse, mientras que la contraseña (`changeme`) sí puede sustituirse por otra. Esta cuenta ofrece privilegios administrativos (acceso de lectura y escritura) sobre todos los componentes, funciones y comandos de ILOM.

La primera vez que se accede a ILOM, en el nivel del SP o el CMM, es preciso iniciar la sesión como usuario `root` con la contraseña predeterminada, `changeme`. Después de iniciar la sesión de ILOM y establecer la conexión de red con el sistema, debería considerar la posibilidad de cambiar la contraseña (`changeme`) asociada a la cuenta `root` de ILOM a fin de proteger el sistema contra accesos no autorizados. Si utiliza un servidor blade, cambie la contraseña en cada CMM y módulo blade instalado en el chasis del sistema. Para obtener más información sobre la forma de cambiar la contraseña de la cuenta `root`, consulte [“Cambio de contraseña de la cuenta root de ILOM mediante la interfaz web”](#) en la página 68.

▼ Cambio de contraseña de la cuenta root de ILOM mediante la interfaz web

Siga este procedimiento para cambiar la contraseña de la cuenta `root`:

1. **Abra un navegador de web y escriba la dirección IP de un CMM o un SP del servidor.**

Se abre la página de inicio de sesión de la interfaz web de ILOM.

2. **En esta página, haga lo siguiente:**

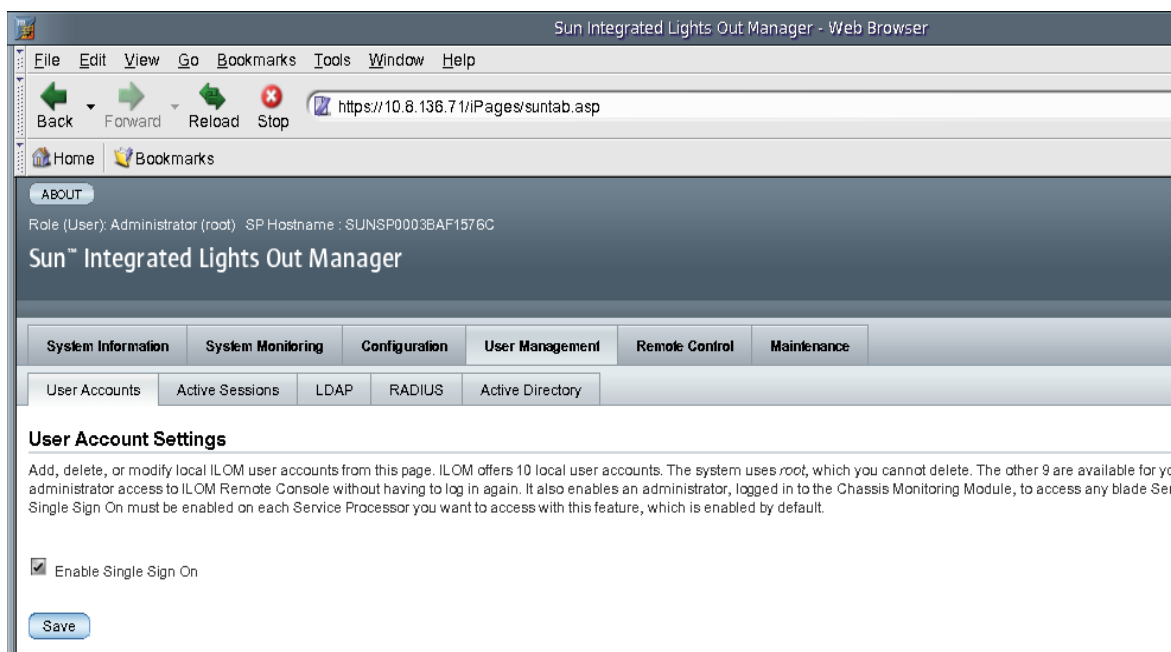
- a. **Escriba el nombre de usuario predeterminado (`root`) y la contraseña correspondiente (`changeme`).**

- b. **Haga clic en Log In (iniciar sesión).**

Aparece la interfaz web de ILOM.

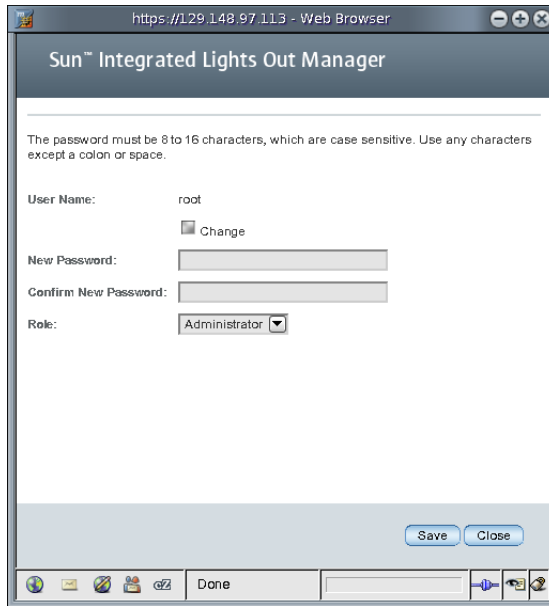
3. En esta interfaz, haga lo siguiente:
 - Para cambiar la contraseña de administrador preconfigurada, haga clic en el dispositivo del panel de navegación izquierdo y continúe con el paso 4.
 - Para cambiar la contraseña de administrador preconfigurada en el nivel de SP de un blade, haga clic en el blade adecuado del panel de navegación izquierdo y continúe con el paso 4.
4. En la interfaz web de ILOM, haga clic en **User Management (administración de usuarios)** --> **User Accounts (cuentas de usuario)**.
Se abre la página User Account Settings (configuración de cuentas de usuario).

FIGURA 5-1 Página de configuración de cuentas de usuario



5. En esta página, seleccione el botón de opción situado junto a `root` y haga clic en **Edit (editar)**.
Aparece un mensaje de seguridad.
6. Haga clic en **OK (aceptar)** para continuar. Se abre la página **User Account Password (contraseña de la cuenta de usuario)**.

FIGURA 5-2 Cuadro de diálogo de cambio de contraseña



The screenshot shows a web browser window titled "Sun™ Integrated Lights Out Manager" with the URL "https://129.148.97.113 - Web Browser". The page contains a form for changing the password. At the top, it states: "The password must be 8 to 16 characters, which are case sensitive. Use any characters except a colon or space." The form fields are: "User Name:" with the value "root"; a checkbox labeled "Change"; "New Password:" with an empty text input field; "Confirm New Password:" with an empty text input field; and "Role:" with a dropdown menu showing "Administrator". At the bottom right of the form are "Save" and "Close" buttons. The browser's address bar shows "Done" and navigation icons.

7. En esta página, haga lo siguiente:
 - a. Seleccione la casilla situada junto a Change (cambiar).
 - b. Escriba la nueva contraseña en el cuadro New Password (contraseña nueva).
 - c. Vuelva a introducir la contraseña nueva en el cuadro Confirm Password (confirmar contraseña).
 - d. Haga clic en Save (guardar).

Queda activada la nueva contraseña identificada en los pasos 6b y 6c para la cuenta de administrador root.
8. Si es necesario, repita los pasos del 2 al 6d si quiere cambiar la contraseña para cada dispositivo instalado.

▼ Cambio de contraseña de la cuenta root de ILOM mediante la línea de comandos

- Escriba el comando siguiente para cambiar la contraseña de la cuenta root de ILOM:

```
-> set /SP/users/root password=contraseña
```

Por ejemplo:

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

Single Sign On

Single Sign On (inicio de sesión con clave única) es un cómodo servicio de autenticación que reduce el número de veces que necesita introducir una contraseña para poder acceder a ILOM. Single Sign On (SSO) está habilitado de forma predeterminada. Como en cualquier otro servicio de autenticación, las credenciales se transmiten a través de la red. Si esto no es aconsejable, considere la posibilidad de inhabilitar el servicio SSO.

▼ Habilitación o inhabilitación de Single Sign On mediante la línea de comandos

Single Sign On está habilitado de forma predeterminada. Sólo los administradores pueden inhabilitarlo o habilitarlo.

- **Escriba el comando siguiente para habilitar el servicio SSO:**

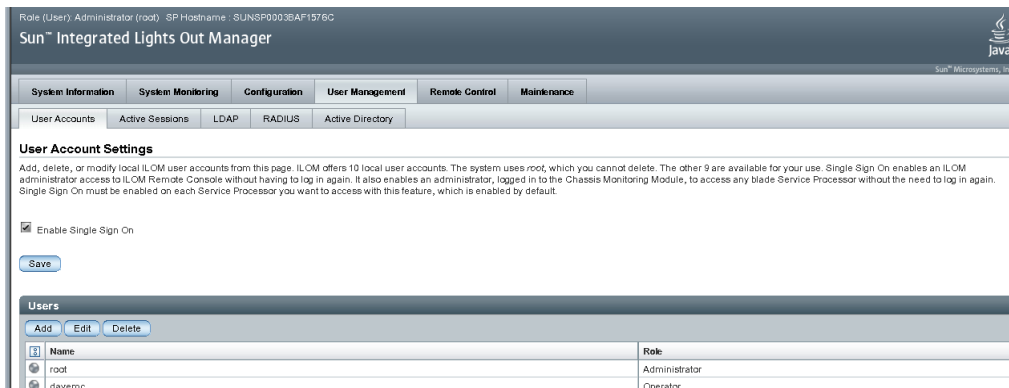
```
-> set /SP/services/sso state=disabled|enabled
```

▼ Habilitación o inhabilitación de Single Sign On mediante la interfaz web

Siga estos pasos para habilitar o inhabilitar el servicio SSO:

1. **Inicie la sesión en la interfaz web de ILOM como administrador.**
2. **Seleccione User Management (administración de usuarios) --> User Accounts (cuentas de usuario).**
Se abre al página User Account Settings (configuración de cuentas de usuario).
3. **Seleccione la casilla situada junto a Enable Single Sign On para habilitar el servicio SSO o borre la marca de selección de la casilla para inhabilitarlo.**

FIGURA 5-3 Página de configuración de cuentas de usuario con Single Sign On habilitado



Administración de cuentas de usuario mediante la línea de comandos

En esta sección se explica cómo administrar las cuentas de usuario utilizando la interfaz de la línea de comandos de ILOM.

▼ Adición de una cuenta de usuario mediante la línea de comandos

- Escriba el comando siguiente para agregar una cuenta de usuario local:

```
-> create /SP/users/nombreusuario password=contraseña role=administrator|operator
```

Por ejemplo:

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


▼ Modificación de una cuenta de usuario mediante la línea de comandos

- Escriba el comando siguiente para modificar una cuenta de usuario local:

```
-> set /SP/users/nombreusuario password=contraseña role=administrator|operator
```

▼ Supresión de una cuenta de usuario mediante la línea de comandos

1. Escriba el comando siguiente para borrar una cuenta de usuario local:

```
-> delete /SP/users/nombreusuario
```

Por ejemplo:

```
->delete /SP/users/davemc
```

```
Are you sure you want to delete /SP/users/davemc (y/n)?
```

2. Escriba **y** (sí) para borrar la cuenta o **n** para cancelar la operación.

▼ Visualización de la lista de cuentas de usuario mediante la línea de comandos

- Escriba el comando siguiente para ver información sobre todas las cuentas de usuario locales:

```
-> show -display targets /SP/users
```

Por ejemplo:

```
-> show -display targets /SP/users
/SP/users
Targets:
    root
    davemc
```

▼ Visualización de una cuenta de usuario específica mediante la línea de comandos

- Escriba el comando siguiente para ver información sobre una cuenta de usuario concreta:

```
-> show /SP/users/nombreusuario
```

Por ejemplo:

```
-> show /SP/users/davemc
/SP/users/davemc
Targets:
Properties:
  role = Operator
  password = *****
Commands:
  cd
  set
  show
```

▼ Configuración de una cuenta de usuario mediante la línea de comandos

Utilice el comando `set` para cambiar los destinos, las propiedades, las contraseñas y los valores de las cuentas de usuario configuradas.

- **Escriba el comando siguiente para configurar una cuenta de usuario local:**

```
-> set <destino> [<propiedad>=valor]
```

Destinos, propiedades y valores

Éstos son los destinos, propiedades y valores válidos para las cuentas de usuario locales.

TABLA 5-1 Destinos, propiedades y valores válidos para las cuentas de usuario locales

Destino	Propiedad	Valor	Contraseña	Valor predeterminado
/SP/users/ <i>nombrequesuario</i>	role	administrator operator		operator
	password	<cadena>		

Por ejemplo, para cambiar la función de administrador del `usuario1` por la función de operador, escriba:

```
-> set /SP/users/usuario1 role=operator
```

Para cambiar la contraseña del `usuario1`, escriba:

```
-> set /SP/users/usuario1 contraseña
Changing password for user /SP/users/usuario1/password...
Enter new password:*****
Enter new password again:*****
New password was successfully set for user /SP/users/usuario1
```

Nota – Es necesario tener privilegios de administrador para cambiar las propiedades de los usuarios.

▼ Visualización de la lista de sesiones de usuario mediante la línea de comandos

- Escriba el comando siguiente para ver información sobre todas las sesiones de usuario locales:

→ **show /SP/sessions**

Por ejemplo:

```
-> show /SP/sessions
/SP/sessions
Targets:
  108
Properties:
Commands:
  cd
  show
```

▼ Visualización de una sesión de usuario específica mediante la línea de comandos

- Escriba el comando siguiente para ver información sobre una determinada sesión de usuario:

→ **show /SP/sessions/108**

Por ejemplo:

```
-> show /SP/sessions/108
/SP/sessions/108
Targets:
Properties:
  username = root
  starttime = Tue Jun  5 10:04:05 2007
  type = shell
Commands:
  cd
  show
```

Administración de cuentas de usuario mediante la interfaz web

En esta sección se explica la forma de agregar, modificar y borrar cuentas de usuario utilizando la interfaz web.

▼ Adición de cuentas de usuario y establecimiento de privilegios mediante la interfaz web

1. Inicie la sesión en la interfaz web de ILOM con privilegios de administrador.

Sólo las cuentas con privilegios de administrador pueden agregar, modificar o borrar cuentas de usuario, aunque los operadores sí pueden modificar sus propias contraseñas.

Si un usuario nuevo recibe privilegios de administrador, esos privilegios son válidos automáticamente para la interfaz de la línea de comandos (CLI) y la interfaz IPMI (Intelligent Platform Management Interface) de ILOM.

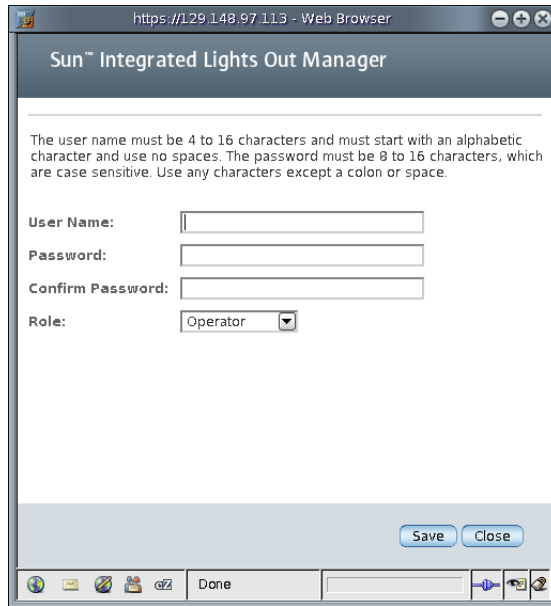
2. Seleccione **User Management (administración de usuarios)** --> **User Accounts (cuentas de usuario)**.

Se abre la página User Account Settings (configuración de cuentas de usuario).

3. En la tabla de usuarios, haga clic en **Add (agregar)**.

Se abre el cuadro de diálogo Add User (agregar usuario).

FIGURA 5-4 Cuadro de diálogo de adición de usuarios



The screenshot shows a web browser window titled "Sun™ Integrated Lights Out Manager". The address bar shows "https://129.148.97.113 - Web Browser". The main content area contains the following text: "The user name must be 4 to 16 characters and must start with an alphabetic character and use no spaces. The password must be 8 to 16 characters, which are case sensitive. Use any characters except a colon or space." Below this text are four input fields: "User Name:" (text box), "Password:" (password box), "Confirm Password:" (password box), and "Role:" (dropdown menu with "Operator" selected). At the bottom right of the dialog are "Save" and "Close" buttons. The browser's status bar at the bottom shows "Done" and navigation icons.

4. Introduzca la información siguiente:

a. Escriba un nombre en el campo User Name (nombre de usuario).

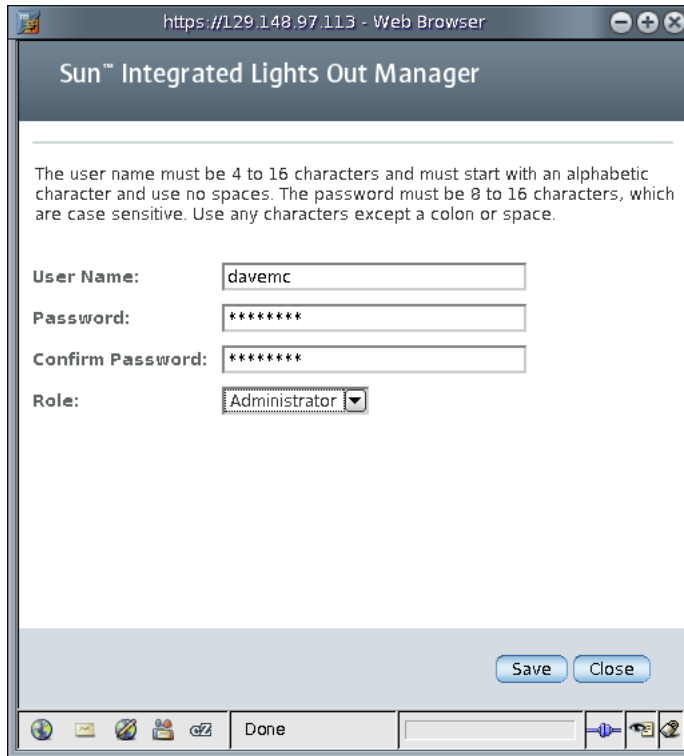
b. Escriba una contraseña en el campo Password.

La contraseña debe tener 8 caracteres como mínimo y no más de 16 caracteres. Existe diferencia entre mayúsculas y minúsculas. Utilice letras, números y caracteres especiales para mayor seguridad. Puede utilizar cualquier carácter excepto el signo de dos puntos. No incluya espacios en las contraseñas.

c. Vuelva a escribir la contraseña en el campo Confirm Password (confirmar contraseña).

d. Seleccione Administrator (administrador) u Operator (operador) en la lista desplegable Role (función).

FIGURA 5-5 Cuadro de diálogo de adición de usuarios con los campos rellenos

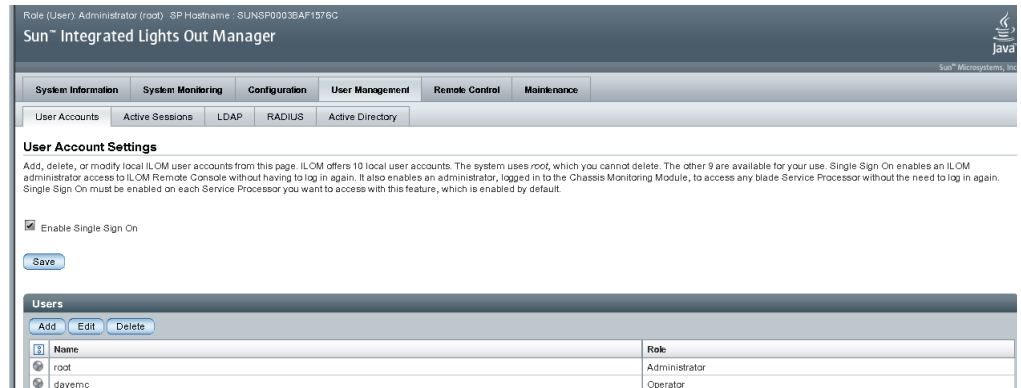


The screenshot shows a web browser window titled "https://129.148.97.113 - Web Browser" displaying the "Sun™ Integrated Lights Out Manager" interface. The page contains a form for adding a new user. At the top, there is a header bar with the title "Sun™ Integrated Lights Out Manager". Below the header, a message states: "The user name must be 4 to 16 characters and must start with an alphabetic character and use no spaces. The password must be 8 to 16 characters, which are case sensitive. Use any characters except a colon or space." The form includes four input fields: "User Name" with the value "davenc", "Password" with "*****", "Confirm Password" with "*****", and "Role" with a dropdown menu set to "Administrator". At the bottom right of the form area, there are two buttons: "Save" and "Close". The browser's status bar at the bottom shows "Done" and various navigation icons.

- e. **Cuando haya terminado de introducir la información del nuevo usuario, haga clic en Save (guardar).**

Vuelve a abrirse la página User Account Settings (configuración de cuentas de usuario). La nueva cuenta y la información asociada aparecerán en la lista de esta página.

FIGURA 5-6 Página de configuración de cuentas de usuario con el nuevo usuario



▼ Modificación de una cuenta de usuario mediante la interfaz web

En esta sección se explica cómo modificar una cuenta de usuario de ILOM.

La modificación puede consistir en cambiar la contraseña del usuario, así como sus privilegios de acceso a la red y la conexión serie.

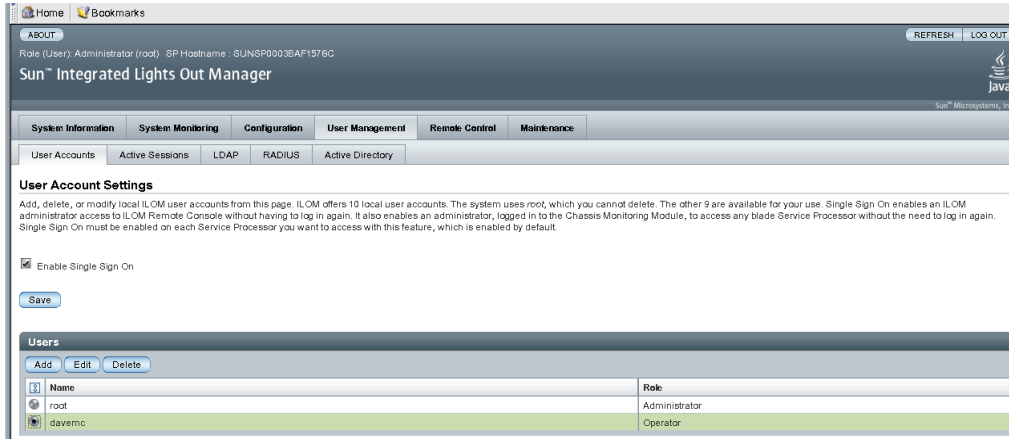
Nota – Sólo las cuentas con privilegios de administrador pueden agregar, modificar o borrar cuentas de usuario, aunque los operadores sí pueden modificar sus propias contraseñas.

Si un usuario nuevo recibe privilegios de administrador, esos privilegios son válidos automáticamente para la interfaz de la línea de comandos (CLI) y la interfaz IPMI (Intelligent Platform Management Interface) de ILOM.

1. **Inicie la sesión de ILOM como administrador para abrir la interfaz web.**
2. **Seleccione User Management (administración de usuarios) --> User Accounts (cuentas de usuario).**

Se abre la página User Account Settings (configuración de cuentas de usuario).

FIGURA 5-7 Página de configuración de cuentas de usuario



3. En la tabla Users (usuarios), seleccione el botón de opción situado junto a la cuenta que quiera modificar.

4. Haga clic en Edit (editar).

Se abre el cuadro de diálogo Edit User (editar usuario).

FIGURA 5-8 Cuadro de diálogo de edición de usuarios

The screenshot shows a web browser window titled "Sun™ Integrated Lights Out Manager" with the URL "https://129.148.97.113 - Web Browser". The main content area contains a message: "The password must be 8 to 16 characters, which are case sensitive. Use any characters except a colon or space." Below this, there are four input fields: "User Name:" with the value "davemc", "New Password:" (empty), "Confirm New Password:" (empty), and "Role:" with a dropdown menu set to "Administrator". A "Change" checkbox is located between the "User Name" and "New Password" fields. At the bottom right of the dialog are "Save" and "Close" buttons. The browser's status bar at the bottom shows "Done" and various navigation icons.

5. **Modifique la contraseña si es necesario.**
 - a. **Marque la casilla Change (cambiar) si desea cambiar la contraseña del usuario. Si no desea cambiarla, quite la marca de selección de la casilla.**
 - b. **Escriba la contraseña nueva en el campo New Password.**

La contraseña debe tener entre 8 y 16 caracteres. Existe diferencia entre mayúsculas y minúsculas. Utilice letras, números y caracteres especiales para mayor seguridad. Puede utilizar cualquier carácter excepto el signo de dos puntos. No incluya espacios en las contraseñas.
 - c. **Vuelva a escribir la contraseña en el campo Confirm New Password (confirmar la nueva contraseña).**
6. **Seleccione Administrator (administrador) u Operator (operador) en la lista desplegable Role (función).**
7. **Una vez modificada la información de la cuenta, haga clic en Save (guardar) para que los cambios tengan efecto o en Close (cerrar) para recuperar la configuración anterior.**

Vuelve a abrirse la página User Account Settings (configuración de cuentas de usuario).

▼ Supresión de una cuenta de usuario mediante la interfaz web

1. Inicie la sesión de ILOM como administrador para abrir la interfaz web.
2. Seleccione User Management (administración de usuarios) --> User Accounts (cuentas de usuario).
Se abre la página User Account Settings (configuración de cuentas de usuario).
3. Seleccione el botón de opciones situado junto a la cuenta de usuario que quiera borrar.

Nota – No es posible borrar la cuenta root.

FIGURA 5-9 Página de configuración de cuentas de usuario

User Account Settings

Add, delete, or modify local ILOM user accounts from this page. ILOM offers 10 local user accounts. The system uses root, which you cannot delete. The other 9 are available for your use. Single Sign On enables an ILOM administrator access to ILOM Remote Console without having to log in again. It also enables an administrator, logged in to the Chassis Monitoring Module, to access any blade Service Processor without the need to log in again. Single Sign On must be enabled on each Service Processor you want to access with this feature, which is enabled by default.

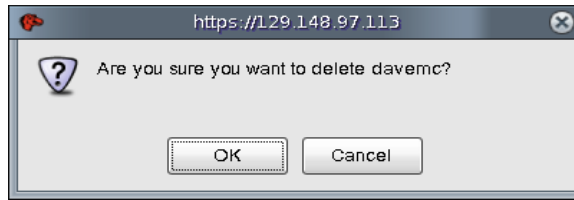
Enable Single Sign On

Users

Name	Role
root	Administrator
davemc	Operator

4. En la tabla Users (usuarios), haga clic en Delete (borrar).
Se abre un cuadro de diálogo de confirmación.

FIGURA 5-10 Cuadro de diálogo de confirmación de la supresión



5. Haga clic en **OK (aceptar)** para borrar la cuenta o en **Cancel (cancelar)** para detener el proceso.

Se abre la página de configuración de cuentas de usuario sin la cuenta recién borrada.

▼ Visualización de las sesiones de usuario mediante la interfaz web

1. Inicie la sesión en la interfaz web de ILOM.
2. Seleccione **User Management (administración de usuarios) --> Active Sessions (sesiones activas)**.

Se abre la página de sesiones activas. En ella encontrará el nombre de usuario, la fecha y hora de inicio de la sesión y los tipos de sesión de los usuarios conectados a ILOM en ese momento.

FIGURA 5-11 Página de sesiones activas



Role (User): Administrator (davemc) SP Hostname : SUNSP00144F1FABF9

Sun™ Integrated Lights Out Manager

System Information System Monitoring Configuration **User Management** Remote Control Maintenance

User Accounts Active Sessions LDAP RADIUS Active Directory

Active Sessions

View the users currently logged in to ILOM, and the type of session they initiated. ILOM supports 10 concurrent sessions of any type, either web or shell.

User Name	Start Time	Type
davemc	Tue May 15 12:45:54 2007	web

Active Directory

ILOM es compatible con Active Directory, el servicio de directorio distribuido que se incluye en los sistemas operativos Windows Server 2003 y Windows 2000 Server de Microsoft.

Introducción a Active Directory

Un servicio de directorio es un sistema de almacenamiento de una base de datos (almacén del directorio) y un conjunto de servicios que proporcionan los medios para agregar, modificar, borrar y localizar los datos en ese almacén de una forma segura. En un entorno distribuido, un servicio de directorio proporciona un punto centralizado donde almacenar la información sobre los dispositivos y servicios de la red, y sobre las personas que los utilizan. También implementa los servicios que ponen esa información a disposición de los usuarios, los equipos informáticos y las aplicaciones.

Active Directory normalmente se utiliza para uno de estos tres propósitos:

- **Directorio interno:** los directorios internos se utilizan dentro de la red corporativa para publicar información sobre los usuarios y recursos existentes en la empresa.
- **Directorio externo:** estos directorios suelen ubicarse en servidores situados en el perímetro o DMZ (zona desmilitarizada) de la red, los límites entre la red local (LAN) corporativa e Internet.
- **Directorio de aplicaciones:** estos directorios almacenan en un directorio local (quizás en el mismo servidor que la aplicación) datos “privados” del directorio que son relevantes exclusivamente para la aplicación sin necesidad de realizar ningún tipo de configuración adicional para Active Directory.

Active Directory puede utilizarse para autenticar las credenciales de los usuarios. Es posible configurar niveles de acceso u obtenerlos del servidor según criterios de pertenencia a diferentes grupos. También es posible utilizar varios “dominios” de usuarios, que se probarán en el orden en que se hayan configurado.

Configuración de Active Directory

Para configurar Active Directory, necesita establecer algunas propiedades globales y suministrar la información de tres tablas que representan:

- Dominio de usuarios
- Grupos de administradores
- Grupos de operadores

▼ Configuración de Active Directory mediante la interfaz web

1. Inicie la sesión de ILOM con privilegios de administrador para abrir la interfaz web.
2. Seleccione **User Management (administración de usuarios)** --> **Active Directory**.
Se abre la página Active Directory. En la mitad superior de esta página se encuentran las opciones de configuración y las tablas de Active Directory.

FIGURA 5-12 Opciones de configuración de Active Directory

The screenshot displays the Sun Integrated Lights Out Manager (ILOM) web interface. At the top, there is a navigation bar with tabs for System Information, System Monitoring, Configuration, User Management, Remote Control, and Maintenance. Under the User Management tab, there are sub-tabs for User Accounts, Active Sessions, LDAP, RADIUS, and Active Directory. The Active Directory sub-tab is selected, showing the configuration page. The page title is "Active Directory". Below the title, there is a brief instruction: "Configure Active Directory settings on this page. Select a default role for all Active Directory users, either Administrator, Operator or none. Enter the IP address of your server. To change the port used to communicate with your server, uncheck Autoselect. Enter a timeout value in seconds. To upload a certificate type in the TFTP server and then the Path and file name. Click Save Certificate to complete the process." The configuration fields are: State (checkbox checked, Enabled), Configure User Role (dropdown menu, None), IP Address (text input, 0.0.0.0), Port (text input, 0), Autoselect (checkbox checked), Timeout (text input, 4), and Strict Certificate Mode (checkbox checked, Enabled). A Save button is located below these fields. Below the configuration fields is the "Certificate Information" section. It shows "Certificate File Status: certificate not present; certificate backup not present." There are three text input fields: "TFTP Server:", "Path and File Name:", and a Save button, a Restore Certificate button, and a Remove Certificate button. At the bottom of the page, there are three expandable sections: Admin Groups, Operator Groups, and User Domains.

Propiedades de la página de configuración de Active Directory

En la [TABLA 5-2](#) se describen las opciones que es preciso configurar para utilizar Active Directory.

TABLA 5-2 Opciones de configuración de Active Directory (variables globales)

Propiedad (web)	Propiedad (CLI)	Valor predeterminado	Descripción
State (estado)	adminState	Enabled	Enabled Disabled (habilitado o inhabilitado)
Role (función)	defaultRole	None	None Administrator Operator (ninguna, administrador, operador) Función de acceso otorgada a todos los usuario autenticados para un caso de configuración sencillo. En principio, esta función no está configurada para proporcionar el enfoque más integrado posible de manera predeterminada. El nivel de acceso se obtiene del servidor Active Directory.
IP Address (dirección IP)	ipaddress		Dirección IP del servidor Active Directory.
Port (puerto)	port	0 (selección automática)	Especifique el puerto utilizado para establecer la comunicación con el servidor o especifique selección automática. Indica el uso del puerto estándar para las transacciones SSL-LDAP. Está disponible en el caso improbable de que se esté utilizando un puerto TCP que no sea estándar.
Timeout (tiempo de espera)	timeout	5	Valor de tiempo de espera en segundos. Número de segundos que es posible esperar para que finalice cada transacción LDAP. El valor no representa el tiempo total de todas las transacciones porque el número de transacciones puede diferir en función de la configuración. Esta propiedad permite ajustar el tiempo de espera cuando un servidor no responde o no se encuentra accesible.

TABLA 5-2 Opciones de configuración de Active Directory (variables globales) (continuación)

Propiedad (web)	Propiedad (CLI)	Valor predeterminado	Descripción
Strict Certificate Mode (modo de certificado estricto)	<code>strictcertmode</code>	Enabled	Enabled Disabled (habilitado o inhabilitado) Si está habilitado, debe cargarse el certificado del servidor de forma que realice una validación de certificados más restrictiva.
Certificate File Status (estado del archivo de certificado)	<code>certfilestatus</code>		<code>certificate present</code> <code>not present</code> ; <code>certificate.backup present</code> <code>not present</code> (archivo de certificado presente o no presente; copia de seguridad presente o no presente)
No hay ninguna propiedad correspondiente en la interfaz web.	<code>getcertfile</code>	none	Método utilizado para cargar un archivo de certificado si es necesario. También es posible suprimir y restaurar certificados desde aquí.
TFTP Server (servidor TFTP)	No hay ninguna propiedad correspondiente en la CLI.	none	Servidor TFTP utilizado para recuperar el archivo de certificado.
Path and File Name (ruta y nombre del archivo)	No hay ninguna propiedad correspondiente en la CLI.	none	Ruta de acceso completa y nombre del archivo de certificado del servidor.
Restore Certificate (restaurar certificado)	No hay ninguna propiedad correspondiente en la CLI.	none	Se utiliza cuando se ha cargado un archivo de certificado sobre otro ya existente. El archivo existente se guarda como copia de seguridad. La restauración recupera la copia de seguridad y la convierte en la copia de uso normal.
Remove Certificate (suprimir certificado)	No hay ninguna propiedad correspondiente en la CLI.	none	No es posible suprimir el certificado si se encuentra habilitada la opción Strict Certificate Mode.

Tablas de destinos de Active Directory

Las tres tablas situadas en la mitad inferior de la página Active Directory (FIGURA 5-13) se utilizan para configurar dominios y grupos con los que autenticar y autorizar a los usuarios. Las tablas de destinos almacenan información sobre:

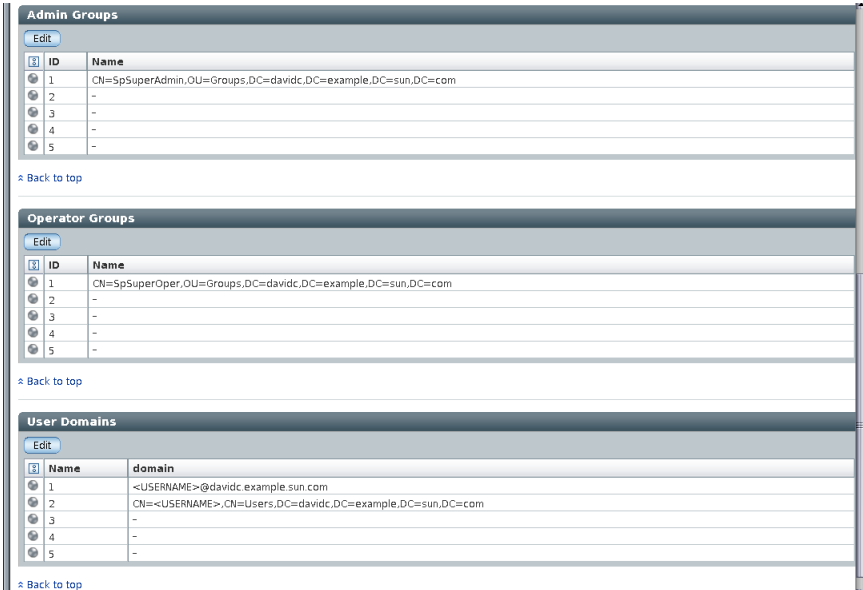
- Grupos de administradores
- Grupos de operadores
- Dominios de usuarios

Las entradas de las tablas Administrator Groups (grupos de administradores) y Operator Groups (grupos de operadores) contienen los nombres de los grupos de MS Active Directory en formato de nombre distintivo. Si un usuario es miembro de un determinado grupo, entonces recibe derechos de acceso como operador o administrador en función de las correspondencias existentes entre los grupos de usuarios y las tablas.

Los dominios de usuarios son los dominios de autenticación a los que pertenece cada usuario. Normalmente, cuando un usuario inicia la sesión, el nombre utilizado recibe el formato de dominio/nombre específicamente suministrado por estas entradas. La autenticación de los usuarios se realiza tomando como referencia los datos de dominio de usuarios introducidos y el nombre de acceso suministrado por el usuario.

En el caso de las tres tablas, se suministran algunos datos predeterminados para mostrar el formato que se espera de la información. En los mensajes de error también se explica qué tipo de datos debería introducir el usuario.

FIGURA 5-13 Tablas de Active Directory



The screenshot displays three configuration tables in a web interface. Each table has an 'Edit' button and a 'Back to top' link. The tables are as follows:

ID	Name
1	CN=SpSuperAdmin,OU=Groups,DC=davidc,DC=example,DC=sun,DC=com
2	-
3	-
4	-
5	-

ID	Name
1	CN=SpSuperOper,OU=Groups,DC=davidc,DC=example,DC=sun,DC=com
2	-
3	-
4	-
5	-

Name	domain
1	<USERNAME>@davidc.example.sun.com
2	CN=<USERNAME>,CN=Users,DC=davidc,DC=example,DC=sun,DC=com
3	-
4	-
5	-

Propiedades de las tablas de destinos de Active Directory

En la [TABLA 5-3](#) y la [TABLA 5-4](#) se ofrece un ejemplo más detallado de las tablas de grupos de administradores y operadores. En la columna Nombre aparecen los nombres distintivos completos.

TABLA 5-3 Tabla de grupos de administradores

ID	Nombre
1	CN=SpSuperAdmin,OU=Groups,DC=davidc,DC=ejemplo,DC=sun,DC=com
2	

TABLA 5-4 Tabla de grupos de operadores

ID	Nombre
1	CN=SpSuperOper,OU=Groups,DC=davidc,DC=ejemplo,DC=sun,DC=com
2	
3	
4	
5	

En la [TABLA 5-5](#) se incluye un ejemplo de la tabla de dominios de usuarios representada en la [FIGURA 5-13](#). El dominio que aparece en la entrada 1 muestra el formato principal, que se utiliza en el primer intento de autenticación. En la entrada 2 aparece el nombre distintivo completo (dn), que se utilizaría en caso de que fallase la autenticación con el formato principal.

Nota – En el ejemplo de la [TABLA 5-5](#), <USERNAME> es una cadena que se sustituirá por el verdadero nombre de acceso del usuario.

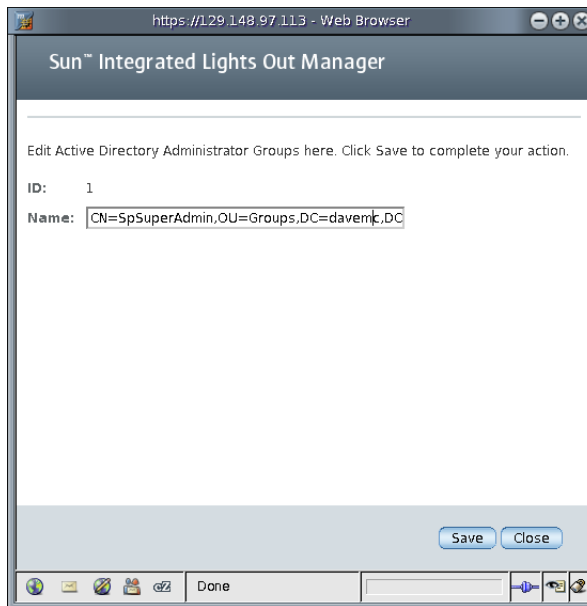
TABLA 5-5 Tabla de dominios de usuarios

Nombre	Dominio
1	<USERNAME>@davidc.ejemplo.sun.com
2	CN=<USERNAME>,CN=Users,DC=davidc,DC=ejemplo,DC=sun,DC=com
3	
4	
5	

▼ Edición de las tablas de Active Directory mediante la interfaz web

1. **Inicie la sesión de ILOM con privilegios de administrador para abrir la interfaz web.**
2. **Seleccione User Management (administración de usuarios) --> Active Directory.**
Se abre la página Active Directory.
3. **En la parte inferior de la página Active Directory, seleccione el botón de opciones situado junto a la fila que desee modificar y haga clic en Edit (editar).**
Se abre la página correspondiente: Edit Active Directory Administrator Groups, Edit Active Directory Operator Groups o Edit Active Directory User Domains (edición de grupos de administradores, grupos de operadores o dominios de usuarios de Active Directory). Cada página de edición proporciona un campo de nombre para agregar o modificar la información.

FIGURA 5-14 Página de edición de grupos de administradores de Active Directory



4. **Agregue o modifique los datos en la página de edición.**
5. **Haga clic en Save (guardar) para que los cambios tengan efecto.**
Se abre la página Active Directory.

6. Especifique el texto adecuado en el campo Name de la tabla de dominios de usuarios. Utilice <USERNAME> a modo de comodín sustituible por el verdadero nombre de usuario en las peticiones LDAP.

Por ejemplo:

```
domain = <USERNAME>@davemc.ejemplo.sun.com
```

```
domain = CN=<USERNAME>,CN=Users,DC=davemc,DC=ejemplo,DC=sun,  
DC=com
```

El usuario recibiría acceso a ILOM con cualquiera de los nombres suministrados, tal y como se muestra en los ejemplos siguientes.

EJEMPLO DE CÓDIGO 5-1 Acceso a Active Directory con el formato principal

```
/home/dc150698> ssh -l davemc 10.x.xxx.xxx  
Password:*****  
Sun(TM) Integrated Lights Out Manager  
Version 1.1  
Copyright 2005 Sun Microsystems, Inc. All rights reserved.  
->
```

EJEMPLO DE CÓDIGO 5-2 Acceso a Active Directory con el nombre distintivo

```
/home/dc150698> ssh -l "David A. Ingeniero" 10.x.xxx.xxx  
Password:*****  
Sun(TM) Integrated Lights Out Manager  
Version 1.1  
Copyright 2005 Sun Microsystems, Inc. All rights reserved.  
->
```

Determinación de los niveles de autorización de los usuarios

Una vez autenticado un usuario, su nivel de acceso puede determinarse de las maneras siguientes. En el caso más sencillo, el acceso como operador o administrador se conoce directamente a través de la configuración de Active Directory en el SP. Existe un método más integrado que consiste en ejecutar una serie de consultas LDAP para conocer a qué grupos de Active Directory está asociado el usuario.

- El primer método es el más fácil de configurar. El usuario sigue autenticándose utilizando la opción `defaultRole`, pero no se precisa ninguna consulta para averiguar su pertenencia a los grupos. La configuración de los usuarios en la base de datos de Active Directory es más sencilla, ya que sólo necesita una contraseña y es independiente de los grupos a los que pertenezca. En el SP, la opción

`defaultRole` se configurará como `administrator` u `operator`. Es decir, todos los usuarios autenticados a través de Active Directory recibirán los privilegios asociados a la función de administrador u operador tomando como base exclusivamente esta configuración.

- El segundo método es más complicado y exige mucha más labor administrativa tanto para la configuración como para la autenticación de cada usuario. Para la configuración, es preciso rellenar las tablas de grupos de administradores y operadores del SP con los nombres correspondientes a cada grupo tomados de la base de datos de Active Directory, los cuales se utilizarán para determinar los niveles de acceso. Es posible introducir hasta cinco grupos de Active Directory para designar un administrador y otros cinco para asignar privilegios de operador.

La pertenencia de un usuario a un grupo se utilizará para identificar el nivel de acceso adecuado (como administrador u operador), para lo cual se examinará cada nombre de los grupos en las tablas de Active Directory configuradas en el SP. Con el segundo método, cinco grupos de usuarios se identifican como operadores y cinco grupos se identifican como administradores, cada uno con sus correspondientes privilegios. Si la lista de grupos a los que pertenece el usuario no se encuentra en ninguno de los grupos de usuarios definidos en el SP, se le deniega el acceso.

Seguridad de la conexión de Active Directory

La autenticación con certificado SSL se utiliza para garantizar una conexión segura, impedir ataques enmascarados y proteger las transacciones LDAP. La validación con certificado es opcional y depende del nivel de seguridad que precise el sistema.

Establecimiento de la seguridad en la conexión de Active Directory mediante la línea de comandos

En los procedimientos siguientes se explica la forma de proteger la seguridad de la conexión de Active Directory mediante la interfaz de la línea de comandos.

▼ Acciones con `getcertfile` desde la línea de comandos

`getcertfile` es el método utilizado para cargar un archivo de certificado si es necesario.

- Para cargar un certificado, escriba lo siguiente:

```
-> set getcertfile=tftp://dirección_IP/ruta-archivo/nombrearchivo
```

- Para suprimir o restaurar un certificado, escriba lo siguiente:

```
-> set getcertfile=remove|restore
```

Por ejemplo:

```
-> set getcertfile=remove
```

El archivo de certificado que se hubiese cargado se suprimirá. La restauración sólo funciona si existe una copia de seguridad del archivo de certificado. La idea es guardar un archivo de copia de seguridad cada vez que se carga un certificado nuevo. Si algo va mal, es posible recuperar el archivo antiguo.

▼ Habilitación de `strictcertmode` mediante la línea de comandos

El modo `strictcertmode` está inhabilitado de manera predeterminada. Aunque se utiliza SSL, sólo se realiza una validación limitada del certificado. Si se habilita `strictcertmode`, el certificado del servidor tiene que haberse cargado en el servidor para que sus firmas de certificación puedan validarse durante el protocolo de negociación de SSL.

- Para habilitar `strictcertmode`, escriba lo siguiente:

```
-> set strictcertmode=enabled
```

▼ Comprobación de `certfilestatus` mediante la línea de comandos

`certfilestatus` es una variable operativa que debería reflejar el estado actual del certificado y la existencia o no de una copia de seguridad del mismo. Ni el certificado ni la copia de seguridad tienen por qué existir si el modo `strictcertmode` está inhabilitado. No obstante, para que `strictcertmode` pueda habilitarse, tiene que haberse cargado un certificado. La copia de seguridad del certificado siempre es opcional y sólo se almacena cuando se va a sobrescribir el certificado existente.

- Para comprobar el estado del certificado, escriba lo siguiente:

```
-> show /SP/clients/activedirectory certfilestatus
```

Por ejemplo:

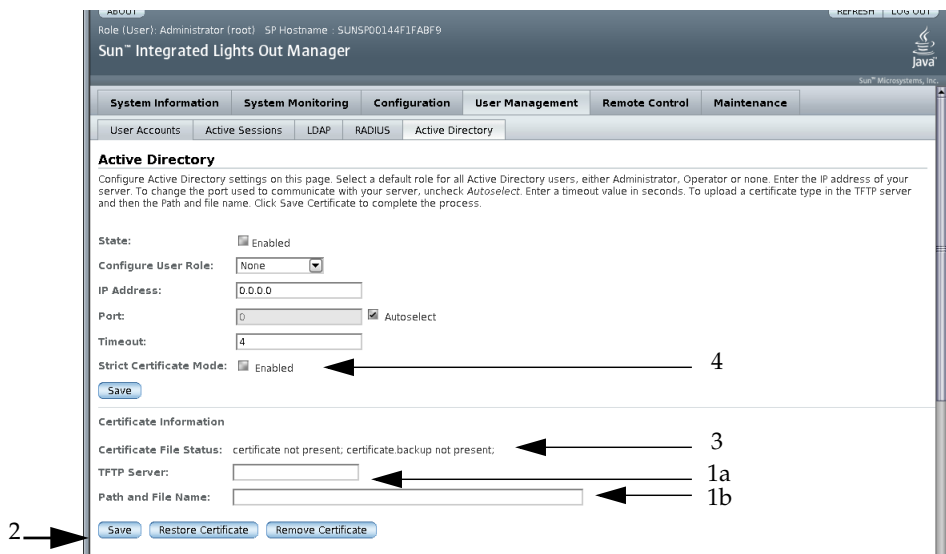
```
-> show /SP/clients/activedirectory certfilestatus
Properties:
certfilestatus = certificate not present;certificate.backup not
present;
```

Establecimiento de la seguridad en la conexión de Active Directory mediante la interfaz web

En los procedimientos siguientes se explica la forma de establecer la seguridad de la conexión de Active Directory mediante la interfaz web.

En la [FIGURA 5-15](#) se ilustran las propiedades de seguridad de Active Directory y el orden en que deben introducirse los datos.

FIGURA 5-15 Propiedades de seguridad de Active Directory y orden de introducción de los datos



▼ Carga de un certificado mediante la interfaz web

1. Inicie la sesión de ILOM con privilegios de administrador para abrir la interfaz web.
2. Seleccione **User Management (administración de usuarios)** --> **Active Directory**. Se abre la página Active Directory. La [FIGURA 5-15](#) muestra el orden en que deben rellenarse los campos de seguridad.
3. Especifique el servidor TFTP, y la ruta y el nombre del archivo en los campos correspondientes (**TFTP Server** y **Path and File Name**). Observe la [FIGURA 5-15](#), puntos 1a y 1b.

4. Haga clic en el botón **Save** (guardar) para iniciar la transferencia del certificado. Observe la [FIGURA 5-15](#), punto 2.

Nota – Las opciones para restaurar y suprimir el certificado están disponibles según las necesidades y se ejecutan mediante los botones **Restore Certificate** y **Remove Certificate** respectivamente.

▼ Comprobación del estado del archivo de certificado mediante la interfaz web

1. Inicie la sesión de ILOM con privilegios de administrador para abrir la interfaz web.
2. Seleccione **User Management** (administración de usuarios) --> **Active Directory**.
Se abre la página **Active Directory**. Observe la [FIGURA 5-15](#), punto 3.
3. Verifique el estado del archivo de certificado.

▼ Habilitación del modo de certificado estricto mediante la interfaz web

1. Inicie la sesión de ILOM con privilegios de administrador para abrir la interfaz web.
2. Seleccione **User Management** (administración de usuarios) --> **Active Directory**.
Se abre la página **Active Directory**. Observe la [FIGURA 5-15](#), punto 4.
3. Haga clic en la casilla situada junto a la opción **Enabled** (habilitado) para habilitar la opción **Strict Certificate Mode**.

LDAP (Lightweight Directory Access Protocol)

ILOM permite autenticar a los usuarios utilizando el protocolo LDAP (Lightweight Directory Access Protocol) a través del software OpenLDAP. LDAP es un servicio de directorio de propósito general. Un servicio de directorio es una base de datos centralizada destinada a aplicaciones distribuidas diseñadas para administrar las entradas de un directorio. De esta manera, varias aplicaciones pueden compartir una misma base de datos de usuarios. Para obtener más información sobre LDAP, consulte <http://www.openldap.org/>.

Introducción a LDAP

LDAP se basa en un modelo cliente-servidor. LDAP proporciona el directorio y los clientes utilizan el servicio de directorio para acceder a las entradas. Los datos almacenados en un directorio pueden distribuirse entre varios servidores LDAP.

Los datos de LDAP se organizan de forma jerárquica, empezando por una raíz y ramificándose hasta cada entrada en particular. Las entradas situadas en la parte superior de la jerarquía representan organizaciones más grandes, bajo las cuales se incluyen las entradas de organizaciones de menor tamaño. Al final de la jerarquía se encuentran las entradas de cada persona o recurso a nivel individual.

Clientes y servidores LDAP

En el modelo cliente-servidor de LDAP, los servidores LDAP ponen la información sobre personas, organizaciones y recursos a disposición de los clientes LDAP. Los clientes realizan cambios en la base de datos de LDAP empleando una utilidad cliente, normalmente entregada con el servidor LDAP. Cuando se efectúa un cambio en dicha base de datos, todas las aplicaciones cliente lo ven de forma inmediata, por lo que no es necesario actualizar cada aplicación distribuida.

Por ejemplo, para actualizar una entrada en el directorio, el cliente LDAP envía al servidor LDAP el nombre distintivo de la entrada con la información de atributos actualizada. El servidor LDAP utiliza este nombre (dn) para encontrar la entrada y la modifica para actualizar los datos en el directorio. La información actualizada está disponible de forma inmediata para todas las aplicaciones distribuidas que utilizan ese servidor LDAP.

Un cliente LDAP puede realizar, entre otras, las siguientes operaciones:

- Búsqueda y recuperación de entradas del directorio
- Adición de nuevas entradas al directorio
- Actualización de entradas en el directorio
- Supresión de entradas del directorio
- Cambio de nombre de las entradas del directorio

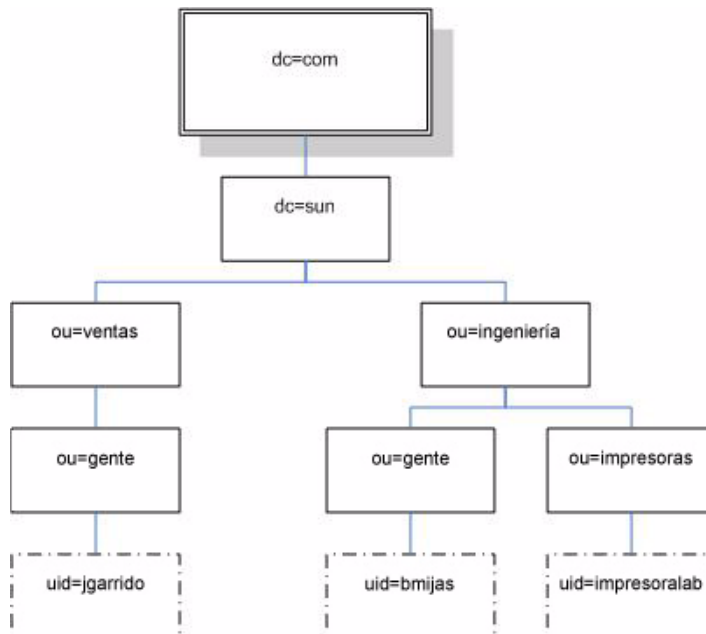
Para realizar cualquiera de estas operaciones, el cliente LDAP necesita establecer una conexión con el servidor LDAP. Para ello, el protocolo especifica el uso del puerto 389 de TCP/IP, aunque los servidores pueden ejecutarse en otros puertos.

Su servidor Sun puede ser cliente de un servidor LDAP. Para poder utilizar la autenticación LDAP, necesita crear un usuario en el servidor LDAP que el servidor Sun pueda autenticar, o enlazarse a él, de forma que el cliente tenga permiso para hacer búsquedas en el directorio adecuado del servidor LDAP.

Organización del directorio en los servidores LDAP

Los datos de LDAP se organizan jerárquicamente, tal y como se ilustra en la [FIGURA 5-16](#).

FIGURA 5-16 Estructura del directorio de LDAP



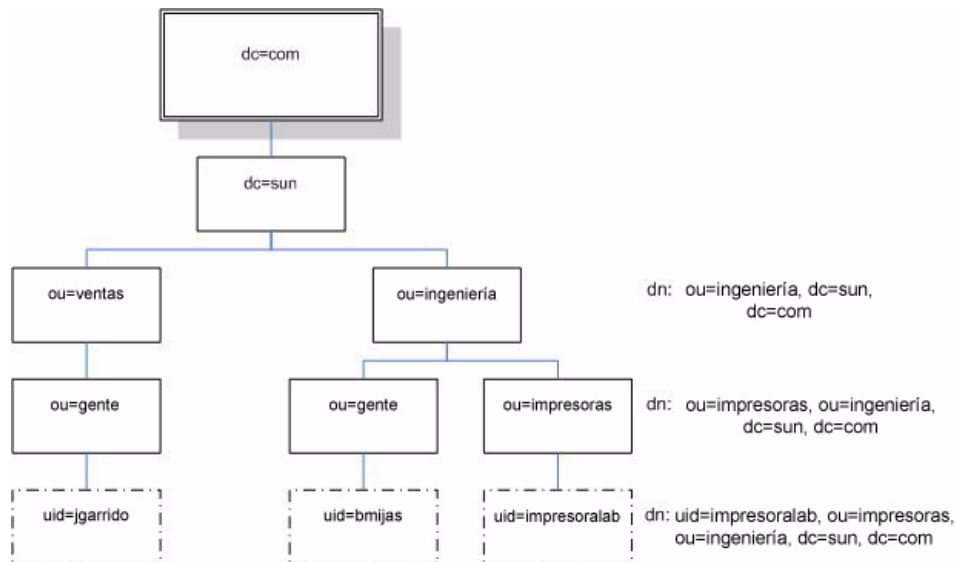
Cada entrada se identifica mediante un nombre distintivo (dn) exclusivo. El DN consiste en un nombre que identifica la entrada de manera exclusiva en ese nivel de la jerarquía y una ruta de acceso que especifica su posición en el árbol desde la raíz.

Por ejemplo, el DN de jgarrido es:

```
dn: uid=jgarrido, ou=gente, dc=sun.com
```

En este caso, `uid` representa el ID de usuario de la entrada, `ou` representa la unidad organizativa a la que pertenece la entrada y `dc` la organización de mayor tamaño en la que está contenida esa entrada. El diagrama siguiente muestra cómo se utilizan los nombres distintivos para identificar las entradas del directorio de forma exclusiva en la jerarquía.

FIGURA 5-17 Nombres distintivos de LDAP



Configuración de LDAP

Para utilizar LDAP, es preciso configurar el servidor LDAP siguiendo las instrucciones de la documentación entregada con él. También es necesario configurar ILOM utilizando la interfaz de la línea de comandos o la interfaz web.

Para realizar el procedimiento siguiente, es preciso conocer en detalle la configuración del servidor LDAP. Antes de empezar, recopile la información de red básica sobre su servidor LDAP, incluida la dirección IP.

Nota – Esta tarea es similar a la de la configuración de LDAP como servicio de nombres para Linux o Solaris.

▼ Configuración del servidor LDAP

1. **Asegúrese de que todos los usuarios que se autenticuen en ILOM tengan contraseñas almacenadas en formato “crypt” o la extensión GNU de crypt, generalmente conocida como “MD5 crypt”.**

Por ejemplo:

```
userPassword: {CRYPT}ajCa2He4PJhNo
```

o

```
userPassword: {CRYPT}$1$pzKng1$du1Bf0NWBjh9t3FbUgf46.
```

ILOM sólo admite la autenticación LDAP de contraseñas almacenadas en estas dos variantes del formato crypt.

2. **Agregue las clases de objetos `posixAccount` y `shadowAccount`, y especifique los valores de propiedades necesarios para este esquema (RFC 2307).**

TABLA 5-6 Valores de propiedades LDAP

Propiedad necesaria	Descripción
uid	Nombre de usuario para iniciar la sesión en ILOM
uidNumber	Cualquier número exclusivo
gidNumber	Cualquier número exclusivo
userPassword	Contraseña
homeDirectory	Cualquier valor (ILOM no tiene en cuenta esta propiedad)
loginShell	Cualquier valor (ILOM no tiene en cuenta esta propiedad)

3. **Proporcione acceso mediante ILOM para las cuentas de usuario del servidor LDAP.**

Permita que su servidor LDAP acepte enlaces anónimos o cree un usuario proxy en el servidor LDAP que tenga acceso de sólo lectura a todas las cuentas de usuario que se vayan a autenticar a través de ILOM.

Consulte la documentación del servidor LDAP para obtener más información.

▼ Configuración de ILOM para LDAP mediante la línea de comandos

1. Especifique el nombre de usuario y la contraseña del usuario proxy. Escriba:

```
-> set /SP/clients/ldap binddn="cn=proxyuser, ou=gente, ou=ventas, dc=sun, dc=com" bindpw=contraseña
```

2. Especifique la dirección IP del servidor LDAP. Escriba:

```
-> set /SP/clients/ldap ipaddress=direcciónipldap
```

3. Asigne el puerto de comunicación con el servidor LDAP (el puerto predeterminado es 389). Escriba:

```
-> set /SP/clients/ldap port=puertoldap
```

4. Introduzca el nombre distintivo de la rama de su árbol LDAP que contenga los usuarios y grupos. Escriba:

```
-> set /SP/clients/ldap searchbase="ou=gente, ou=ventas, dc=sun, dc=com"
```

Ésta es la ubicación del árbol de LDAP en la que quiere buscar los datos para la autenticación de los usuarios.

5. Establezca el estado del servicio LDAP como habilitado. Escriba:

```
-> set /SP/clients/ldap state=enabled
```

6. Para comprobar si funciona la autenticación LDAP, inicie la sesión en ILOM utilizando un nombre de usuario y una contraseña de LDAP.

Nota – ILOM hará la búsqueda entre los usuarios locales antes de buscar entre los usuarios de LDAP. Si existe un nombre de usuario de LDAP como usuario local, ILOM utiliza la cuenta local para la autenticación.

▼ Configuración de ILOM para LDAP mediante la interfaz web

1. Inicie la sesión de ILOM como administrador para abrir la interfaz web.

2. Seleccione User Management (administración de usuarios) --> LDAP.

Se abre la página LDAP Settings (configuración de LDAP).

FIGURA 5-18 Página de configuración de LDAP

LDAP Settings

Configure ILOM access for LDAP users on this page. Select a default role for all of your LDAP users, either Administrator or Operator. Enter the IP address of your LDAP server. Enter the port used to communicate with your LDAP server, the default port is 389. Enter the searchbase, or portion of your LDAP tree, where ILOM should look for LDAP user accounts (ou=docs, dn=writers). Enter the distinguished name (DN) and password for a proxy user ILOM can use to access your LDAP tree.

State: Enabled

Role:

IP Address:

Port:

Searchbase:

Bind DN:

Bind Password:

3. Introduzca los valores siguientes:

- **State (estado):** seleccione la casilla Enabled (habilitado) para autenticar a los usuarios de LDAP.
- **Role (función):** función predeterminada de los usuarios de LDAP. Seleccione Operator o Administrator en la lista desplegable.
- **IP Address (dirección IP):** dirección IP del servidor LDAP.
- **Port (puerto):** número de puerto del servidor LDAP.
- **Searchbase (base de datos de búsqueda):** tipo de rama del servidor LDAP en la que se buscará a los usuarios.
- **Bind DN (DN de enlace):** escriba el nombre distintivo de un usuario proxy con acceso de sólo lectura existente en el servidor LDAP. ILOM debe tener acceso de sólo lectura al servidor LDAP para buscar y autenticar a los usuarios.
- **Bind Password (contraseña de enlace):** escriba la contraseña del usuario con acceso de sólo lectura.

4. Haga clic en Save (guardar).

5. Para comprobar si funciona la autenticación LDAP, inicie la sesión en ILOM utilizando un nombre de usuario y una contraseña de LDAP.

Nota – ILOM hará la búsqueda entre los usuarios locales antes de buscar entre los usuarios de LDAP. Si existe un nombre de usuario de LDAP como usuario local, ILOM utiliza la cuenta local para la autenticación.

Autenticación RADIUS

ILOM permite utilizar la autenticación RADIUS (Remote Authentication Dial-In User Service). RADIUS es un protocolo de autenticación que facilita la administración centralizada de usuarios. Para ello, proporciona a numerosos servidores acceso compartido a los datos de usuario contenidos en una base de datos central, lo que mejora la seguridad y facilita la administración. Un servidor RADIUS puede trabajar en combinación con varios servidores RADIUS y otros tipos de servidores de autenticación.

Clientes y servidores RADIUS

RADIUS se basa en un modelo cliente-servidor. El servidor RADIUS proporciona los datos de autenticación de los usuarios y puede otorgar o denegar el acceso. Por su parte, los clientes envían datos de los usuarios al servidor y reciben la respuesta de acceso aceptado o denegado. En el modelo cliente-servidor de RADIUS, el cliente envía una petición de acceso (Access-Request) al servidor RADIUS. Cuando el servidor recibe esta petición de un cliente, busca la información de autenticación de ese usuario en la base de datos. Si no la encuentra, envía un mensaje de acceso denegado (Access-Reject) y el usuario no puede acceder al servicio solicitado. Si encuentra la información del usuario, el servidor responde con un mensaje de acceso aceptado (Access-Accept). Este mensaje confirma los datos de autenticación del usuario y le proporciona acceso al servicio solicitado.

Todas las transacciones entre el cliente y el servidor RADIUS se autentican mediante el uso de un texto de contraseña específico que se conoce como “secreto compartido”. Ambos, cliente y servidor, han de conocer ese secreto porque nunca se transfiere a través de la red. El administrador debe conocer el secreto compartido a fin de configurar la autenticación RADIUS para ILOM.

Para utilizar la autenticación RADIUS con ILOM, debe configurar este último como cliente RADIUS.

Parámetros de RADIUS

En la [TABLA 5-7](#) se describen los parámetros de RADIUS en la interfaz web y la línea de comandos.

TABLA 5-7 Opciones de configuración de RADIUS en la interfaz web y la línea de comandos

Interfaz web	Línea de comandos	Descripción
State (estado)	<code>state enabled disabled</code>	Permite autenticar usuarios de RADIUS.
Role (función)	<code>defaultrole administrator operator</code>	Establece la función predeterminada de todos los usuarios de RADIUS: administrador u operador.
IP Address (dirección IP)	<code>ipaddress direcciónip</code>	Dirección IP del servidor RADIUS.
Port (puerto)	<code>port númpuerto</code>	Número de puerto utilizado para la comunicación con el servidor RADIUS. El puerto predeterminado es 1812.
Shared Secret (secreto compartido)	<code>secret texto</code>	Secreto compartido utilizado para obtener acceso a RADIUS.

Configuración de RADIUS

Si necesita proporcionar acceso a ILOM para más de 10 cuentas de usuario locales y se ha configurado el servidor RADIUS de la forma adecuada, puede configurar ILOM para que utilice la autenticación RADIUS.

Antes de realizar este procedimiento, recopile la información adecuada sobre el entorno RADIUS, según lo explicado en [“Administración de cuentas de usuario” en la página 65](#).

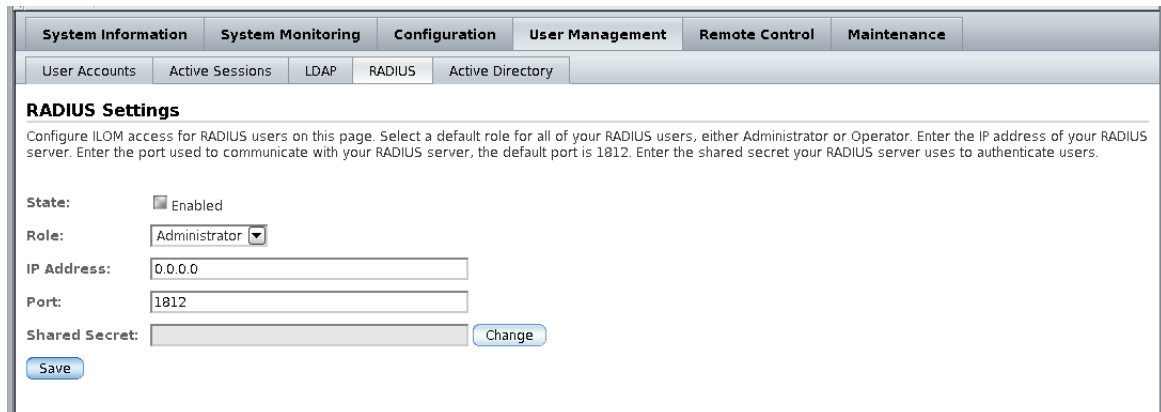
▼ Configuración de RADIUS mediante la línea de comandos

1. **Inicie la sesión en la interfaz de la línea de comandos de ILOM con privilegios de administrador.**
2. **Sitúese en `/SP/clients/radius`. Consulte [“Comandos de RADIUS” en la página 104](#).**
3. **Configure los parámetros indicados en la [TABLA 5-7](#).**

▼ Configuración de RADIUS mediante la interfaz web

1. Inicie la sesión de ILOM como administrador para abrir la interfaz web.
2. Seleccione User Management (administración de usuarios) --> RADIUS.
Se abre la página RADIUS Settings (configuración de RADIUS).

FIGURA 5-19 Página de configuración de RADIUS



The screenshot shows the RADIUS Settings page in the ILOM web interface. The page has a navigation bar with tabs for System Information, System Monitoring, Configuration, User Management, Remote Control, and Maintenance. Under the Configuration tab, there are sub-tabs for User Accounts, Active Sessions, LDAP, RADIUS, and Active Directory. The RADIUS Settings page contains the following fields and controls:

- State:** A checkbox labeled "Enabled" which is checked.
- Role:** A dropdown menu with "Administrator" selected.
- IP Address:** A text input field containing "0.0.0.0".
- Port:** A text input field containing "1812".
- Shared Secret:** A text input field with a "Change" button next to it.
- Save:** A button at the bottom left of the form.

3. Introduzca los valores de configuración.
Para obtener más información, consulte la [TABLA 5-7](#).
4. Haga clic en Save (guardar) para que los cambios tengan efecto.

Comandos de RADIUS

En esta sección se describen los comandos de RADIUS.

```
show /SP/clients/radius
```

Este comando está disponible para los administradores y operadores.

Finalidad

Utilice este comando para ver las propiedades asociadas a la autenticación RADIUS.

Sintaxis

```
show /SP/clients/radius
```

Propiedades

defaultrole: función asignada a todos los usuarios de RADIUS, Administrator u Operator (administrador u operador).

ipaddress: dirección IP del servidor RADIUS.

port: número de puerto utilizado para la comunicación con el servidor RADIUS. El puerto predeterminado es 1812.

secret: secreto compartido utilizado para obtener acceso al servidor RADIUS.

state: este valor se habilita o inhabilita para otorgar o denegar el acceso a los usuarios de RADIUS.

Ejemplo

```
-> show /SP/clients/radius

/SP/clients/radius
Targets:

Properties:
  defaultrole = Operator
  ipaddress = 129.144.36.142
  port = 1812
  secret = (none)
  state = enabled

Commands:
  cd
  set
  show

->
```

```
set /SP/clients/radius
```

Este comando está disponible para los administradores.

Finalidad

Utilice este comando para configurar las propiedades asociadas a la autenticación RADIUS en un procesador de servicios.

Sintaxis

```
set /SP/clients/radius [defaultrole=[Administrator|Operator]  
ipaddress=IPservidorradius port=nºpuerto secret=secretoradius  
state=[enabled|disabled]]
```

Propiedades

- **defaultrole:** debe asignar un nivel de permisos que se aplicará a todos los usuarios de RADIUS y puede ser Administrator u Operator (administrador u operador).
- **ipaddress:** dirección IP del servidor RADIUS.
- **port:** número de puerto utilizado para la comunicación con el servidor RADIUS. El puerto predeterminado es 1812.
- **secret:** especifique el secreto compartido utilizado para obtener acceso al servidor RADIUS. Se conoce también como clave de cifrado.
- **state:** elija enabled (habilitado) o disabled (inhabilitado) para otorgar o denegar el acceso a los usuarios de RADIUS.

Ejemplo

```
-> set /SP/clients/radius state=enabled ipaddress=10.8.145.77  
Set 'state' to 'enabled'  
Set 'ipaddress' to '10.8.145.77'
```

```
show /SP/clients
```

Este comando está disponible para los administradores y operadores.

Finalidad

Utilice el comando para ver los clientes que pueden recibir datos desde un procesador de servicios, incluidos los clientes LDAP, NTP, RADIUS y SYSLOG.

Sintaxis

```
show /SP/clients
```

Ejemplo

```
-> show /SP/clients

/SP/clients
  Targets:
ldap
ntp
radius
syslog

  Properties:

  Commands:
    cd
    show
```

Nota – Los usuarios con privilegios de operador sólo pueden ver los destinos ntp y syslog. Los destinos radius y ldap se mantienen ocultos.

Administración del inventario y los componentes

Con ILOM, es posible ver detalles de los componentes tales como el nombre y tipo de componente, o su estado de funcionamiento. Asimismo, ILOM permite preparar los componentes para su retirada e instalación.

Este capítulo contiene las secciones siguientes:

- “Visualización de la información de los componentes y administración del inventario” en la página 110
 - “Visualización de la información de los componentes mediante la línea de comandos” en la página 110
 - “Visualización de la información de los componentes mediante la interfaz web” en la página 111
- “Realización de acciones con los componentes” en la página 113
 - “Preparación para retirar un componente mediante la línea de comandos” en la página 113
 - “Forma de saber si un componente está listo para su retirada mediante la línea de comandos” en la página 114
 - “Puesta en servicio de un componente mediante la línea de comandos” en la página 114
 - “Preparación para retirar un componente mediante la interfaz web” en la página 115
 - “Puesta de un componente en servicio mediante la interfaz web” en la página 115
- “Habilitación e inhabilitación de componentes” en la página 116
 - “Habilitación e inhabilitación de los componentes mediante la línea de comandos” en la página 116
 - “Habilitación e inhabilitación de los componentes mediante la interfaz web” en la página 116

- “Configuración de normas” en la página 117
 - “Configuración de las normas mediante la línea de comandos” en la página 117
 - “Configuración de las normas mediante la interfaz web” en la página 118

Nota – Los ejemplos de sintaxis de este capítulo utilizan el destino que empieza por `/SP/`, pero podría cambiarse por el destino que empieza por `/CMM/` en función de cuál sea la plataforma de servidor Sun utilizada. Los destinos subordinados son comunes para todas las plataformas de servidor Sun.

Visualización de la información de los componentes y administración del inventario

En los procedimientos siguientes se explica cómo ver la información de los componentes. Tanto los administradores como los operadores pueden ver esta información.

▼ Visualización de la información de los componentes mediante la línea de comandos

1. Inicie la sesión en la interfaz de la línea de comandos de ILOM como administrador u operador.
2. Cuando aparezca el indicador de comandos, escriba:

-> **show nombre_componentetype**

Por ejemplo:

```
-> show /SYS/MB type
Properties:
    type = Motherboard
Commands:
    show
```

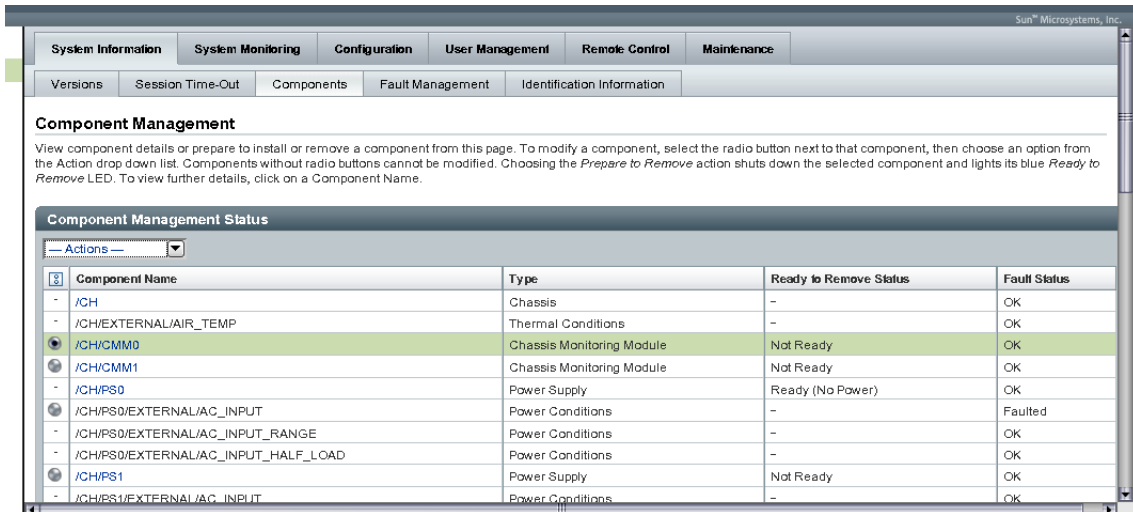
Las propiedades que muestran información de inventario figuran en la lista siguiente. La posibilidad de ver unas propiedades u otras depende del tipo de destino utilizado.

- fru_part_number
- fru_manufacturer
- fru_serial_number
- fru_name
- fru_description
- fru_version
- chassis_serial_number
- chassis_part_number
- product_name
- product_serial_number
- product_part_number
- customer_frudata

▼ Visualización de la información de los componentes mediante la interfaz web

1. **Inicie la sesión de la interfaz web de ILOM como administrador u operador.**
2. **Seleccione System Information (información del sistema) -> Components (componentes).**
Se abre la página Component Management (administración de componentes).

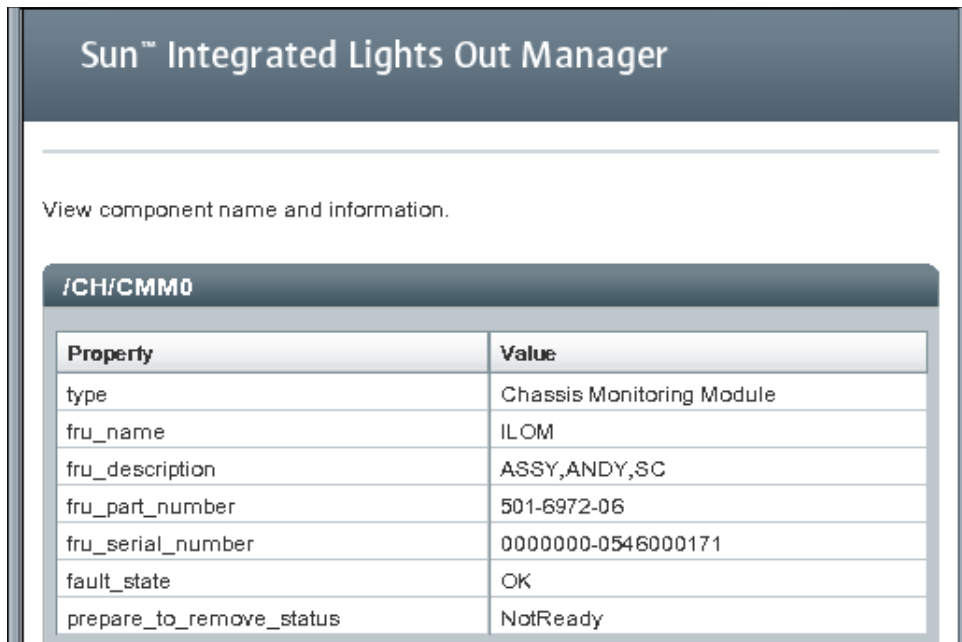
FIGURA 6-1 Página de administración de componentes



3. Haga clic en el nombre de un componente de la tabla **Component Management Status** (estado de la administración de componentes).

Se abre un cuadro de diálogo con información sobre el componente seleccionado.

FIGURA 6-2 Cuadro de diálogo de información del componente



Realización de acciones con los componentes

Además de ver el inventario, es posible realizar las siguientes acciones con los componentes:

- Prepararlos para su retirada o puesta en servicio, consulte [“Retirada y sustitución de los componentes” en la página 113](#).
- Habilitarlos o inhabilitarlos, consulte [“Habilitación e inhabilitación de componentes” en la página 116](#).
- Borrar errores, consulte [“Administración de errores” en la página 131](#).

Retirada y sustitución de los componentes

Es posible sustituir muchos componentes mientras el sistema está en funcionamiento, basta utilizar un procedimiento de desinstalación y sustitución. El procedimiento implica retirar e introducir módulos en un sistema. Antes de retirar un módulo, es preciso prepararlo mediante el uso de la interfaz web o la línea de comandos de ILOM.

▼ Preparación para retirar un componente mediante la línea de comandos

1. Inicie la sesión en la interfaz de la línea de comandos de ILOM como administrador u operador.
2. Cuando aparezca el indicador de comandos de ILOM, escriba:

```
-> set <destino> prepare_to_remove_action=true
```

Por ejemplo:

```
-> set /CH/RFM0 prepare_to_remove_action=true  
Set 'prepare_to_remove_action' to 'true'
```

▼ Forma de saber si un componente está listo para su retirada mediante la línea de comandos

Después de preparar un componente para su retirada, puede verificar si está listo para ser físicamente extraído.

1. Inicie la sesión en la interfaz de la línea de comandos de ILOM como administrador u operador.
2. Cuando aparezca el indicador de comandos de ILOM, escriba:

→ **show <destino> prepare_to_remove_status**

Por ejemplo:

```
-> show /CH/RFM0 prepare_to_remove_status
Properties:
  prepare_to_remove_status = Ready|NotReady
Commands:
  cd
  set
  show
  start
  stop
```

La sentencia Ready|NotReady del ejemplo indica si el dispositivo está listo o no para su retirada.

▼ Puesta en servicio de un componente mediante la línea de comandos

Si ha preparado un componente para su extracción y desea cancelar la acción, puede hacerlo de forma remota.

1. Inicie la sesión en la interfaz de la línea de comandos de ILOM como administrador u operador.
2. Cuando aparezca el indicador de comandos de ILOM, escriba:

→ **set <destino> return_to_service_action=true**

Por ejemplo:

```
-> set /CH/RFM0 return_to_service_action=true
Set 'return_to_service_action' to 'true'
```

▼ Preparación para retirar un componente mediante la interfaz web

1. Inicie la sesión de la interfaz web de ILOM como administrador u operador.
2. Seleccione System Information (información del sistema) -> Components (componentes).

Se abre la página Component Management (administración de componentes).

FIGURA 6-3 Página de administración de componentes

Component Management

View component details or prepare to install or remove a component 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 Management Status

Actions: [Dropdown]

Component Name	Type	Ready to Remove Status	Fault Status
- /CH	Chassis	-	OK
- /CH/EXTERNAL/AIR_TEMP	Thermal Conditions	-	OK
<input checked="" type="radio"/> /CH/CMM0	Chassis Monitoring Module	Not Ready	OK
<input type="radio"/> /CH/CMM1	Chassis Monitoring Module	Not Ready	OK
- /CH/PS0	Power Supply	Ready (No Power)	OK
<input type="radio"/> /CH/PS0/EXTERNAL/AC_INPUT	Power Conditions	-	Faulted
- /CH/PS0/EXTERNAL/AC_INPUT_RANGE	Power Conditions	-	OK
- /CH/PS0/EXTERNAL/AC_INPUT_HALF_LOAD	Power Conditions	-	OK
<input type="radio"/> /CH/PS1	Power Supply	Not Ready	OK
- /CH/PS1/EXTERNAL/AC_INPUT	Power Conditions	-	OK

3. Seleccione el botón de opción situado junto al componente que quiera retirar.
Los componentes que carezcan de botón de opción no pueden retirarse.
4. Seleccione **Prepare to Remove** (preparar para retirar) en la lista desplegable **Actions** (acciones).

▼ Puesta de un componente en servicio mediante la interfaz web

1. Inicie la sesión de la interfaz web de ILOM como administrador u operador.
2. Seleccione System Information (información del sistema) -> Components (componentes).

Se abre la página Component Management (administración de componentes).

3. Seleccione el botón de opción situado junto al componente que quiera volver a poner en servicio.
4. Seleccione **Return to Service** (poner en servicio) en la lista desplegable **Actions** (acciones).

Habilitación e inhabilitación de componentes

En función de la plataforma de servidor Sun utilizada, puede que sea posible habilitar o inhabilitar ciertos componentes. Consulte la documentación específica de la plataforma de servidor para obtener más información.

▼ Habilitación e inhabilitación de los componentes mediante la línea de comandos

1. Inicie la sesión en la interfaz de la línea de comandos de ILOM como administrador.
2. Cuando aparezca el indicador de comandos de ILOM, escriba:

```
-> set /SYS/MB/CMP0/P0/C0 component_state=enabled | disabled
```

▼ Habilitación e inhabilitación de los componentes mediante la interfaz web

1. Inicie la sesión en la interfaz web de ILOM como administrador.
2. Seleccione **System Information** (información del sistema) -> **Components** (componentes).
Se abre la página **Component Management** (administración de componentes).
3. Seleccione el botón de opción situado junto al componente que quiera habilitar o inhabilitar.
4. Seleccione **Enable** (habilitar) o **Disable** (inhabilitar) en la lista desplegable **Actions** (acciones).

El componente se habilita o inhabilita en función de la selección que realice.

Configuración de normas

Las normas son valores que controlan el comportamiento del sistema. Las normas se entregan con los valores predeterminados para el sistema, pero pueden modificarse fácilmente utilizando la interfaz web o la línea de comandos de ILOM.

▼ Configuración de las normas mediante la línea de comandos

1. Inicie la sesión en la interfaz de la línea de comandos de ILOM como administrador.

2. Cuando aparezca el indicador de comandos de ILOM, escriba:

```
-> show /CMM/policy
```

Por ejemplo

```
-> show /CMM/policy  
/CMM/policy  
  Targets:  
  Properties:  
NombreNorma1= enabled  
NombreNorma3 = enabled  
NombreNorma3 = enabled  
  Commands:  
    cd  
    set  
    show
```

3. Cuando aparezca el indicador de comandos de ILOM, escriba:

```
-> set /CMM/policy
```

Por ejemplo

```
-> set /CMM/Policy1Name=enabled
```

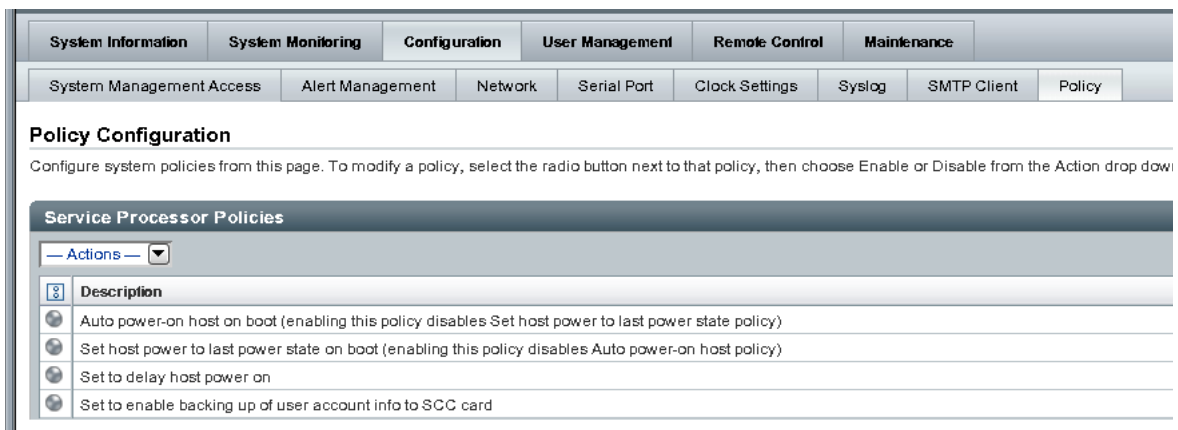
```
/CMM/NombreNormal=enabled
```

▼ Configuración de las normas mediante la interfaz web

En función de la plataforma de servidor Sun utilizada, es posible que pueda configurar los valores de las normas.

1. **Inicie la sesión en la interfaz web de ILOM como administrador.**
2. **Seleccione Configuration (configuración) --> Policy (normas).**
Se abre al página Policy Configuration (configuración de normas).
3. **Seleccione el botón de opción situado junto a la norma que quiera modificar.**
4. **Seleccione Enable (habilitar) o Disable (inhabilitar) en la lista de acciones.**

FIGURA 6-4 Página de configuración de normas



Supervisión del sistema y administración de alertas

Las funciones de supervisión del sistema de ILOM permiten vigilar de forma proactiva el estado en que se encuentra el sistema. Las funciones de administración de alertas le notifican con antelación los eventos que se producen en el sistema. Puede ver y administrar las funciones de supervisión y administración de alertas de ILOM desde la interfaz web o la interfaz de la línea de comandos.

Este capítulo incluye las siguientes secciones:

- “Descripción de la supervisión del sistema” en la página 121
 - “Lecturas de los sensores” en la página 121
 - “Indicadores del sistema” en la página 125
 - “Registro de eventos de ILOM” en la página 128
 - “Marcas de tiempo del registro de eventos y configuración del reloj de ILOM” en la página 129
 - “Información de Syslog” en la página 130
 - “Administración de errores” en la página 131
- “Supervisión de los sensores del sistema, los indicadores y el registro de eventos de ILOM” en la página 134
 - “Identificación del estado de los indicadores mediante la interfaz web” en la página 134
 - “Obtención de las lecturas de los sensores mediante la interfaz web” en la página 135
 - “Visualización o borrado del registro de eventos de ILOM mediante la interfaz web” en la página 136
 - “Visualización o borrado del registro de eventos de ILOM mediante la línea de comandos” en la página 138
 - “Visualización y configuración del reloj mediante la línea de comandos” en la página 130

- “Visualización y configuración del reloj mediante la interfaz web” en la página 140
- “Configuración de las direcciones IP de un destinatario de Syslog remoto mediante la interfaz web” en la página 141
- “Configuración de las direcciones IP de un destinatario de Syslog remoto mediante la línea de comandos” en la página 142
- “Introducción a la administración de alertas” en la página 143
 - “Configuración de las reglas de alertas” en la página 144
 - “Definición de propiedades para las reglas de alertas” en la página 144
- “Administración de las reglas de alertas mediante la interfaz web de ILOM” en la página 147
 - “Requisitos previos” en la página 148
 - “Modificación de una regla de alerta mediante la interfaz web” en la página 149
 - “Inhabilitación de una regla de alerta mediante la interfaz web” en la página 150
 - “Generación de pruebas de alertas mediante la interfaz web” en la página 150
- “Administración de las reglas de alertas mediante la línea de comandos de ILOM” en la página 151
 - “Comandos para administrar las reglas de alertas desde la línea de comandos” en la página 152
 - “Modificación de las reglas de alertas mediante la línea de comandos” en la página 154
 - “Inhabilitación de una regla de alerta mediante la línea de comandos” en la página 155
- “Configuración de un cliente SMTP para alertas de notificación por correo electrónico” en la página 157
 - “Habilitación del cliente SMTP mediante la interfaz web” en la página 158
 - “Habilitación de un cliente SMTP mediante la línea de comandos” en la página 158

Descripción de la supervisión del sistema

Las funciones de supervisión del sistema de ILOM permiten conocer con facilidad el estado de funcionamiento del sistema y detectar errores de un vistazo cuando se producen. Por ejemplo, en ILOM, puede:

- Obtener lecturas instantáneas de los sensores de temperatura, voltaje, corriente, velocidad y presencia de los componentes del sistema. Para obtener más información, consulte [“Lecturas de los sensores” en la página 121](#).
- Conocer el estado de los indicadores de todo el sistema. Para obtener más información, consulte [“Indicadores del sistema” en la página 125](#).
- Identificar los errores del sistema y ver información sobre los eventos en el registro de eventos de ILOM. Para obtener más información, consulte [“Registro de eventos de ILOM” en la página 128](#).
- Ver el estado de funcionamiento de un componente del sistema. Tenga presente que, en la actualidad, esta función está disponible en todas las plataformas de servidor Sun a excepción de los servidores Sun Fire de las series X4100 y X4200. Para obtener más información, consulte [“Administración de errores” en la página 131](#).
- Recibir notificaciones anticipadas sobre eventos del sistema a través de alertas PET de IPMI, capturas de eventos SNMP o avisos por correo electrónico. Para obtener más información, consulte [“Introducción a la administración de alertas” en la página 143](#).

Lecturas de los sensores

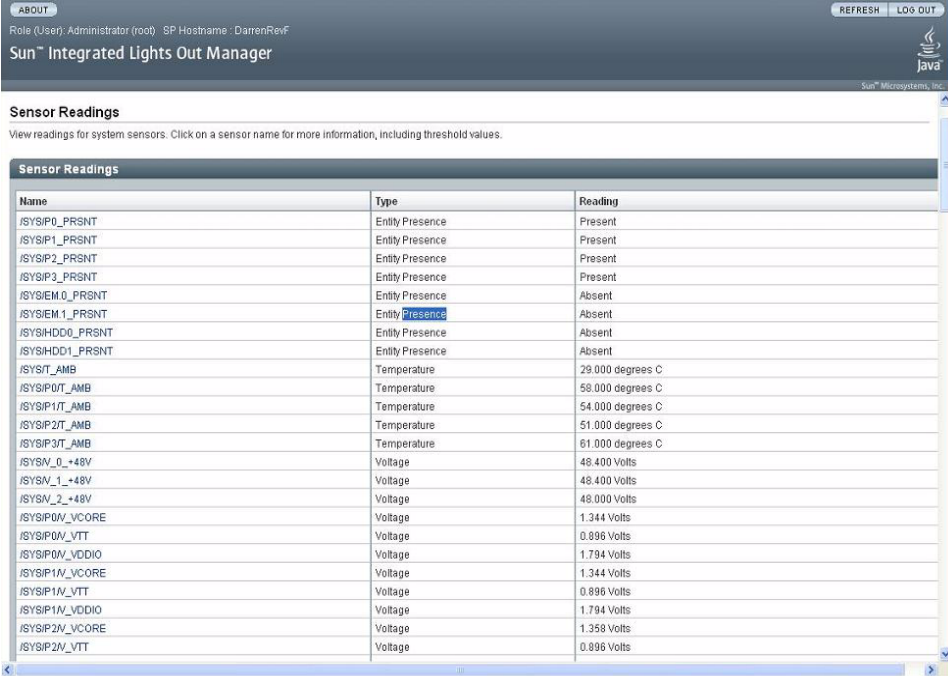
Todas las plataformas de servidor Sun están dotadas de una serie de sensores que miden el voltaje, las temperaturas, la velocidad de los ventiladores y otros atributos del sistema. Cada sensor de ILOM contiene nueve propiedades que describen los distintos valores que lo definen, lo que incluye, el tipo y la clase de sensor, el valor que genera y los umbrales superior e inferior del sensor.

ILOM sondea periódicamente los sensores y anota en su registro de eventos cualquier evento que detecte en relación con posibles cambios de estado o la superación de los umbrales. Asimismo, si se ha establecido en el sistema una regla de envío de alertas que se active al superar un determinado umbral y se alcanza ese valor, ILOM envía automáticamente un mensaje de alerta al destino definido.

Obtención de lecturas de los sensores mediante la interfaz web

En la página System Monitoring (supervisión del sistema) --> Sensor Readings (lecturas de sensores) de la interfaz web de ILOM, pueden obtenerse lecturas instantáneas de los sensores de las unidades sustituibles en campo (FRU) y otros componentes del sistema.

FIGURA 7-1 Página de lecturas de los sensores

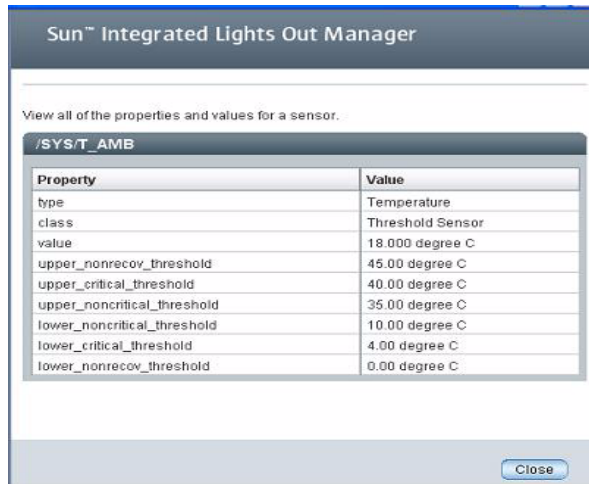


The screenshot shows the 'Sensor Readings' page in the Sun Integrated Lights Out Manager. The page title is 'Sun™ Integrated Lights Out Manager' and it includes a 'Role (User): Administrator (root) SP Hostname : DannerRevF' and 'Sun™ Microsystems, Inc.' logo. Below the title, there is a section for 'Sensor Readings' with a sub-header 'Sensor Readings' and a description: 'View readings for system sensors. Click on a sensor name for more information, including threshold values.' The main content is a table with three columns: 'Name', 'Type', and 'Reading'.

Name	Type	Reading
/SYS/IP0_PRSNT	Entity Presence	Present
/SYS/IP1_PRSNT	Entity Presence	Present
/SYS/IP2_PRSNT	Entity Presence	Present
/SYS/IP3_PRSNT	Entity Presence	Present
/SYS/EM0_PRSNT	Entity Presence	Absent
/SYS/EM1_PRSNT	Entity Presence	Absent
/SYS/HDD0_PRSNT	Entity Presence	Absent
/SYS/HDD1_PRSNT	Entity Presence	Absent
/SYS/T_AMB	Temperature	29.000 degrees C
/SYS/IP0/T_AMB	Temperature	58.000 degrees C
/SYS/IP1/T_AMB	Temperature	54.000 degrees C
/SYS/IP2/T_AMB	Temperature	51.000 degrees C
/SYS/IP3/T_AMB	Temperature	61.000 degrees C
/SYS/V_0_+48V	Voltage	48.400 Volts
/SYS/V_1_+48V	Voltage	48.400 Volts
/SYS/V_2_+48V	Voltage	48.000 Volts
/SYS/IP0/V_VCORE	Voltage	1.344 Volts
/SYS/IP0/V_VTT	Voltage	0.896 Volts
/SYS/IP0/V_VDDIO	Voltage	1.794 Volts
/SYS/IP1/V_VCORE	Voltage	1.344 Volts
/SYS/IP1/V_VTT	Voltage	0.896 Volts
/SYS/IP1/V_VDDIO	Voltage	1.794 Volts
/SYS/IP2/V_VCORE	Voltage	1.358 Volts
/SYS/IP2/V_VTT	Voltage	0.896 Volts

En la página de lecturas de los sensores figuran los valores de cada sensor por nombre, tipo y lectura. Para obtener más información sobre un determinado sensor de umbrales, haga clic en el nombre del sensor situado en la página y aparecerán otras propiedades relativas a los umbrales. Por ejemplo, si hace clic en el sensor denominado `/SYS/T_AMB`, el cuadro de diálogo que aparece presenta información complementaria sobre ese sensor.

FIGURA 7-2 Cuadro de diálogo de propiedades del sensor /SYS/T_AMB



Property	Value
type	Temperature
class	Threshold Sensor
value	18.00 degree C
upper_nonrecov_threshold	45.00 degree C
upper_critical_threshold	40.00 degree C
upper_noncritical_threshold	35.00 degree C
lower_noncritical_threshold	10.00 degree C
lower_critical_threshold	4.00 degree C
lower_nonrecov_threshold	0.00 degree C

Si precisa más información sobre la forma de obtener las lecturas de los sensores a través de la interfaz web de ILOM, consulte [“Identificación del estado de los indicadores mediante la interfaz web”](#) en la página 134.

Obtención de lecturas de los sensores mediante la línea de comandos

En la interfaz de la línea de comandos de ILOM, puede obtener lecturas instantáneas de los sensores de las FRU y otros componentes del sistema situados en el espacio de nombres /SYS o /CH. Ambos espacios de nombres admiten dos clases de lecturas de sensores a las que es posible acceder. Estas clases se conocen como *lecturas de sensores de umbrales* y *lecturas de sensores discretos*. A continuación se incluye una breve descripción de ambas.

Sensores de umbrales

Estos sensores proporcionan el valor de una propiedad del sensor junto con los umbrales superior e inferior predefinidos como críticos y no críticos. Este tipo de sensores normalmente incluyen lecturas de las temperaturas y voltajes de los componentes o las velocidades de los ventiladores.

Para obtener las lecturas de los sensores mediante la interfaz de la línea de comandos de ILOM, debe utilizar el comando `cd` para situarse en el destino del sensor y luego el comando `show` para ver sus propiedades.

Por ejemplo, en algunas plataformas de servidor, puede especificar la ruta siguiente para conocer la temperatura en la entrada de aire de un servidor.

```
cd /SYS/T_AMB  
show
```

Aparecen las propiedades que describen el destino del sensor. Por ejemplo:

- Type = Sensor
- Class = Threshold Sensor
- Value = 32.000 degree C
- Upper = non-recov_threshold = 80.00 degree C
- Upper critical_threshold = 75.00 degree C
- Upper noncritical_threshold = 70.00 degree C
- Lower non_recov_threshold = 0.00 degree C
- Lower critical_threshold = 0.00 degree C
- Lower noncritical_threshold = 0.00 degree C

Para obtener datos específicos sobre los tipos de destinos de sensores de umbrales a los que tiene acceso, así como las rutas para acceder a ellos, consulte la documentación de usuario suministrada con la plataforma de servidor Sun.

Sensores discretos

Estos sensores ofrecen un conjunto de valores bien definidos asociados al destino del sensor. Normalmente proporcionan información sobre la presencia o el estado de funcionamiento de un componente, o el estado de una fuente de alimentación.

Para obtener la lectura de un sensor discreto mediante la interfaz de la línea de comandos de ILOM, debe utilizar el comando `cd` para situarse en el destino del sensor y luego el comando `show` para ver las propiedades del destino. Por ejemplo, en algunas plataformas de servidor Sun, puede averiguar si una determinada unidad de disco duro está presente en la ranura 0 especificando la ruta siguiente:

```
cd /SYS/HDD0_PRSENT  
show
```

Aparecen las propiedades que describen el destino del sensor. Por ejemplo:

- Type = Entity Presence
- Class = Discrete Indicator
- Value = Present

Para obtener datos específicos sobre los tipos de destinos de sensores discretos a los que tiene acceso, así como las rutas para acceder a ellos, consulte la documentación de usuario suministrada con la plataforma de servidor Sun.

Indicadores del sistema

En general, ILOM ilumina los indicadores LED del sistema siguiendo las normas específicas de la plataforma de servidor Sun. Normalmente, los ilumina cuando se produce una de las situaciones siguientes:

- Detección de un fallo o error en un componente.
- Necesidad de mantenimiento de una unidad sustituible en campo (FRU).
- Presencia de un módulo conectable en marcha preparado para su retirada.
- Actividad en una FRU o en el sistema.

Puede ver los estados de los indicadores del sistema desde la interfaz web o la línea de comandos de ILOM. Asimismo, en algunos casos, es posible modificar el estado de un indicador del sistema.

Posibles estados de los indicadores del sistema

ILOM admite los siguientes estados para los indicadores del sistema:

- **Apagado:** estado de funcionamiento normal. El sistema no necesita la intervención del servicio técnico.
- **Continuamente iluminado:** el componente está listo para su retirada.
- **Parpadeo lento:** el componente está cambiando de estado.
- **Parpadeo rápido:** ayuda a localizar el sistema en un CPD.
- **Parpadeo periódico:** el componente está preparado para su activación pero no está operativo en ese momento.

Tipos de estados de los indicadores del sistema

ILOM admite dos tipos de estados para los indicadores del sistema: *modificables por el usuario* y *asignados por el sistema*.

- **Estados modificables por el usuario:** algunos LED del sistema de ILOM ofrecen estados que el usuario puede cambiar. Normalmente, este tipo de indicadores proporcionan los estados operativos de varios componentes del sistema. Los tipos de estados presentados vienen determinados por el indicador del sistema. Por ejemplo, según cuál sea el indicador, pueden aparecer los siguientes estados modificables por el usuario:
 - **Apagado:** estado de funcionamiento normal. El sistema no necesita la intervención del servicio técnico.
 - **Parpadeo rápido:** ayuda a localizar el sistema en un CPD.

Para obtener más información sobre la visualización y administración de los indicadores del sistema desde la interfaz web o la línea de comandos de ILOM, consulte [“Visualización y administración de los indicadores mediante la interfaz web”](#) en la página 126 o [“Visualización y administración de los indicadores mediante la línea de comandos”](#) en la página 127.

- **Estados asignados por el sistema:** estos indicadores *no* son configurables por el usuario. Este tipo de indicadores proporcionan valores de sólo lectura sobre el estado operativo de un componente. En la mayoría de las plataformas de servidor Sun, los indicadores asignados por el sistema son *LED para intervención del servicio técnico*. Este tipo de LED normalmente se iluminan cuando se detecta alguna de las siguientes situaciones:
 - Detección de un fallo o error en un componente del sistema.
 - Presencia de un módulo conectable en marcha preparado para su retirada.
 - Necesidad de mantenimiento de una unidad sustituible en campo (FRU).

Visualización y administración de los indicadores mediante la interfaz web

En la página Indicators (indicadores) de la interfaz web de ILOM puede ver y manejar los indicadores del sistema. La página contiene la lista de indicadores clasificados por nombre y estado. Aquellos que ofrecen estados modificables por el usuario aparecen con un botón de opción. Para cambiar un estado modificable por el usuario, seleccione el botón de opción y elija un estado en la lista desplegable Actions (acciones).

FIGURA 7-3 Página de indicadores

Indicators

Manage the system Locator indicators and view the status of other indicators from this page. To modify an indicator, select the radio button next to that indicator, then choose an option from the Action drop down list. The Locate indicators are the white LEDs.

Name	Status
/SYS/LOCATE	Off
/SYS/OK	Standby Blink
/SYS/OK2RM	Off
/SYS/SERVICE	Off
/SYS/PO/SERVICE	Off
/SYS/IP1/SERVICE	Off

Si precisa información sobre la forma de ver lecturas instantáneas de los sensores a través de la interfaz web de ILOM, consulte [“Obtención de las lecturas de los sensores mediante la interfaz web”](#) en la página 135.

Visualización y administración de los indicadores mediante la línea de comandos

En la interfaz de la línea de comandos de ILOM, es posible acceder a todos los indicadores del sistema del espacio de nombres `/SYS` o `/CH`. Normalmente, deberá utilizar el comando `cd` para situarse en el destino del indicador del sistema y luego el comando `show` para ver las propiedades del destino. Puede cambiar el estado de un indicador del sistema utilizado el comando `set`. El comando `set` sólo puede utilizarse con indicadores que tengan un estado modificable por el usuario. Para saber si puede cambiar el estado de un indicador del sistema, utilice el comando `cd` para desplazarse hasta el destino del indicador y luego el comando `show` para ver sus propiedades. Por ejemplo:

```
cd /SYS/destino_indicador o cd /CH/destino_indicador
show
```

Aparecerán los destinos, propiedades y comandos asociados a ese indicador del sistema, por ejemplo:

```
Targets:
Properties:
Type = indicator
Value = Off
Commands:
  cd
  set
  show
```

Si aparece el comando `set` en la lista `Commands`, quiere decir que puede modificar el estado del indicador. Para modificar el estado, utilice la sintaxis siguiente:

```
set value=nombre_estado
```

Para obtener más información sobre los indicadores del sistema incluidos en su sistema y las rutas para acceder a ellos, consulte la documentación de usuario suministrada con la plataforma de servidor Sun.

Registro de eventos de ILOM

El registro de eventos de ILOM permite ver información sobre cualquier suceso ocurrido en el sistema. Algunos de estos eventos pueden incluir cambios en la configuración de ILOM, eventos de software, avisos, alertas, fallos de componentes y eventos de IPMI. Los tipos de eventos anotados en el registro vienen determinados por la plataforma de servidor Sun. Para obtener información específica sobre los datos que se guardan en el registro de eventos de ILOM, consulte la documentación de usuario suministrada con la plataforma de servidor.

El registro de eventos de ILOM se puede consultar y administrar desde la interfaz web o la línea de comandos de ILOM. Para obtener más información sobre la forma de ver y administrar el registro de eventos de ILOM, consulte [“Visualización o borrado del registro de eventos de ILOM mediante la interfaz web”](#) en la página 136 o [“Visualización o borrado del registro de eventos de ILOM mediante la línea de comandos”](#) en la página 138.

FIGURA 7-4 Ejemplo de registro de eventos de ILOM

ABOUT REFRESH LOG OUT

Role (User): Administrator (root) SP Hostname: DarenRevF

Sun™ Integrated Lights Out Manager

Sun™ Microsystems, Inc.

Event Log

Displays every event in the system, including IPMI, Audit, and FMA events. Click the Clear Log button to delete all current log entries.

Event Log

Clear Log

Event ID	Class	Type	Severity	Date/Time	Description
1570	Audit	Log	minor	Wed May 9 08:49:00 2007	root: Open Session : object = /session/type : value = www : success
1569	Audit	Log	minor	Wed May 9 08:44:50 2007	root: Close Session : object = /session/type : value = www : success
1568	Audit	Log	minor	Wed May 9 08:28:46 2007	root: Open Session : object = /session/type : value = www : success
1567	Audit	Log	minor	Wed May 9 08:22:50 2007	root: Close Session : object = /session/type : value = www : success
1566	Audit	Log	minor	Wed May 9 07:58:44 2007	root: Open Session : object = /session/type : value = www : success
1565	Audit	Log	minor	Wed May 9 06:51:02 2007	root: Close Session : object = /session/type : value = www : success
1564	Audit	Log	minor	Wed May 9 06:30:58 2007	root: Open Session : object = /session/type : value = www : success
1563	Audit	Log	minor	Wed May 9 05:55:22 2007	root: Close Session : object = /session/type : value = www : success
1562	Audit	Log	minor	Wed May 9 05:39:18 2007	root: Open Session : object = /session/type : value = www : success
1561	Audit	Log	minor	Wed May 9 05:23:17 2007	root: Close Session : object = /session/type : value = www : success
1560	Audit	Log	minor	Wed May 9 05:07:11 2007	root: Open Session : object = /session/type : value = www : success
1559	Audit	Log	minor	Wed May 9 04:53:52 2007	root: Close Session : object = /session/type : value = www : success
1558	Audit	Log	minor	Wed May 9 04:42:09 2007	root: Open Session : object = /session/type : value = www : success
1557	Audit	Log	minor	Tue May 8 14:57:07 2007	root: Open Session : object = /session/type : value = shell : success
1556	Audit	Log	minor	Tue May 8 14:55:55 2007	root: Close Session : object = /session/type : value = shell : success
1555	Audit	Log	minor	Tue May 8 14:54:58 2007	root: Open Session : object = /session/type : value = shell : success
1554	Audit	Log	minor	Tue May 8 14:53:47 2007	root: Close Session : object = /session/type : value = shell : success
1553	Audit	Log	minor	Tue May 8 14:51:08 2007	root: Open Session : object = /session/type : value = shell : success
1552	Audit	Log	minor	Tue May 8 14:50:01 2007	root: Close Session : object = /session/type : value = shell : success
1551	Audit	Log	minor	Tue May 8 14:49:50 2007	root: Open Session : object = /session/type : value = shell : success
1550	Audit	Log	minor	Tue May 8 14:49:12 2007	root: Close Session : object = /session/type : value = shell : success

Marcas de tiempo del registro de eventos y configuración del reloj de ILOM

ILOM anota la hora del evento en el registro de eventos utilizando la hora del meridiano de Greenwich (GMT) o el formato UTC (horario universal coordinado) del servidor host. No obstante, si examina el registro de eventos desde un sistema cliente situado en una zona horaria diferente, estas marcas se adaptan automáticamente al huso horario en el que se encuentre dicho sistema. Por tanto, un mismo evento del registro podría aparecer con dos marcas de tiempo diferentes.

Configuraciones admitidas para el reloj

Es posible configurar manualmente el reloj de ILOM utilizando la hora GMT o UTC del servidor host o, si se prefiere, sincronizar este reloj con otros sistemas de la red asignándole la dirección IP de un servidor NTP.

Visualización o configuración del reloj mediante la interfaz web

En la página Configuration (configuración) --> Clock Settings (configuración del reloj) de la interfaz web de ILOM, puede ver o configurar los valores del reloj de esta aplicación.

FIGURA 7-5 Página de configuración del reloj

The screenshot displays the ILOM web interface with the 'Clock Settings' page selected. The navigation menu at the top includes 'System Information', 'System Monitoring', 'Configuration', 'User Management', 'Remote Control', and 'Maintenance'. The 'Configuration' menu is expanded, showing sub-items: 'System Management Access', 'Alert Management', 'Network', 'Serial Port', 'Clock Settings', 'Syslog', 'SMTP Client', and 'Policy'. The 'Clock Settings' page contains the following fields and controls:

- Date:** A text input field containing '5/24/2007'.
- Time:** Two dropdown menus for hour and minute, currently set to '12' and '59'.
- Synchronize Time Using NTP:** A checkbox labeled 'Enabled' which is currently unchecked.
- Server 1:** A text input field containing '0.0.0.0'.
- Server 2:** A text input field containing '0.0.0.0'.
- Save:** A button to save the configuration.

Below the fields, there is a small instructional text: "To set the Service Processor clock manually, type the date in the format mm/dd/yyyy, then select the hour and minute. To synchronize the Service Processor clock with an NTP server, select the Enable check box, then type the IP addresses of the NTP servers to use."

Si precisa más información sobre la forma de ver y configurar las opciones del reloj desde la interfaz web de ILOM, consulte [“Visualización y configuración del reloj mediante la interfaz web”](#) en la página 140.

Visualización y configuración del reloj mediante la línea de comandos

Puede ver la configuración del reloj de ILOM desde la interfaz de la línea de comandos utilizando el comando `show`. Por ejemplo, en algunas plataformas de servidor, puede ver las opciones de configuración especificando la ruta de acceso siguiente:

```
show /sp/clock
```

También puede configurar manualmente los valores desde la línea de comandos utilizando la siguiente sintaxis del comando `set`:

```
set destino nombre_propiedad=valor
```

Asimismo, puede configurar el reloj de ILOM para sincronizarlo con otros sistemas de la red estableciendo la dirección IP de un servidor NTP. Por ejemplo, en algunas plataformas de servidor Sun, podría especificar la ruta siguiente para establecer la dirección IP de un servidor NTP y luego habilitar la sincronización mediante NTP.

- Ejemplo de configuración de la dirección IP de un servidor NTP:

```
set /SP/clients/ntp/server/1 address=dirección_ip
```

- Ejemplo de habilitación de la sincronización:

```
set /SP/clock/usentpserver=enabled
```

Para obtener más información sobre la forma de configurar el reloj de ILOM desde la línea de comandos, consulte la documentación de usuario suministrada con la plataforma de servidor Sun.

En dicha documentación encontrará también información sobre el reloj específica de la plataforma que le permitirá saber si:

- La hora señalada por ILOM se mantiene después de rearrancar el SP.
- La hora señalada por ILOM puede sincronizarse con el host en el momento de arrancar éste.
- Existe algún elemento de reloj de tiempo real que almacene la hora.

Información de Syslog

Syslog es una utilidad de registro estándar que se utiliza en multitud de entornos. Se encarga de definir un conjunto común de funciones de registro de eventos, así como un protocolo para transmitirlos a un host de registros remoto. Puede utilizar Syslog para combinar los eventos de distintas instancias de ILOM en un mismo lugar. La entrada del registro contiene la misma información que se vería en el registro de eventos local, lo que incluye la clase, el tipo, la gravedad y la descripción. Si precisa información sobre la forma de configurar ILOM para enviar syslog a una o dos

direcciones IP, consulte [“Configuración de las direcciones IP de un destinatario de Syslog remoto mediante la interfaz web”](#) en la página 141 o [“Configuración de las direcciones IP de un destinatario de Syslog remoto mediante la línea de comandos”](#) en la página 142.

Administración de errores

La mayoría de las plataformas de servidor Sun incluyen la función de administración de errores en ILOM. Esta función permite supervisar el estado del hardware del sistema de forma proactiva, así como diagnosticar problemas de funcionamiento tan pronto como se producen. Además de supervisar el hardware del sistema, el software de administración de errores supervisa las condiciones del entorno e informa de si alguna condición está fuera de los parámetros aceptables. Hay varios sensores situados en los componentes del sistema que se supervisan continuamente. Cuando se detecta algún problema, el software de administración de errores hace lo siguiente de manera automática:

- Ilumina el LED de Mantenimiento (Server Action Required) del componente defectuoso.
- Actualiza las interfaces de administración de ILOM para que reflejen la condición de error.
- Anota la información sobre el error en el registro de eventos de ILOM.

Es posible ver el estado de los componentes defectuosos desde la interfaz web o desde la línea de comandos de ILOM. Para obtener más información, consulte:

- [“Visualización de los estados de error mediante la interfaz web”](#) en la página 132
- [“Visualización de los estados de error mediante la línea de comandos”](#) en la página 133.

Los tipos de componentes del sistema y condiciones ambientales supervisados por el software de administración de errores vienen determinados por la plataforma del servidor Sun. Para obtener más información sobre el tipo de componentes que supervisa este software, consulte la documentación de usuario suministrada con la plataforma de servidor.

Nota – La función de administración de errores de ILOM está disponible en todas las plataformas de servidor Sun a excepción de los servidores Sun Fire de las series X4100 y X4200.

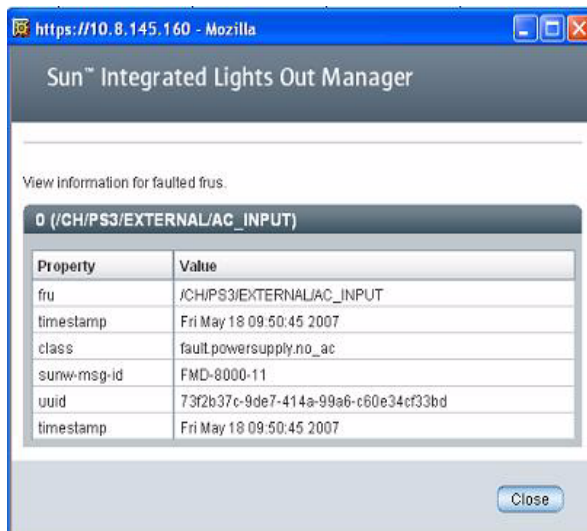
Visualización de los estados de error mediante la interfaz web

En la página Fault Management (administración de errores) de la interfaz web de ILOM, puede ver los componentes del sistema que presentan alguna condición de error.

FIGURA 7-6 Ejemplo de una página de administración de errores

Versions	Session Time-Out	Components	Fault Management	Identification Information
Fault Management				
View the components that are currently in a faulted state.				
Faulted Components				
ID	FRU	Timestamp		
0 (/CH/PS3/EXTERNAL/AC_INPUT)	/CH/PS3/EXTERNAL/AC_INPUT	Fri May 18 09:50:45 2007		
1 (/CH/PS2/EXTERNAL/AC_INPUT)	/CH/PS2/EXTERNAL/AC_INPUT	Fri May 18 09:50:53 2007		

La página de administración de errores presenta la lista de los componentes defectuosos clasificados por ID, FRU y marca de tiempo. Puede obtener información complementaria sobre el componente defectuoso haciendo clic en su ID. Por ejemplo, si hace clic en el ID del componente 0 (CH/PS3/EXTERNAL/AC_INPUT), se abre el cuadro de diálogo siguiente con más datos sobre el componente y el error.



Como alternativa, puede utilizar la página Component Management (administración de componentes) de la interfaz web de ILOM para identificar posibles estados de error de los componentes incluidos en esa página.

FIGURA 7-7 Página de administración de componentes: estado de error

Component Management Status			
Component Name	Type	Ready to Remove Status	Fault Status
/	Container	-	OK
/SYS	Host System	-	OK
/SYS/BIOS	BIOS	-	-
/SYS/IP0	Host Processor	-	OK
/SYS/IP0/D0	DIMM	-	OK
/SYS/IP0/D1	DIMM	-	OK
/SYS/IP1	Host Processor	-	OK
/SYS/IP2	Host Processor	-	OK
/SYS/IP3	Host Processor	-	OK
/SYS/HDD0	Hard Disk	-	OK

Si precisa más información sobre las funciones de administración de errores de ILOM ofrecidas por su sistema, consulte la documentación de usuario suministrada con la plataforma de servidor Sun.

Visualización de los estados de error mediante la línea de comandos

Es posible ver los componentes que presentan condiciones de error desde la interfaz de la línea de comandos de ILOM utilizando el comando `show`. Por ejemplo, en función de la plataforma de servidor Sun utilizada, puede especificar una de estas rutas de acceso:

```
show /SP/faultmgmt
show /CH/faultmgmt
```

Si precisa más información sobre las funciones de administración de errores de ILOM ofrecidas por su sistema, consulte la documentación de usuario suministrada con la plataforma de servidor Sun.

Supervisión de los sensores del sistema, los indicadores y el registro de eventos de ILOM

Utilice los procedimientos siguientes para supervisar los sensores e indicadores del sistema, y la información del registro de eventos de ILOM.

- “Identificación del estado de los indicadores mediante la interfaz web” en la página 134
- “Obtención de las lecturas de los sensores mediante la interfaz web” en la página 135
- “Visualización o borrado del registro de eventos de ILOM mediante la interfaz web” en la página 136
- “Visualización o borrado del registro de eventos de ILOM mediante la línea de comandos” en la página 138
- “Visualización y configuración del reloj mediante la interfaz web” en la página 140
- “Configuración de las direcciones IP de un destinatario de Syslog remoto mediante la interfaz web” en la página 141
- “Configuración de las direcciones IP de un destinatario de Syslog remoto mediante la línea de comandos” en la página 142

▼ Identificación del estado de los indicadores mediante la interfaz web

Siga estos pasos para conocer el estado de los indicadores del sistema desde la interfaz web de ILOM:

1. **Abra un navegador de web y escriba la dirección IP del CMM o el SP del servidor.**

Se abre la página de inicio de sesión de la interfaz web de ILOM.

2. **En la página de inicio de sesión, especifique un nombre de usuario y una contraseña, y haga clic en OK (aceptar).**

Aparece la interfaz web de ILOM.

3. En la página abierta, seleccione **System Monitoring (supervisión del sistema)** -> **Indicators (indicadores)**.

Se abre la página Indicators (indicadores).

Nota – Si el servidor está apagado, muchos indicadores presentarán el mensaje “no reading” (no hay lectura).

4. En esta página, haga lo siguiente:
 - a. Busque el nombre del indicador que quiera supervisar.
 - b. Para cambiar el estado de un indicador, haga clic en el botón de opción asociado a ese indicador y luego en la lista desplegable **Actions (acciones)**. En esta lista, seleccione **Turn LED Off (apagar LED)** o **Set LED to Fast Blink (poner LED en parpadeo rápido)**.

Aparece un cuadro de diálogo para solicitar la confirmación del cambio.
 - c. Haga clic en **OK** para confirmarlo.

▼ Obtención de las lecturas de los sensores mediante la interfaz web

Siga este procedimiento para obtener las lecturas de los sensores desde la interfaz web de ILOM:

1. **Abra un navegador de web y escriba la dirección IP del CMM o el SP del servidor.**

Se abre la página de inicio de sesión de la interfaz web de ILOM.
2. **En la página de inicio de sesión, especifique un nombre de usuario y una contraseña, y haga clic en OK (aceptar).**

Aparece la interfaz web de ILOM.
3. **En la página abierta, seleccione System Monitoring (supervisión del sistema) -> Sensors Readings (lecturas de los sensores).**

Se abre la página Sensor Readings (lecturas de los sensores).

Nota – Si el servidor está apagado, muchos componentes presentarán el mensaje “no reading” (no hay lectura).

4. En esta página, haga lo siguiente:
 - a. Busque el nombre del sensor que quiera supervisar.
 - b. Haga clic en el nombre del sensor para ver los valores de las propiedades asociadas al sensor.

Para obtener datos específicos sobre los tipos de destinos de sensores discretos a los que tiene acceso, así como las rutas para acceder a ellos, consulte la documentación de usuario suministrada con la plataforma de servidor Sun.

▼ Visualización o borrado del registro de eventos de ILOM mediante la interfaz web

Siga este procedimiento para ver o borrar la información del registro de eventos de ILOM utilizando la interfaz web:

1. **Abra un navegador de web y escriba la dirección IP del CMM o el SP del servidor.**

Se abre la página de inicio de sesión de la interfaz web de ILOM.
2. **En la página de inicio de sesión, especifique un nombre de usuario y una contraseña, y haga clic en OK (aceptar).**

Aparece la interfaz web de ILOM.
3. **En la página abierta, seleccione System Monitoring (supervisión del sistema) -> Event Logs (registros del sistema).**

Se abre la página Event Log (registro del sistema).
4. **En esta página, puede realizar cualquiera de estas acciones:**
 - **Desplazarse por las entradas:** utilice los controles de navegación situados al principio y al final de la tabla para recorrer sus datos hacia delante o hacia atrás.

Tenga presente que, si selecciona un gran número de entradas, la respuesta de la interfaz puede ser más lenta que si selecciona menos entradas.
 - **Ver las entradas de la pantalla recorriendo la lista:** la tabla siguiente contiene la descripción de cada columna que aparece en el registro.

Nombre de la columna	Descripción
Event ID (ID del evento)	Número del evento anotado por orden consecutivo a partir del 1.
Class/Type (clase/tipo)	<ul style="list-style-type: none"> • Audit/Log (auditoría/registro): comandos que dan como resultado un cambio en la configuración. En la descripción se incluye el usuario, el comando, los parámetros del comando y la condición de correcto (success) o error (fail). • IPMI/Log (IPMI/registro): cualquier evento que aparezca en el registro de eventos del sistema (SEL) de IPMI también se incluye en el registro de administración. • Chassis/State (chasis/estado): cambios del inventario y del estado del sistema en general. • Chassis/Action (chasis/acción): eventos de cierre del sistema del módulo o el chasis del servidor, instalación o retirada de una FRU con el sistema en marcha y uso del botón Reset Parameters (restablecer parámetros). • FMA/Fault (FMA/error): errores de la arquitectura de administración de errores (FMA). La descripción proporciona la hora a la que la FMA ha detectado el error y el componente sospechoso de haberlo provocado. • FMA/Repair (FMA/reparación): reparaciones indicadas por la FMA. En la descripción se especifica el componente.
Severity (gravedad)	Critical, Major o Minor (crítica, mayor o menor).
Date/Time (fecha/hora)	Día y hora a la que se produjo el evento. Si se ha habilitado el servidor NTP (Network Time Protocol) para establecer la hora de ILOM, el reloj de ILOM utilizará el formato de hora universal (UTC).
Descripción	Descripción del evento.

- **Borrar el registro de eventos:** para borrarlo, haga clic en el botón Clear Event Log (borrar registro de eventos). Se abrirá un cuadro de diálogo de confirmación. Haga clic en el botón OK del cuadro para borrar las entradas del registro.

Nota – El registro de eventos de ILOM recoge muchos tipos de eventos, incluidas las copias de las entradas de IPMI. Al borrarlo, se borran todas las entradas que contiene, lo que incluye también las de IPMI, pero no se borran las entradas que se hayan anotado directamente en los registros de IPMI.

▼ Visualización o borrado del registro de eventos de ILOM mediante la línea de comandos

Siga este procedimiento para ver o borrar la información del registro de eventos de ILOM utilizando la interfaz de la línea de comandos:

1. Establezca una conexión de consola serie o una conexión SSH con el CMM o el SP del servidor:

- **Conexión de la consola serie local**

Conecte una consola serie al puerto serie del servidor o el CMM.

Para obtener más información, consulte la documentación de usuario suministrada con la plataforma de servidor Sun.

o

- **Conexión Secure Shell (SSH) remota**

Establezca una conexión Secure Shell con el CMM o el SP del servidor.

Desde el cliente remoto, acceda como usuario root y establezca una conexión segura con el CMM activo o el SP del servidor.

Por ejemplo, puede establecer una conexión segura con el SP del servidor desde un cliente SSH remoto escribiendo lo siguiente:

```
ssh -l root dirección_ip_servidor
```

```
Password: changeme
```

Aparece el indicador de comandos predeterminado (->).

2. Escriba una de las siguientes rutas de comandos para establecer el directorio de trabajo:

- Para el SP de un servidor montado en un bastidor: **cd /SP/logs/event**

- Para el SP de un servidor blade instalado en un chasis: **cd /CH/BLn/SP/logs/event**

- Para un CMM: **cd /CMM/logs/event**

3. Escriba la siguiente ruta de comando para ver la lista del registro de eventos.

```
show list
```

Aparece en pantalla el contenido del registro de eventos. He aquí un ejemplo.

```
ID      Date/Time                Class  Type      Severity
-----
1522    Sun Jul 30 01:11:36 2006  Audit    Log       minor
      root : Close Session : object = /session/type : value = www : success
1521    Sun Jul 30 01:05:34 2006  Audit    Log       minor
      root : Close Session : session ID = 1307912184 : success
```

4. En el registro de eventos puede realizar cualquiera de estas acciones:

- **Desplazarse por la lista para ver las entradas:** pulse cualquier tecla excepto la “q”. En la tabla siguiente se describe cada columna del registro.

Nombre de la columna	Descripción
Event ID (ID del evento)	Número del evento anotado por orden consecutivo a partir del 1.
Class/Type (clase/tipo)	<ul style="list-style-type: none">• Audit/Log (auditoría/registo): comandos que dan como resultado un cambio en la configuración. En la descripción se incluye el usuario, el comando, los parámetros del comando y la condición de correcto (success) o error (fail).• IPMI/Log (IPMI/registo): cualquier evento que aparezca en el registro de eventos del sistema (SEL) de IPMI también se incluye en el registro de administración.• Chassis/State (chasis/estado): cambios del inventario y el estado del sistema en general.• Chassis/Action (chasis/acción): eventos de cierre del sistema del módulo o el chasis del servidor, instalación o retirada de una FRU con el sistema en marcha y uso del botón Reset Parameters (restablecer parámetros).• FMA/Fault (FMA/error): errores de la arquitectura de administración de errores (FMA). La descripción proporciona la hora a la que la FMA ha detectado el error y el componente sospechoso de haberlo provocado.• FMA/Repair (FMA/reparación): reparaciones indicadas por la FMA. En la descripción se especifica el componente.
Severity (gravedad)	Critical, Major o Minor (crítica, mayor o menor)
Date/Time (fecha/hora)	Día y hora a la que se produjo el evento. Si se ha habilitado el servidor NTP (Network Time Protocol) para establecer la hora de ILOM, el reloj de ILOM utilizará el formato de hora universal (UTC).
Descripción	Descripción del evento.

- **Salir del registro (dejar de verlo en pantalla)**– : pulse la tecla “q”.
- **Borrar las entradas del registro de eventos**– : lleve a cabo este procedimiento:
 - a. **Escriba: `set clear=true`**

Aparece un mensaje de confirmación.
 - b. **Elija una de estas posibilidades:**
 - Borrar las entradas. Escriba: **y**.
 - Cancelar el borrado del registro. Escriba: **n**.

Nota – El registro de eventos de ILOM recoge muchos tipos de eventos, incluidas las copias de las entradas de IPMI. Al borrarlo, se borran todas las entradas que contiene, lo que incluye también las de IPMI, pero no se borran las entradas que se hayan anotado directamente en los registros de IPMI.

▼ Visualización y configuración del reloj mediante la interfaz web

Necesita conocer la dirección IP de sus servidores NTP para llevar a cabo este procedimiento.

1. **Abra un navegador de web y escriba la dirección IP del CMM o el SP del servidor.**

Se abre la página de inicio de sesión de la interfaz web de ILOM.

2. **En la página de inicio de sesión, especifique un nombre de usuario y una contraseña, y haga clic en OK (aceptar).**

Aparece la interfaz web de ILOM.

3. **En la página abierta, seleccione Configuration (configuración) --> Clock Settings (configuración del reloj).**

Se abre la página Clock Settings (configuración del reloj).

4. **En esta página, puede hacer lo siguiente:**

- Ver los valores existentes.
- Configurar la fecha y hora del SP del servidor host:
 - a. **En el cuadro Date, escriba la fecha con el formato mm/dd/aa.**
 - b. **En las listas desplegables Time, especifique la hora y los minutos.**
- Configurar la dirección IP de un servidor NTP y habilitar la sincronización.

- a. **Seleccione la casilla Enabled (habilitada) situada junto a la opción Synchronize Time Using NTP (sincronizar la hora mediante NTP).**

- b. **En la casilla Server 1, escriba la dirección IP del servidor que vaya a utilizar como servidor NTP principal.**

- c. **(Opcional) En la casilla Server 2, escriba la dirección IP del servidor que vaya a utilizar como servidor NTP secundario.**

5. **Haga clic en Save (guardar) para que los cambios tengan efecto.**

▼ Configuración de las direcciones IP de un destinatario de Syslog remoto mediante la interfaz web

Siga este procedimiento para configurar en ILOM la dirección IP del destinatario de Syslog remoto utilizando la interfaz web.

1. Abra un navegador de web y escriba la dirección IP del CMM o el SP del servidor.

Se abre la página de inicio de sesión de la interfaz web de ILOM.

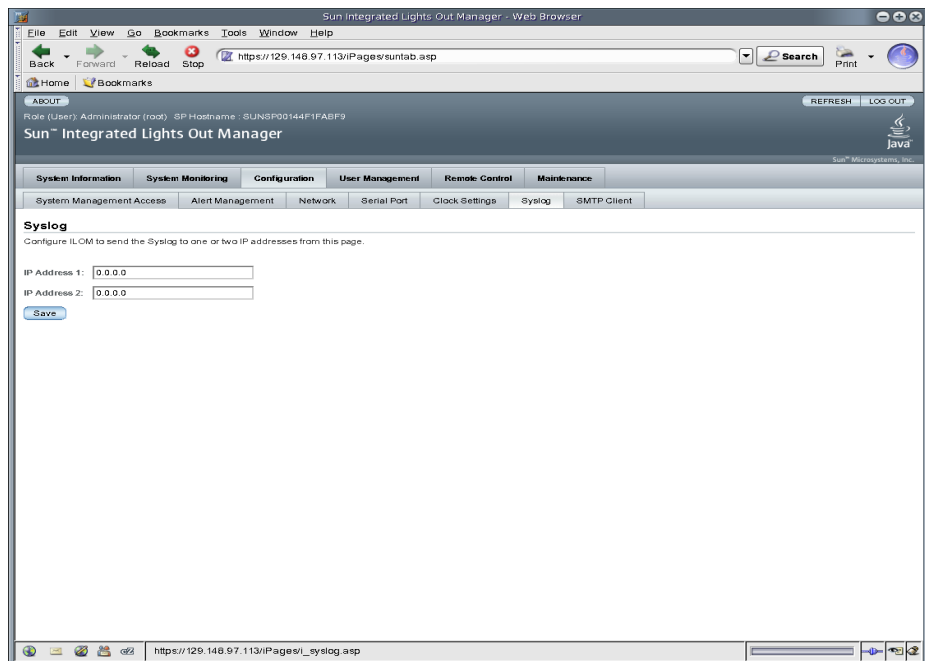
2. En la página de inicio de sesión, especifique un nombre de usuario y una contraseña, y haga clic en OK (aceptar).

Aparece la interfaz web de ILOM.

3. En la página abierta, seleccione Configuration (configuración) --> Syslog.

Se abre la página Syslog.

FIGURA 7-8 Página Syslog



4. En los campos IP Address 1 y 2, especifique las direcciones IP de las dos ubicaciones a las que desea enviar los datos de Syslog.
5. Haga clic en Save (guardar) para que la configuración tenga efecto.

▼ Configuración de las direcciones IP de un destinatario de Syslog remoto mediante la línea de comandos

Siga este procedimiento para configurar la dirección IP de un destinatario de Syslog remoto utilizando la interfaz de la línea de comandos:

1. Establezca una conexión de consola serie o una conexión SSH con el CMM o el SP del servidor:

■ Conexión de la consola serie local

Conecte una consola serie al puerto serie del servidor o el CMM.

Para obtener más información, consulte la documentación de usuario suministrada con la plataforma de servidor Sun.

o

■ Conexión Secure Shell (SSH) remota

Establezca una conexión Secure Shell con el CMM o el SP del servidor.

Desde el cliente remoto, acceda como usuario root y establezca una conexión segura con el CMM activo o el SP del servidor.

Por ejemplo, puede establecer una conexión segura con el SP del servidor desde un cliente SSH remoto escribiendo lo siguiente:

```
ssh -l root dirección_ip_servidor
```

Password: **changeme**

Aparece el indicador de comandos predeterminado (->).

2. Escriba una de las siguientes rutas de comandos para establecer el directorio de trabajo:

■ Para el SP de un servidor montado en un bastidor: **cd**

/SP/clients/syslog

■ Para el SP de un servidor blade instalado en un chasis: **cd**

/CH/BLn/SP/clients/syslog

■ Para un CMM: **cd /CMM/clients/syslog**

3. Escriba el comando **show** para ver las propiedades de Syslog.

Aparecen las propiedades correspondientes. Por ejemplo, al acceder por primera vez a las propiedades de Syslog en un SP, el resultado sería similar a éste:

```
/SP/clients/syslog
Targets:
Properties:
  destination_ip1 = 0.0.0.0
```

```
destination_ip2 = 0.0.0.0
Commands:
  cd
  set
  show
```

4. Utilice el comando `set` para asignar una dirección IP de destino para IP 1 (y, si procede, IP 2).

Por ejemplo, para establecer 11.222.33.4 como dirección IP de destino, debería escribir:

```
set destination_ip1=111.222.33.4
```

5. Pulse Intro para que el valor tenga efecto.

Aparecen los resultados de la configuración realizada. Por ejemplo, si ha establecido la dirección IP de destino como 111.222.33.4, aparece la siguiente información:

```
Set 'destination_ip1' to '111.222.33.4'
```

Introducción a la administración de alertas

Las alertas advierten de posibles fallos del sistema con antelación. Cada plataforma de servidor Sun está dotada de una serie de sensores que miden los voltajes, las temperaturas, la velocidad de los ventiladores y otros atributos relacionados con los servicios del sistema. ILOM sondea estos sensores automáticamente, anota en el registro de eventos de ILOM cualquier evento que indique la superación de alguno de los umbrales y genera uno o varios mensajes de alerta a una o varias direcciones de destino especificadas por el cliente.



Precaución – ILOM marca todos los eventos o acciones con `LocalTime=GMT` (o UTC). Los clientes del navegador muestran estos eventos en hora local (`LocalTime`). Esto puede provocar discrepancias aparentes en el registro de eventos. Cuando se produce un evento en ILOM, el registro lo anota con el formato de hora UTC, pero el cliente lo hace en la hora local (`LocalTime`). Para obtener más información sobre las marcas de tiempo y la configuración del reloj de ILOM, consulte [“Marcas de tiempo del registro de eventos y configuración del reloj de ILOM”](#) en la página 129.

Configuración de las reglas de alertas

En ILOM puede configurarse un total de 15 reglas de alertas utilizando la interfaz web o la línea de comandos. Por cada regla configurada, y en función del tipo de alerta, es preciso definir tres o más propiedades relativas a la alerta.

El *tipo de alerta* indica el formato de los mensajes de alerta y el método para enviarlos y recibirlos. ILOM admite estos tres tipos de alertas:

- Alertas PET de IPMI
- Alertas de captura de eventos SNMP
- Alertas de notificación por correo electrónico

Todas las plataformas de servidor Sun admiten los tres tipos de alertas a excepción del módulo de supervisión del chasis (CMM) de Sun. Éste admite las alertas de capturas de eventos SNMP y las de notificación por correo electrónico, pero no las alertas PET de IPMI.

La sección siguiente, [“Definición de propiedades para las reglas de alertas” en la página 144](#), contiene una breve explicación sobre cada tipo de alerta y las propiedades que pueden utilizarse para definir sus reglas.

Definición de propiedades para las reglas de alertas

ILOM ofrece hasta cinco propiedades para definir una regla de alerta, son las siguientes:

- Alert Type
- Alert Level
- Alert Destination
- SNMP Version (*versión de SNMP, sólo alertas de captura de eventos SNMP*)
- SNMP Community Name or User Name (*nombre de usuario o comunidad SNMP, sólo alertas de captura de eventos SNMP*)

Para obtener más información sobre los valores de estas propiedades, consulte la tabla [TABLA 7-1](#).

TABLA 7-1 Propiedades para definir las reglas de alertas

Nombre de la propiedad	Requisito	Descripción
Alert Type	Obligatorio	<p>El tipo de alerta indica el formato del mensaje y el método de entrega que ILOM utilizará cuando cree y envíe la notificación de alerta. Puede configurar uno de estos tipos de alerta:</p> <ul style="list-style-type: none"> IPMI PET Alerts (alertas PET de IPMI). Las alertas de captura de eventos de plataforma (PET) de IPMI se admiten en todos los módulos y plataformas de servidor Sun a excepción del módulo de supervisión del chasis (CMM). Por cada alerta de este tipo que se configure en ILOM, es preciso especificar una dirección IP de destino para el mensaje y uno de los cuatro niveles de alerta admitidos. Recuerde que el destino especificado para la alerta también debe admitir la recepción de mensajes PET de IPMI. Si el destino no puede recibir mensajes PET, el destinatario no podrá decodificar el mensaje de alerta. SNMP Trap Alerts (alertas de captura de eventos SNMP). ILOM permite generar alertas de captura de eventos SNMP y enviarlas al destino especificado por el usuario. Todos los destinos especificados deben admitir la recepción de mensajes de captura de eventos SNMP. Recuerde que las alertas de eventos SNMP pueden utilizarse tanto en los servidores de bastidor y como en los módulos de servidores blade. Email Notification Alerts (alertas de notificación por correo electrónico). ILOM permite generar alertas de notificación por correo electrónico y enviarlas a la dirección de correo electrónico especificada por el usuario. Para que el sistema ILOM cliente pueda generar este tipo de alertas, ILOM necesita que configure el nombre del servidor SMTP de correo saliente que enviará los mensajes. Para obtener más información, consulte “Habilitación del cliente SMTP mediante la interfaz web” en la página 158.
Alert Destination	Obligatorio	<p>El destino de la alerta indica el lugar al que debe enviarse el mensaje de notificación. El tipo de alerta determina los destinos a los que puede enviarse el mensaje. Por ejemplo, las alertas PET de IPMI y las de captura de eventos SNMP necesitan una dirección IP de destino. Las alertas de notificación por correo electrónico necesitan la especificación de una dirección de correo electrónico. Si no se introduce el formato adecuado como destino de una alerta, ILOM indicará un error.</p>

TABLA 7-1 Propiedades para definir las reglas de alertas (*continuación*)

Nombre de la propiedad	Requisito	Descripción
Alert Level	Obligatorio	<p>El nivel de alerta actúa como mecanismo de filtro para garantizar que los destinatarios sólo reciban los mensajes que más les interesan. Cada vez que se define una regla de alerta en ILOM, es preciso especificar un nivel de alerta.</p> <p>El nivel de alerta determina qué eventos generan una alerta. La alerta de nivel inferior genera alertas para ese nivel y para todas las alertas que están por encima de él.</p> <p>ILOM ofrece los siguientes niveles de alerta, de los cuales Minor (menor) es el más bajo:</p> <ul style="list-style-type: none"> • Minor (menor). Este nivel genera alertas por eventos de tipo informativo, eventos no críticos de nivel inferior y superior, eventos críticos de nivel superior e inferior y eventos de errores irre recuperables de nivel superior e inferior. • Mayor (mayor). Este nivel genera alertas por eventos no críticos de nivel superior e inferior, eventos críticos de nivel superior e inferior y eventos de errores irre recuperables de nivel superior e inferior. • Critical (crítico). Este nivel genera alertas por eventos críticos de nivel superior e inferior y eventos de errores irre recuperables de nivel superior e inferior. • Down (caída). Este nivel genera alertas por eventos de errores irre recuperables de nivel superior e inferior. • Disabled (inhabilitada). Inhabilita la alerta. ILOM no genera ningún mensaje de notificación. <p>Todos los niveles de alerta permiten el envío de mensaje con la excepción de <i>Disabled</i>.</p> <p>Importante: ILOM admite el filtro de los niveles de alerta en todas las capturas de eventos IPMI y eventos notificados por correo electrónico. ILOM no admite el filtro de niveles de alerta para capturas de eventos SNMP. Para habilitar el envío de capturas de eventos SNMP (pero sin filtrarlos por nivel de alerta), puede elegir cualquiera de las siguientes opciones: <i>minor</i>, <i>major</i>, <i>critical</i> o <i>down</i>. Para inhabilitar el envío de capturas de eventos SNMP, puede elegir la opción <i>disabled</i>.</p>
SNMP Version	Opcional	<p>La versión de SNMP permite especificar qué versión de la captura de evento SNMP está enviando. Puede elegir entre las siguientes opciones: 1, 2c o 3.</p> <p>Esta propiedad sólo es aplicable a las alertas de eventos SNMP.</p>
SNMP Community Name o User Name	Opcional	<p>La propiedad de nombre de usuario o comunidad SNMP permite especificar la cadena de comunidad o el nombre de usuario de SNMP v3 utilizado en la alerta de captura de eventos SNMP.</p> <ul style="list-style-type: none"> • En el caso de eventos SNMP v1 o v2c, puede especificar un nombre de comunidad para la alerta. • En el caso de eventos SNMP v3, puede especificar un nombre de usuario para la alerta. <p>Importante: si opta por especificar un nombre de usuario para SNMP v3, tiene que definir ese usuario en ILOM como usuario de SNMP. Si no lo define, el destinatario del evento no podrá decodificar el mensaje de alerta. Para obtener más información sobre la definición de usuarios de SNMP en ILOM, consulte el Capítulo 10.</p>

Opción de SMTP	Descripción
SMTP State	Seleccione esta casilla para habilitar el estado de SMTP.
SMTP Server IP	Escriba en este campo la dirección IP del servidor SMTP de correo saliente que procesará las notificaciones de correo electrónico.
SMTP Port	Escriba el número de puerto del servidor SMTP de correo saliente.

Para obtener más información sobre la forma de crear y administrar reglas de alertas en ILOM, consulte las secciones siguientes:

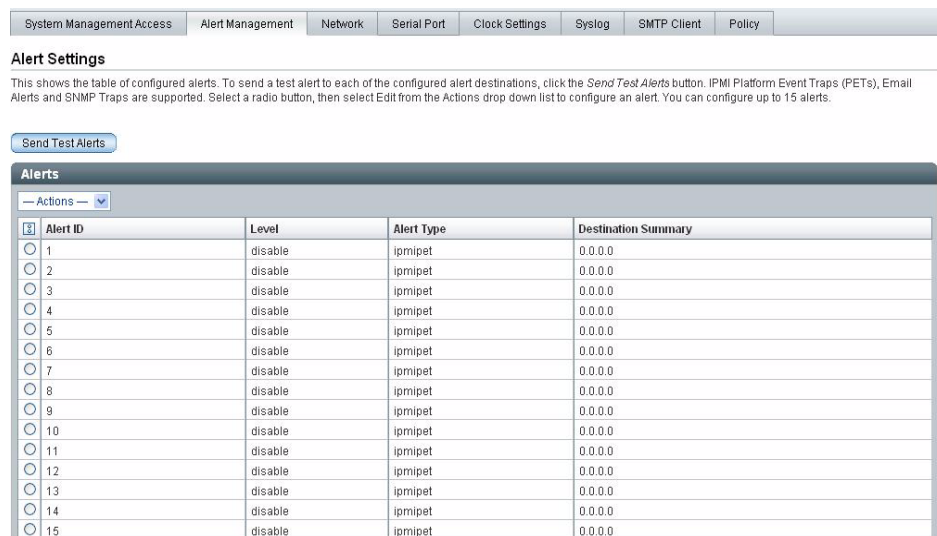
- [“Administración de las reglas de alertas mediante la interfaz web de ILOM” en la página 147.](#)
- [“Administración de las reglas de alertas mediante la línea de comandos de ILOM” en la página 151.](#)
- [“Configuración de un cliente SMTP para alertas de notificación por correo electrónico” en la página 157.](#)

Administración de las reglas de alertas mediante la interfaz web de ILOM

Desde la página Alert Settings (configuración de alertas) de la interfaz web, es posible habilitar, modificar o inhabilitar la configuración de cualquier regla de alerta de ILOM. Las 15 configuraciones de alertas presentadas en esta página se entregan inhabilitadas de forma predeterminada. La lista desplegable Actions (acciones) permite editar las propiedades asociadas a cada regla. Para habilitar una regla de alerta en la página de administración de alertas, debe definir el tipo y el nivel de alerta, y un destino válido al que enviar el mensaje de notificación.

La página de configuración de alertas también incluye el botón Send Test Alert (enviar alerta de prueba). Con él, puede comprobar si cada destinatario especificado para recibir los mensajes en una regla de alerta habilitada recibe el mensaje.

FIGURA 7-9 Página de configuración de alertas



Para obtener más información sobre la forma de crear y administrar reglas de alertas de ILOM utilizando la interfaz web, consulte las secciones siguientes:

- “Requisitos previos” en la página 148.
- “Modificación de una regla de alerta mediante la interfaz web” en la página 149.
- “Inhabilitación de una regla de alerta mediante la interfaz web” en la página 150.
- “Generación de pruebas de alertas mediante la interfaz web” en la página 150.

Requisitos previos

- Si va a definir una alerta de notificación por correo electrónico, es preciso configurar en ILOM el servidor de correo saliente que se utilizará para enviar el mensaje de notificación. Si no se configura el servidor de correo saliente, ILOM no será capaz de generar este tipo de alertas correctamente.
- Si va a definir una alerta de captura de eventos SNMP con la versión SNMP v3, el nombre de usuario de SNMP debe estar definido como usuario de SNMP en ILOM. Si no lo está, el destinatario no podrá decodificar el mensaje de alerta. Para obtener más información sobre la definición de usuarios de SNMP en ILOM, consulte el [Capítulo 10](#).
- Para crear, modificar o inhabilitar reglas de alertas en ILOM, es preciso abrir la sesión de ILOM como administrador.

▼ Modificación de una regla de alerta mediante la interfaz web

Utilice el procedimiento siguiente para modificar la configuración de cualquier regla de alerta en ILOM:

1. **Abra un navegador de web y escriba la dirección IP del CMM o el SP del servidor.**

Se abre la página de inicio de sesión de la interfaz web de ILOM.

2. **En la página de inicio de sesión, especifique el nombre de usuario y la contraseña de administrador, y haga clic en OK (aceptar).**

Aparece la interfaz web de ILOM.

3. **En la página abierta, seleccione Configuration (configuración) --> Alert Management (administración de alertas).**

Nota – También puede administrar las reglas de alertas del SP de un servidor desde la interfaz web del CMM. Para hacerlo, seleccione el SP del servidor (blade) en el panel izquierdo de la página y haga clic en la opción Configuration (configuración) ->Alert Management (administración de alertas) del panel derecho.

Se abre la página de configuración de alertas.

4. **En esta página, haga lo siguiente:**

- a. **Seleccione el botón de opción correspondiente a la regla que desee crear o editar.**

- b. **Seleccione Edit (editar) en la lista desplegable Actions (acciones).**

Se abre un cuadro de diálogo con las propiedades asociadas a esa regla.

- c. **En este cuadro, especifique los valores de tipo, nivel y destino de la alerta.**

Si especifica SNMP Trap como tipo de alerta, tiene la opción de definir un nombre de comunidad o de usuario para autenticar la recepción del mensaje de notificación.

Para obtener más información sobre las propiedades que puede especificar al configurar las reglas de alerta, consulte [“Propiedades para definir las reglas de alertas” en la página 145](#).

- d. **Haga clic en Save (guardar) para aplicar los valores especificados y cerrar el cuadro de diálogo.**

▼ Inhabilitación de una regla de alerta mediante la interfaz web

Utilice el procedimiento siguiente para inhabilitar la configuración de cualquier regla de alerta en ILOM:

1. **Abra un navegador de web y escriba la dirección IP del CMM o el SP del servidor.**

Se abre la página de inicio de sesión de la interfaz web de ILOM.

2. **En la página de inicio de sesión, especifique el nombre de usuario y la contraseña de administrador, y haga clic en OK (aceptar).**

Aparece la interfaz web de ILOM.

3. **En la página abierta, seleccione Configuration (configuración) --> Alert Management (administración de alertas).**

Nota – También puede administrar las reglas de alertas del SP de un servidor desde la interfaz web del CMM. Para hacerlo, seleccione el SP del servidor (blade) en el panel izquierdo de la página y haga clic en la opción Configuration (configuración) ->Alert Management (administración de alertas) del panel derecho.

Se abre la página de configuración de alertas.

4. **En esta página, haga clic en el botón de opción de la regla que quiera modificar y seleccione Edit en la lista desplegable Actions.**

Se abre un cuadro de diálogo con las propiedades que puede definir para esa regla.

5. **En el cuadro de diálogo de propiedades, seleccione Disabled (inhabilitada) en la lista desplegable Alerts Level (niveles de alerta).**

▼ Generación de pruebas de alertas mediante la interfaz web

Puede comprobar el funcionamiento de cada regla de alerta *habilitada* en ILOM enviando una alerta de prueba.

Para enviar este tipo de pruebas a los destinos especificados en la configuración de las alertas, siga este procedimiento:

1. **Abra un navegador de web y escriba la dirección IP del CMM o el SP del servidor.**

Se abre la página de inicio de sesión de la interfaz web de ILOM.

2. En la página de inicio de sesión, especifique el nombre de usuario y la contraseña de administrador, y haga clic en OK (aceptar).

Aparece la interfaz web de ILOM.

3. En la página abierta, seleccione Configuration (configuración) --> Alert Management (administración de alertas).

Nota – También puede administrar las reglas de alertas del SP de un servidor desde la interfaz web del CMM. Para hacerlo, seleccione el SP del servidor (blade) en el panel izquierdo de la página y haga clic en la opción Configuration (configuración) ->Alert Management (administración de alertas) del panel derecho.

Se abre la página de configuración de alertas.

4. En la página de configuración de alertas, haga clic en el botón Send Test Alert (enviar alerta de prueba).

ILOM genera alertas de prueba por cada regla habilitada en la página.

Administración de las reglas de alertas mediante la línea de comandos de ILOM

Es posible habilitar, modificar o inhabilitar la configuración de cualquier regla de alerta de ILOM desde la interfaz de la línea de comandos. Las 15 configuraciones de reglas definidas en ILOM se entregan inhabilitadas de forma predeterminada. Para habilitarlas, es preciso configurar los valores de las siguientes propiedades: tipo de alerta, nivel de alerta y destino de la alerta.

También puede utilizar la interfaz de la línea de comandos para generar alertas de prueba por cada regla de alerta *habilitada* en ILOM. Las alertas de prueba permiten comprobar si cada destinatario especificado en una regla *habilitada* recibe el mensaje de alerta.

Para obtener más información sobre la forma de crear y administrar reglas de alertas en ILOM utilizando la línea de comandos, consulte las secciones siguientes:

- [“Comandos para administrar las reglas de alertas desde la línea de comandos” en la página 152](#)
- [“Requisitos previos” en la página 154](#)
- [“Modificación de las reglas de alertas mediante la línea de comandos” en la página 154](#)

- “Inhabilitación de una regla de alerta mediante la línea de comandos” en la página 155
- “Generación de pruebas de alertas mediante la línea de comandos” en la página 156

Comandos para administrar las reglas de alertas desde la línea de comandos

En la [TABLA 7-2](#) figuran los comandos necesarios para administrar la configuración de las reglas de alertas desde la interfaz de la línea de comandos (CLI) de ILOM.

TABLA 7-2 Comandos para administrar las reglas de alertas desde la línea de comandos

Comando de la CLI	Descripción
show	<p>El comando show permite ver cualquier nivel del árbol de comandos de administración de alertas especificando la ruta de acceso completa o relativa.</p> <p>Ejemplos:</p> <ul style="list-style-type: none"> • Para ver una regla de alerta y sus propiedades utilizando una ruta completa, debería escribir lo siguiente en el indicador de comandos: <pre>show /SP/alertmgmt/rules/1</pre> <pre>/SP/alertmgmt/rules/1 Properties: community_or_username = public destination = 129.148.185.52 level = minor snmp_version = 1 type = snmptrap Commands: cd set show</pre> • Para ver una sola propiedad utilizando la ruta completa, debería escribir lo siguiente en el indicador de comandos: <pre>show /SP/alertmgmt/rules/1 type</pre> <pre>Properties: type = snmptrap Commands: set show</pre>

TABLA 7-2 Comandos para administrar las reglas de alertas desde la línea de comandos (*continuación*)

Comando de la CLI	Descripción
	<ul style="list-style-type: none"> Para especificar una ruta de acceso relativa si la ubicación actual del árbol es <code>/SP/alertmgmt/rules</code>, debería escribir lo siguiente en el indicador de comandos: show 1/ <code>/SP/alertmgmt/rules/1</code> Targets: Properties: <code>community_or_username = public</code> <code>destination = 129.148.185.52</code> <code>level = minor</code> <code>snmp_version = 1</code> <code>type = snmptrap</code> Commands: <code>cd</code> <code>set</code> <code>show</code>
<code>cd</code>	<p>Con el comando <code>cd</code> puede establecer el directorio de trabajo. Para establecer la administración de alertas como directorio de trabajo en el SP de un servidor, debería escribir lo siguiente en el indicador de comandos: cd /SP/alertmgmt</p>
<code>set</code>	<p>El comando <code>set</code> permite definir los valores de las propiedades desde cualquier lugar del árbol. Puede especificar la ruta de acceso completa o relativa de la propiedad en función de la ubicación del árbol. Por ejemplo:</p> <ul style="list-style-type: none"> En el caso de la ruta completa, especificaría la siguiente ruta en el indicador de comandos: set /SP/alertmgmt/rules/1 type=ipmipet En el caso de la ruta relativa (la ubicación en el árbol es <code>/SP/alertmgmt</code>), escribiría la ruta siguiente en el indicador de comandos: set rules/1 type=ipmipet En el caso de la ruta relativa (la ubicación en el árbol es <code>/SP/alertmgmt/rules/1</code>), escribiría la ruta siguiente en el indicador de comandos: set type=ipmipet

Requisitos previos

- Si va a definir una alerta de notificación por correo electrónico, es preciso configurar en ILOM el servidor de correo saliente que se utilizará para enviar el mensaje de notificación. Si no se configura el servidor de correo saliente, ILOM no será capaz de generar este tipo de alertas correctamente.
- Si va a definir una alerta de captura de eventos SNMP con la versión SNMP v3, el nombre de usuario de SNMP debe estar definido como usuario de SNMP en ILOM. Si no lo está, el destinatario no podrá decodificar el mensaje de alerta. Para obtener más información sobre la definición de usuarios de SNMP en ILOM, consulte el [Capítulo 10](#).
- Para crear, modificar o inhabilitar reglas de alertas en ILOM, es preciso abrir la sesión de ILOM como administrador.

▼ Modificación de las reglas de alertas mediante la línea de comandos

1. Establezca una conexión de consola serie o una conexión SSH con el CMM o el SP del servidor:

■ Conexión de la consola serie local

Conecte una consola serie al puerto serie del servidor o el CMM.

Para obtener más información, consulte la documentación de usuario suministrada con la plataforma de servidor Sun.

o

■ Conexión Secure Shell (SSH) remota

Establezca una conexión Secure Shell con el CMM o el SP del servidor.

Desde el cliente remoto, acceda como usuario root y establezca una conexión segura con el CMM activo o el SP del servidor.

Por ejemplo, puede establecer una conexión segura con el SP del servidor desde un cliente SSH remoto escribiendo lo siguiente:

```
ssh -l root dirección_ip_servidor
```

```
Password: changeme
```

Aparece el indicador de comandos predeterminado (->).

2. Escriba una de las siguientes rutas de comandos para establecer el directorio de trabajo:

- Para un servidor montado en un bastidor: **cd /SP/alertmgmt**
- Para un módulo de servidor blade: **cd /SP/alertmgmt**
- Para un CMM del chasis: **cd /CMM/alertmgmt**

3. Escriba el comando `show` para ver las propiedades asociadas a una determinada regla de alerta.

Por ejemplo, para ver las propiedades de la primera regla, escribiría uno de estos comandos:

- Para un servidor montado en un bastidor: `show /SP/alertmgmt/rules/1`
- Para un módulo de servidor blade: `show /CH/BLn/SP/alertmgmt/rules/1`
- Para un CMM del chasis: `show /CMM/alertmgmt/CMM/rules/1`

4. Escriba el comando `set` para asignar valores a las propiedades asociadas a una determinada regla de alerta.

Por ejemplo, para establecer PET de IPMI como tipo de alerta de la regla 1, escribiría los siguientes comandos:

```
set type=ipmipet
```

Nota – Para habilitar una regla de alerta configurada, debe especificar el tipo y nivel de alerta y el destino de la alerta. Si define captura de eventos SNMP como tipo de alerta, tiene la opción de definir un valor para autenticar la recepción de las alertas.

Para obtener más información sobre cada una de las propiedades que puede definir al configurar las reglas de alertas, consulte la [TABLA 7-1 “Propiedades para definir las reglas de alertas”](#) en la página 145.

▼ Inhabilitación de una regla de alerta mediante la línea de comandos

Utilice el procedimiento siguiente para inhabilitar las reglas de alertas configuradas en ILOM desde la interfaz de la línea de comandos:

1. Establezca una conexión de consola serie o una conexión SSH con el CMM o el SP del servidor:

■ **Conexión de la consola serie local**

Conecte una consola serie al puerto serie del servidor o el CMM.

Para obtener más información, consulte la documentación de usuario suministrada con la plataforma de servidor Sun.

o

■ **Conexión Secure Shell (SSH) remota**

Establezca una conexión Secure Shell con el CMM o el SP del servidor.

Desde el cliente remoto, acceda como usuario root y establezca una conexión segura con el CMM activo o el SP del servidor.

Por ejemplo, puede establecer una conexión segura con el SP del servidor desde un cliente SSH remoto escribiendo lo siguiente:

```
ssh -l root dirección_ip_servidor
```

```
Password: changeme
```

Aparece el indicador de comandos predeterminado (->).

2. Utilice el comando `cd` para establecer la regla de administración de alertas que desea inhabilitar como directorio de trabajo.

Por ejemplo:

- Para el SP de un servidor montado en un bastidor, escriba: `cd /SP/alertngnt/rules/n`
- Para el SP de un servidor blade, escriba: `cd /CH/BLn/SP/alertmgmt/rules/n`
- Para un CMM de un chasis, escriba: `cd /CMM/alertmgmt/CMM/rules/n` donde *n* representa un número de regla de alerta del 1 al 15.

3. Para inhabilitar la regla de alerta, escriba el comando siguiente:

```
set level=disable
```

▼ Generación de pruebas de alertas mediante la línea de comandos

Puede comprobar el funcionamiento de cada regla de alerta *habilitada* en ILOM enviando una alerta de prueba.

Para enviar este tipo de pruebas a los destinos especificados en la configuración de las alertas, siga este procedimiento:

1. Establezca una conexión de consola serie o una conexión SSH con el CMM o el SP del servidor:

- **Conexión de la consola serie local**

Conecte una consola serie al puerto serie del servidor o el CMM.

Para obtener más información, consulte la documentación de usuario suministrada con la plataforma de servidor Sun.

o

- **Conexión Secure Shell (SSH) remota**

Establezca una conexión Secure Shell con el CMM o el SP del servidor.

Desde el cliente remoto, acceda como usuario root y establezca una conexión segura con el CMM activo o el SP del servidor.

Por ejemplo, puede establecer una conexión segura con el SP del servidor desde un cliente SSH remoto escribiendo lo siguiente:

```
ssh -l root dirección_ip_servidor
```

```
Password: changeme
```

Aparece el indicador de comandos predeterminado (->).

2. Utilice el comando `cd` para establecer las reglas de administración de alertas como directorio de trabajo.

Por ejemplo:

- Para el SP de un servidor montado en un bastidor, escriba: `cd /SP/alertmgmt/rules`
- Para el SP de un servidor blade, escriba: `cd /CH/BL1/SP/alertmgmt/rules`
- Para un CMM de un chasis, escriba: `cd /CMM/alertmgmt/CMM/rules`

3. Escriba el comando siguiente para generar una alerta de prueba:

```
set testalert=true
```

Configuración de un cliente SMTP para alertas de notificación por correo electrónico

Para generar alertas de notificación por correo electrónico, debe habilitar el cliente ILOM para que actúe como un cliente SMTP encargado de enviar los mensajes. Para habilitar el cliente ILOM como cliente SMTP, debe especificar la dirección IP y el número de puerto de un servidor SMTP de correo saliente que procese las notificaciones enviadas por correo electrónico.

Si precisa más información sobre la forma de configurar un cliente SMTP para enviar las alertas de notificación por correo electrónico en ILOM, consulte las secciones siguientes:

- [“Habilitación del cliente SMTP mediante la interfaz web” en la página 158](#)
- [“Habilitación de un cliente SMTP mediante la línea de comandos” en la página 158](#)

Requisito previo:

- Antes de habilitar el cliente ILOM como cliente SMTP, debería obtener la dirección IP y el número de puerto del servidor SMTP de correo saliente.

▼ **Habilitación del cliente SMTP mediante la interfaz web**

Siga el procedimiento siguiente para configurar un cliente SMTP en ILOM utilizando la interfaz web:

1. **Abra un navegador de web y escriba la dirección IP del CMM o el SP del servidor.**

Se abre la página de inicio de sesión de la interfaz web de ILOM.

2. **En la página de inicio de sesión, especifique el nombre de usuario y la contraseña de administrador, y haga clic en OK (aceptar).**

Aparece la interfaz web de ILOM.

3. **En la página abierta, seleccione Configuration (configuración) --> SMTP Client (cliente SMTP).**

4. **En la página SMTP Client, especifique los valores de configuración siguientes para habilitar las alertas de notificación por correo electrónico.**

Opción de SMTP	Descripción
SMTP State	Seleccione esta casilla para habilitar el estado de SMTP.
SMTP Server IP	Escriba en este campo la dirección IP del servidor SMTP de correo saliente que procesará las notificaciones de correo electrónico.
SMTP Port	Escriba el número de puerto del servidor SMTP de correo saliente.

5. **Haga clic en Save (guardar) para aplicar la configuración de SMTP.**

▼ **Habilitación de un cliente SMTP mediante la línea de comandos**

Siga el procedimiento siguiente para configurar un cliente SMTP en ILOM utilizando la interfaz de la línea de comandos:

1. **Establezca una conexión de consola serie o una conexión SSH con el CMM o el SP del servidor:**

- **Conexión de la consola serie local**

Conecte una consola serie al puerto serie del servidor o el CMM.

Para obtener más información, consulte la documentación de usuario suministrada con la plataforma de servidor Sun.

o

- **Conexión Secure Shell (SSH) remota**

Establezca una conexión Secure Shell con el CMM o el SP del servidor.

Desde el cliente remoto, acceda como usuario root y establezca una conexión segura con el CMM activo o el SP del servidor.

Por ejemplo, puede establecer una conexión segura con el SP del servidor desde un cliente SSH remoto escribiendo lo siguiente:

```
ssh -l root dirección_ip_servidor
```

Password: **changeme**

Aparece el indicador de comandos predeterminado (->).

2. **Utilice el comando `cd` para establecer `clients/sntp` como directorio de trabajo.**

Por ejemplo:

- Para el SP de un servidor montado en un bastidor, escriba: **`cd /SP/clients/sntp`**
- Para el SP de un servidor blade, escriba: **`cd /CH/BLn/SP/clients/sntp`**
- Para un CMM de un chasis, escriba: **`cd /CMM/clients/sntp`**

3. **Escriba el comando `show` para ver las propiedades de SMTP.**

Por ejemplo, al acceder por primera vez a las propiedades de SMTP en un SP, el resultado sería similar a éste:

```
show  
/SP/clients/sntp  
Targets  
  Properties  
    address = 0. 0. 0. 0  
    port = 25  
    state = enabled  
Commands:  
  cd  
  set  
  show
```

4. **Utilice el comando `set` para especificar la dirección IP del cliente SMTP o cambiar el valor de puerto o estado.**

Por ejemplo:

```
set address=222.333.44.5
```

5. Pulse Intro para que el valor tenga efecto.

Por ejemplo, si ha escrito `set address=222.333.44.5`, aparecerá el siguiente resultado:

```
Set 'address=222.333.44.5'
```


Configuración de la comunicación en ILOM

La comunicación avanzada de ILOM se establece configurando las opciones de red, el puerto serie y el servidor web.

Este capítulo contiene las secciones siguientes:

- “Administración de la configuración de red de ILOM mediante la línea de comandos” en la página 162
 - “Visualización de la configuración de red mediante la línea de comandos” en la página 163
 - “Configuración de los valores de red mediante la línea de comandos” en la página 163
 - “Visualización de la configuración del puerto serie mediante la línea de comandos” en la página 165
 - “Configuración del puerto serie mediante la línea de comandos” en la página 166
 - “Habilitación del acceso HTTP o HTTPS a la web mediante la línea de comandos” en la página 167
- “Configuración de Secure Shell” en la página 168
 - “Establecimiento de una conexión remota segura para ejecutar los comandos de la línea de comandos” en la página 168
 - “Visualización de la clave actual mediante la línea de comandos” en la página 169
 - “Habilitación o inhabilitación de SSH mediante la línea de comandos” en la página 170
 - “Habilitación o inhabilitación de SSH mediante la interfaz web” en la página 170
 - “Generación de una clave nueva mediante la línea de comandos” en la página 171
 - “Generación de una clave nueva mediante la interfaz web” en la página 172

- “Reinicio del servidor SSH mediante la línea de comandos” en la página 172
- “Reinicio del servidor SSH mediante la interfaz web” en la página 172
- “Administración de la configuración de red de ILOM mediante la interfaz web” en la página 173
 - “Visualización de la configuración de red mediante la interfaz web” en la página 173
 - “Configuración de los valores de red mediante la interfaz web” en la página 173
 - “Visualización de la configuración del puerto serie mediante la interfaz web” en la página 175
 - “Configuración de los valores del puerto serie mediante la interfaz web” en la página 176
 - “Habilitación del acceso HTTP o HTTPS a la web mediante la interfaz web” en la página 176

Nota – Los ejemplos de sintaxis de este capítulo utilizan el destino que empieza por `/SP/`, pero podría cambiarse por el destino que empieza por `/CMM/` en función de cuál sea la plataforma de servidor Sun utilizada. Los destinos subordinados son comunes para todas las plataformas de servidor Sun.

Administración de la configuración de red de ILOM mediante la línea de comandos

En esta sección se explica cómo configurar los valores de red de ILOM utilizando la interfaz de la línea de comandos.

Introducción a la configuración de red

Los valores de configuración de red tienen dos conjuntos de propiedades: pendientes y activas. Las propiedades activas son las que está utilizando ILOM. Son valores de sólo lectura. Si quiere cambiar la configuración, introduzca los nuevos valores como valores pendientes (`pendingipaddress` o `pendingipgateway`) y luego configure la propiedad `commitpending` como `true`. Esto impide desconexiones accidentales tanto en la configuración del puerto como de la red.

Nota – Asegúrese de que ILOM tenga asignada la misma dirección IP en todo momento, bien asignándole una dirección estática tras la configuración inicial o configurando el servidor DHCP para que siempre asigne la misma dirección IP a ILOM. Esto permite localizar ILOM con facilidad en la red.

▼ Visualización de la configuración de red mediante la línea de comandos

1. Inicie la sesión en la interfaz de la línea de comandos de ILOM como administrador u operador.
2. Cuando aparezca el indicador de comandos, escriba:
→ `show /SP/network`

▼ Configuración de los valores de red mediante la línea de comandos

Utilice el comando `set` para cambiar las propiedades y los valores de configuración de red.

1. Inicie la sesión en la interfaz de la línea de comandos de ILOM como administrador.
2. Cuando aparezca el indicador de comandos, escriba:
→ `set /SP/network`

Destinos, propiedades y valores

Éstos son los destinos, propiedades y valores válidos para la configuración de red de ILOM.

TABLA 8-1 Destinos, propiedades y valores de red de ILOM

Destino	Propiedad	Valor	Valor predeterminado
/SP/network	ipaddress	Estos valores son de sólo lectura y los actualiza el sistema	
	ipdiscovery		
	ipgateway		
	ipnetmask		
	macaddress	Dirección MAC de ILOM	
	commitpending	true none	(none)
	pendingipaddress	<direcciónip none>	none
	pendingipdiscovery	dhcp static	dhcp
	pendingipgateway	<direcciónip none>	none
	pendingipnetmask	<ipnotacióndecimal>	255.255.255.255

Ejemplo

Para cambiar la dirección IP de ILOM, escriba:

```
-> set /SP/network pendingipaddress=nnn.nn.nn.nn commitpending=true
```

Nota – Al cambiar la dirección IP, se desconectará la sesión activa en caso de que se haya conectado a ILOM a través de una red.

Para sustituir los valores de red asignados mediante DHCP por valores estáticos, escriba:

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

Nota – La nueva configuración entra en efecto tan pronto como la propiedad commitpending se define con true.

Configuración del puerto serie

El puerto serie proporciona acceso a la interfaz web de ILOM, la interfaz de la línea de comandos y la consola del sistema mediante la redirección del puerto serie.

- El puerto serie interno establece la conexión entre el servidor host e ILOM, y permite al usuario de ILOM acceder a la consola serie del host. La velocidad de este puerto tiene que coincidir con la del puerto de la consola serie del servidor host, normalmente conocido como puerto serie 0, COM1 o /dev/ttyS0.

Nota – Normalmente, la configuración de la consola serie del host coincide con la configuración predeterminada de ILOM (9600 baudios, 8N1 [ocho bits de datos, sin paridad, un bit de parada], sin control de flujo).

- El puerto serie externo de ILOM es el puerto serie RJ-45. En general, las conexiones de los puertos serie interno y externo deberían funcionar a la misma velocidad para evitar problemas de control del flujo de datos al establecer la conexión con la consola del host desde el puerto serie externo de ILOM.

▼ Visualización de la configuración del puerto serie mediante la línea de comandos

1. Inicie la sesión en la interfaz de la línea de comandos de ILOM como administrador u operador.
2. Cuando aparezca el indicador de comandos:
 - Escriba el comando siguiente para ver los valores de configuración del puerto serie externo:
-> **show /SP/serial/external**
 - Escriba el comando siguiente para ver los valores de configuración del puerto serie del host:
-> **show /SP/serial/host**

▼ Configuración del puerto serie mediante la línea de comandos

Utilice el comando `set` para cambiar las propiedades y los valores de configuración del puerto serie. Los valores de configuración del puerto tienen dos conjuntos de propiedades: pendientes y activas. Las propiedades activas son las que está utilizando ILOM. Son valores de sólo lectura. Si quiere cambiar la configuración, introduzca los nuevos valores como valores pendientes y luego configure la propiedad `commitpending` como `true`. Esto impide desconexiones accidentales tanto en la configuración del puerto como de la red.

1. Inicie la sesión en la interfaz de la línea de comandos de ILOM como administrador u operador.
2. Cuando aparezca el indicador de comandos, escriba:

```
-> set destino [nombrepropiedad=valor]
```

Destinos, propiedades y valores

Éstos son los destinos, propiedades y valores válidos para los puertos serie de ILOM.

TABLA 8-2 Destinos, propiedades y valores válidos para los puertos serie de ILOM

Destino	Propiedad	Valor	Valor predeterminado
/SP/serial/external	<code>commitpending</code>	<code>true (none)</code>	<code>(none)</code>
	<code>flowcontrol</code>	<code>none</code>	<code>none</code>
	<code>pendingspeed</code>	<code><decimal></code>	<code>9600</code>
	<code>speed</code>	<code>9600</code>	<code>9600</code>
/SP/serial/host	<code>commitpending</code>	<code>true (none)</code>	<code>(none)</code>
	<code>pendingspeed</code>	<code><decimal></code>	<code>(none)</code>
	<code>speed</code>	<code>9600</code>	<code>9600</code>

Ejemplo

Para cambiar la velocidad (tasa de baudios) del puerto serie de 9600 a 57600, escriba:

```
-> set /SP/serial/host pendingspeed=57600 commitpending=true
```

Nota – La velocidad del puerto serie del host tiene que coincidir con la del puerto serie 0, COM1 o /dev/ttyS0 del sistema operativo host para que ILOM pueda comunicarse adecuadamente con el host.

▼ Habilitación del acceso HTTP o HTTPS a la web mediante la línea de comandos

ILOM admite conexiones HTTP o HTTPS y permite redirigir automáticamente el acceso HTTP a HTTPS. También permite configurar los puertos de HTTP y HTTPS.

1. Inicie la sesión en la interfaz de la línea de comandos de ILOM como administrador.

2. Cuando aparezca el indicador de comandos, escriba:

```
-> set /SP/services/http
```

Las propiedades están situadas en /SP/services/http y /SP/services/https.

Destinos, propiedades y valores

En la [TABLA 8-3](#) figuran los destinos, las propiedades y los valores admitidos para HTTP y HTTPS.

TABLA 8-3 Destinos, propiedades y valores válidos para HTTP y HTTPS

Destino	Propiedad	Valor	Valor predeterminado
/SP/services/http	securerredirect	enabled disabled	enabled
	servicestate	enabled disabled	disabled
	port	<número>	80
/SP/services/https	servicestate	enabled disabled	enabled
	port	<número>	443

En la [TABLA 8-4](#) se indican los valores posibles para HTTP, HTTPS y la redirección automática.

TABLA 8-4 Valores posibles para HTTP, HTTPS y la redirección automática

Estado deseado	Destino	Propiedad	Valor
Habilitar sólo HTTP	/SP/services/http	securerredirect	disabled
	/SP/services/http	servicestate	enabled
	/SP/services/https	servicestate	disabled
Habilitar HTTP y HTTPS	/SP/services/http	securerredirect	disabled

TABLA 8-4 Valores posibles para HTTP, HTTPS y la redirección automática (*continuación*)

Estado deseado	Destino	Propiedad	Valor
	/SP/services/http	servicestate	enabled
	/SP/services/https	servicestate	enabled
Habilitar sólo HTTPS	/SP/services/http	secureredirect	disabled
	/SP/services/http	servicestate	disabled
	/SP/services/https	servicestate	enabled
Redirigir HTTP automáticamente a HTTPS	/SP/services/http	secureredirect	enabled
	/SP/services/http	servicestate	disabled
	/SP/services/https	servicestate	enabled

Configuración de Secure Shell

Secure Shell (SSH) es el protocolo estándar utilizado para establecer conexiones remotas seguras con la interfaz de la línea de comandos de ILOM (CLI). El uso de SSH garantiza que todas las interacciones de administración con ILOM sean cifradas y seguras. Ambos extremos de la conexión del servidor se autentican mediante claves digitales y las contraseñas están cifradas. La conexión de ILOM está protegida con cifrado de claves RSA y DSA.

▼ Establecimiento de una conexión remota segura para ejecutar los comandos de la línea de comandos

- Necesitará establecer una conexión segura desde un cliente SSH remoto con el SP del servidor. Para establecer una conexión segura, escriba lo siguiente:

```
ssh -l nombreusuario dirección_ip_servidor
```

```
Password: *****
```

Aparece el indicador predeterminado (->) y el sistema está listo para ejecutar los comandos de la línea de comandos con los que se establecerán los valores de configuración de red.

▼ Visualización de la clave actual mediante la línea de comandos

Sólo es necesario ver las claves para operaciones de configuración avanzada. La mayoría de las veces no necesitará verlas. Puede ver la clave pública completa o la huella digital abreviada de la clave.

Nota – Todas las propiedades que figuran debajo de `/SP/services/ssh/keys/rsa|dsa` son de sólo lectura.

● Para ver la clave RSA, escriba:

```
-> show /SP/services/ssh/keys/rsa
    Por ejemplo:
    /SP/services/ssh/keys/rsa
    Targets:
        Properties:
            fingerprint =
ca:c0:05:ff:b7:75:15:a0:30:df:1b:a1:76:bd:fe:e5
            length = 1024
            publickey
AAAAB3NzaC1yc2EAAAABIwAAAIEAthvlggXbPIxN40EvkukKupdFPPr8GDaOsKGG
BESVlnny4nX8yd8JC/hrw3qDHmXIZ8JAFwoLQgjtZCbEsgpn9nNIMb6nSfu6Y1t
TtUZXSgFBZ48ROmU0SqqfR3i3bgDUR0siphlpGv6Yu0Zd1h3549wQ+RwK3vxqHQ
Ffzhv9c=
        Commands:
            cd
            show
```

● Para ver la clave DSA, escriba:

```
-> show /SP/services/ssh/keys/dsa
    Por ejemplo:
    /SP/services/ssh/keys/dsa
    Targets:

        Properties:
            fingerprint =
6a:90:c7:37:89:e6:73:23:45:ff:d6:8e:e7:57:2a:60
            length = 1024
            publickey =
AAAAB3NzaC1kc3MAAACBAInrYecNH86imBbUqE+3FoUfm/fei2ZZtQzqrMx5zBm
bHFIAfDRQKeoQ7gqjc9jQb07ajLxwk2vZzkg3ntnmqHz/hwHvdho2KaolBtAFGc
fLIdzGVxi4I3phVb6anmTlbqI2AILAa7JvQ8dEGbyATYR9A/pf5VTac/TQ700/J
AAAAFQCIUavkex7wtEhC0CH3s25ON0I3CwAAAIbNfHUop6ZN7i46ZuQOKhD7Mkj
```

```
gdHy+8MTBkupVfXqfRE9Zw9yrBZCNsoD8XEeIeyP+pu05k5dJvzkzqSqrTVoAXyY  
qewyZMFE7stutugw/XEmyj+XqBWaiOAQskdiMvNHa3MSg8PKJyWP8eIMxD3rIu  
PTzkV632uBxzwSwfAQAAAIAtA8/3odDJUprnxLgHTowc8ksGBj/wJDgPfpGGJHB  
B1FDBMhSsRbwh6Z+s/gAf1f+S67HJBTUPsVSMz+czmamc1oZeOazT4+zeNG6uCl  
u/5/JmJSdkguc1FcoxtBFqfO/fKjyR0ecWau7L4kjbvWoSsydHJ0pMHasEecEBEr  
lg==
```

```
Commands :  
cd  
show
```

▼ Habilitación o inhabilitación de SSH mediante la línea de comandos

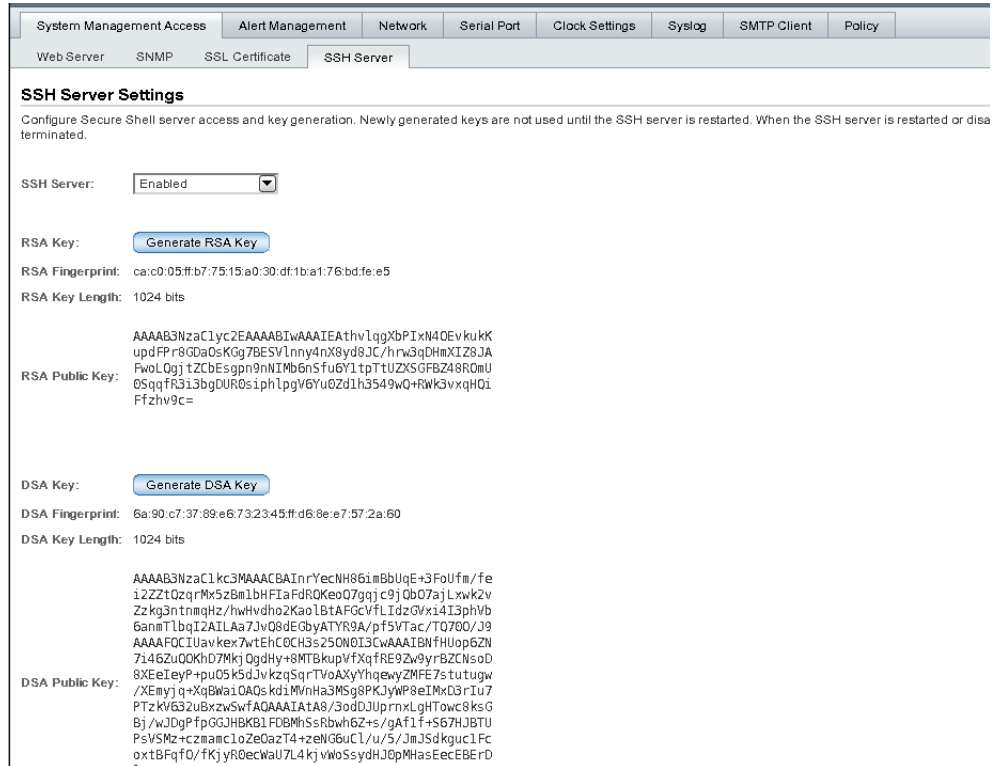
- Si no desea proporcionar acceso a través de la red, o prefiere no utilizar SSH, escriba lo siguiente:

```
-> set /SP/services/ssh state=enabled | disabled
```

▼ Habilitación o inhabilitación de SSH mediante la interfaz web

1. Inicie la sesión de ILOM como administrador.
2. Seleccione Configuration (configuración) --> System Management Access (acceso a la administración del sistema) --> SSH Server (servidor SSH).
3. En la lista desplegable SSH Server, seleccione Enabled (habilitado) o Disabled (inhabilitado).

FIGURA 8-1 Página de configuración del servidor SSH



▼ Generación de una clave nueva mediante la línea de comandos

1. Establezca el tipo de clave escribiendo lo siguiente:

```
-> set /SP/services/ssh generate_new_key_type=dsa | rsa
```

2. Configure la acción como true.

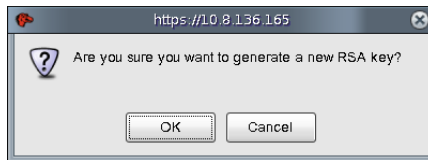
```
-> set /SP/services/ssh generate_new_key_action=true
```

Aparecerán una huella digital y una clave diferentes.

▼ Generación de una clave nueva mediante la interfaz web

1. Inicie la sesión de ILOM como administrador.
2. Seleccione Configuration (configuración) --> System Management Access (acceso a la administración del sistema) --> SSH Server (servidor SSH).
3. Seleccione RSA o DSA haciendo clic en los botones Generate RSA Key (generar clave RSA) o Generate DSA Key (generar clave DSA) respectivamente.
Cuando aparezca el mensaje de confirmación, confirme o cancele la selección haciendo clic en los botones OK (aceptar) o Cancel (cancelar).

FIGURA 8-2 Cuadro de diálogo de confirmación



▼ Reinicio del servidor SSH mediante la línea de comandos

Ninguna clave nueva entrará en efecto hasta que se reinicie el servidor SSH.

Nota – La operación de reinicio interrumpirá cualquier conexión SSH existente.

- Para reiniciar el servidor SSH, escriba lo siguiente:

```
-> set /SP/services/ssh restart_sshd_action=true
```

▼ Reinicio del servidor SSH mediante la interfaz web

Ninguna clave nueva entrará en efecto hasta que se reinicie el servidor SSH.

Nota – La operación de reinicio interrumpirá cualquier conexión SSH existente.

1. Inicie la sesión de ILOM como administrador.

2. Seleccione **Configuration (configuración)** --> **System Management Access (acceso a la administración del sistema)** --> **SSH Server (servidor SSH)**.
3. En la lista desplegable **SSH Server**, seleccione **Restart SSH Server (reiniciar el servidor SSH)**.

Administración de la configuración de red de ILOM mediante la interfaz web

En esta sección se explica cómo configurar los parámetros de red de ILOM utilizando la interfaz web.

ILOM configura automáticamente sus direcciones IP utilizando el protocolo DHCP (Dynamic Host Configuration Protocol). Si su red no admite este protocolo, deberá configurar los parámetros de forma manual.

▼ Visualización de la configuración de red mediante la interfaz web

1. **Inicie la sesión de ILOM como administrador u operador para abrir la interfaz web.**
2. **Seleccione Configuration (configuración) --> Network (red).**
En la página Network Settings (configuración de red), puede ver las direcciones MAC y configurar las direcciones de red de los módulos de supervisión del chasis y los procesadores de servicios del servidor.

Nota – DHCP es el modo predeterminado, pero puede configurar manualmente la dirección IP, la máscara de red y la puerta de enlace.

▼ Configuración de los valores de red mediante la interfaz web

1. **Inicie la sesión de ILOM como administrador para abrir la interfaz web de la aplicación.**
2. **Seleccione Configuration (configuración) --> Network (red).**
Se abre la página Network Settings (configuración de red).

FIGURA 8-3 Página de configuración de red

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 r appropriate mode, then enter settings as needed.

MAC Address: 00:14:4F:1F:AB:F9

Obtain an IP Address Automatically (use DHCP)

Use the Following IP Address

IP Address:

Subnet Mask:

Gateway:

3. Rellene la información de la página de configuración de red.

Al especificar los datos, tome como referencia las descripciones de la [TABLA 8-5](#).

TABLA 8-5 Campos de la página de configuración de red

Opción	Descripción
MAC Address (dirección MAC)	La dirección MAC (Media Access Control) de ILOM se establece en la fábrica. Se trata de una dirección de hardware y es exclusiva de cada dispositivo conectado a una red. La dirección MAC de ILOM se suministra en una etiqueta adherida al servidor o el CMM, en la hoja de información del cliente (Customer Information Sheet) entregada con el servidor y en la pantalla de configuración de la BIOS.
Obtain an IP Address Automatically (use DHCP) (obtener la dirección IP automáticamente, usar DHCP)	Haga clic en el botón de opción para que el protocolo DHCP obtenga la dirección IP.
IP Address (dirección IP)	Escriba la dirección IP de ILOM. La dirección IP es un nombre que identifica el sistema de forma exclusiva en una red TCP/IP.
Subnet Mask (máscara de subred)	Escriba la máscara de subred perteneciente a la red en la que reside ILOM.
Gateway (puerta de enlace)	Escriba la dirección de acceso a la puerta de enlace de ILOM.

4. Haga clic en **Save (guardar)** para que la configuración tenga efecto.

Los valores introducidos no se considerarán definitivos hasta que haga clic en **Save**. Al cambiar la dirección IP, finalizará la sesión de ILOM.

Aparecerá un mensaje solicitando que cierre el navegador de web.

5. **Vuelva a iniciar la sesión de ILOM utilizando la nueva dirección IP.**

Nota – Si ha cambiado la configuración de red, puede que necesite volver a conectarse a ILOM con una nueva sesión del navegador.

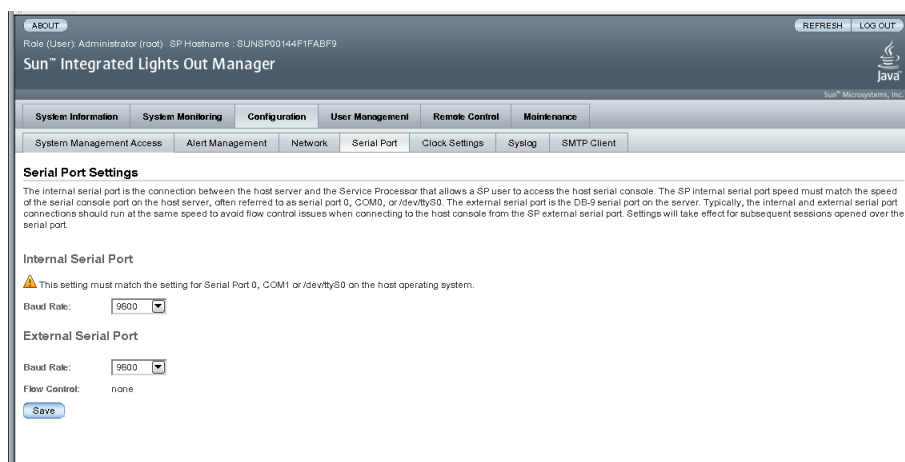
▼ Visualización de la configuración del puerto serie mediante la interfaz web

1. **Inicie la sesión de la interfaz web de ILOM como administrador u operador.**

2. **Seleccione Configuration (configuración) --> Serial Port (puerto serie).**

Se abre la página Serial Port Settings (configuración del puerto serie).

FIGURA 8-4 Página de configuración del puerto serie



3. **Vea la velocidad de baudios del puerto serie externo.**

▼ Configuración de los valores del puerto serie mediante la interfaz web

En esta sección se explica cómo configurar el puerto serie de ILOM. Los valores predeterminados son 9600 baudios sin control de flujo.

1. Inicie la sesión de ILOM como administrador para abrir la interfaz web de la aplicación.

2. Seleccione Configuration (configuración) --> Serial Port (puerto serie).

Se abre la página Serial Port Settings (configuración del puerto serie).

3. Seleccione la velocidad de baudios del puerto serie interno en la lista desplegable Internal Serial Port Baud Rate (baudios del puerto serie interno).

Este valor debe coincidir con el del puerto serie 0, COM1 o /dev/ttyS0 del sistema operativo host.

El número de baudios debe coincidir con la velocidad especificada en la función de redirección serie de la BIOS (el predeterminado es 9600 baudios), así como con la velocidad indicada para el cargador de arranque y la configuración del sistema operativo.

Para establecer conexión con la consola del sistema utilizando ILOM, ILOM debe tener configurados sus valores predeterminados (9600 baudios, 8N1 [ocho bits de datos, sin paridad, un bit de parada], sin control de flujo).

4. Seleccione la velocidad de baudios del puerto serie externo en la lista desplegable External Serial Port Baud Rate (baudios del puerto serie externo).

Este valor debe coincidir con la velocidad de baudios del puerto serie RJ-45 del servidor Sun.

5. Haga clic en Save para que los cambios tengan efecto o en Cancel para recuperar los valores anteriores.

▼ Habilitación del acceso HTTP o HTTPS a la web mediante la interfaz web

En esta sección se explica cómo ver y modificar los valores de configuración del servidor web.

ILOM ofrece la posibilidad de controlar el tipo de acceso a la interfaz web. Dispone de cuatro opciones:

- Sólo HTTP
- Sólo HTTPS
- HTTP y HTTPS

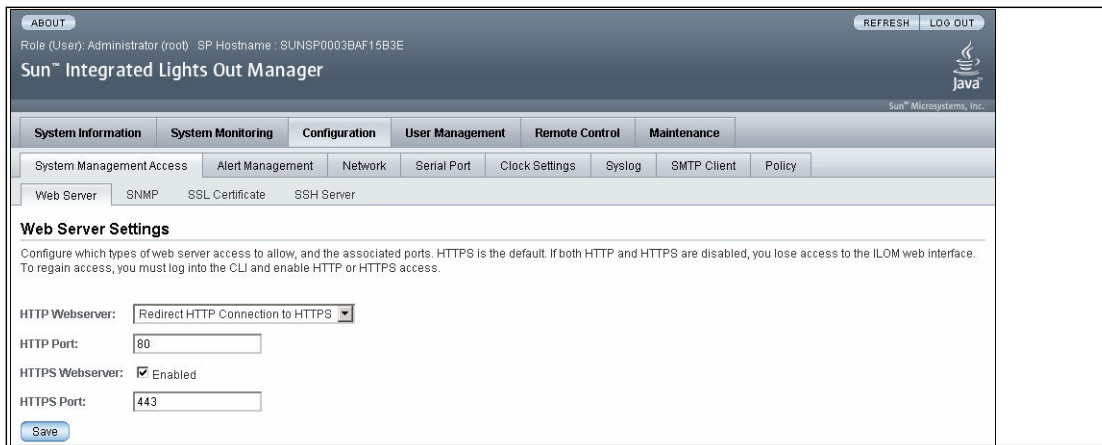
- HTTPS y redirección automática de HTTP a HTTPS

La opción HTTPS está habilitada de forma predeterminada.

1. **Inicie la sesión de ILOM como administrador para abrir la interfaz web de la aplicación.**
2. **Seleccione Configuration (configuración) --> System Management Access (acceso a la administración del sistema) --> Web Server (servidor web).**

Se abre la página Web Server Settings (configuración del servidor web).

FIGURA 8-5 Página de configuración del servidor web



3. **Seleccione el servidor web HTTP o HTTPS.**

- **Para habilitar HTTP:** seleccione Enabled en la lista desplegable. También puede seleccionar:
 - Redirect HTTP Connection to HTTPS: las conexiones HTTP se redirigen automáticamente a HTTPS.
 - Disabled: inhabilita HTTP.
- **Para habilitar HTTPS:** seleccione la casilla HTTPS Web Server Enabled (servidor web HTTPS habilitado).

El servidor web HTTPS está habilitado de forma predeterminada.

Nota – Si inhabilita HTTP o selecciona Redirect HTTP Connection to HTTPS y luego inhabilita HTTPS, no podrá acceder a la interfaz web de ILOM. Para restablecer el acceso, utilice los comandos `/SP/services/http` o `/SP/services/https` de la línea de comandos como se describe en [“Habilitación del acceso HTTP o HTTPS a la web mediante la línea de comandos”](#) en la página 167.

4. **Asigne un número de puerto HTTP o HTTPS.**
5. **Haga clic en Save (guardar) para que la nueva configuración tenga efecto.**

IPMI (Intelligent Platform Management Interface)

ILOM es compatible con IPMI (Intelligent Platform Management Interface), una interfaz de administración inteligente de plataformas que permite utilizar una interfaz de línea de comandos para supervisar y controlar la plataforma del servidor, así como recuperar información sobre dicha plataforma.

Este capítulo contiene las secciones siguientes:

- [“Descripción de IPMI” en la página 179](#)
- [“ILOM e IPMI” en la página 180](#)
- [“Uso de IPMItool” en la página 180](#)
- [“Alertas de IPMI” en la página 181](#)
- [“Ejemplos de IPMItool” en la página 182](#)

Descripción de IPMI

IPMI (Intelligent Platform Management Interface) es una interfaz estándar diseñada principalmente para administrar sistemas de servidor fuera de banda a través de una serie de redes diferentes. Entre sus funciones se incluyen la generación de informes de inventario de las unidades FRU (unidades sustituibles en campo), la supervisión del sistema, el registro de eventos del sistema, la recuperación del sistema (lo que incluye el reinicio de sistemas locales y remotos, así como funciones de encendido y apagado) y el envío de alertas. IPMI funciona con independencia del procesador principal y el sistema operativo.

Las funciones independientes de supervisión, registro y acceso disponibles a través de IPMI proporcionan una cierta capacidad de administración integrada en el hardware de la plataforma. Además, este protocolo también funciona con equipos

donde no hay ningún software de administración de sistemas disponible para un determinado sistema operativo y resulta útil cuando se opta por no instalar ni cargar aplicaciones de administración de sistemas.

ILOM es conforme con IPMI v1.5 y v2.0.

Encontrará información complementaria, incluidas las especificaciones detalladas de IPMI, en los sitios siguientes:

<http://www.intel.com/design/servers/ipmi/spec.htm>

<http://openipmi.sourceforge.net>

ILOM e IPMI

IPMI establece un método específico de que los subsistemas de administración integrados se comuniquen entre sí. La información de esta interfaz se intercambia a través de los BMC (Baseboard Management Controllers), unos controladores de administración de la placa base situados en los componentes de hardware conformes con las especificaciones IPMI. El uso de inteligencia en el nivel del hardware en lugar del nivel del sistema operativo tiene dos ventajas fundamentales: en primer lugar, esta configuración permite administrar el servidor fuera de banda y, en segundo lugar, el sistema operativo no debe soportar la carga de transportar los datos de estado del sistema.

Los procesadores de servicios (SP) del servidor o los blades son conformes con IPMI v2.0. Puede acceder a las funciones de IPMI a través de la línea de comandos empleando la utilidad IPMItool tanto en banda como fuera de banda. Asimismo, puede generar capturas de eventos específicos de IPMI desde la interfaz web de ILOM o administrar las funciones de IPMI del SP desde cualquier solución de administración externa que sea conforme con IPMI v1.5 o v2.0.

Uso de IPMItool

IPMItool es una sencilla utilidad de código abierto basada en una interfaz de línea de comandos (CLI) que sirve para administrar y configurar dispositivos conformes con IPMI. Es posible administrar las funciones de IPMI en el sistema local o en un sistema remoto. Puede usar IPMItool para realizar las funciones de IPMI con un controlador de dispositivos del núcleo o a través de una interfaz de LAN. IPMItool puede descargarse desde este sitio:

<http://ipmitool.sourceforge.net/>

IPMItool permite hacer lo siguiente:

- Leer el depósito de datos SDR (Sensor Data Record).
- Ver en pantalla los valores de los sensores.
- Ver el contenido del registro de eventos del sistema (SEL).
- Ver la información de inventario de las unidades sustituibles en campo (FRU).
- Leer y configurar los parámetros de configuración de la LAN.
- Controlar el apagado y encendido del chasis de forma remota.

Encontrará información más amplia sobre IPMItool en una página del comando man disponible en este sitio:

<http://ipmitool.sourceforge.net/manpage.html>

Alertas de IPMI

ILOM admite el envío de alertas de captura de eventos de plataforma (PET) de IPMI. Las alertas advierten sobre posibles errores del sistema de forma anticipada. Su configuración puede realizarse desde el blade o el SP del servidor. Las alertas PET de IPMI se admiten en todos los módulos y plataformas de servidor Sun a excepción del módulo de supervisión del chasis (CMM).

Cada plataforma de servidor Sun está dotada de una serie de sensores conformes con IPMI que miden los voltajes, las temperaturas y otros atributos del sistema relacionados con los servicios. ILOM sondea automáticamente estos sensores y anota en el registro de eventos de ILOM cualquier cambio que indique que se ha superado algún umbral. Asimismo, ILOM genera mensajes de alerta y los envía a uno o varios destinos especificados mediante direcciones IP. El destino especificado para la alerta también debe admitir la recepción de mensajes PET de IPMI. Si el destino no admite mensajes PET, el destinatario no podrá decodificar el mensaje de alerta.

Al configurar alertas PET de IPMI, es preciso especificar un nivel de alerta, que filtra los mensajes para que los destinatarios sólo reciban aquellos que más les interesan. ILOM ofrece cinco niveles de alerta, de los cuales **Minor (menor)** es el más bajo:

- **Minor (menor):** genera alertas por eventos de tipo informativo, eventos no críticos de nivel superior e inferior, eventos críticos de nivel superior e inferior y eventos de errores irreversibles de nivel superior e inferior.
- **Major (mayor):** genera alertas por eventos no críticos de nivel superior e inferior, eventos críticos de nivel superior e inferior y eventos de errores irreversibles de nivel superior e inferior.
- **Critical (crítico):** genera alertas por eventos críticos de nivel superior e inferior y eventos de errores irreversibles de nivel superior e inferior.
- **Down (caída):** genera alertas por eventos de errores irreversibles de nivel superior e inferior.
- **Disabled (inhabilitada):** inhabilita la alerta. ILOM no genera ningún mensaje de alerta.

Para obtener información sobre la forma de administrar las reglas de alertas configuradas, lo que incluye la forma de modificar o inhabilitar las reglas y generar alertas de prueba, consulte [“Administración de las reglas de alertas mediante la interfaz web de ILOM”](#) en la página 147 y [“Administración de las reglas de alertas mediante la línea de comandos de ILOM”](#) en la página 151.

Si precisa una descripción de los comandos de la línea de comandos de ILOM utilizados para administrar la configuración de las reglas de alertas, consulte [“Comandos para administrar las reglas de alertas desde la línea de comandos”](#) en la página 152.

Ejemplos de IPMItool

He aquí algunos ejemplos de cómo puede utilizarse la herramienta IPMItool. En ellos, 10.8.136.165 es la dirección IP de ILOM. Los comandos son comunes para todas las plataformas, sin embargo, el resultado de su ejecución (nombre, valores y umbrales de los sensores, etc.) varía según la plataforma.

▼ Visualización de la lista de sensores y sus valores

```
$ ipmitool -H 10.8.136.165 -I lanplus -U root -P changeme sdr list
/SYS/T_AMB | 24 degrees C | ok
/RFM0/FAN1_SPEED | 7110 RPM | ok
/RFM0/FAN2_SPEED | 5880 RPM | ok
/RFM1/FAN1_SPEED | 5880 RPM | ok
/RFM1/FAN2_SPEED | 6360 RPM | ok
/RFM2/FAN1_SPEED | 5610 RPM | ok
/RFM2/FAN2_SPEED | 6510 RPM | ok
/RFM3/FAN1_SPEED | 6000 RPM | ok
/RFM3/FAN2_SPEED | 7110 RPM | ok
/RFM4/FAN1_SPEED | 6360 RPM | ok
/RFM4/FAN2_SPEED | 5610 RPM | ok
/RFM5/FAN1_SPEED | 5640 RPM | ok
/RFM5/FAN2_SPEED | 6510 RPM | ok
/RFM6/FAN1_SPEED | 6180 RPM | ok
/RFM6/FAN2_SPEED | 6000 RPM | ok
/RFM7/FAN1_SPEED | 6330 RPM | ok
/RFM7/FAN2_SPEED | 6330 RPM | ok
/RFM8/FAN1_SPEED | 6510 RPM | ok
/RFM8/FAN2_SPEED | 5610 RPM | ok
```

Nota – La salida anterior está abreviada. El resultado real del comando presenta 163 sensores.

▼ Visualización de los datos de un sensor

```
$ ipmitool -H 10.8.136.165 -v -I lanplus -U root -P changeme sensor get /SYS/T_AMB
Locating sensor record...
Sensor ID          : /SYS/T_AMB (0x8)
Entity ID          : 41.0
Sensor Type (Analog) : Temperature
Sensor Reading     : 24 (+/- 0) degrees C
Status             : ok
Lower Non-Recoverable : 0.000
Lower Critical      : 4.000
Lower Non-Critical  : 10.000
Upper Non-Critical  : 35.000
Upper Critical      : 40.000
Upper Non-Recoverable : 45.000
Assertions Enabled  : lnc- lcr- lnr- unc+ ucr+ unr+
Deassertions Enabled : lnc- lcr- lnr- unc+ ucr+ unr+
```

▼ Encendido del host

```
$ ipmitool -H 10.8.136.165 -v -I lanplus -U root -P changeme chassis power on
```

▼ Apagado del host

```
$ ipmitool -H 10.8.136.165 -v -I lanplus -U root -P changeme chassis power off
```

▼ Apagado y encendido del host

```
$ ipmitool -H 10.8.136.165 -v -I lanplus -U root -P changeme chassis power cycle
```

▼ Cierre normal del host

```
$ ipmitool -H 10.8.136.165 -v -I lanplus -U root -P changeme chassis power soft
```

▼ Visualización de la información de fabricación de las unidades FRU

```
$ ipmitool -H 10.8.136.165 -v -I lanplus -U root -P changeme fru print
```

```
FRU Device Description : Builtin FRU Device (ID 0)
Board Product         : ASSY,ANDY,4SKT_PCI-E,BLADE
Board Serial          : 0000000-7001
Board Part Number     : 501-7738-01
Board Extra           : AXX_RevE_Blade
Product Manufacturer  : SUN MICROSYSTEMS
Product Name          : ILOM

FRU Device Description : /SYS (ID 4)
Chassis Type          : Rack Mount Chassis
Chassis Part Number   : 541-0251-05
Chassis Serial        : 00:03:BA:CD:59:6F
Board Product         : ASSY,ANDY,4SKT_PCI-E,BLADE
Board Serial          : 0000000-7001
Board Part Number     : 501-7738-01
Board Extra           : AXX_RevE_Blade
Product Manufacturer  : SUN MICROSYSTEMS
Product Name          : SUN BLADE X8400 SERVER MODULE
Product Part Number   : 602-0000-00
Product Serial        : 0000000000
Product Extra         : 080020ffffffffffffffff0003baf15c5a

FRU Device Description : /P0 (ID 5)
Product Manufacturer  : ADVANCED MICRO DEVICES
Product Part Number   : 0F21
Product Version       : 2

FRU Device Description : /P0/D0 (ID 6)
Product Manufacturer  : MICRON TECHNOLOGY
Product Name          : 1024MB DDR 400 (PC3200) ECC
Product Part Number   : 18VDDF12872Y-40BD3
Product Version       : 0300
Product Serial        : D50209DA
Product Extra         : 0190
Product Extra         : 0400

FRU Device Description : /P0/D1 (ID 7)
Product Manufacturer  : MICRON TECHNOLOGY
Product Name          : 1024MB DDR 400 (PC3200) ECC
Product Part Number   : 18VDDF12872Y-40BD3
Product Version       : 0300
Product Serial        : D50209DE
Product Extra         : 0190
Product Extra         : 0400
```


▼ Visualización del registro de eventos del sistema de IPMI

```
$ ipmitool -H 10.8.136.165 -I lanplus -U root -P changeme sel list
```

100		Pre-Init Time-stamp		Power Unit #0x78		State Deasserted		
200		Pre-Init Time-stamp		Power Supply #0xa2		Predictive Failure Asserted		
300		Pre-Init Time-stamp		Power Supply #0xba		Predictive Failure Asserted		
400		Pre-Init Time-stamp		Power Supply #0xc0		Predictive Failure Asserted		
500		Pre-Init Time-stamp		Power Supply #0xb4		Predictive Failure Asserted		
600		04/05/2007		12:03:24		Power Supply #0xa3		Predictive Failure Deasserted
700		04/05/2007		12:03:25		Power Supply #0xaa		Predictive Failure Deasserted
800		04/05/2007		12:03:25		Power Supply #0xbc		Predictive Failure Deasserted
900		04/05/2007		12:03:26		Power Supply #0xa2		Predictive Failure Asserted
a00		04/05/2007		12:03:26		Power Supply #0xa8		Predictive Failure Deasserted
b00		04/05/2007		12:03:26		Power Supply #0xb6		Predictive Failure Deasserted
c00		04/05/2007		12:03:26		Power Supply #0xbb		Predictive Failure Deasserted
d00		04/05/2007		12:03:26		Power Supply #0xc2		Predictive Failure Deasserted
e00		04/05/2007		12:03:27		Power Supply #0xb0		Predictive Failure Deasserted
f00		04/05/2007		12:03:27		Power Supply #0xb5		Predictive Failure Deasserted
1000		04/05/2007		12:03:27		Power Supply #0xba		Predictive Failure Asserted
1100		04/05/2007		12:03:27		Power Supply #0xc0		Predictive Failure Asserted
1200		04/05/2007		12:03:28		Power Supply #0xa9		Predictive Failure Deasserted
1300		04/05/2007		12:03:28		Power Supply #0xae		Predictive Failure Deasserted
1400		04/05/2007		12:03:28		Power Supply #0xb4		Predictive Failure Asserted
1500		04/05/2007		12:03:28		Power Supply #0xbe		Predictive Failure Deasserted

SNMP (Simple Network Management Protocol)

ILOM es compatible con el uso del protocolo SNMP (Simple Network Management Protocol), que se utiliza para intercambiar datos sobre la actividad de la red. Se trata de un protocolo estándar de código abierto.

Este capítulo contiene las secciones siguientes:

- “Descripción de SNMP” en la página 188
- “Funcionamiento de SNMP” en la página 189
- “Archivos MIB de SNMP” en la página 190
- “Alertas y capturas de eventos de SNMP” en la página 191
- “Administración de usuarios de SNMP mediante la línea de comandos” en la página 192
 - “Adición de una cuenta de usuario de SNMP mediante la línea de comandos” en la página 192
 - “Edición de una cuenta de usuario de SNMP mediante la línea de comandos” en la página 192
 - “Supresión de una cuenta de usuario de SNMP mediante la línea de comandos” en la página 193
 - “Adición o edición de una comunidad SNMP mediante la línea de comandos” en la página 193
 - “Supresión de una comunidad SNMP mediante la línea de comandos” en la página 193
 - “Configuración de los destinos de capturas de eventos de SNMP mediante la línea de comandos” en la página 195
- “Administración de cuentas de usuario de SNMP mediante la interfaz web” en la página 196
 - “Configuración de SNMP mediante la interfaz web” en la página 196

- “Adición o edición de una cuenta de usuario de SNMP mediante la interfaz web” en la página 197
- “Supresión de una cuenta de usuario de SNMP mediante la interfaz web” en la página 199
- “Adición o edición de una comunidad SNMP mediante la interfaz web” en la página 200
- “Supresión de una comunidad SNMP mediante la interfaz web” en la página 200
- “Configuración de los destinos de capturas de eventos de SNMP mediante la interfaz web” en la página 201
- “Ejemplos de SNMP” en la página 202
 - “Visualización y configuración de los valores de SNMP” en la página 202
 - “Obtención de información mediante los comandos `snmpget` o `snmpwalk net-snmp`” en la página 204
 - “Configuración de la información mediante `snmpset`” en la página 204
 - “Recepción de capturas de eventos mediante `snmptrapd`” en la página 205

Nota – Los ejemplos de sintaxis de este capítulo utilizan el destino que empieza por `/SP/`, aunque podría cambiarse por el destino que empieza por `/CMM/` en función de la plataforma de servidor Sun utilizada. Los destinos subordinados son comunes para todas las plataformas de servidor Sun.

Descripción de SNMP

SNMP (Simple Network Management Protocol) es una tecnología de código abierto que permite administrar redes y los dispositivos, o nodos, conectados a ellas. Mediante SNMP, los datos viajan entre un dispositivo administrado (nodo) y una estación de administración de la red. Por dispositivo administrado se entiende cualquier dispositivo que ejecute SNMP, lo que incluye hosts, encaminadores, servidores web y otros servidores de la red. Los mensajes de SNMP se envían a través de IP utilizando paquetes UDP (User Datagram Protocol). Puede utilizar cualquier aplicación de administración compatible con SNMP para administrar su servidor.

ILOM es compatible con las versiones 1, 2c y 3 de SNMP, pero se recomienda el uso de SNMP v3 con preferencia porque esta versión proporciona mayores niveles de seguridad, autenticación y confidencialidad que SNMP v1 y v2c.

SNMP es un protocolo, no un sistema operativo, por lo que es necesaria una aplicación para utilizar los mensajes que genera. El software de administración de SNMP le puede proporcionar esta funcionalidad, pero también puede utilizar una herramienta de código abierto como net-SNMP, que está disponible en:

<http://net-snmp.sourceforge.net/>

Tanto los agentes como las estaciones de administración utilizan mensajes de SNMP para comunicarse. Las estaciones de administración pueden enviar y recibir información. Los agentes pueden responder a las peticiones y enviar mensajes no solicitados bajo la forma de captura de eventos. Las estaciones de administración y los agentes utilizan las funciones siguientes:

- Get
- GetNext
- GetResponse
- Set
- Trap

Funcionamiento de SNMP

Para que SNMP pueda funcionar, es necesaria la presencia de estos dos componentes:

- **Estación de administración de red:** esta estación aloja las aplicaciones de administración encargadas de supervisar y controlar los nodos administrados.
- **Nodo administrado:** es un dispositivo (por ejemplo, un servidor, un enrutador o un concentrador) que aloja los agentes de administración SNMP responsables de transmitir las peticiones procedentes de estaciones de administración, por ejemplo, un SP donde se ejecute ILOM.

La estación de administración supervisa los nodos sondeando a los agentes de administración mediante consultas con las que obtienen la información adecuada. Los nodos administrados también pueden suministrar a la estación de administración información de estado no solicitada en forma de capturas de eventos. SNMP es el protocolo utilizado para comunicar la información de administración entre las estaciones y los agentes de administración.

El agente SNMP se entrega preinstalado en la plataforma de servidor Sun y se ejecuta sobre ILOM, de modo que todos los procesos de administración de SNMP tienen lugar a través de ILOM. Para poder utilizar esta funcionalidad, el sistema operativo debe tener una aplicación SNMP cliente.

Archivos MIB de SNMP

El componente básico de cualquier implementación de SNMP es la base de datos de información de administración o MIB (Management Information Base). Una MIB es un archivo de texto en el que se describe la información disponible sobre un nodo administrado y el lugar donde está almacenada. Su sistema jerárquico en forma de árbol clasifica la información sobre los recursos de una red. La MIB define las variables a las que puede acceder el agente SNMP. Cuando una estación de administración solicita información de un nodo, el agente recibe esa petición y recupera la información necesaria de los archivos MIB. La MIB se encarga de proporcionar acceso a la información sobre el estado, los datos estadísticos y la configuración de red del servidor.

En ILOM se utilizan los siguientes archivos MIB de SNMP:

- Los grupos de sistema y snmp de SNMPv2 MIB (RFC1907)
- SNMP-FRAMEWORK-MIB (RFC2271.txt)
- SNMP-USER-BASED-MIB (RFC 2574)
- SNMP-MPD-MIB (RFC 2572)
- La tabla entPhysicalTable de ENTITY-MIB (RFC2737)
- SUN-PLATFORM-MIB

Esta MIB representa un inventario del hardware del chasis y el servidor, incluidos todos los sensores e indicadores y su estado.

- SUN-ILOM-CONTROL-MIB

Esta MIB representa una configuración del CMM o el SP de Sun como puede ser la administración de usuarios y accesos o las alertas, entre otras.

- SUN-HW-TRAP-MIB

Esta MIB describe las capturas de eventos de hardware que pueda generar un CMM o un SP de Sun.

- SUN-ILOM-PET-MIB

Esta MIB describe las capturas de eventos de plataforma (PET) de IPMI que pueda genera un SP de Sun. Para obtener más información sobre las alertas PET, consulte [“Introducción a la administración de alertas”](#) en la [página 143](#).

Alertas y capturas de eventos de SNMP

A través de ILOM, puede configurar un total de 15 reglas de alertas. Por cada regla configurada, y en función del tipo de alerta, es preciso definir tres o más propiedades relativas a la alerta. El tipo de alerta determina el formato de los mensajes de alerta y el método para enviarlos y recibirlos. ILOM admite estos tres tipos de alertas: alertas PET de IPMI, alertas de notificación por correo electrónico y capturas de eventos de SNMP.

ILOM permite generar alertas de captura de eventos de SNMP y enviarlas a una dirección IP especificada por el usuario. Todos los destinos especificados deben admitir la recepción de mensajes de eventos de SNMP.

ILOM incluye un agente SNMP preinstalado que tiene capacidad para entregar capturas de SNMP a la aplicación de administración SNMP.

Para utilizar esta capacidad, debe hacer lo siguiente:

- Integrar y guardar los archivos MIB específicos de la plataforma en el directorio SNMP.
- Informar a la estación de administración sobre el servidor utilizado.
- Configurar ILOM para que envíe las capturas de eventos de SNMP a la estación de administración.

No existe ningún destino configurado de forma predeterminada para el envío de las capturas. En principio, los agentes “escuchan” el puerto 161 para conocer las peticiones SNMP y envían las capturas al puerto 162.

Administración de usuarios de SNMP mediante la línea de comandos

Es posible agregar, borrar o configurar cuentas y comunidades de usuarios de SNMP utilizando la interfaz de la línea de comandos (CLI) de ILOM.

Nota – Al trabajar desde la línea de comandos de ILOM, si la opción Set Requests está inhabilitada, todos los objetos SNMP serán de sólo lectura.

▼ Adición de una cuenta de usuario de SNMP mediante la línea de comandos

1. Inicie la sesión en la interfaz de la línea de comandos de ILOM como administrador.
2. Para agregar una cuenta de usuario de SNMP v3 de sólo lectura, escriba el comando siguiente:

```
create /SP/services/snmp/users/nombreusuario authenticationpassword=
contraseña
```

▼ Edición de una cuenta de usuario de SNMP mediante la línea de comandos

1. Inicie la sesión en la interfaz de la línea de comandos de ILOM como administrador.
2. Para editar una cuenta de usuario de SNMP v3, escriba el comando siguiente:

```
edit /SP/services/snmp/users/nombreusuario authenticationpassword=
contraseña
```

Nota – Al modificar los parámetros de los usuarios de SNMP, debe suministrar un valor para la propiedad `authenticationpassword` aunque no esté cambiando la contraseña.

▼ Supresión de una cuenta de usuario de SNMP mediante la línea de comandos

1. Inicie la sesión en la interfaz de la línea de comandos de ILOM como administrador.
2. Para borrar una cuenta de usuario de SNMP v3, escriba el comando siguiente:
`delete /SP/services/snmp/users/nombreusuario`

▼ Adición o edición de una comunidad SNMP mediante la línea de comandos

1. Inicie la sesión en la interfaz de la línea de comandos de ILOM como administrador.
2. Para agregar una comunidad SNMP v1/v2c, escriba el siguiente comando:
`create /SP/services/snmp/communities/nombrecomunidad`

▼ Supresión de una comunidad SNMP mediante la línea de comandos

1. Inicie la sesión en la interfaz de la línea de comandos de ILOM como administrador.
2. Para borrar una comunidad SNMP v1/v2c, escriba el siguiente comando:
`delete /SP/services/snmp/communities/nombrecomunidad`

Destinos, propiedades y valores

Éstos son los destinos, propiedades y valores válidos para las cuentas de usuario de SNMP.

TABLA 10-1 Destinos, propiedades y valores de las cuentas de usuario de SNMP

Destino	Propiedad	Valor	Valor predeterminado
/SP/services/snmp/ communities/ nombrecomunidad	permissions	ro rw	ro
/SP/services/snmp/users/ nombreusuario	authenticationprotocol	MD5 SHA	MD5
	authenticationpassword*	<cadena>	(cadena nula)
	permisos	ro rw	ro
	privacyprotocol	none DES	none
	privacypassword*	<cadena>	(cadena nula)
/SP/services/snmp	engineid = none	<cadena>	(cadena nula)
	port = 161	<entero>	161
	sets = enabled	enabled disabled	disabled
	v1 = disabled	enabled disabled	disabled
	v2c = disabled	enabled disabled	disabled
	v3 = disabled	enabled disabled	enabled

* Si la propiedad `privacyprotocol` tiene un valor distinto de `none`, es preciso definir un valor para `privacypassword`.
Es necesario proporcionar un valor para `authenticationpassword` al crear o modificar usuarios (sólo en SNMP v3).

Por ejemplo, para cambiar el valor de `privacyprotocol` del usuario `a1` por el valor `DES`, debería escribir:

```
-> set /SP/services/snmp/users/a1 privacyprotocol=DES  
privacypassword=contraseña authenticationprotocol=SHA  
authenticationpassword=contraseña
```

Los cambios no tendrían validez si sólo escribiera:

```
-> set /SP/services/snmp/users/a1 privacyprotocol=DES
```

Nota – Puede cambiar los permisos de los usuarios de SNMP sin necesidad de restablecer las propiedades de privacidad y autenticación.

▼ Configuración de los destinos decapturas de eventos de SNMP mediante la línea de comandos

Siga este procedimiento para configurar los destinos a los que se enviarán las capturas de eventos de SNMP.

1. **Inicie la sesión en la interfaz de la línea de comandos de ILOM como administrador.**
2. **Escriba el comando `show` para ver la configuración actual de la regla de alerta.**
Por ejemplo:

```
-> show
/SP/alertmgmt/rules/1
Targets:
Properties:
  community_or_username = public
  destination = 0.0.0.0
  level = disable
  snmp_version = 1
  type = snmptrap
Commands:
  cd
  set
  show
```

3. **Vaya al directorio `/SP/alertmgmt/rules/snmp`. Escriba:**
`-> cd /SP/alertmgmt/rules/snmp`
4. **Elija la regla (del destino 1 al 15) para la que quiera configurar el destino de los eventos de SNMP y sitúese en ese directorio.**

Por ejemplo:

```
-> cd 4
```

5. **Una vez en el directorio de esa regla, escriba el comando `set` para cambiar las propiedades de la regla.**

Por ejemplo:

```
-> set type=snmptrap level=critical destination=direcciónIP  
snmp_version=2c community_or_username=public
```

Administración de cuentas de usuario de SNMP mediante la interfaz web

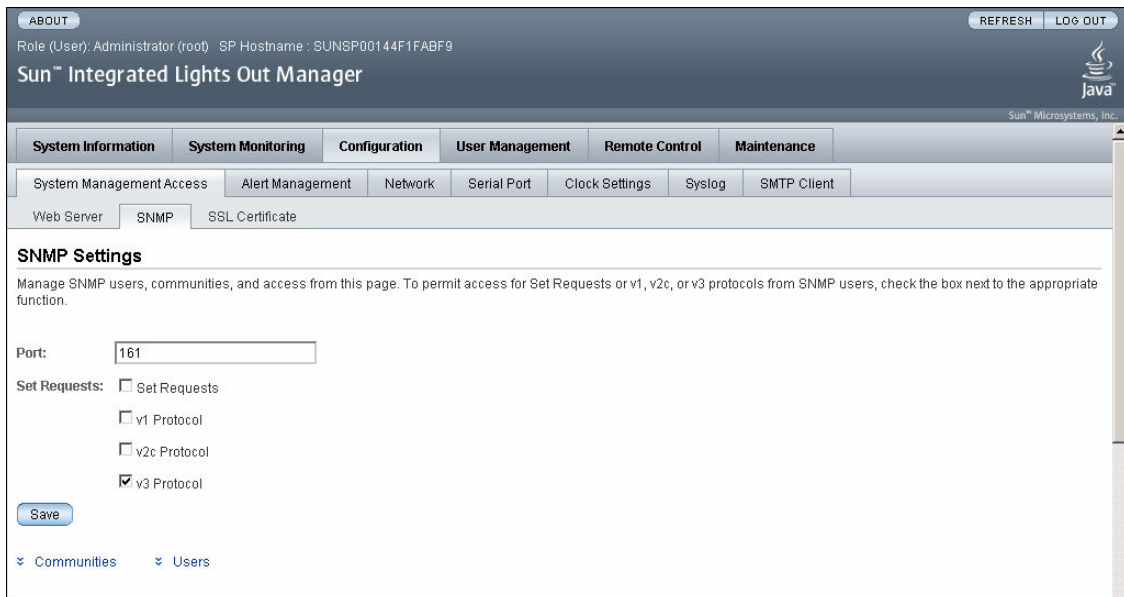
En esta sección se explica la forma de usar la interfaz web de ILOM para administrar usuarios y comunidades de SNMP.

▼ Configuración de SNMP mediante la interfaz web

Siga este procedimiento para configurar los valores de SNMP:

- 1. Inicie la sesión de ILOM como administrador para abrir la interfaz web.**
Sólo podrá modificar la configuración de SNMP si inicia la sesión de ILOM con privilegios de administrador.
- 2. Seleccione Configuration (configuración) --> System Management Access (acceso a la administración del sistema) --> SNMP.**
Se abre la página SNMP Settings (configuración de SNMP).

FIGURA 10-1 Página de configuración de SNMP



3. Escriba el número de puerto en el campo Port.
4. Seleccione o quite la marca de selección de la casilla Set Requests (establecer peticiones) para habilitar o inhabilitar esa opción.
Si inhabilita Set Requests, todos los objetos de SNMP serán de sólo lectura.
5. Seleccione una de las casillas para habilitar SNMP v1, v2c o v3.
SNMP v3 es la versión habilitada de forma predeterminada. Puede habilitar o inhabilitar las versiones v1, v2c y v3 del protocolo.
6. Haga clic en Save (guardar).

Nota – En la parte inferior de la página, también puede agregar, editar o borrar comunidades o usuarios de SNMP como se ilustra en la [FIGURA 10-2](#).

FIGURA 10-2 Comunidades y usuarios de SNMP

The screenshot displays two configuration sections: 'SNMP Communities' and 'SNMP Users'. Each section has 'Add', 'Edit', and 'Delete' buttons. Below the buttons are tables listing the configured items.

SNMP Communities Table:

Community Name	Permission
private	rw
public	ro

SNMP Users Table:

User Name	Authentication Protocol	Permission	Privacy Protocol
789	MD5	ro	DES

▼ Adición o edición de una cuenta de usuario de SNMP mediante la interfaz web

Siga este procedimiento para agregar o editar una cuenta de usuario de SNMP v3.

1. Inicie la sesión de ILOM como administrador para abrir la interfaz web.

Sólo podrá agregar usuarios o cuentas de usuario de SNMP si abre la sesión de ILOM con privilegios de administrador.

2. **Seleccione Configuration (configuración) --> System Management Access (acceso a la administración del sistema) --> SNMP.**

Se abre la página SNMP Settings (configuración de SNMP).

3. **Haga clic en el vínculo Users (usuarios) o desplácese hasta la lista SNMP Users (usuarios de SNMP).**

4. **Haga clic en los botones Add (agregar) o Edit (editar) de la lista de usuarios de SNMP.**

Se abre el cuadro de diálogo de adición o edición tal y como se ilustra en la [FIGURA 10-3](#).

FIGURA 10-3 Cuadro de diálogo de adición de usuarios de SNMP

https://129.148.97.113 - Mozilla Firefox

Sun™ Integrated Lights Out Manager

To grant an SNMP user access to ILOM, enter the SNMP user account details here. Click Save to add the user.

User Name:

Authentication Protocol: MD5

Authentication Password:

Confirm Password:

Permission: ro

Privacy Protocol: DES

Privacy Password:

Confirm Password:

Save Close

Done 129.148.97.113

5. **Escriba un nombre en el campo User Name (nombre de usuario).**

El nombre de usuario puede estar formado por 35 caracteres como máximo. Debe empezar por un carácter alfabético y no puede contener espacios.

6. **Seleccione MD5 (Message Digest 5) o SHA (Secure Hash Algorithm) como protocolo de autenticación en la lista Authentication Protocol.**

7. **Escriba una contraseña en el campo Authentication Password (contraseña de autenticación).**

La contraseña debe contener entre 8 y 16 caracteres, sin espacios ni signos de dos puntos. Existe diferencia entre mayúsculas y minúsculas.

8. **Vuelva a escribir la contraseña de autenticación en el campo Confirm Password (confirmar contraseña).**
9. **Seleccione ro (sólo lectura) o rw (lectura y escritura) en la lista desplegable Permissions (permisos).**
10. **Seleccione DES o None (ninguno) como protocolo de privacidad en la lista Privacy Protocol.**
11. **Escriba una contraseña en el campo Privacy Password (contraseña de privacidad).**
La contraseña debe contener entre 8 y 16 caracteres, sin espacios ni signos de dos puntos. Existe diferencia entre mayúsculas y minúsculas.
12. **Vuelva a escribir la contraseña en el campo Confirm Password (confirmar contraseña).**
13. **Haga clic en Save (guardar).**

▼ **Supresión de una cuenta de usuario de SNMP mediante la interfaz web**

Siga este procedimiento para borrar una cuenta de usuario de SNMP v3.

1. **Inicie la sesión de ILOM como administrador para abrir la interfaz web.**
Sólo podrá modificar la configuración de SNMP si abre la sesión en cuentas con privilegios de administrador.
2. **Seleccione Configuration (configuración) --> System Management Access (acceso a la administración del sistema) --> SNMP.**
Se abre la página SNMP Settings (configuración de SNMP).
3. **Haga clic en el vínculo Users (usuarios) o desplácese hasta la lista SNMP Users (usuarios de SNMP).**
4. **Seleccione el botón de la cuenta de usuario que quiera suprimir.**
5. **Haga clic en el botón Delete (borrar) de la lista SNMP Users.**
Se abre un cuadro de diálogo de confirmación.
6. **Haga clic en OK (aceptar) para borrar la cuenta.**

▼ Adición o edición de una comunidad SNMP mediante la interfaz web

Siga este procedimiento para agregar o editar una comunidad SNMP v1 o v2c.

- 1. Inicie la sesión de ILOM como administrador para abrir la interfaz web.**
Sólo podrá agregar o editar comunidades de SNMP si abre la sesión en cuentas con privilegios de administrador.
- 2. Seleccione Configuration (configuración) --> System Management Access (acceso a la administración del sistema) --> SNMP.**
Se abre la página SNMP Settings (configuración de SNMP).
- 3. Haga clic en el vínculo Communities (comunidades) o desplácese hasta la lista Communities.**
- 4. Haga clic en el botón Add (agregar) o Edit (editar) de la lista SNMP Communities.**
Se abre el cuadro de diálogo de adición o edición.
- 5. Escriba el nombre de la comunidad en el campo Community Name.**
El nombre de comunidad puede estar formado por 35 caracteres como máximo. Debe empezar por un carácter alfabético y no puede contener ningún espacio.
- 6. Seleccione ro (sólo lectura) o rw (lectura y escritura) en la lista desplegable Permissions (permisos).**
- 7. Haga clic en Save (guardar).**

▼ Supresión de una comunidad SNMP mediante la interfaz web

Siga este procedimiento para suprimir una comunidad de SNMP v1 o v2c:

- 1. Inicie la sesión de ILOM como administrador para abrir la interfaz web.**
Sólo podrá borrar comunidades SNMP si abre la sesión en cuentas con privilegios de administrador.
- 2. Seleccione Configuration (configuración) --> System Management Access (acceso a la administración del sistema) --> SNMP.**
Se abre la página SNMP Settings (configuración de SNMP).
- 3. Haga clic en el vínculo Communities (comunidades) o desplácese hasta la lista Communities.**

4. **Seleccione el botón de opción de la comunidad que quiera suprimir.**
5. **Haga clic en Delete (borrar).**
Se abrirá un cuadro de diálogo de confirmación.
6. **Haga clic en OK para suprimir la comunidad SNMP.**

▼ Configuración de los destinos de capturas de eventos de SNMP mediante la interfaz web

Siga este procedimiento para configurar los destinos a los que se enviarán las capturas de eventos de SNMP.

1. **Inicie la sesión de ILOM como administrador para abrir la interfaz web.**
Sólo podrá configurar los destinos de eventos de SNMP si abre la sesión en cuentas con privilegios de administrador.
2. **Seleccione Configuration (configuración) --> Alert Management (administración de alertas).**
Se abre la página de administración de alertas. En ella se muestra la tabla de alertas configuradas.
3. **Seleccione Edit (editar) en la lista desplegable Actions (acciones).**
Se abre el cuadro de diálogo Create or Modify Alert (creación o modificación de alertas).
4. **Seleccione el nivel de la alerta en la lista desplegable.**
5. **En la lista desplegable Type (tipo), elija SNMP Trap (captura de eventos de SNMP).**
6. **Especifique la dirección IP del destino de la alerta, la versión de SNMP y la comunidad o el nombre de usuario de SNMP.**
7. **Haga clic en Save (guardar) para que los cambios tengan efecto.**

Ejemplos de SNMP

En esta sección se incluyen varios ejemplos de uso de `net-snmp` para consultar al agente SNMP de un SP donde se ejecuta ILOM.

Para empezar, descargue e instale la última versión (la 5.2.1 o superior) de `net-snmp` que funcione con el sistema operativo de la estación de administración:

<http://net-snmp.sourceforge.net/>

`net-snmp` instala todas las MIB estándar (SNMPv2-MIB, SNMP-FRAMEWORK-MIB y ENTITY-MIB) admitidas por ILOM. Debe descargar los archivos `SUN-PLATFORM-MIB.mib`, `SUN-ILOM-CONTROL-MIB.mib`, `SUN-HW-TRAP-MIB.mib` y `SUN-ILOM-PET-MIB.mib` y situarlos en el directorio donde las herramientas de `net-snmp` carguen las MIB. Consulte la siguiente URL para obtener más información:

http://net-snmp.sourceforge.net/wiki/index.php/TUT:Using_and_loading_MIBS

▼ Visualización y configuración de los valores de SNMP

Configure el SP o el CMM según lo descrito en las secciones anteriores y luego siga este procedimiento para ver y configurar los parámetros de SNMP.

1. **Sitúese en el directorio** `/SP/services/snmp` **escribiendo:**
-> `cd /SP/services/snmp`
2. **Una vez en ese directorio, escriba el comando** `show` **para ver la configuración de SNMP.**

```
-> show
/SP/services/snmp
Targets:
  communities
  users
Properties:
  engineid = none
  port = 161
  sets = disabled
  v1 = disabled
  v2c = disabled
  v3 = enabled
Commands:
  cd
  set
  show
```

3. Configure los valores de SNMP.

Por ejemplo:

- Configure v2c con el valor enabled escribiendo:
-> **set v2c=enabled**
- Configure sets con el valor enabled escribiendo:
-> **set sets=enabled**

4. Vea la lista de comunidades escribiendo:

-> **show communities**

```
-> show communities
/SP/services/snmp/communities
Targets:
  public
Properties:
Commands:
  cd
  create
  delete
  show
```

5. Vea la lista de comunidades públicas escribiendo:

-> **show communities/public**

```
-> show communities/public
/SP/services/snmp/communities/public
Targets:
Properties:
  permission = ro
Commands:
  cd
  set
  show
```

6. Cree comunidades privadas con acceso de lectura y escritura escribiendo:

-> **create communities/private permission=rw**

▼ Obtención de información mediante los comandos `snmpget` o `snmpwalk net-snmp`

1. Escriba el comando `snmpget` para obtener información específica.

Por ejemplo:

```
$ snmpget -v 2c -c public -m ALL <ip_sp> sysObjectID.0 sysUpTime.0 sysLocation.0
SNMPv2-MIB::sysObjectID.0 =
OID:SUN-FIRE-SMI-MIB::sunBladeX8400ServerModule
SNMPv2-MIB::sysUpTime.0 = Timeticks: (17523) 0:02:55.23
SNMPv2-MIB::sysLocation.0 = STRING:
```

2. Escriba el comando `snmpwalk` si quiere obtener información sobre los componentes discretos.

Por ejemplo:

```
$ snmpwalk -v 2c -c public -m ALL <ip_sp> entPhysicalName
ENTITY-MIB::entPhysicalName.1 = STRING: /SYS
ENTITY-MIB::entPhysicalName.2 = STRING: /SYS/OK2RM
ENTITY-MIB::entPhysicalName.3 = STRING: /SYS/SERVICE
ENTITY-MIB::entPhysicalName.4 = STRING: /SYS/OK
ENTITY-MIB::entPhysicalName.5 = STRING: /SYS/LOCATE
ENTITY-MIB::entPhysicalName.6 = STRING: /SYS/LOCATE_BTN
ENTITY-MIB::entPhysicalName.7 = STRING: /SYS/POWER_BTN
ENTITY-MIB::entPhysicalName.8 = STRING: /SYS/T_AMB
ENTITY-MIB::entPhysicalName.9 = STRING: /SYS/P0
```

▼ Configuración de la información mediante `snmpset`

- Escriba el comando `snmpset` si quiere cambiar la ubicación de los dispositivos.

Por ejemplo:

```
$ snmpset -v 2c -c private -m ALL <ip_sp> sysLocation.0 s "<ubicación>"
```

Por ejemplo:

```
SNMPv2-MIB::sysLocation.0 = STRING: ILOM Dev Lab
```

▼ Recepción de capturas de eventos mediante `snmptrapd`

- Escriba el comando `snmptrapd` para recibir la información de las capturas de eventos.

Por ejemplo:

```
$ /usr/sbin/snmptrapd -m ALL -f -Lo
Ejemplo de captura de evento de SNMP:
2007-05-21 08:46:41 ban3c9sp4 [10.8.136.94]:
SNMPv2-MIB::sysUpTime.0 = Timeticks: (1418) 0:00:14.18
SNMPv2-MIB::snmpTrapOID.0 = OID:
SUN-HW-TRAP-MIB::sunHwTrapPowerSupplyError
SUN-HW-TRAP-MIB::sunHwTrapSystemIdentifier.0 = STRING:
SUN-HW-TRAP-MIB::sunHwTrapChassisId.0 = STRING:
ban6c4::0000000000 SUN-HW-TRAP-MIB::sunHwTrapProductName.0
= STRING: SUN-HW-TRAP-MIB::sunHwTrapComponentName.0 =
STRING: /PS3/FAN_ERR
SUN-HW-TRAP-MIB::sunHwTrapAdditionalInfo.0 = STRING: Predictive
Failure Asserted SUN-HW-TRAP-MIB::sunHwTrapAssocObjectId.0 =
OID: SNMPv2-SMI::zeroDotZero
```


Actualización del firmware de ILOM

El proceso de actualización del firmware de ILOM permite instalar nuevas versiones del firmware de ILOM y actualizar otros módulos de la plataforma tales como la BIOS en x64, OpenBoot PROM y el software Hypervisor en SPARC.

Este capítulo contiene las secciones siguientes:

- “Proceso de actualización del firmware” en la página 207
- “Descripción de la actualización del firmware de ILOM” en la página 208
 - “Visualización de la información de versión de ILOM mediante la línea de comandos” en la página 208
 - “Actualización del firmware de ILOM mediante la línea de comandos” en la página 209
 - “Visualización de la información de versión de ILOM mediante la interfaz web” en la página 209
 - “Actualización del firmware de ILOM mediante la interfaz web” en la página 210
 - “Reinicio del SP de ILOM” en la página 211

Proceso de actualización del firmware

Tenga en cuenta las siguientes directrices cuando actualice el firmware:



Precaución – Cierre el sistema operativo host antes de proceder a la actualización. ILOM intenta cerrar el SO de forma regular. Si no es posible, efectúa un cierre forzoso, lo que podría causar daños en el sistema de archivos.

- La actualización del firmware dura unos cinco minutos. Durante este tiempo, no debería realizarse ninguna otra operación en ILOM.

- Un fallo de la red durante la carga del archivo de firmware da como resultado la anulación del proceso. Esto hace que ILOM vuelva a arrancar con la versión que se encuentre instalada *en ese momento*.

Descripción de la actualización del firmware de ILOM

1. Descargue la nueva imagen del firmware.
2. Copie la imagen en un servidor TFTP si va a hacer la actualización mediante la interfaz de la línea de comandos o en un sistema de archivos local si va a efectuarla mediante la interfaz web.
3. Inicie la sesión como cualquier usuario con privilegios de administrador.
4. Actualice el firmware en cada procesador de servicios (SP) o módulo de supervisión del chasis (CMM) del sistema utilizando la interfaz web o la línea de comandos.
5. Una vez finalizada la actualización del firmware, el sistema vuelve a arrancar de *forma automática*.

▼ Visualización de la información de versión de ILOM mediante la línea de comandos

1. **Inicie una sesión de Secure Shell como usuario con privilegios de administrador.**
2. **En el indicador de comandos, escriba `version`.**
Aparece la información siguiente:

```
SP firmware #.#.#.#
SP firmware build number: #####
SP firmware date: Fri Apr 27 14:03:21 EDT 2007
SP filesystem version: #.#.#.#
```


▼ Actualización del firmware de ILOM mediante la línea de comandos

1. Inicie la sesión como cualquier usuario con privilegios de administrador.
2. Escriba el siguiente comando para descargar la nueva imagen del firmware de ILOM.

```
->load -source URLtftp
```

Por ejemplo:

```
-> load -source tftp://xxx.xxx.xxx.xxx/nombreadarchivo.pkg
```

```
NOTE: A firmware upgrade will cause the server and ILOM to
      be reset. It is recommended that a clean shutdown of
      the server be done prior to the upgrade procedure.
      An upgrade takes about 6 minutes to complete. ILOM
      will enter a special mode to load new firmware. No
      other tasks can be performed in ILOM until the
      firmware upgrade is complete and ILOM is reset.
```

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

```
Do you want to preserve the configuration (y/n)? y
```

```
.....
Preserving configuration. Please wait.
Done preserving configuration.
```

```
Firmware update is complete.
```

```
ILOM will now be restarted with the new firmware.
```

▼ Visualización de la información de versión de ILOM mediante la interfaz web

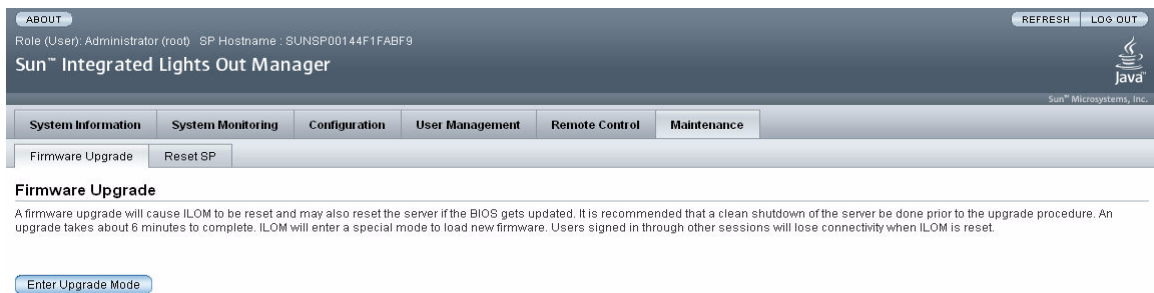
1. Inicie la sesión como cualquier usuario con privilegios de administrador.
2. Seleccione User Management (administración de usuarios) --> Version (versión).

Aparece información sobre la versión actual del firmware.

▼ Actualización del firmware de ILOM mediante la interfaz web

1. **Inicie la sesión como cualquier usuario con privilegios de administrador.**
2. **Seleccione Maintenance (mantenimiento) --> Firmware Upgrade (actualización del firmware).**
Se abre la página Firmware Upgrade (actualización del firmware).
3. **Haga clic en Enter Upgrade Mode (entrar en modo de actualización).**
Se abre un cuadro de diálogo solicitando confirmación para entrar en el modo de actualización.
4. **Haga clic en OK (aceptar) para entrar en dicho modo o en Cancel (cancelar) para abandonar el proceso.**
ILOM detiene su funcionamiento normal y se prepara para una actualización flash.
5. **Especifique la ruta de acceso al archivo de imagen de actualización de ILOM en el campo Select Image File to Upload (seleccionar archivo de imagen para cargar) o haga clic en Browse (examinar) para buscar y seleccionar el archivo.**
Pueden utilizarse archivos con las extensiones .pkg o .ima, aunque es preferible la extensión .pkg.

FIGURA 11-1 Página de actualización del firmware



6. **Haga clic en Upload (cargar) o en Cancel (cancelar) para abandonar el proceso.**
El archivo elegido se carga y se verifica para comprobar si es la imagen de actualización correcta para ese SP o CMM.
Este proceso dura alrededor de un minuto con una conexión de red rápida.

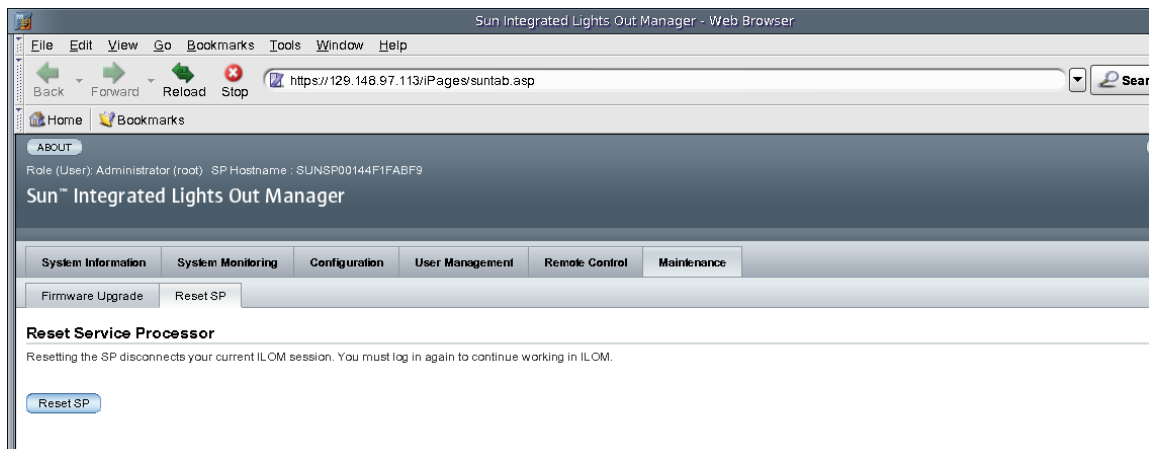
7. Cuando se abra la página Verify Firmware Image (verificar imagen de firmware), haga clic en OK.
8. Seleccione Preserve Configuration (conservar la configuración) para mantener los valores de configuración de ILOM. Si no lo hace, quedarán sustituidos por los valores predeterminados del firmware.
9. Haga clic en Start Upgrade (iniciar actualización) o en Cancel (cancelar) para abandonar el proceso.
Al iniciar la actualización, una pantalla de progreso indica que la imagen del firmware se está actualizando. Cuando este proceso alcanza el 100%, significa que la actualización ha finalizado.
Una vez finalizada la actualización, el sistema vuelve a arrancar de *forma automática*.
10. Cuando el SP o el CMM terminen de arrancar, utilice el navegador para volver a establecer la conexión con ILOM.

▼ Reinicio del SP de ILOM

Si necesita reiniciar el procesador de servicios (SP) de ILOM, puede hacerlo sin que ello afecte al SO host. No obstante, al reiniciar un SP, se desconecta la sesión de ILOM en curso y el SP no puede administrarse durante el proceso.

1. Inicie la sesión como cualquier usuario con privilegios de administrador.
2. Seleccione Maintenance (mantenimiento) --> Reset SP (reiniciar el SP).
Aparece la página Reset Service Processor (reinicio del procesador de servicios).

FIGURA 11-2 Página de reinicio del procesador de servicios



- 3. Haga clic en el botón Reset SP (reiniciar el SP) para reiniciar el procesador de servicios de ILOM.**

ILOM vuelve a arrancar y la interfaz web permanece fuera de servicio durante el proceso.

Administración remota de los servidores x64 mediante Sun ILOM Remote Console

La aplicación Remote Console de ILOM puede utilizarse con todos los servidores Sun basados en el procesador x64. Remote Console no es compatible con los servidores Sun SPARC.

Este capítulo contiene las secciones siguientes:

- “Descripción de Remote Console” en la página 214
 - “Vistas de administración de uno o varios servidores host remotos” en la página 215
 - “Requisitos de instalación” en la página 216
 - “Puertos y protocolos de comunicación en red” en la página 217
 - “Cuenta de usuario con función de administrador: autenticación de sesión obligatoria” en la página 217
- “Ejecución y configuración de ILOM para administración remota” en la página 218
 - “Conexión con la interfaz web de ILOM” en la página 218
 - “Configuración de las opciones de control remoto de ILOM mediante la interfaz web” en la página 219
- “Ejecución y configuración de Sun ILOM Remote Console para administrar servidores x64 remotos” en la página 222
 - “Ejecución de Remote Console mediante la interfaz web de ILOM” en la página 222
 - “Adición de una sesión de servidor” en la página 224
 - “Inicio, detención o reinicio de la redirección de dispositivos” en la página 224
 - “Redirección del teclado y el ratón” en la página 225
 - “Control de los modos de teclado y el envío de funciones de teclas” en la página 226
 - “Redirección de dispositivos de almacenamiento” en la página 227
 - “Salida de Sun ILOM Remote Console” en la página 228
- “Situaciones de uso de la redirección de CD y disquetes” en la página 229

Descripción de Remote Console

Sun ILOM Remote Console es una aplicación Java que puede ejecutarse desde la interfaz web de ILOM. Si utiliza Remote Console, puede redirigir y controlar de forma remota los siguientes dispositivos de un servidor host x64:

- Teclado
- Ratón
- Consola de visualización de vídeo
- Dispositivos o imágenes de almacenamiento (CD/DVD, disquete)

Sun ILOM Remote Console permite a los dispositivos del cliente local comportarse como si estuviesen directamente conectados al servidor host remoto. Por ejemplo, la función de redirección (mediante una conexión de red con el servidor remoto) permite hacer lo siguiente:

- Instalar software de la unidad de almacenamiento local en un servidor host remoto.
- Ejecutar utilidades de la línea de comandos en un servidor host remoto desde un cliente local.
- Acceder a programas basados en una interfaz gráfica y ejecutarlos en un servidor host remoto desde un cliente local.
- Configurar las funciones de un servidor con procesador x64 de forma remota desde un cliente local.
- Administrar las normas de un servidor con procesador x64 de forma remota desde un cliente local.
- Supervisar los componentes de un servidor con procesador x64 de forma remota desde un cliente local.
- Realizar, desde un cliente local, prácticamente cualquier operación de software que haría si estuviese sentado junto a un servidor host remoto basado en un procesador x64.

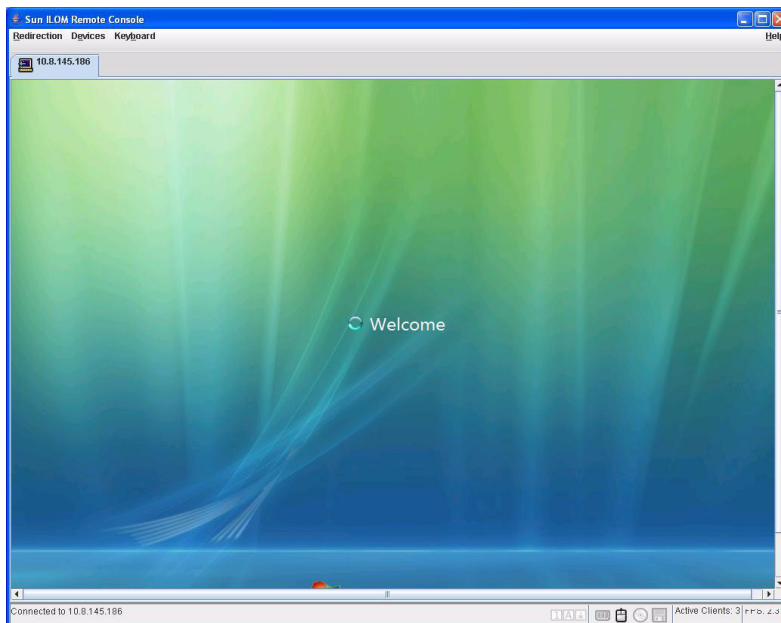
Vistas de administración de uno o varios servidores host remotos

Remote Console de ILOM permite obtener vistas de uno o varios servidores administrados. En la actualidad, las vistas de administración pueden utilizarse con todos los servidores basados en procesadores x64.

- **Vista de administración de un servidor x64 remoto:** puede ejecutar Remote Console para administrar un solo servidor host remoto desde una ventana y utilizar las funciones de control remoto del teclado, el vídeo, el ratón y los medios de almacenamiento (Keyboard, Video, Mouse, Storage - KVMS).

Nota – Las vistas de un solo servidor remoto pueden utilizarse cuando se establece conexión con la dirección IP de cualquier procesador de servicios (SP) de un servidor x64. Para obtener más información, consulte [“Ejecución y configuración de Sun ILOM Remote Console para administrar servidores x64 remotos”](#) en la página 222.

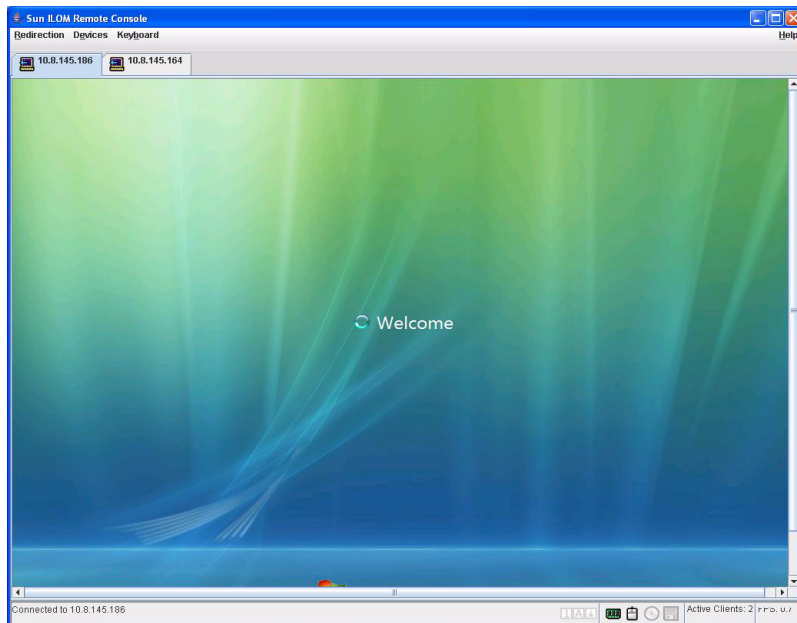
FIGURA 12-1 Vista de administración de un servidor



- **Vistas de administración de varios servidores x64 remotos:** puede ejecutar Remote Console para administrar varios servidores x64 remotos desde una ventana y utilizar las funciones de control remoto del teclado, el vídeo, el ratón y los medios de almacenamiento (Keyboard, Video, Mouse, Storage - KVMS).

Nota – Las vistas de varios servidores remotos pueden utilizarse en cualquiera de estos casos: (1) si establece conexión con la dirección IP de un módulo de supervisión del chasis (CMM) de un servidor blade x64, o (2) si agrega una nueva sesión de Remote Console para administrar otro servidor x64 remoto. Para obtener más información, consulte “Ejecución y configuración de Sun ILOM Remote Console para administrar servidores x64 remotos” en la página 222.

FIGURA 12-2 Vistas de administración de varios servidores



Requisitos de instalación

Sun ILOM Remote Console no exige la instalación de ningún componente de hardware o software suplementario. Está integrada en el software de ILOM. No obstante, para ejecutarla, es preciso tener instalado el siguiente software en el cliente local:

- **Navegador de web:** los navegadores compatibles son: Internet Explorer 6.0 o una versión posterior, Mozilla 1.7.5 o una versión posterior y Mozilla Fire Fox 1.0 o una versión posterior.
- **JRE 1.5 o una versión superior (Java 5.0 o una versión superior):** para descargar el entorno de ejecución Java 1.5, consulte la información de <http://java.com>.

Puertos y protocolos de comunicación en red

La aplicación Remote Console de ILOM se comunica con el SP del servidor host remoto utilizando los siguientes puertos y protocolos de red.

TABLA 12-1 Puertos y protocolos de red para la comunicación entre Remote Console y el SP

Puerto	Protocolo	SP: ILOM Remote Console
5120	TCP	CD
5123	TCP	Disquete
5121	TCP	Teclado y ratón
7578	TCP	Vídeo

Nota – Al administrar servidores de forma remota utilizando ILOM en el CMM, es preciso configurar el acceso a todos los puertos de Remote Console en los SP (5120, 5121, 5123 y 7578).

Cuenta de usuario con función de administrador: autenticación de sesión obligatoria

Para ejecutar Sun ILOM Remote Console desde la interfaz web de ILOM, es necesario iniciar la sesión con una cuenta de administrador (nombre de usuario y contraseña para la función Administrator).

- Si ha iniciado la sesión en ILOM mediante una *cuenta con función de operador* e intenta ejecutar Remote Console, ILOM le pedirá que abra la sesión con una cuenta de administrador válida desde el cuadro de diálogo Login.
- Si ha iniciado la sesión de ILOM mediante una *cuenta con función de administrador* y ha ejecutado Remote Console, aparecerá automáticamente la página de redirección de Sun ILOM Remote Console. No obstante, Remote Console le pedirá que vuelva a iniciar la sesión cada vez que detenga, inicie o reinicie la redirección.

Nota – Si la función Single Sign On (SSO) está inhabilitada en ILOM, los usuarios con privilegios de administrador recibirán un mensaje indicándoles que vuelvan a iniciar la sesión de ILOM utilizando el cuadro de diálogo Login. Para obtener más información sobre la función SSO, consulte [“Single Sign On” en la página 71](#).

Ejecución y configuración de ILOM para administración remota

Antes de ejecutar Remote Console, es preciso ejecutar la interfaz web de ILOM y configurar la aplicación para realizar funciones de administración remota.

- **Conexión con la interfaz web de ILOM:** debe establecer conexión con la interfaz web de ILOM del servidor (SP o CMM) que quiera administrar de forma remota. Para obtener instrucciones al respecto, consulte [“Conexión con la interfaz web de ILOM” en la página 218](#).
- **Configuración de las opciones de control remoto de ILOM:** antes de administrar un servidor Sun x64 de forma remota con Remote Console, debe configurar los parámetros de ILOM para administración remota: *redirección de la consola*, *modo de ratón admitido*, *estados de alimentación del host remoto* y *pruebas de diagnóstico del PC al encendido*. Para obtener más información, consulte [“Configuración de las opciones de control remoto de ILOM mediante la interfaz web” en la página 219](#).

Nota – Normalmente, configurará las opciones de administración remota una vez dentro de ILOM, a excepción de los estados de alimentación del host remoto.

▼ Conexión con la interfaz web de ILOM

Siga este procedimiento para conectar con la interfaz web de ILOM:

1. **Abra un navegador de web y especifique la dirección IP del SP del servidor x64 o el CMM x64 que quiera administrar de forma remota. A continuación, pulse Intro.**

Aparece la pantalla Login (inicio de sesión) de ILOM.

FIGURA 12-3 Página de inicio de sesión de ILOM



2. En la página de inicio de sesión, especifique el nombre de usuario y la contraseña de una cuenta de administrador válida y pulse Intro.

Sugerencia – La cuenta con función de administrador preconfigurada en ILOM es root/ changeme. Si precisa más información sobre esta cuenta, consulte [“Cuentas de administrador de ILOM preconfiguradas”](#) en la página 68.

▼ Configuración de las opciones de control remoto de ILOM mediante la interfaz web

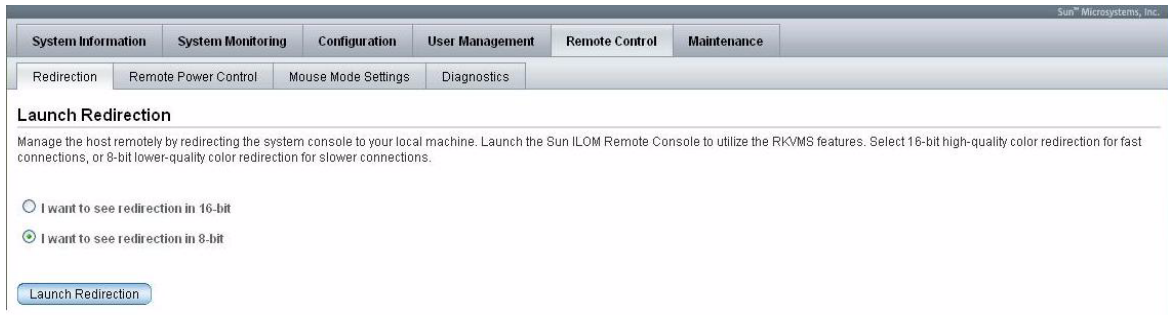
Requisito previo:

- Haber establecido conexión con la interfaz web de ILOM del servidor host remoto (SP o CMM). Para obtener instrucciones al respecto, consulte [“Conexión con la interfaz web de ILOM”](#) en la página 218.

Siga este procedimiento para configurar las opciones de ILOM destinadas a la administración remota:

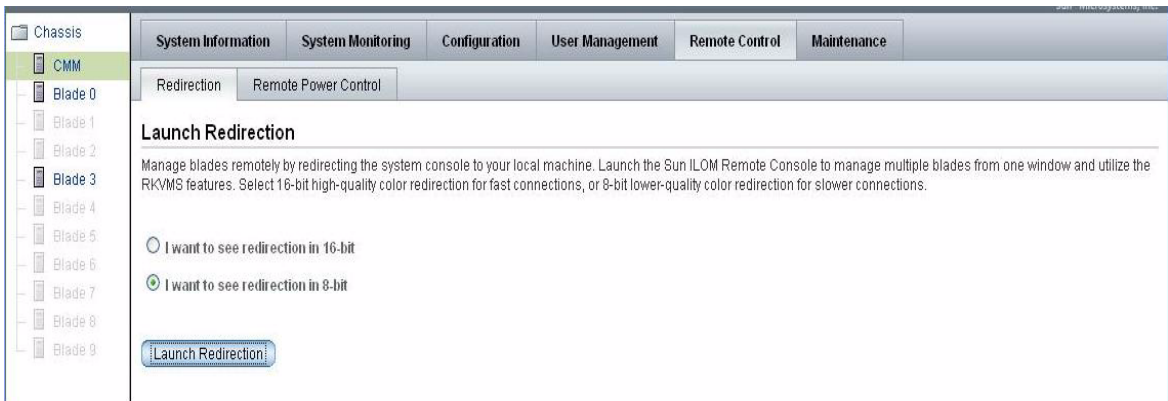
1. Haga clic en la ficha **Remote Control (control remoto)** de la interfaz web de ILOM en el CMM o el SP.
 - **Para la interfaz web de ILOM en el SP.** Se abre la página Remote Control con cuatro fichas secundarias: *Redirection*, *Remote Power Control*, *Mouse Mode Settings* y *Diagnostics* (redirección, control remoto de la alimentación, configuración del modo de ratón y diagnóstico).

FIGURA 12-4 Ficha de control remoto de ILOM en el SP



- para la interfaz web de ILOM en el CMM. Se abre la página Remote Control con dos fichas secundarias: *Redirection* y *Remote Power Control* (redirección y control remoto de la alimentación).

FIGURA 12-5 Ficha de control remoto de ILOM en el CMM



Nota – Como alternativa, puede configurar las opciones de control remoto de cada SP de servidor asociado al CMM. Para acceder a los valores de control remoto de los demás SP del servidor que aparezcan en la interfaz web de ILOM en el CMM, haga clic en el SP situado en el panel izquierdo de la página y luego en la ficha Remote Control del panel derecho.

2. En la página Remote Control, configure las siguientes opciones de control remoto.

<p>Opciones de redirección de la consola</p>	<p>Haga clic en la ficha Redirection (redirección) y seleccione una de las siguientes opciones de redirección de la consola:</p> <ul style="list-style-type: none"> • 8-bit. Redirección de 8 bits para conexiones de red más lentas. • 16-bit. Redirección de 16 bits para conexiones de red más rápidas.
<p>Configuración del modo de ratón <i>(sólo para el SP)</i></p>	<p>Haga clic en la ficha Mouse Mode Settings (configuración del modo de ratón) y seleccione uno de los modos siguientes:</p> <ul style="list-style-type: none"> • Absolute. Seleccione el modo absoluto para tener el mejor rendimiento cuando utilice Solaris o sistemas operativos Windows. Es el modo predeterminado. • Relative. Seleccione el modo relativo cuando utilice el sistema operativo Linux. No todos los sistemas operativos Linux admiten el modo absoluto.
<p>Configuración del estado de la alimentación</p>	<p>Haga clic en la ficha Remote Power Control (control remoto de la alimentación) para seleccionar uno de los siguientes estados del servidor host:</p> <ul style="list-style-type: none"> • Immediate Power Off. Seleccione la opción de apagado inmediato para desactivar al instante la alimentación del servidor host remoto. • Graceful Shutdown and Power Off. Seleccione la opción de cierre normal y apagado para tratar de cerrar la sesión del sistema operativo de manera regular antes de apagar el servidor remoto. • Power On. Utilice la opción de encendido para activar la alimentación normal del servidor remoto. Es el valor predeterminado. • Power Cycle. Seleccione la opción de apagado y encendido para desactivar la alimentación del servidor remoto y volverla a activar. • Reset. Seleccione la opción reiniciar para rearrancar el servidor remoto de forma inmediata.
<p>Opciones de diagnóstico de PC-Check <i>(sólo para el SP)</i></p> <p>Nota: la función PC-Check sólo puede utilizarse en los sistemas Sun Blade de la serie 8000.</p>	<p>Haga clic en la ficha Diagnostics (diagnóstico) para activar o desactivar las siguientes opciones de comprobación del sistema de PC-Check:</p> <ul style="list-style-type: none"> • Disabled. Utilice la opción inhabilitado si no quiere ejecutar las pruebas de diagnóstico de PC-Check al iniciar un servidor host remoto. • Enabled. Seleccione la opción habilitado si quiere ejecutar las pruebas de diagnóstico básicas de PC-Check al iniciar el servidor remoto. La ejecución de las pruebas básicas suele tardar unos 3 minutos. • Extended. Seleccione la opción de ejecución ampliada si quiere realizar las pruebas de diagnóstico de PC-Check completas al iniciar el servidor remoto. La versión ampliada de las pruebas suele tardar unos 30 minutos en ejecutarse.

Ejecución y configuración de Sun ILOM Remote Console para administrar servidores x64 remotos

Para administrar un servidor x64 de forma remota, es preciso ejecutar la aplicación Remote Console de ILOM y configurar las funciones de la consola necesarias para realizar el control remoto. Para obtener más información, consulte los siguientes procedimientos:

- [“Ejecución de Remote Console mediante la interfaz web de ILOM”](#) en la página 222
- [“Adición de una sesión de servidor”](#) en la página 224
- [“Inicio, detención o reinicio de la redirección de dispositivos”](#) en la página 224
- [“Redirección del teclado y el ratón”](#) en la página 225
- [“Control de los modos de teclado y el envío de funciones de teclas”](#) en la página 226
- [“Redirección de dispositivos de almacenamiento”](#) en la página 227
- [“Inicio, detención o reinicio de la redirección de dispositivos”](#) en la página 224
- [“Salida de Sun ILOM Remote Console”](#) en la página 228

▼ Ejecución de Remote Console mediante la interfaz web de ILOM

Requisitos previos:

- Haber establecido conexión con la interfaz web de ILOM (SP o CMM). Para obtener instrucciones al respecto, consulte [“Conexión con la interfaz web de ILOM”](#) en la página 218.
- Haber configurado las opciones de control remoto de ILOM. Para obtener instrucciones al respecto, consulte [“Configuración de las opciones de control remoto de ILOM mediante la interfaz web”](#) en la página 219.

Para ejecutar Sun ILOM Remote Console desde la interfaz web de ILOM, siga este procedimiento:

1. **Haga clic en la ficha Remote Control (control remoto) de la interfaz web de ILOM correspondiente a un SP del CMM o el servidor.**

Se abre la página Remote Console.

2. Dentro de la página Remote Console, haga clic en la ficha Redirection (redirección).

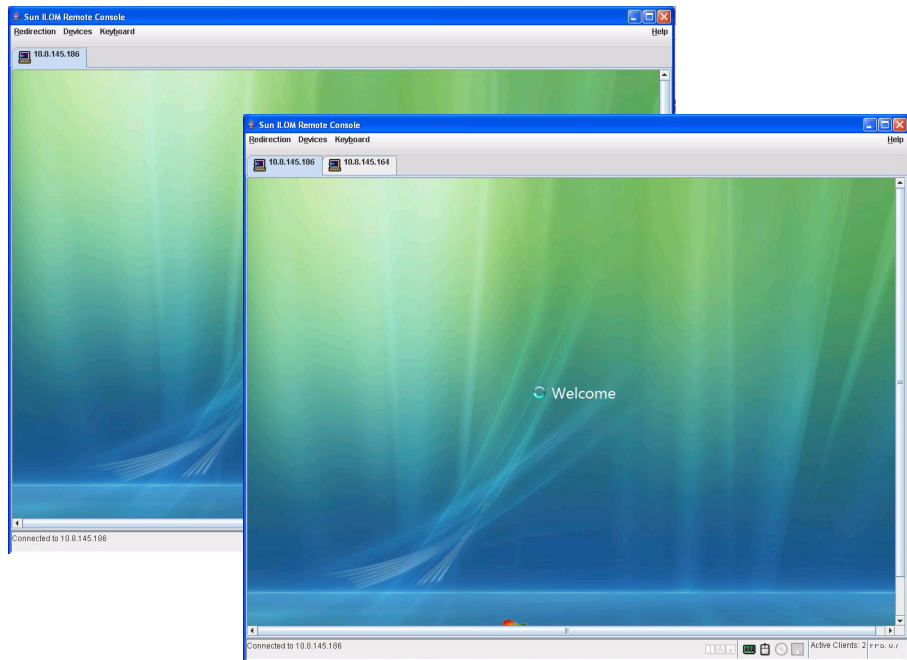
Se abre la página de redirección.

3. En la página Redirection, haga clic en Launch Redirection (ejecutar redirección).

Puede que aparezca un mensaje de advertencia donde se indica que el nombre del sitio no coincide con el nombre del certificado. Si aparece este mensaje, haga clic en Run (ejecutar) para proseguir.

Se abre la ventana de Sun ILOM Remote Console. Si se ha conectado al SP de un servidor x64, sólo aparecerá la ficha de una sesión de servidor. Si se ha conectado a un CMM x64, pueden aparecer varias fichas de sesión (tantas como servidores haya en el chasis).

FIGURA 12-6 Sun ILOM Remote Console



Nota – Si procede, también puede ejecutar Remote Console por cada SP que aparezca en la interfaz web de ILOM en el CMM. Para ejecutar la consola remota de ILOM correspondiente a un servidor incluido en un CMM, haga clic en el SP del servidor situado en el panel izquierdo de la página y luego haga clic en Remote Console --> Redirection --> Launch Redirection.

▼ Adición de una sesión de servidor

Requisito previo:

- Haber establecido conexión con Sun ILOM Remote Console. Para obtener instrucciones al respecto, consulte [“Ejecución de Remote Console mediante la interfaz web de ILOM” en la página 222.](#)

Siga este procedimiento para agregar una nueva sesión de servidor a Remote Console de ILOM:

1. **En la ventana Sun ILOM Remote Console, seleccione Redirection (redirección) --> New Session (sesión nueva).**

Se abre el cuadro de diálogo New Session Creation (creación de una sesión nueva).

2. **En el cuadro de diálogo New Session Creation, escriba la dirección IP del SP de un servidor host x64 remoto y haga clic en OK (aceptar).**

Se abre el cuadro de diálogo Login (inicio de sesión).

3. **En el cuadro de diálogo de inicio de sesión, escriba el nombre de usuario y la contraseña de una cuenta de administrador.**

A las fichas de la página Sun ILOM Remote Console se agregará la ficha de sesión correspondiente al servidor remoto recién incorporado.

▼ Inicio, detención o reinicio de la redirección de dispositivos

Requisito previo:

- Haber establecido conexión con Sun ILOM Remote Console. Para obtener instrucciones al respecto, consulte [“Ejecución de Remote Console mediante la interfaz web de ILOM” en la página 222.](#)

Siga estos pasos para iniciar, detener o reiniciar la redirección de los dispositivos:

1. **En la ventana Sun ILOM Remote Console, haga clic en el menú Redirection (redirección).**

2. En el menú Redirection puede especificar cualquiera de las siguientes opciones:

Start Redirection (iniciar redirección)	Esta opción se utiliza para habilitar la redirección de los dispositivos. Start Redirection está activada de forma predeterminada.
Restart Redirection (reiniciar redirección)	Esta opción permite detener y volver a iniciar la redirección de los dispositivos. Normalmente se utiliza cuando sigue establecido un proceso de redirección válido.
Stop Redirection (detener redirección)	Esta opción se utiliza para inhabilitar la redirección de los dispositivos.

Aparece un mensaje solicitando confirmación para cambiar la configuración de redirección.

3. En la ventana de confirmación, haga clic en Yes (sí) para continuar o en No para cancelar la operación.

▼ Redirección del teclado y el ratón

Requisito previo:

- Haber establecido conexión con Sun ILOM Remote Console. Para obtener instrucciones al respecto, consulte [“Ejecución de Remote Console mediante la interfaz web de ILOM” en la página 222.](#)

Siga este procedimiento para redirigir el teclado y el ratón de un servidor host remoto a un sistema cliente local:

1. En la ventana Sun ILOM Remote Console, haga lo siguiente:

- a. Seleccione Devices (dispositivos) --> Mouse (ratón) para habilitar o inhabilitar la redirección del ratón.**

La casilla Enable (habilitada) está seleccionada de manera predeterminada.

- b. Seleccione Devices (dispositivos) --> Keyboard (teclado) para habilitar o inhabilitar la redirección del teclado.**

La casilla Enable (habilitada) está seleccionada de manera predeterminada.

▼ Control de los modos de teclado y el envío de funciones de teclas

Requisito previo:

- Haber establecido conexión con Sun ILOM Remote Console. Para obtener instrucciones al respecto, consulte [“Ejecución de Remote Console mediante la interfaz web de ILOM” en la página 222.](#)

Siga este procedimiento para controlar los modos del teclado y el envío de funciones correspondientes a determinadas teclas:

1. En la ventana Sun ILOM Remote Console, haga clic en el menú **Keyboard (teclado)**.
2. En el menú de teclado puede especificar cualquiera de las siguientes opciones:

Auto-keybreak Mode (modo de interrupción automática del teclado)	Se utiliza para enviar una interrupción después de presionar cada tecla. Esta opción es útil para resolver problemas del teclado en conexiones de red lentas. El modo Auto-keybreak está habilitado de forma predeterminada.
Stateful Key Locking (bloqueo del teclado con estado)	Utilice esta opción si el sistema cliente usa este tipo de bloqueo de teclas (Solaris con XSun, OSX). Stateful Key Locking se aplica a estos tres tipos de teclas: Bloqueo de mayúsculas, Bloqueo de números, Bloqueo del desplazamiento.
Left Alt Key (tecla Alt izquierda)	Seleccione esta opción para activar o desactivar la tecla Alt izquierda.
Right Alt Key (tecla Alt derecha)	Seleccione esta opción para activar o desactivar la tecla Alt derecha en teclados que no sean estadounidenses. Si se habilita, esta opción permite escribir el tercer carácter de las teclas. Proporciona la misma funcionalidad que la tecla Alt Gr.
F10	Utilice esta opción para aplicar la tecla de función F10 (normalmente utilizada con la BIOS).
Control Alt Delete (Control Alt Suprimir)	Seleccione esta opción para enviar la secuencia de teclas Control-Alt-Supr.
Control Space (Control Espacio)	Utilice esta opción para enviar una secuencia Control-Espacio que habilite la introducción de datos en el host remoto.
Caps Lock (bloqueo de mayúsculas)	Utilice esta opción para enviar la función Bloq Mayús a fin de habilitar la introducción de datos con teclados rusos y griegos.

▼ Redirección de dispositivos de almacenamiento

Requisitos previos:

- Haber establecido conexión con Sun ILOM Remote Console. Para obtener instrucciones al respecto, consulte [“Ejecución de Remote Console mediante la interfaz web de ILOM”](#) en la página 222.
- Si se utilizan sistemas cliente Solaris, es preciso realizar el siguiente procedimiento antes de redirigir los dispositivos de almacenamiento:
 - Si está habilitada la aplicación Volume Manager, es preciso inhabilitarla.
 - Asignar privilegios de root sobre el procesador donde se ejecute Sun ILOM Remote Console introduciendo estos comandos:

```
su to root

ppriv -s +file_dac_read pid_javarconsole
```
- Para obtener más información, consulte [“Situaciones de uso de la redirección de CD y disquetes”](#) en la página 229.

Siga este procedimiento para redirigir un dispositivo de almacenamiento o una imagen ISO:

1. En la ventana Sun ILOM Remote Console, seleccione el menú **Devices (dispositivos)**.
2. En el menú de dispositivos, haga lo siguiente:
 - a. **Habilite la opción de dispositivo de almacenamiento o imagen apropiada:**

CD-ROM	Seleccione esta opción para habilitar el dispositivo de CD local. Este valor hace que la unidad de CD-ROM local se comporte como si estuviese directamente conectada al servidor host remoto.
Floppy (disquete)	Seleccione esta opción para habilitar la unidad de disquete local. Este valor hace que la unidad de disquete local se comporte como si estuviese directamente conectada al servidor host remoto.
CD-ROM Image (imagen de CD-ROM)	Esta opción se utiliza para especificar la ubicación de una imagen de CD-ROM situada en el cliente local o en un espacio compartido de la red.
Floppy Image (imagen de disquete)	Esta opción se utiliza para especificar la ubicación de una imagen de disquete situada en el cliente local o en un espacio compartido de la red.

Sugerencia – Sólo hay dos opciones para la redirección de CD/DVD. Puede redirigir una unidad de CD-ROM o una imagen de CD-ROM.

Sugerencia – Si va a instalar software desde un CD/DVD de distribución, introduzca el CD/DVD en la unidad redirigida y seleccione la unidad de CD-ROM.

Sugerencia – Si va a instalar software desde una imagen ISO, coloque la imagen en el cliente local o en un sistema de archivos compartido de la red y seleccione la opción CD-ROM image.

Se abre un cuadro de diálogo solicitando la ubicación de la unidad de almacenamiento o el archivo de imagen.

b. Para indicar dónde se encuentra la unidad de almacenamiento o el archivo de imagen, realice uno de estos procedimientos:

- En el cuadro de diálogo Drive Selection (selección de unidad), elija o escriba la ubicación de una unidad de CD y haga clic en OK (aceptar).
o
- En el cuadro de diálogo File Open (abrir archivo), busque la ubicación de la imagen y haga clic en OK.

3. Para volver a utilizar esta configuración de los dispositivos de almacenamiento en el host en el futuro, haga clic en Devices (dispositivos) --> Save as Host Default (guardar como predeterminado del host).

▼ Salida de Sun ILOM Remote Console

Siga este procedimiento para salir de Remote Console y cerrar cualquier sesión de servidor remoto que haya quedado abierta:

1. En la ventana Sun ILOM Remote Console, seleccione el menú **Redirection**.
2. Seleccione la opción **Quit (salir)** del menú.

Situaciones de uso de la redirección de CD y disquetes

Utilice la [TABLA 12-2](#) como referencia para saber cómo se comporta la función de redirección de unidades de CD o disquete en distintas situaciones durante una sesión de Remote Console.

TABLA 12-2 Funcionamiento de Remote Console con unidades de DVD y disquete

Caso	Estado	DVD visto por el host remoto	Disquete visto por el host remoto
1	No se ha iniciado la aplicación Remote Console, o se ha iniciado la aplicación pero no se ha iniciado la redirección de la unidad de DVD o disquete.	El dispositivo de DVD está presente. ILOM envía una indicación de ausencia de medio de almacenamiento al host cuando éste pregunta.	El dispositivo de disquete está presente. ILOM envía una indicación de ausencia de medio de almacenamiento al host cuando éste pregunta.
2	Se ha iniciado la aplicación Remote Console pero no hay ningún medio de almacenamiento en la unidad.	El dispositivo de DVD está presente. Cuando el host pregunta (puede ser automáticamente o cuando se accede al dispositivo del host), el cliente remoto envía un mensaje de estado. En este caso no hay ningún medio de almacenamiento, de modo que el mensaje indica la ausencia de medio de almacenamiento.	El dispositivo de disquete está presente. Cuando el host pregunta (por ejemplo, al hacer doble clic sobre una unidad), el cliente remoto envía un mensaje de estado. En este caso no hay ningún medio de almacenamiento, de modo que el mensaje indica la ausencia de medio de almacenamiento.
3	Se ha iniciado la aplicación Remote Console sin ningún medio de almacenamiento y luego se introduce el medio.	El dispositivo de DVD está presente. Cuando el host pregunta (de forma automática o manual), el cliente remoto envía un mensaje de estado en el que indica que ha habido un cambio y que existe un medio de almacenamiento.	El dispositivo de disquete está presente. Cuando el host pregunta (manual), el cliente remoto envía un mensaje de estado en el que indica que ha habido un cambio y que existe un medio de almacenamiento.
4	La aplicación Remote Console se ha iniciado con un medio de almacenamiento introducido en la unidad.	Igual que en el caso 3.	Igual que en el caso 3.
5	Se ha iniciado la aplicación Remote Console con un medio de almacenamiento que luego se ha extraído.	El siguiente comando del host recibirá un mensaje de estado indicando que no hay ningún medio de almacenamiento presente.	El siguiente comando del host recibirá un mensaje de estado indicando que no hay ningún medio de almacenamiento presente.

TABLA 12-2 Funcionamiento de Remote Console con unidades de DVD y disquete *(continuación)*

Caso	Estado	DVD visto por el host remoto	Disquete visto por el host remoto
6	La aplicación Remote Console se ha iniciado con redirección de imagen.	Igual que en el caso 3.	Igual que en el caso 3.
7	La aplicación Remote Console se ha iniciado con la imagen, pero la redirección se ha detenido (que es el único medio de interrumpir la redirección ISO).	El controlador sabe que se ha detenido la redirección de DVD, por lo que envía un estado de ausencia de medio de almacenamiento en la siguiente consulta del host.	El controlador sabe que se ha detenido la redirección de DVD, por lo que envía un estado de ausencia de medio en la siguiente consulta del host sobre el disquete.
8	Error de la red.	El software tiene un mecanismo de conexión persistente. Dado que no existe comunicación, considerará que hay un fallo del mecanismo de conexión y cerrará el socket al presuponer que el cliente no responde. El controlador enviará un estado de ausencia de medio de almacenamiento al host.	El software tiene un mecanismo de conexión persistente. Detectará que el cliente no responde y cerrará el socket, además de indicar al controlador que se ha interrumpido la conexión remota. El controlador enviará un estado de ausencia de medio de almacenamiento al host.
9	El cliente se bloquea.	Igual que en el caso 8.	Igual que en el caso 8.

Información de referencia de la interfaz de la línea de comandos de ILOM

Esta apéndice contiene las secciones siguientes:

- [“Referencia abreviada de los comandos de la CLI” en la página 231](#)
- [“Información de referencia de los comandos de la CLI” en la página 237](#)

Referencia abreviada de los comandos de la CLI

Esta sección contiene los comandos de ILOM utilizados habitualmente para administrar el servidor Sun desde la interfaz de la línea de comandos (CLI).

Nota – Los ejemplos de sintaxis de este capítulo utilizan el destino que empieza por /SP/, aunque podría cambiarse por el destino que empieza por /CMM/ en función de la plataforma de servidor Sun utilizada. Los destinos subordinados son comunes para todas las plataformas de servidor Sun.

TABLA A-1 Sintaxis y uso de los comandos

Contenido	Tipo de letra	Descripción
Datos introducidos por el usuario	Letra de paso fijo en negrita	Texto introducido por el usuario. Debe escribirse tal y como aparece.
Resultado en la pantalla	Letra de paso fijo normal	Texto que muestra el sistema.
Variable	<i>Cursiva</i>	Se sustituye por un nombre o valor elegido por el usuario.
Corchetes []		El texto que aparece entre corchetes es optativo.
Barras verticales		El texto separado por una barra vertical representa los únicos valores disponibles. Debe seleccionarse uno.

TABLA A-2 Comandos generales

Descripción	Comando
Ver todos los destinos válidos.	help targets
Cerrar la sesión de la CLI.	exit
Ver la versión del firmware de ILOM que se está ejecutando.	version
Ver la información del reloj.	show /SP/clock
Ver todos los comandos de la CLI.	show /SP/cli/commands
Ver las sesiones de ILOM activas.	show /SP/sessions
Ver información sobre los comandos y destinos.	help
Ver información sobre un determinado comando.	help create
Actualizar el firmware de ILOM y la BIOS.	load -source ftp://nuevaimagenSP
Ver una lista de registros de eventos de ILOM.	show /SP/logs/event/list

TABLA A-3 Comandos de administración de usuarios

Descripción	Comando
Agregar un usuario local.	create /SP/users/usuario1 password=contraseña role=administrator operator
Suprimir un usuario local.	delete /SP/users/usuario1
Cambiar las propiedades de un usuario local.	set /SP/users/usuario1 role=operator
Ver información sobre todos los usuarios locales.	show -display [targets properties all] -level all /SP/users
Ver información sobre la configuración de LDAP.	show /SP/clients/ldap
Cambiar la configuración de LDAP.	set /SP/clients/ldap binddn=usuarioproxy bindpw=contraseñausuarioproxy defaultrole=administrator operator ipaddress=direcciónip

TABLA A-4 Comandos de configuración de la red y el puerto serie

Descripción	Comando
Ver la información de configuración de red.	show /SP/network
Cambiar las propiedades de red de ILOM. El cambio de ciertas propiedades de red, como la dirección IP, hará que se desconecte la sesión activa.	set /SP/network pendingipaddress=direcciónip pendingipdiscovery=dhcp static pendingipgateway=ippuertaenlace pendingipnetmask=ipmáscarared commitpending=true
Ver información sobre el puerto serie externo.	show /SP/serial/external
Cambiar la configuración del puerto serie externo.	set /SP/serial/external pendingspeed=entero commitpending=true
Ver información sobre la conexión serie con el host.	show /SP/serial/host
Cambiar la configuración del puerto serie del host.	set /SP/serial/host pendingspeed=entero commitpending=true
Nota: el valor de velocidad de este puerto debe coincidir con el del puerto serie 0, COM1 o /dev/ttyS0 del sistema operativo host.	

TABLA A-5 Comandos de administración de alertas

Descripción	Comando
Ver información sobre las alertas. Es posible configurar un total de 15 alertas.	show /SP/alertmgmt/rules/1...15
Configurar una alerta PET de IPMI.	set /SP/alertmgmt/rules/1...15 type=ipmipet destination=direcciónip level=down critical major minor
Configurar una alerta de captura de eventos SNMP v3.	set /SP/alertmgmt/rules/1...15 type=snmptrap snmp_version=3 community_or_username=nombreusuario destination=direcciónip level=down critical major minor
Configurar una alerta de correo electrónico.	set /SP/alertmgmt/rules/1...15 type=email destination=dirección_correoelectrónico level=down critical major minor

TABLA A-6 Comandos de acceso a la administración del sistema

Descripción	Comando
Ver información sobre la configuración de HTTP.	show /SP/services/http
Cambiar la configuración de HTTP, por ejemplo, habilitando la redirección automática a HTTPS.	set /SP/services/http port=númeropuerto secureredirect enabled disabled servicestate=enabled disabled
Ver información sobre el acceso HTTPS.	show /SP/services/https
Cambiar la configuración de HTTPS.	set /SP/services/https port=númeropuerto servicestate=enabled disabled
Ver la configuración de claves DSA de SSH.	show /SP/services/ssh/keys/dsa
Ver la configuración de claves RSA de SSH.	show /SP/services/ssh/keys/rsa

TABLA A-7 Comandos de SNMP

Descripción	Comando
Ver información sobre la configuración de SNMP. El puerto de SNMP es el 161 y v3 está habilitado de forma predeterminada.	show /SP/services/snmp engineid=idmotorsnmp port=númeropuertosnmp sets=enabled disabled v1=enabled disabled v2c=enabled disabled v3=enabled disabled
Ver los usuarios de SNMP.	show /SP/services/snmp/users
Agregar un usuario de SNMP.	create /SP/services/snmp/users/nombreusuariosnmp authenticationpassword=contraseña authenticationprotocol=MD5 SHA permissions=rw ro privacypassword=contraseña privacyprotocol=none DES
Suprimir un usuario de SNMP.	delete /SP/services/snmp/users/nombreusuariosnmp
Ver información sobre las comunidades SNMP públicas (sólo lectura).	show /SP/services/snmp/communities/public
Agregar este dispositivo a una comunidad SNMP pública.	create /SP/services/snmp/communities/public/comun1
Suprimir este dispositivo de una comunidad SNMP pública.	delete /SP/services/snmp/communities/public/comun1
Ver información sobre las comunidades SNMP privadas (lectura-escritura).	show /SP/services/snmp/communities/private
Agregar este dispositivo a una comunidad SNMP privada.	create /SP/services/snmp/communities/private/comun2
Borrar este dispositivo de una comunidad SNMP privada.	delete /SP/services/snmp/communities/private/comun2

TABLA A-8 Comandos de administración del sistema host

Descripción	Comando
Encender el sistema host o el chasis.	start /SYS o start /CH
Apagar el sistema host o el chasis (cierre normal del sistema).	stop /SYS o stop /CH
Apagar el sistema host o el chasis (cierre forzoso del sistema).	stop -f /SYS o stop -f /CH
Reiniciar el sistema host o el chasis.	reset /SYS o reset /CH

TABLA A-8 Comandos de administración del sistema host (*continuación*)

Descripción	Comando
Iniciar una sesión para establecer conexión con la consola del host.	start /SP/console
Detener la sesión conectada a la consola del host (cierre de sesión normal).	stop /SP/console
Detener la sesión conectada a la consola del host (cierre de sesión forzoso).	stop -force [-f] /SP/console

TABLA A-9 Comandos de configuración del reloj

Descripción	Comando
Configurar el reloj de ILOM para sincronizarlo con un servidor NTP principal.	set /SP/clients/ntp/server/1 address=direcciónIPntp
Configurar el reloj de ILOM para sincronizarlo con un servidor NTP secundario.	set /SP/clients/ntp/server/2 address=direcciónIPntp2

Información de referencia de los comandos de la CLI

Esta sección proporciona información de referencia sobre los comandos de la CLI.

Uso del comando `cd`

El comando `cd` se utiliza para navegar por el espacio de nombres. Cuando `cd` se emplea para llegar a una ubicación de destino, esa ubicación se convierte en el destino predeterminado para los otros comandos. Si especifica la opción `-default` sin destino, el comando le sitúa en la parte superior del espacio de nombres. Escribir `cd -default` equivale a escribir `cd /`. Si escribe sólo `cd`, aparece en pantalla la ubicación actual en el espacio de nombres. Si escribe `help targets`, aparece una lista con todos los destinos del espacio de nombres completo.

Sintaxis

`cd destino`

Opciones

`[-default] [-h|help]`

Destinos y propiedades

Cualquier ubicación del espacio de nombres.

Ejemplos

Para crear un usuario llamado `emmett`, utilice `cd` para situarse en `/SP/users` y ejecute el comando `create` con `/SP/users` como destino predeterminado.

```
-> cd /SP/users
-> create emmett
```

Para averiguar la ubicación actual, escriba `cd`.

```
-> cd /SP/users
```

Uso del comando create

El comando `create` se utiliza para agregar objetos al espacio de nombres. A menos que especifique propiedades con `create`, los objetos quedarán vacíos.

Sintaxis

```
create [opciones] destino [nombrepropiedad=valor]
```

Opciones

```
[-h|help]
```

Destinos, propiedades y valores

TABLA A-10 Destinos, propiedades y valores del comando `create`

Destinos válidos	Properties	Valores	Valor predeterminado
<i>/SP/users/nombreusuario</i>	password role	<cadena> administrator operator	(none) operator
<i>/SP/services/snmp/communities</i> <i>/nombrecomunidad</i>	permissions	ro rw	ro
<i>/SP/services/snmp/user/</i> <i>nombreusuario</i>	authenticationprotocol authenticationpassword permissions privacyprotocol privacypassword	MD5 <cadena> ro rw none DES <cadena>	MD5 (cadena nula) ro DES (cadena nula)

Ejemplo

```
-> create /SP/users/susan role=administrator
```

Uso del comando delete

El comando `delete` se utiliza para borrar objetos del espacio de nombres. Al usar `delete`, aparece un mensaje de confirmación. Puede evitar que aparezca ese mensaje utilizando la opción `-script`.

Sintaxis

```
delete [opciones] [-script] destino
```

Opciones

```
[-f|force] [-h|help] [-script]
```

Destinos

TABLA A-11 Destinos del comando `delete`

Destinos válidos
<code>/SP/users/nombreusuario</code>
<code>/SP/services/snmp/communities/nombrecomunidad</code>
<code>/SP/services/snmp/user/nombreusuario</code>

Ejemplos

```
-> delete /SP/users/susan  
-> delete /SP/services/snmp/communities/public
```

Uso del comando exit

El comando `exit` se utiliza para finalizar la sesión de la CLI.

Sintaxis

```
exit [opciones]
```

Opciones

```
[-h|help]
```

Uso del comando help

El comando `help` se utiliza para ver información de ayuda sobre los comandos y destinos. Si utiliza la opción `-output terse`, sólo aparece información de uso. La opción `-output verbose` muestra la información de uso, la descripción y otra información que incluye ejemplos de uso del comando. Si no utiliza la opción `-output`, aparece la información de uso y una breve descripción del comando.

Si especifica `command targets`, aparece una lista completa de los destinos válidos para ese comando desde los destinos fijos `/SP` y `/SYS`. Los destinos fijos son aquellos que no pueden crear los usuarios.

Al especificar `command targets legal`, aparece información sobre la propiedad intelectual y los derechos de uso del producto.

Sintaxis

```
help [opciones] comando [destino]
```

Opciones

```
[-h|help] [-output terse|verbose]
```

Comandos

```
cd, create, delete, exit, help, load, reset, set, show, start,  
stop, version
```

Ejemplos

```
■ -> help load
```

The `load` command is used to transfer a file from a server to a target.

```
Usage: load -source URL [destino]
```

`-source`: Specify the location to get a file.

```
■ -> help -output verbose reset
```

The `reset` command is used to reset a target.

```
Usage: reset [-script] [target]
```

Available options for this command:

`-script`: Do not prompt for yes/no confirmation and act as if yes were specified.

For example:

```
-> reset /SYS
Are you sure you want to reset /SYS (y/n)? y
Performing hard reset on /SYS
-> reset
/SP Are you sure you want to reset /SP (y/n)? n
Command aborted. ->
```

Uso del comando load

El comando `load` se utiliza para transferir un archivo de imagen desde un origen indicado por una dirección URI (Uniform Resource Indicator) para actualizar el firmware de ILOM. El URI puede especificar un protocolo y las credenciales utilizadas para la transferencia. Sólo admite el protocolo TFTP, por lo que la dirección URI debe empezar por `tftp://`. Si se precisan credenciales y no se especifican, el comando solicita una contraseña. El uso de la opción `-script` evita la aparición del mensaje de confirmación y el comando actúa como si se hubiese respondido sí a ese mensaje.

Nota – Utilice este comando para actualizar el firmware de ILOM y la BIOS.

Sintaxis

```
load -source URI
```

Opciones

```
[-h|help] [-source] [-script]
```

Ejemplo

```
-> load -source tftp://<direcciónip>/newmainimage
```

Nota – La actualización del firmware provoca el reinicio de ILOM y del servidor. Se recomienda realizar un cierre normal del servidor antes de proceder a la actualización. Una actualización dura aproximadamente cinco minutos. ILOM entra en un modo especial para cargar el nuevo firmware. No se realiza ninguna otra tarea en ILOM hasta que éste finaliza la actualización y se reinicia.

```
-> load -source tftp://archive/newmainimage
Are you sure you want to load the specified file (y/n)? y
File upload is complete.
Firmware image verification is complete.
Do you want to preserve the configuration (y/n)? n
Updating firmware in flash RAM:
.
Firmware update is complete.
ILOM will not be restarted with the new firmware.
```

Uso del comando `reset`

El comando `reset` se utiliza para restablecer el estado del destino. Al usarlo, aparece un mensaje de confirmación. Puede evitar la aparición de ese mensaje utilizando la opción `-script`.

Nota – El comando `reset` no afecta al estado de la alimentación de los dispositivos de hardware.

Sintaxis

```
reset [opciones] destino
```

Opciones

```
[-h|help] [-script]
```

Destinos

TABLA A-12 Destinos del comando `reset`

Destinos válidos
<code>/SP</code>
<code>/SYS</code>

Ejemplos

```
-> reset /SP
-> reset /SYS
```

Uso del comando set

El comando `set` se utiliza para especificar las propiedades del destino.

Sintaxis

```
set [opciones] destino [nombrepropiedad=valor]
```

Opciones

```
[-h|help]
```

Destinos, propiedades y valores

TABLA A-13 Destinos, propiedades y valores del comando `set`

Destinos válidos	Propiedades	Valores	Valor predeterminado
/SP/users/nombreusuario	password	<cadena>	(ninguno)
	role	administrator operator	operator
/SP/alertmgmt/rules	testalert	true	(ninguno)
/SP/alertmgmt/rules/ nombreregla (nombreregla = del 1 al 15)	community_or_username	<cadena>	public
	destination	dirección_correo_electrónico	(ninguno)
	level	down critical major minor	(ninguno)
	snmp_version	1 2c 3	3
	type	email ipmipet snmptrap	(ninguno)
/SP/clock	usentpserver	enabled disabled	disabled
	datetime	día mes hora año	<cadena>
/SP/services/http	puerto	<entero>	80
	securedirect	enabled disabled	enabled
	servicestate	enabled disabled	disabled
/SP/services/https	puerto	<entero>	443
	servicestate	enabled disabled	disabled
/SP/services/snmp	engineid	<hexadecimal>	dirección IP
	port	<entero>	161
	sets	enabled disabled	disabled
	v1	enabled disabled	disabled
	v2c	enabled disabled	disabled
	v3	enabled disabled	enabled
/SP/services/snmp/ communities/private	permission	ro rw	rw
/SP/services/snmp/ communities/public	permission	ro rw	ro

TABLA A-13 Destinos, propiedades y valores del comando `set` (continuación)

Destinos válidos	Propiedades	Valores	Valor predeterminado
/SP/services/snmp/user <i>/nombreusuario</i>	authenticationprotocol	MD5	MD5
	authenticationpassword	<cadena>	(cadena nula)
	permissions	ro rw	ro
	privacyprotocol	none DES	DES
	privacypassword	<cadena>	(cadena nula)
/SP/services/ssh	generate_new_key_action	true	(ninguno)
	generate_new_key_type	rsa dsa	(ninguno)
	restart_sshd_action	true	(ninguno)
	state	enabled disabled	enabled
/SP/services/sso	state		
/SP/users/nombreusuario	role	administrator operator	(ninguno)
	password	<cadena>	(ninguno)
/SP/clients/activedirectory	state	enabled disabled	disabled
	certfilestatus	<cadena>	(ninguno)
	defaultrole	<cadena>	(ninguno)
	getcertfile	<cadena>	(ninguno)
	ipaddress	<cadena>	(ninguno)
	puerto	<cadena>	(ninguno)
	strictcertmode	enabled disabled	disabled
	timeout	<entero>	(ninguno)
	name	<cadena>	(ninguno)
/SP/clients/activedirectory/admingroups/n donde <i>n</i> es 1-5	name	<cadena>	(ninguno)
/SP/clients/activedirectory/opergroups/n donde <i>n</i> es 1-5	name	<cadena>	(ninguno)
/SP/clients/activedirectory/userdomains/n donde <i>n</i> es 1-5	dominio	<cadena>	(ninguno)
/SP/clients/ldap	binddn	<nombreusuario>	(ninguno)
	bindpw	<cadena>	(ninguno)
	defaultrole	administrator operator	operator
	ipaddress	<direcciónip> none	(ninguno)
	port	<entero>	389
	searchbase	<cadena>	(ninguno)
	state	enable disabled	disabled

TABLA A-13 Destinos, propiedades y valores del comando `set` (continuación)

Destinos válidos	Propiedades	Valores	Valor predeterminado
<code>/SP/clients/ntp/server/[1 2]</code>	address	<direcciónip>	(ninguno)
<code>/SP/clients/radius</code>	defaultrole	administrator operator	operator
	ipaddress	<direcciónip> none	(ninguno)
	port	<entero>	1812
	secret	<cadena> none	(ninguno)
	state	enable disabled	disabled
<code>/SP/clients/smtp</code>	address	<direcciónip>	<i>dirección IP</i>
	port	<entero>	25
	state	enabled disabled	enabled
<code>SP/clients/syslog</code>	destination_ip1	<direcciónip>	<i>dirección IP</i>
	destination_ip2	<direcciónip>	<i>dirección IP</i>
<code>/SP/network</code>	commitpending	true	(ninguno)
	ipaddress	<direcciónip>	<i>dirección IP</i>
	ipdiscovery	<direcciónip>	<i>dirección IP</i>
	ipgateway	<direcciónip>	<i>dirección IP</i>
	ipnetmask	<direcciónip>	<i>dirección IP</i>
	pendingipaddress	<direcciónip> none	(ninguno)
	pendingdiscovery	dhcp static	dhcp
	pendingipgateway	<direcciónip> none	(ninguno)
	pendingipnetmask	<IP decimal separado por puntos>	255.255.255.255
<code>/SP/serial/external</code>	commitpending	true	(ninguno)
	flowcontrol	none	none
	pendingspeed	<entero de la lista>	9600
	speed	<entero de la lista>	9600
<code>/SP/serial/host</code>	commitpending	true	(ninguno)
	pendingspeed	<entero de la lista>	9600
	speed		9600
<code>/SP/</code>	system_identifier	<cadena>	(ninguno)
<code>/SP/</code>	hostname	<cadena>	valor predeterminado basado en la dirección MAC

Ejemplos

```
-> set /SP/users/susan role=administrator
-> set /SP/clients/ldap state=enabled binddn=proxyuser bindpw=ez24get
```

Uso del comando show

El comando `show` se utiliza para ver información sobre los destinos y las propiedades.

La opción `-display` del comando determina el tipo de información mostrada. Si especifica `-display targets`, se muestran todos los destinos del espacio de nombres situados por debajo del destino actual. Si especifica `-display properties`, aparecen todas las propiedades y valores del destino. Con esta opción, puede especificar ciertos nombres de propiedades y sólo se mostrarán los valores correspondientes. Si especifica `-display all`, se muestran todos los destinos del espacio de nombres situados debajo del destino actual y las propiedades del destino especificado. Si no escribe la opción `-display`, el comando `show` actúa como si se hubiese especificado `-display all`.

La opción `-level` controla la profundidad del comando `show` y la aplica a todos los modos de la opción `-display`. Si especifica `-level 1`, se muestra el nivel del espacio de nombres en el que reside el objeto. Los valores mayores de 1 devuelven información sobre el nivel actual del destino en el espacio de nombres y los niveles situados debajo del <valor especificado>. Si el argumento es `-level all`, se aplica al nivel actual del espacio de nombres y todos lo que estén por debajo.

La opción `-o|output` indica la salida del comando y el formato de salida. ILOM sólo admite el formato `-o table`, que presenta los destinos y propiedades en forma de tabla.

Sintaxis

```
show [opciones] [-display targets|properties|all] [-level  
valor|all] destino [nombrepropiedad]
```

Opciones

```
[-d|-display] [-l|level] [-o|output]
```

Destinos y propiedades

TABLA A-14 Destinos del comando show

Destinos válidos	Propiedades
<code>/SYS</code>	
<code>/SP</code>	
<code>/SP/alertmgmt/rules/ nombreregla (nombreregla = del 1 al 15)</code>	community username destination level snmp_version type

TABLA A-14 Destinos del comando `show` (continuación)

Destinos válidos	Propiedades
<code>/SP/clients/ activedirectory</code>	state certfilestatus defaultrole getcertfile ipaddress puerto strictcertmode timeout
<code>/SP/clients/ activedirectory/ admingroups/n</code> donde <i>n</i> es 1-5	name
<code>/SP/clients/ activedirectory/ opergroups/n</code> donde <i>n</i> es 1-5	name
<code>/SP/clients/ activedirectory/ userdomains/n</code> donde <i>n</i> es 1-5	dominio
<code>/SP/clients/ldap</code>	binddn bindpw defaultrole ipaddress port searchbase state
<code>/SP/clients/ntp/server/[1 2]</code>	ipaddress
<code>/SP/clock</code>	datetime usentpserver
<code>/SP/logs/event</code>	clear
<code>/SP/network</code>	ipaddress ipdiscovery ipgateway ipnetmask macaddress pendingipaddress pendingdiscovery pendingipgateway pendingipnetmask

TABLA A-14 Destinos del comando `show` (continuación)

Destinos válidos	Propiedades
<code>/SP/serial/external</code>	flowcontrol pendingspeed speed
<code>/SP/serial/host</code>	pendingspeed speed
<code>/SP/services/http</code>	port secureredirect servicestate
<code>/SP/services/https</code>	port servicestate
<code>/SP/services/snmp</code>	engineid port sets v1 v2c v3
<code>/SP/services/snmp/communities/private</code>	permissions
<code>/SP/services/snmp/communities/public</code>	permissions
<code>/SP/services/snmp/users/nombreusuario</code>	password role
<code>/SP/services/ssh</code>	state
<code>/SP/services/ssh/keys/dsa</code>	fingerprint length publickey
<code>/SP/services/ssh/keys/rsa</code>	fingerprint length publickey
<code>/SP/services/sso</code>	state
<code>/SP/sessions</code>	username starttime date
<code>/SP/sessions/idsesión</code>	starttime source type user
<code>/SP/users/nombreusuario</code>	role password

Ejemplos

```
-> show -display properties /SP/users/susan
```

```
/SP/users/susan
```

```
Properties:
```

```
role = Administrator
```

```
-> show /SP/clients -level 2
```

```
/SP/clients
```

```
Targets:
```

```
ldap  
ntp
```

```
Properties:
```

```
Commands:
```

```
cd  
show
```

```
/SP/clients/ldap
```

```
Targets:
```

```
Properties:
```

```
binddn = cn=Manager,dc=sun,dc=com  
bindpw = secret  
defaultrole = Operator  
ipaddress = 129.144.97.180  
port = 389  
searchbase = ou=people,dc=sun,dc=com  
state = disabled
```

```
Commands:
```

```
cd  
show
```

```
/SP/clients/ntp
```

```
Targets:
```

```
server
```

```
Properties:
```

```
Commands:
```

```
cd  
show
```

Uso del comando `start`

El comando `start` se utiliza para activar el destino o iniciar un conexión con la consola del host. El uso de la opción `-script` evita la aparición del mensaje de confirmación y el comando actúa como si se hubiese respondido sí a ese mensaje.

Sintaxis

```
start [opciones] destino
```

Opciones

```
[-h|help] [-script]
```

Destinos

TABLA A-15 Destinos del comando `start`

Destinos válidos	Descripción
<code>/SYS</code> o <code>/CH</code>	Inicia (enciende) el sistema o el chasis.
<code>/SP/console</code>	Inicia una sesión interactiva con la consola.

Ejemplos

```
-> start /SP/console  
-> start /SYS
```

Uso del comando `stop`

El comando `stop` se utiliza para desactivar el destino o cerrar la conexión de otro usuario con la consola del host. Al usar este comando, aparece un mensaje de confirmación. Puede evitar la aparición de ese mensaje utilizando la opción `-script`.

Sintaxis

```
stop [opciones] [-script] destino
```

Opciones

```
[-f|force] [-h|help]
```

Destinos

TABLA A-16 Destinos del comando `stop`

Destinos válidos	Descripción
<code>/SYS</code> o <code>/CH</code>	Realiza un cierre normal del sistema y, a continuación, apaga el sistema o chasis especificado. Utilice la opción <code>-force</code> si quiere evitar el cierre normal y forzar el apagado inmediato.
<code>/SP/console</code>	Interrumpe la conexión de otro usuario con la consola del host.

Ejemplos

```
-> stop /SP/console  
-> stop -force /SYS
```

Uso del comando `version`

El comando `version` se utiliza para ver información sobre la versión de ILOM.

Sintaxis

`version`

Opciones

`[-h|help]`

Ejemplo

```
-> version  
version SP firmware version: 1.0.0  
SP firmware build number: 4415  
SP firmware date: Mon Mar 28 10:39:46 EST 2005  
SP filesystem version: 0.1.9
```


Glosario

A

- address** En el contexto de las redes, es un código que identifica de forma exclusiva un nodo de la red. El servicio de nombres de dominio (DNS) traduce nombres como "host1.sun.com" en una dirección de cuatro cifras separadas por puntos similar a esta "168.124.3.4".
- administración de sistemas en banda** Capacidad de administración de los servidores que se habilita sólo cuando se ha inicializado el sistema operativo y el servidor funciona adecuadamente.
- administración de sistemas fuera de banda (OOB)** Capacidad de administración de los servidores que se habilita cuando los controladores de red del sistema operativo o el servidor no funcionan adecuadamente.
- administrador** Persona que posee todos los privilegios de acceso (root) al host administrado.
- agente** Proceso de software, normalmente perteneciente a un determinado host local administrado, que efectúa peticiones al software de administración y pone la información local de los sistemas y las aplicaciones a disposición de los usuarios remotos.
- alerta** Mensaje o archivo de registro generado por la recopilación y el análisis de eventos de error. Las alertas indican que es preciso realizar algún tipo de acción correctiva en el hardware o el software.
- algoritmo RSA** Algoritmo criptográfico desarrollado por RSA Data Security, Inc. Puede utilizarse para operaciones de cifrado y firmas digitales.

ancho de banda Medida del volumen de información que puede transmitirse a través de un enlace de comunicación. A menudo se describe como el número de bits por segundo que puede transferir una red.

aplicación
Java™ Web Start Aplicación para la ejecución de aplicaciones web. Con Java Web Start, las aplicaciones se ejecutan haciendo clic en el vínculo web. Si la aplicación no está presente en el sistema, Java Web Start la descarga y la guarda en la caché del sistema. Una vez hecho, puede ejecutarse mediante un icono del escritorio o el navegador.

archivo del núcleo central Archivo creado por el sistema operativo Solaris o Linux cuando un programa deja de funcionar normalmente e interrumpe su ejecución. Este archivo ofrece una instantánea del estado en que se encontraba la memoria en el momento de producirse el error. También se denomina “archivo de volcado por caída del sistema”.

ARP (Address Resolution Protocol) Protocolo utilizado para asociar una dirección IP (Internet Protocol) a una dirección del hardware de red (dirección MAC).

ASF (Alert Standard Format) Formato de alertas estándar. Especificación de administración de plataformas antes del arranque o fuera de banda que permite a dispositivos tales como una controladora Ethernet inteligente examinar de forma autónoma los sensores conformes con ASF de la placa base para conocer el voltaje, la temperatura y otros parámetros, así como enviar alertas RMPC (Remote Management and Control Protocol) de acuerdo con la especificación PET (Platform Event Trap). ASF se creó inicialmente para realizar funciones de administración fuera de banda relacionadas con los sistemas cliente de sobremesa. La definición de la norma ASF es competencia de la DMTF (Distributed Management Task Force).

autenticación Proceso que verifica la identidad de un usuario, un dispositivo u otra entidad de un sistema informático en una sesión de comunicación antes de que ese usuario, dispositivo o entidad pueda acceder a los recursos del sistema. La autenticación de sesiones puede funcionar en dos direcciones. El servidor verifica la autenticidad del cliente para tomar decisiones de control de acceso. El cliente también puede autenticar el servidor. Con el protocolo SSL (Secure Sockets Layer), el cliente siempre autentica la identidad del servidor.

autoridad de certificación (CA) Autoridad de confianza que emite certificados de clave pública e identifica al propietario del certificado. La autoridad emite certificados que establecen la relación entre una entidad designada en el certificado y una clave pública que pertenece a esta entidad y que también está presente en el certificado.

autorización Proceso por el que se otorgan privilegios de acceso específicos a un usuario. La autorización se basa en los procesos de autenticación y control de acceso.

B

BIOS (sistema básico de entrada y salida)

Software del sistema que controla la carga del sistema operativo y comprueba el funcionamiento del hardware durante el encendido. El sistema BIOS se almacena en la memoria de sólo lectura (ROM)

bits por segundo (bps)

Unidad de medida de la velocidad de transmisión de los datos.

BMC (Baseboard Management Controller)

Dispositivo utilizado para administrar funciones de configuración, servicio y control del entorno, y para recibir datos de eventos procedentes de otras partes del sistema. Recibe los datos a través de las interfaces de los sensores y los interpreta utilizando el registro de datos de sensores (SDR), para el que proporciona una interfaz. El BMC proporciona otra interfaz con el registro de eventos del sistema (SEL). Las funciones típicas del BMC son medir la temperatura de los procesadores, los valores de las fuentes de alimentación y el estado de los ventiladores. Además, puede emprender acciones de forma autónoma para mantener la integridad del sistema.

C

caché

Copia de los datos originales que se almacena de forma local, a menudo con instrucciones o con la información a la que se accede con más frecuencia. De esta forma, los datos de la caché no tienen que recuperarse desde un servidor remoto cuando vuelvan a solicitarse. La caché incrementa de forma efectiva la velocidad de transferencia desde la memoria y la velocidad del procesador.

captura de eventos

Notificación de eventos realizada por iniciativa de los agentes SNMP (Simple Network Management Protocol) cuando se detectan ciertas condiciones. SNMP define formalmente siete tipos de capturas y permite definir otros siete subtipos.

cargador de arranque

Programa de la memoria de sólo lectura (ROM) que se ejecuta automáticamente cuando se enciende el sistema para controlar la primera etapa de inicialización del sistema y comprobación del hardware. Posteriormente, el cargador transfiere el control a un programa más complejo que carga el sistema operativo.

certificado

Datos de clave pública asignados por una autoridad de certificación (CA) de confianza para avalar la identidad de una entidad. Se trata de un documento con firma digital. Tanto los clientes como los servidores pueden tener certificados. También se denomina “certificado de clave pública”.

certificado de servidor	Certificado utilizado con HTTPS (Hypertext Transfer Protocol Secure) para autenticar las aplicaciones web. Puede ser autofirmado o emitirse a través de una autoridad de certificación (CA).
certificado X.509	Es el estándar de certificación más común. Los certificados X.509 son documentos que contienen una clave pública y llevan asociados datos de identificación con una firma digital emitida por una autoridad de certificación (CA).
ciclo de apagado y encendido	Proceso de apagar un sistema y volverlo a encender.
cifrado de clave pública	Método criptográfico que utiliza una clave (código) de dos partes formado por componentes públicos y privados. Para cifrar los mensajes, se utilizan las claves públicas conocidas de los destinatarios. Para descifrarlos, los destinatarios utilizan sus claves privadas, que sólo ellos conocen. El conocimiento de la clave pública no da la posibilidad de deducir la clave privada correspondiente.
cliente	En el modelo cliente/servidor, sistema o software de una red que accede de forma remota a los recursos de un servidor de la red.
componentes sustituibles en campo (FRU)	Componente del sistema que puede sustituirse en la propia instalación del usuario.
conexión en marcha	Indica la posibilidad de retirar o añadir un componente con seguridad mientras el sistema está en funcionamiento. No obstante, antes de retirar el componente, el administrador debe preparar el sistema para la operación de conexión. Una vez introducido el nuevo componente, debe dar instrucciones al sistema para que reconfigure el dispositivo.
conmutación por error	Cambio automático de un servicio informático de un sistema (normalmente un subsistema) a otro para proporcionar redundancia.
consola	Terminal o ventana especial de una pantalla donde se muestran los mensajes del sistema. En la ventana de la consola es posible configurar, supervisar, mantener y resolver problemas de muchos componentes de software del servidor.
consola serie	Terminal o línea tip conectada al puerto serie del procesador de servicios. Esta consola se utiliza para configurar el sistema a fin de realizar otras tareas de administración.
cuenta de usuario	Registro de la información esencial que se almacena en el sistema sobre un usuario. Cada usuario que accede a un sistema tiene una cuenta de usuario.

D

DES (Data Encryption Standard)

Estándar de cifrado de datos. Algoritmo de uso común para cifrar y descifrar datos.

DHCP (Dynamic Host Configuration Protocol)

Protocolo de configuración dinámica de hosts. Permite a un servidor DHCP asignar direcciones IP dinámicas a los sistemas de una red TCP/IP (Transmission Control Protocol/Internet Protocol).

dirección física

Dirección del hardware que corresponde a una ubicación de la memoria. Los programas que hacen referencia a direcciones virtuales se redirigen a las direcciones física correspondientes.

dirección IP (Internet Protocol)

En TCP/IP (Transmission Control Protocol/Internet Protocol), número de 32 bits que identifica de forma exclusiva a cada host o sistema de hardware de una red. Se compone de una serie de números separados por puntos, como en "192.168.255.256", que especifica la ubicación de una máquina en Internet o en una intranet.

dirección MAC (Media Access Control)

Número de 48 bits exclusivo a nivel mundial que indica una dirección de hardware y se programa en cada tarjeta de interfaz de red en el momento de su fabricación.

directorio raíz

Directorio de base al que se subordinan el resto de directorios, directa o indirectamente.

DMA (Direct Memory Access)

Acceso directo a la memoria. Proceso por el que los datos se transfieren directamente a la memoria sin la supervisión del procesador.

DMI (Desktop Management Interface)

Interfaz de administración de sistemas de escritorio. Especificación que establece las normas para acceder a la información técnica de los componentes de hardware y software de los equipos. Es una interfaz independiente del sistema operativo y puede administrar estaciones de trabajo, servidores y otros sistemas informáticos. La definición de la interfaz DMI es competencia de la DMTF (Distributed Management Task Force).

DMTF (Distributed Management Task Force)

Consortio formado por más de 200 compañías que autoriza y promueve normas destinadas a mejorar la capacidad de administrar los sistemas informáticos de forma remota. Las especificaciones de la DTMF incluyen las normas DMI (Desktop Management Interface), CIM (Common Information Model) y ASF (Alert Standard Format).

dominio Grupo de hosts que se identifica mediante un nombre. Normalmente, los hosts del grupo pertenecen a la misma dirección de red IP (Internet Protocol). El dominio también hace referencia a la última parte de un nombre de dominio completo (FQDN) que identifica a la compañía u organización propietaria del mismo. Por ejemplo, "sun.com" identifica a Sun Microsystems como propietaria del dominio en el FQDN "docs.sun.com".

DNS (Domain Name Server)

Servidor de nombres de dominio. Es el servidor que normalmente administra los nombres de los hosts en un dominio. Los servidores DNS traducen nombres de host tales como "www.example.com" en direcciones IP (Internet Protocol) tales como "030.120.000.168".

DNS (Domain Name System)

Sistema de nombres de dominio. Un sistema de resolución de nombres distribuido que permite a los equipos informáticos encontrar otros equipos en la red o Internet utilizando el nombre de dominio. El sistema asocia direcciones IP (Internet Protocol) estándar tales como "00.120.000.168" a nombres de host tales como "www.sun.com". Las máquinas normalmente obtienen esta información de un servidor DNS.

DSA (Digital Signature Algorithm)

Algoritmo de firma digital. Algoritmo de cifrado estándar especificado por la norma DSS (Digital Signature Standard). Se utiliza para crear firmas digitales.

E

encaminador Sistema que asigna una ruta por la que dirigir los paquetes de red u otro tráfico de Internet. Aunque tanto los hosts como las puertas de enlace hacen funciones de encaminamiento, el término "encaminador" normalmente hace referencia a un dispositivo que conecta dos redes.

enlace En LDAP (Lightweight Directory Access Protocol), hace referencia al proceso de autenticación que este protocolo solicita cuando los usuarios acceden al directorio LDAP. La autenticación se produce cuando el cliente LDAP establece el enlace con el servidor LDAP.

EPP (Enhanced Parallel

Port) Puerto paralelo mejorado. Estándar de hardware y software gracias al cual los sistemas pueden transmitir datos al doble de velocidad que los puertos paralelos estándar.

espacio de nombres Conjunto de nombres exclusivos contenidos en la estructura del directorio LDAP (Lightweight Directory Access Protocol) a partir del cual se derivan e interpretan los nombres de los objetos. Por ejemplo, los archivos reciben su nombre dentro del espacio de nombres de archivo y las impresoras, dentro del espacio de nombres de impresora.

esquema Definiciones que describen el tipo de información que puede almacenarse como entrada en el directorio. Si se almacena información que no se ajusta al esquema, es posible que los clientes que traten de acceder al directorio no puedan ver los resultados adecuados.

estación de administración de red (NMS)

Estación de trabajo de gran capacidad donde se instalan una o varias aplicaciones de administración de red. Se utiliza para administrar una red de forma remota.

Ethernet Tipo de red de área local (LAN) estándar que permite a varios sistemas comunicarse entre sí en tiempo real mediante la conexión de cables. Ethernet utiliza el algoritmo CSMA/CD (Carrier Sense Multiple Access/Collision Detection) como método de acceso, por el cual todos los nodos escuchan las peticiones y cualquiera de ellos puede empezar a transmitir datos. Si varios nodos intentan transmitir datos al mismo tiempo (colisión), esperan un periodo de tiempo aleatorio antes de volver a intentar la transmisión.

evento Cambio de estado de un objeto administrado. El subsistema de administración de eventos puede enviar una notificación a la que el sistema de software de destino debe responder cuando se produce, pero que no ha solicitado ni controla.

evento crítico Evento del sistema que afecta gravemente al servicio y requiere atención inmediata.

evento mayor Evento del sistema que afecta al servicio, pero no de forma grave.

evento menor Evento del sistema que no afecta al servicio, pero necesita corrección antes de que se vuelva más grave.

F

- Fast Ethernet** Tecnología Ethernet que transfiere los datos a velocidades de hasta 100 millones de bits por segundo. Fast Ethernet es compatible con instalaciones Ethernet a 10 Mbits por segundo.
- firma digital** Forma de certificar el origen de los datos digitales. La firma digital es un número derivado de un proceso de cifrado de claves públicas. Si los datos se modifican después de crear la firma, ésta queda invalidada. Por este motivo, la firma digital puede garantizar la integridad de los datos y detectar la modificación de los mismos.
- firmware** Software utilizado normalmente para ayudar en la fase inicial de arranque de los sistemas y en la administración de los sistemas. El firmware está integrado en la memoria de sólo lectura (ROM) o la ROM programable (PROM) del sistema.
- Formato UTC (horario universal coordinado)** Norma internacional utilizada para expresar las horas. Antes se denominaba Hora del Meridiano de Greenwich (GMT). UTC es el formato utilizado por los servidores NTP (Network Time Protocol) para sincronizar los sistemas y dispositivos de las redes.
- FTP (File Transfer Protocol)** Protocolo de transferencia de archivos. Protocolo básico de internet que utiliza TCP/IP (Transmission Control Protocol/Internet Protocol) para transferir archivos de un sistema a otro en Internet con independencia de los sistemas operativos o las arquitecturas de los sistemas implicados en la transferencia.

G

- Gigabit Ethernet** Tecnología Ethernet que transfiere los datos a velocidades de hasta 1000 millones de bits por segundo.

H

- host** Sistema, como puede ser un servidor central, que tiene asignada una dirección IP (Internet Protocol) y un nombre de sistema. A él acceden otros sistemas remotos de la red.
- host local** Procesador o sistema en el que se ejecuta una aplicación de software.

HTTP (Hypertext Transfer Protocol)

Protocolo de Internet que recupera objetos de hipertexto procedentes de hosts remotos. Los mensajes HTTP constan de peticiones del cliente al servidor y respuestas del servidor al cliente. HTTP se basa en el protocolo TCP/IP (Transmission Control Protocol/Internet Protocol).

HTTPS (Hypertext Transfer Protocol Secure)

Extensión de HTTP que utiliza el protocolo SSL (Secure Sockets Layer) para la realización de transmisiones seguras en redes TCP/IP (Transmission Control Protocol/Internet Protocol).



I

ICMP (Internet Control Message Protocol)

Protocolo de mensajes de control de Internet. Extensión de IP (Internet Protocol) que proporciona direccionamiento, fiabilidad, control del flujo y secuenciación de los datos. Se encarga de especificar los mensajes de error y control utilizados con IP.

ID de host

Parte de la dirección IP (Internet Protocol) de 32 bits utilizada para identificar un host en una red.

identificación de usuario

Cadena con la que se identifica a un usuario de forma exclusiva en un sistema.

identificador de objeto (OID)

Número que identifica la posición de un objeto en un árbol de registro de objetos global. Cada nodo del árbol tiene asignado un número, por lo que un OID es una secuencia de números. En Internet, el uso de los números de OID está delimitado por puntos, por ejemplo, "0.128.45.12". En LDAP (Lightweight Directory Access Protocol), los OID se utilizan para identificar de forma exclusiva los elementos de los esquemas, incluidos los tipos de atributos y las clases de objetos.

Integrated Lights Out Manager (iLOM)

Solución integrada de hardware, firmware y software utilizada para administrar sistemas en chasis o en blades.

intercambio en marcha

Indica la posibilidad de instalar o retirar un componente simplemente extrayéndolo y sustituyéndolo por otro componente mientras el sistema está en funcionamiento. El sistema reconoce automáticamente el componente nuevo y lo configura, o solicita la intervención del usuario para configurarlo. En ninguno de los casos es necesario volver a arrancar el sistema. Todos los componentes intercambiables en marcha son conectables en marcha, pero no todos los componentes conectables en marcha son intercambiables en marcha.

interfaz de la línea de comandos (CLI)	Interfaz basada en texto que permite a los usuarios escribir instrucciones ejecutables desde el indicador de comandos.
interfaz gráfica de usuario (GUI)	Interfaz que utiliza gráficos, junto con un teclado y un ratón, para proporcionar acceso sencillo a una aplicación.
interfaz KCS (Keyboard Controller Style)	Tipo de interfaz implementada en las controladoras de teclado de los PC antiguos. Los datos se transfieren a través de la interfaz KCS utilizando un protocolo de enlace por byte.
IP (Internet Protocol)	Protocolo de la capa de red básico de Internet. Posibilita la transmisión, no siempre fiable, de paquetes de datos de un host a otro. IP no garantiza la entrega de los paquetes, ni el tiempo que tardarán en entregarse, ni si los paquetes se entregarán en el orden en que se enviaron. Los protocolos superpuestos a IP en las capas de comunicación añaden fiabilidad a la conexión.
IPMI (Intelligent Platform Management Interface)	Interfaz de administración inteligente de plataformas. Especificación de interfaz del nivel de hardware que se diseñó principalmente para la administración de servidores fuera de banda a través de una serie de interconexiones físicas diferentes. En ella se describen ampliamente diferentes abstracciones relativas a los sensores. Esto permite a la aplicación de administración ejecutarse en el sistema operativo o en un sistema remoto para comprender la composición del entorno del sistema y registrarse en el subsistema IPMI para recibir eventos. IPMI es compatible con software de administración de diferentes marcas. Entre sus funciones se incluyen la elaboración de informes de inventario de las unidades FRU (unidades sustituibles en campo), la supervisión del sistema, el registro de eventos, la recuperación del sistema (lo que incluye el reinicio de sistemas locales y remotos, y funciones de encendido y apagado) y el envío de alertas.
IPMITool	Utilidad que sirve para administrar dispositivos compatibles con IPMI. IPMITool puede administrar las funciones de IPMI en el sistema local o en un sistema remoto. Las funciones incluyen información de administración de las unidades FRU, la configuración de la red de área local (LAN), las lecturas de los sensores y el control de encendido de los sistemas remotos.

K

KVMS (keyboard, video, mouse, storage)

Serie de interfaces que permiten al sistema responder a eventos del teclado, el video, el ratón y los medios de almacenamiento.

L

LDAP (Lightweight Directory Access Protocol)

Protocolo de servicios de directorio utilizado para almacenar, recuperar y distribuir información que incluye perfiles de usuario, listas de distribución y datos de configuración. LDAP se ejecuta sobre TCP/IP (Transmission Control Protocol/Internet Protocol) y en múltiples plataformas.

Lista de control de acceso (ACL)

Mecanismo de autorización del software que permite controlar qué usuarios tienen acceso a un servidor. El usuario puede definir reglas de ACL específicas para determinados archivos o directorios a fin de otorgar o denegar el acceso a uno o varios usuarios o grupos de usuarios.

LOM (Lights Out Management)

Tecnología que proporciona comunicación fuera de banda con el servidor incluso cuando el sistema operativo no está en funcionamiento. Esto permite al administrador del sistema encender y apagar el servidor, ver las temperaturas del sistema, la velocidad de los ventiladores y otros datos, así como reiniciar el sistema desde un puesto remoto.

M

máscara de red

Número utilizado por el software para separar la dirección de subred local del resto de componentes de una dirección IP (Internet Protocol) dada.

máscara de subred

Código de bits utilizado para seleccionar bits de una dirección de Internet con los que se designará la dirección de una subred. La máscara tiene 32 bits de longitud y selecciona la parte de red de la dirección de Internet y uno o más bits de la parte local. También se denomina “máscara de dirección”.

memoria no volátil

Tipo de memoria que impide que los datos se pierdan cuando se apaga el sistema.

Message Digest 5 (MD5)

Función de hashing que convierte una cadena de datos arbitrariamente larga en un código digital corto de carácter exclusivo y tamaño fijo.

MIB (Management Information Base)

Base de datos de información administrada. Sistema jerárquico en forma de árbol que se utiliza para clasificar la información sobre los recursos de una red. La MIB define las variables a las que el agente SNMP (Simple Network Management Protocol) maestro puede acceder. La MIB se encarga de proporcionar acceso a la información sobre el estado, los datos estadísticos y la configuración de red del servidor. Esta información puede verse desde una estación de administración de red (NMS) utilizando SNMP. Por convención, a cada desarrollador se le asignan porciones de la estructura del árbol a las que puede asociar descripciones específicas de sus propios dispositivos.

módulo de supervisión del chasis (CMM)

Módulo, normalmente conectable en marcha y redundante, que funciona con el procesador de servicios (SP) de cada blade para formar un sistema de administración del chasis completo.

N

NFS (Network File System)

Sistema de archivos de red. Protocolo que hace posible el funcionamiento conjunto y transparente de diferentes configuraciones de hardware.

NIS (Network Information Service)

Servicio de información de red. Sistema de archivos de datos y programas que los sistemas UNIX utilizan para recopilar, organizar y compartir información concreta sobre las máquinas, los usuarios, los sistemas de archivos y los parámetros de red pertenecientes a una red de sistemas informáticos.

nodo

Punto o dispositivo de una red que posee una dirección. Un nodo puede conectar un sistema informático, un terminal o varios dispositivos periféricos a la red.

nombre de dominio

Nombre asignado de forma exclusiva a un sistema o grupo de sistemas en Internet. Los nombres de host de todos los sistemas del grupo poseen el mismo sufijo en el nombre de dominio, como es el caso de "sun.com". Por ejemplo, "sun.com" es, al mismo tiempo, el nombre de dominio de Sun Microsystems y un subdominio del dominio de nivel superior ".com".

nombre de dominio completo (FQDN)

Nombre completo y exclusivo de un sistema en Internet que adopta un formato similar a "www.sun.com". El FQDN incluye el nombre de un servidor central (www) y sus nombres de dominio de nivel superior (.com) y segundo nivel (.sun). Este nombre puede hacerse corresponder con una dirección IP (Internet Protocol) del sistema.

nombre de sistema

Nombre de una determinada máquina dentro de un dominio. Estos nombres siempre corresponden a una dirección IP (Internet Protocol) concreta.

nombre de usuario	Combinación de letras, y posiblemente números, con la que se identifica a un usuario en un sistema.
nombre distintivo (DN)	En el protocolo LDAP (Lightweight Directory Access Protocol), cadena de texto que identifica de forma exclusiva el nombre y la ubicación de una entrada dentro del directorio. Un DN puede ser un nombre de dominio completo (FQDN) que incluye la ruta de acceso íntegra, desde la raíz del árbol.
NTP (Network Time Protocol)	Protocolo de hora de red. Estándar de Internet para redes TCP/IP (Transmission Control Protocol/Internet Protocol). Este protocolo utiliza servidores NTP para sincronizar los relojes de los dispositivos de la red hasta el nivel de los milisegundos utilizando el formato de hora universal (UTC).
núcleo	Es el corazón del sistema operativo. Se encarga de administrar el hardware y proporcionar servicios fundamentales que el hardware no suministra, tales como el control de los archivos y la asignación de recursos.
número de identificación de usuario (número UID)	Número asignado a cada usuario que accede a un sistema UNIX. El sistema utiliza este número para identificar a los usuarios de los archivos y directorios.
número de puerto	Número que especifica una determinada aplicación TCP/IP (Transmission Control Protocol/Internet Protocol) de un host a fin de proporcionar un destino a los datos transmitidos.



O

OpenBoot^(TM) PROM	Capa de software que asume el control de los sistemas inicializados una vez que POST (pruebas de diagnóstico al encendido) ha verificado el funcionamiento correcto de los componentes. OpenBoot PROM crea estructuras de datos en la memoria y arranca el sistema operativo.
OpenIPMI	Biblioteca independiente del sistema operativo y controlada por eventos que se utiliza para simplificar el acceso a IPMI (Intelligent Platform Management Interface).
operador	Usuario (Operator) con privilegios de uso restringidos sobre el host administrado.

P

- páginas del comando**
man Documentación en línea sobre UNIX.
- paridad** Método utilizado por los equipos informáticos para comprobar si los datos recibidos coinciden con los enviados. También se refiere a la información que se guarda junto a los datos en el disco para que la controladora pueda reconstruir éstos en caso de que falle la unidad de disco.
- PEF (Platform Event Filtering)** Filtro de eventos de plataforma. Mecanismo que configura el procesador de servicios para que emprenda determinadas acciones cuando recibe mensajes de eventos, por ejemplo, apagar o reiniciar el sistema, o enviar una alerta.
- PEM (Privacy Enhanced Mail)** Correo con privacidad. Estándar para el envío de correo electrónico por Internet que cifra los datos para asegurar su confidencialidad e integridad.
- permisos** Conjunto de privilegios otorgados o denegados a un usuario o grupo de usuarios por los que se especifica su derecho de acceso de lectura, escritura o ejecución de un archivo o un directorio. En el control de acceso, los permisos determinan si se otorga o deniega el derecho de acceso a la información del directorio y el nivel de acceso que se otorga o deniega.
- PET (Platform Event Trap)** Captura de eventos de plataforma. Alerta configurada que se activa por un evento del hardware o el firmware (BIOS). PET es un formato de captura SNMP (Simple Network Management Protocol) específica de IPMI (Intelligent Platform Management Interface) que funciona con independencia del sistema operativo.
- POST (power-on self-test)** Comprobación automática al encendido. Programa que sondea y comprueba el funcionamiento de los componentes del hardware durante la inicialización del sistema. POST configura los componentes útiles en un sistema inicializado y coherente, y envía la información a la OpenBoot PROM. POST sólo pasa a la OpenBoot PROM la lista de aquellos componentes que han superado las pruebas.
- procesador de servicios (SP)** Dispositivo utilizado para administrar funciones de configuración, servicio y control del entorno, y para recibir datos de eventos procedentes de otras partes del sistema. Recibe los datos a través de las interfaces de los sensores y los interpreta utilizando el registro de datos de sensores (SDR), para el que proporciona una interfaz. El SP suministra otra interfaz con el registro de eventos del sistema (SEL). Las funciones típicas del SP son medir la temperatura de los procesadores, los valores de las fuentes de alimentación y el estado de los ventiladores. Además, puede emprender acciones de forma autónoma para mantener la integridad del sistema.

protocolo	Conjunto de reglas que describen la forma en que los sistemas o dispositivos intercambian información en la red.
protocolo SMB (Server Message Block)	Protocolo que permite compartir archivos e impresoras a través de la red. Proporciona un método para que las aplicaciones cliente realicen operaciones de lectura y escritura de archivos y soliciten servicios a los programas de servidor en la red. SMB permite montar sistemas de archivos entre sistemas Windows y UNIX. Fue diseñado por IBM y posteriormente modificado por Microsoft Corp., quien cambió su nombre por el de CIFS (Common Internet File System).
proxy	Mecanismo por el cual un sistema actúa en sustitución de otro al responder a las peticiones de los protocolos.
puerta de enlace	Equipo informático o programa que interconecta dos redes y transmite los paquetes de datos entre ellas. Una puerta de enlace posee más de una interfaz de red.
puerto	Ubicación (socket) con la que se establecen las conexiones TCP/IP (Transmission Control Protocol/Internet Protocol). Normalmente, los servidores web utilizan el puerto 80, el protocolo FTP (File Transfer Protocol) utiliza el puerto 21 y Telnet, el puerto 23. El puerto permite a un programa cliente especificar un determinado programa de servidor instalado en un equipo informático conectado a una red. Cuando se inicia el programa de servidor, enlaza con el número de puerto que tiene designado. Cualquier cliente que quiera utilizar ese servidor, deberá enviar una petición para establecer conexión con el puerto designado.
PXE (Preboot Execution Environment)	Entorno de ejecución previo al arranque. Interfaz cliente/servidor estándar que permite a los servidores arrancar el sistema operativo a través de una red TCP/IP (Transmission Control Protocol/Internet Protocol) utilizando el protocolo DHCP (Dynamic Host Configuration Protocol). La especificación PXE describe cómo interaccionan la tarjeta de red y la BIOS a fin de proporcionar las funciones de red básicas para ejecutar la rutina de carga principal, lo que permite ejecutar otra rutina de carga secundaria a través de la red, como puede ser la carga de una imagen del SO a través de TFTP. De esta forma, la rutina de carga principal, si está codificada según las normas PXE, no necesita conocer el hardware de conexión de red del sistema.

R

- rearranque** Operación del sistema operativo que cierra el sistema y vuelve a arrancarlo. Es preciso disponer de energía para llevarlo a cabo.
- red de área amplia (WAN)** Red compuesta de muchos sistemas que proporciona servicios de transferencia de archivos. Una WAN puede cubrir una zona geográfica de gran extensión, incluso de ámbito mundial.
- red de área local (LAN)** Grupo de sistemas situados a poca distancia entre sí que se comunican a través de componentes de hardware y software de conexión. La tecnología más utilizada para las LAN es Ethernet.
- redirección** Envío de los datos de entrada o salida a un archivo o dispositivo alternativo en lugar de utilizar la entrada o salida estándar de un sistema. Como resultado, la redirección toma los datos de entrada o salida que habitualmente se verían en un sistema y los transmite a la pantalla de otro sistema.
- registro de eventos del sistema (SEL)** Registro que proporciona almacenamiento no volátil de los eventos del sistema, los cuales se registran de forma autónoma a través del procesador de servicios o directamente con los mensajes de eventos enviados desde el host.
- reinicio** Operación realizada en el nivel del hardware por la cual se apaga el sistema y vuelve a encenderse.
- reloj de tiempo real (RTC)** Componente con batería que mantiene la hora y la fecha de los sistemas incluso cuando éstos están apagados.
- resolución de direcciones** Forma de convertir las direcciones de Internet en direcciones MAC (Media Access Control) de acceso físico o direcciones de dominio.
- RMCP (Remote Management and Control Protocol)** Protocolo de red que permite a un administrador responder a una alerta de forma remota apagando o encendiendo el sistema, o bien forzando su rearranque.
- root** Nombre del superusuario (root) en los sistemas operativos UNIX. Este usuario tiene permisos para acceder a cualquier archivo y realizar otras operaciones no permitidas para los usuarios comunes. Equivale, más o menos, al usuario administrador (Administrator) de los sistemas operativos Windows Server.
- RPC (Remote Procedure Call)** Método de programación para red que permite a los sistemas cliente hacer llamadas a funciones situadas en un servidor remoto. El cliente inicia un procedimiento en el servidor y el resultado se transmite de vuelta al cliente.

S

SDR (Sensor Data Record)	Registro de datos de sensores. IPMI (Intelligent Platform Management Interface) incluye este conjunto de registros para facilitar la detección dinámica de recursos y características. Incluye datos de software tales como el número y tipo de sensores presentes, sus eventos y sus umbrales, entre otros. Con estos registros, el software puede interpretar y comunicar la información de los sensores sin ningún conocimiento previo de la plataforma.
servidor de directorio	En el protocolo LDAP (Lightweight Directory Access Protocol), servidor que almacena y suministra información sobre las personas y los recursos de una organización desde una ubicación lógica centralizada.
servidor de seguridad	Configuración de red, normalmente compuesta por elementos de hardware y software, que protege a los equipos conectados de una organización de accesos provenientes del exterior. El servidor de seguridad puede supervisar o prohibir conexiones procedentes de, o dirigidas a, determinados servicios o hosts.
servidor LDAP (Lightweight Directory Access Protocol)	Software de servidor que mantiene un directorio LDAP y le envía las peticiones de información. Sun Directory Services y Netscape Directory Services son implementaciones de un servidor LDAP.
servidor web	Software que proporciona servicios de acceso a Internet o a una intranet. Un servidor web aloja sitios web, proporciona funcionalidad para usar HTTP/HTTPS y otros protocolos, y ejecuta programas de servidor.
sistema de archivos	Método homogéneo que se utiliza para organizar y guardar la información en los medios de almacenamiento físicos. Cada sistema operativo suele tener un sistema de archivos diferente. A menudo, los sistemas de archivos son una red de archivos y directorios estructurados en forma de árbol, con una raíz como directorio superior y sucesivos directorios subordinados situados debajo de ella.
sistema remoto	Sistema distinto de aquel en el que trabaja el usuario.
Sistema X Windows	Sistema de ventanas habitual en UNIX que permite a una estación de trabajo o terminal controlar varias sesiones de forma simultánea.
SMTP (Simple Mail Transfer Protocol)	Protocolo simple de transferencia de correo. Protocolo de TCP/IP (Transmission Control Protocol/Internet Protocol) utilizado para enviar y recibir correo.

SNMP (Simple Network Management Protocol)

Protocolo simple de administración de red. Protocolo simple utilizado para intercambiar datos sobre la actividad de la red. Mediante SNMP, los datos viajan entre un dispositivo administrado y una estación de administración de red (NMS). Por dispositivo administrado se entiende cualquier dispositivo que ejecute SNMP, lo que incluye hosts, encaminadores, servidores web y otros servidores de la red.

SSH (Secure Shell)

Protocolo de shell seguro. Programa de shell UNIX y protocolo de red que permite iniciar sesiones seguras y cifradas, así como ejecutar comandos en un sistema remoto a través de una red no segura.

SSL (Secure Sockets Layer)

Capa de sockets seguros. Protocolo que permite cifrar la comunicación cliente/servidor en una red para garantizar la privacidad. Utiliza un método de intercambio de claves para establecer un entorno en el que todos los datos intercambiados se cifran con un sistema de cifrado y hashing a fin de protegerlos de alteraciones o escuchas furtivas. SSL crea conexiones seguras entre servidores web y clientes web. El protocolo HTTPS (Hypertext Transfer Protocol Secure) utiliza SSL.

subred

Esquema de funcionamiento que divide una red lógica sencilla en redes físicas más pequeñas para simplificar el encaminamiento. La subred es la porción de una dirección IP (Internet Protocol) que identifica un bloque de ID de hosts.

superusuario

Tipo especial de usuario que tiene privilegios para realizar todas las funciones administrativas en un sistema UNIX. También se denomina "root".

T

tarjeta de interfaz de red (NIC)

Placa o tarjeta de circuito impreso interna que conecta una estación o un servidor a un dispositivo de la red.

TCB (Transmission Control Block)

Bloque de control de la transmisión. Parte del protocolo TCP/IP (Transmission Control Protocol/Internet Protocol) que registra y mantiene información sobre el estado de la conexión.

TCP/IP (Transmission Control Protocol/Internet Protocol)

Protocolo de Internet que posibilita la entrega fiable de secuencias de datos de un host a otro. TCP/IP transfiere los datos entre distintos tipos de sistemas de red donde puede ejecutarse software de Solaris, Microsoft Windows o Linux. TCP garantiza la entrega de los paquetes en el mismo orden en el que se hayan enviado.

Telnet	Programa de terminal virtual que permite al usuario de un host iniciar la sesión en un host remoto. El usuario que haya iniciado la sesión en el host remoto puede interactuar como si fuera un usuario de terminal normal de dicho host.
TFTP (Trivial File Transport Protocol)	Protocolo de transporte simple que transfiere archivos a los sistemas utilizando UDP (User Datagram Protocol).
tiempo de espera excedido	Periodo especificado después del cual el servidor debería dejar de intentar terminar la rutina de un servicio que parece haberse bloqueado.
tiempo de espera para finalizar la sesión	Periodo especificado después del cual un servidor puede invalidar una sesión de usuario.

U

UDP (User Datagram Protocol)	Protocolo de datagramas de usuario. Protocolo de transporte sin establecimiento previo de conexión que añade cierta fiabilidad y multiplexación a IP (Internet Protocol). Permite a un programa enviar datagramas (a través de IP) a otro programa situado en otra máquina. El protocolo SNMP (Simple Network Management Protocol) normalmente se implementa sobre UDP.
umbral	Valores mínimo y máximo de una escala que los sensores utilizan como referencia al supervisar la temperatura, el voltaje, la corriente y la velocidad de los ventiladores.
unidad sustituible por el cliente (CRU)	Componente del sistema que el usuario puede reemplazar sin necesidad de formación o herramientas especiales.
USB (Universal Serial Bus)	Bus serie universal. Estándar de bus externo que proporciona tasas de transferencias de datos de 450 millones de bits por segundo (USB 2.0). Los puertos USB permiten conectar dispositivos tales como el ratón.

V

velocidad de baudios	Velocidad a la que se transmite la información entre dispositivos, por ejemplo, entre un terminal y un servidor.
-----------------------------	--

X

XIR (reinicio externo) Una señal que envía una petición de reinicio por software al procesador de un dominio. XIR no arranca el dominio. Normalmente se utiliza para salir de una situación de bloqueo del sistema y entrar en el indicador de la consola. A continuación, el usuario puede generar un archivo de volcado del núcleo, que puede ser de utilidad para diagnosticar la causa del bloqueo.

Índice

A

- acceso a la web mediante HTTP o HTTPS
 - habilitación mediante la interfaz web, 176 a 178
 - habilitación mediante la línea de comandos, 167
- Active Directory
 - configuración, 85 a 89
 - configuración mediante la interfaz web, 85
 - descripción general, 84
 - determinación de los niveles de autorización, 91
 - dominios y grupos, 88
 - finalidades, 84
 - propiedades de configuración, 86
 - seguridad con un certificado SSL, 92
- administración de errores
 - supervisión y diagnóstico del hardware, 131
 - visualización de los componentes defectuosos, 132 a 133
- administrador, función
 - definición, 6
 - necesaria para ejecutar Remote Console, 217
- alertas
 - administración desde la línea de comandos, 152
 - advertencias de errores del sistema, 143
 - definición de reglas de alerta, 144, 147
 - envío de capturas de eventos SNMP, 191
 - especificación del destino, 145
 - generación de alertas de prueba, 150
 - generación de notificaciones por correo electrónico, 157
 - inhabilitación de reglas de alerta, 150
 - modificación de reglas de alertas, 149
 - tipos admitidos, 144, 145, 191
 - tipos de niveles, 146

- asignación de direcciones IP
 - direcciones asignadas mediante DHCP, 23 a 24
 - direcciones estáticas asignadas al CMM, 27 a 28
 - direcciones estáticas asignadas al SP, 25 a 26
 - edición mediante la interfaz web, 29 a 30
 - edición mediante la línea de comandos, 31 a 32
- asignación de los puertos de red
 - identificación para el SP y el CMM, 20 a 21

C

- capturas de eventos de SNMP
 - configuración de los destinos mediante la interfaz web, 201
 - configuración de los destinos mediante la línea de comandos, 195
 - ejemplo, 205
- carga del certificado SSL
 - mediante la interfaz web, 61
- cierre de la sesión de ILOM
 - mediante la interfaz de la línea de comandos, 45
 - mediante la interfaz web, 63
- comandos de la CLI
 - comandos de acceso al sistema, 234
 - comandos de administración de alertas, 234
 - comandos de administración de usuarios, 233
 - comandos de administración del sistema host, 235
 - comandos de configuración de la red y el puerto serie, 233
 - comandos de configuración del reloj, 236
 - comandos de SNMP, 235
 - comandos generales, 232
 - sintaxis, 232

- conexión de la consola serie
 - configuración de los valores serie, 19
- configuración de red
 - configuración mediante la interfaz web, 173 a 175
 - configuración mediante la línea de comandos, 163
 - propiedades pendientes y activas, 163
 - visualización mediante la interfaz web, 173
 - visualización mediante la línea de comandos, 163
- configuración de SSH
 - cifrado de claves mediante la línea de comandos, 169
- configuración del estado de la alimentación
 - configuración para Remote Console, 221
- configuración del modo de ratón
 - configuración para Remote Console, 221
- configuración del puerto serie
 - configuración mediante la interfaz web, 176
 - configuración mediante la línea de comandos, 166
 - propiedades pendientes y activas, 166
 - puertos interno y externo, 165
 - valores predeterminados, 176
 - visualización mediante la interfaz web, 175
 - visualización mediante la línea de comandos, 165
- configuración del reloj
 - mediante la interfaz web, 129, 140
 - mediante la línea de comandos, 130
- consola serie del host, 165
- contraseña de la cuenta root
 - cambio mediante la interfaz web, 68
 - cambio mediante la línea de comandos, 70
- cuenta de administrador
 - nombre de usuario y contraseña predeterminados, 68
- cuentas de usuario
 - adición mediante la línea de comandos, 72
 - adición y establecimiento de privilegios mediante la interfaz web, 76
 - configuración mediante la línea de comandos, 74
 - especificación de los nombres, 67
 - funciones asignadas, 6
 - modificación mediante la interfaz web, 79
 - modificación mediante la línea de comandos, 73
 - número de cuentas admitidas, 67

- privilegios de administrador, 67
- supresión mediante la interfaz web, 82
- supresión mediante la línea de comandos, 73
- visualización de una cuenta específica, 73
- visualización de una lista, 73
- visualización de una sesión específica mediante la línea de comandos, 75
- visualización mediante la interfaz web, 83
- visualización mediante la línea de comandos, 75

- cuentas de usuario de SNMP
 - administración mediante la interfaz web, 196 a 201
 - administración mediante la línea de comandos, 192 a 195
 - destinos, propiedades y valores, 194

D

- DHCP (Dynamic Host Configuration Protocol)
 - requisitos para asignar direcciones IP, 15
 - uso para asignar direcciones IP, 14
- dirección IP (Internet Protocol)
 - asignación de direcciones IP estáticas, 18
 - identificación de la dirección asignada por DHCP, 15
- dirección IP estática
 - requisitos de asignación, 18
- dirección MAC (Media Access Control)
 - obtención para el SP o el CMM, 15

E

- espacios de nombres
 - acceso mediante el SP, 39

F

- funciones de supervisión del sistema
 - descripción general, 121

H

- hardware
 - redirección del teclado y el ratón, 225

I

- indicadores del sistema
 - condiciones de iluminación, 125
 - estados asignados por el sistema, 126
 - estados modificables por el usuario, 125
 - visualización mediante la interfaz web, 126
 - visualización mediante la línea de comandos, 127

- inicio de la sesión de ILOM
 - mediante la interfaz de la línea de comandos, 44
 - mediante la interfaz web, 58
 - Integrated Lights Out Manager (ILOM)
 - actualización del firmware mediante la interfaz web, 210 a 211
 - actualización del firmware mediante la línea de comandos, 209
 - características, 7
 - comandos
 - comando `set` (ILOM), blades, tabla de opciones, 26
 - conexión con, 5
 - configuración inicial, 12
 - configuración para Remote Console, 218
 - contraseña de la cuenta root, 68
 - cuenta de administrador preconfigurada
 - inicio de la sesión, 68
 - descripción general, 1
 - funciones asignadas a las cuentas, 6
 - funciones de supervisión del sistema, 121
 - funciones nuevas de la versión 2.0, 9
 - inicio de la sesión mediante la interfaz web, 58
 - interfaces, 3
 - redirección del teclado y el ratón, 225
 - reinicio del SP mediante la interfaz web, 211
 - Remote Console, configuración y ejecución, 223
 - uso de herramientas de terceros, 9
 - uso de Sun N1 System Manager, 9
 - visualización de la versión mediante la interfaz web, 209
 - visualización de la versión mediante la línea de comandos, 208
 - interfaz de la línea de comandos (CLI)
 - cierre de la sesión de ILOM, 45
 - descripción general, 3, 37
 - especificación de base, 38
 - inicio de la sesión de ILOM, 44
 - referencia abreviada de comandos, 231 a 236
 - referencia de comandos, 237 a 251
 - sintaxis de los comandos, 40
 - tipos de destinos de ILOM, 39
 - uso de la arquitectura jerárquica, 39
 - interfaz web
 - botones, 49
 - carga del certificado SSL, 61
 - componentes, 49
 - Configuration, ficha, 53
 - descripción general, 3, 47
 - inicio de la sesión, 58
 - Maintenance, ficha, 57
 - navegadores compatibles, 48
 - Remote Control, ficha, 56
 - System Information, ficha, 50
 - System Monitoring, ficha, 52
 - tipos de acceso, 176
 - User Management, ficha, 55
 - IPMI (Intelligent Platform Management Interface)
 - alertas PET (Platform Event Trap), 181
 - controlador de administración de la placa base, 180
 - descripción general, 3, 179
 - funciones, 179
 - utilización de IPMITool, 180
 - versiones compatibles con ILOM, 180
 - IPMITool
 - ejemplos de uso, 182 a 185
 - funciones, 181
 - información de referencia, 181
- ## L
- LDAP
 - configuración de ILOM para LDAP, 100 a 101
 - configuración del servidor LDAP, 99
 - descripción general, 96
 - estructura del directorio, 96 a 98
 - modelo cliente-servidor, 96
 - nombres distintivos, 98
 - operaciones de los clientes, 96
 - lecturas de los sensores
 - clases admitidas, 123
 - obtención mediante la interfaz web, 122
 - obtención mediante la línea de comandos, 123
 - supervisión y diagnóstico de fallos, 131
 - tipos de datos comunicados, 121
- ## M
- MIB (Management Information Base)
 - archivos MIB utilizados con ILOM, 190
 - descripción, 190
 - módulo de supervisión del chasis (CMM)
 - administración con ILOM, 2
 - módulo de supervisión del chasis (CMM), configuración de direcciones IP
 - edición mediante una conexión Ethernet, 29 a 30
 - inicialización
 - mediante asignación estática, 27 a 28
 - mediante DHCP, 24

- módulos de servidor blade, configuración de direcciones IP
 - comando `set` (ILOM), tabla de opciones, 26
 - edición mediante una conexión Ethernet, 29 a 30
 - inicialización
 - mediante asignación estática, 25 a 26
 - mediante DHCP, 23 a 24

N

- nombres distintivos
 - utilizados con LDAP, 98

O

- opciones de diagnóstico de PC-Check
 - configuración para Remote Console, 221
- operador, función, 6

P

- procesador de servicios (SP)
 - administración con ILOM, 2
- proceso de actualización del firmware
 - descripción general, 208
- puerto de administración de red
 - conexión con ILOM, 4
- puerto de administración Ethernet
 - conexión con ILOM, 5, 13
 - etiqueta en el servidor, 13
- puerto serie de administración
 - conexión con ILOM, 13
- puerto serie externo
 - configuración de la velocidad de baudios, 176
- puerto serie interno, 165
 - configuración de la velocidad de baudios, 176

R

RADIUS

- comandos, 104 a 106
- configuración, 103
- descripción general, 102
- modelo cliente-servidor, 102
- número de puerto predeterminado, 106
- parámetros de configuración, 103

red de administración

- asignación de direcciones IP, 20
- comparación con una red de datos, 4
- descripción general, 4

red de datos

- comparación con una red de administración, 4, 20

redirección de dispositivos

- comportamiento durante la sesión de Remote Console, 229

registro de eventos

- anotación de las marcas de tiempo, 129
- tipos de eventos visualizados, 128
- visualización y borrado mediante la interfaz web, 136
- visualización y borrado mediante la línea de comandos, 138

reinicio de ILOM

- mediante la interfaz web, 211

Remote Console

- adición de otra sesión de servidor, 224
- conexión mediante la interfaz web, 218 a 219
- configuración de las opciones de control remoto, 219 a 221
- control de la redirección de dispositivos, 224 a 225
- descripción general, 3, 214
- ejecución mediante la interfaz web, 222 a 223
- inicio de sesión como administrador, 217
- opciones de control remoto, 221
- puertos y protocolos de red, 217
- redirección de dispositivos de almacenamiento o imágenes ISO, 227 a 228
- redirección del teclado y el ratón, 225
- requisitos de instalación, 216
- salida de la aplicación, 228
- uso de los modos de control del teclado, 226
- vistas de uno y varios servidores, 215

S

sensores de umbrales

- obtención de lecturas, 123

sensores discretos

- obtención de lecturas, 124

`set`, comando (ILOM)

- opciones de blade, tabla, 26

Single Sign On

- descripción general, 71
- habilitación o inhabilitación mediante la interfaz web, 71
- habilitación o inhabilitación mediante la línea de comandos, 71
- uso para ejecutar Remote Console, 217

sintaxis de los comandos de la CLI

- cd, comando, 237
- create, comando, 238
- delete, comando, 239
- exit, comando, 239
- help, comando, 240
- load, comando, 241
- reset, comando, 242
- set, comando, 243
- show, comando, 246
- start, comando, 250
- stop, comando, 250
- version, comando, 251

sistema operativo Solaris 10, configuración del SO instalado en fábrica

- uso de una conexión Secure Shell (SSH), 168
 - procedimiento, 155, 156, 159

SNMP (Simple Network Management Protocol)

- base de datos de información de administración (MIB), 190
- descripción general, 3, 188
- ejemplos de uso, 202 a 205
- funciones de los agentes, 189
- supervisión de la estación de administración, 189
- versiones admitidas, 188

ssh, comando (Solaris)

- conexión con un SP, 31, 35, 138, 142, 154, 156, 157, 159, 168

U

unidades sustituibles en campo (FRU)

- obtención de lecturas de los sensores, 122

V

- velocidad en baudios, configuración, 176

