Guía de administración del servidor Netra™ T2000

Sun Microsystems, Inc.
www.sun.com

Referencia 819-7336-10
Septiembre 2006, revisión A

Envíe sus comentarios sobre este documento desde: http://www.sun.com/hwdocs/feedback

Papel para reciclar

Contenido

Figuras

Tablas

Prólogo

La *Guía de administración del servidor Netra T2000* proporciona información y procedimientos detallados para administrar y gestionar el servidor Netra™ T2000. Los destinatarios de este documento son los técnicos, administradores de sistema, proveedores de servicio autorizados (ASP) y usuarios que tengan una amplia experiencia en la administración de los sistemas servidor.

Organización del documento

En el Capítulo 1 se explica cómo acceder a la consola del sistema para habilitar la gestión y administración remotas.

En el Capítulo 2 se describe la utilización de Advanced Lights Out Manager (ALOM) para la administración remota del servidor.

En el Capítulo 3 se describe el funcionamiento, los métodos de visualización y la configuración de OpenBoot™ PROM.

En el Capítulo 4 se describen los indicadores de estado y las tareas básicas que se realizan para la administración del sistema.

En el Capítulo 5 se proporciona información importante sobre la seguridad del sistema.

En el Capítulo 6 se describen los conceptos de la matriz redundante de discos independientes (RAID).

En el Apéndice A se proporciona información sobre el modo para aplicaciones del mecanismo de vigilancia del servidor.

En el Apéndice B se proporciona un programa de ejemplo que ilustra cómo se obtiene y define el estado de las alarmas.

Uso de comandos UNIX

Es posible que este documento no contenga información sobre procedimientos y comandos básicos de UNIX® tales como el cierre e inicio del sistema o la configuración de los dispositivos. Para obtener este tipo de información, consulte lo siguiente:

- La documentación del software entregado con el sistema
- La documentación de Solaris™, que se encuentra en:

  http://docs.sun.com

Indicadores de shell

Shell	Indicador
Shell de C	*nombre-máquina*%
Superusuario de C	*nombre-máquina*#
Shells de Bourne y Korn	$
Superusuario de shells de Bourne y Korn	#

Convenciones tipográficas

Tipo de letra*	Significado	Ejemplos
AaBbCc123	Se utiliza para indicar nombres de comandos, archivos y directorios; mensajes-del sistema que aparecen en la pantalla.	Edite el archivo .login. Utilice ls -a para ver la lista de todos los archivos. % Tiene correo.
AaBbCc123	Lo que escribe el usuario, a diferencia de lo que aparece en pantalla.	% **su** Password:
AaBbCc123	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 *Manual del usuario*. Se conocen como opciones de *clase*. Para efectuar esta operación, *debe* estar conectado como superusuario. Para borrar un archivo, escriba rm *nombre de archivo*.

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

Documentación relacionada

Los documentos disponibles en Internet se encuentran en la dirección:

http://www.sun.com/products-n-solutions/hardware/docs/

Aplicación	Título	Número de referencia	Formato	Ubicación
Instalación	*Guía de instalación del servidor Netra T2000*	819-7361-10	PDF	En línea
Actualizaciones	*Netra T2000 Server Product Notes*	819-5840-10	PDF	En línea
Mantenimiento	*Netra T2000 Server Service Manual*	819-5841-10	PDF	En línea
Planificación	*Netra T2000 Server Site Planning Notes*	819-5842-10	PDF	En línea
Cumplimiento	*Netra T2000 Server Safety and Compliance Guide*	819-5843-10	PDF	En línea
Documentación	*Guía de procedimientos iniciales del servidor Netra T2000*	819-7344-10	Impreso PDF	Kit de envío En línea
Referencia	*Guía de ALOM CMT 1.2*	819-7133-10	PDF	En línea

Documentación, asistencia técnica y formación

Servicio de Sun	Dirección
Documentación	http://www.sun.com/documentation/
Servicio técnico	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 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. Para enviar comentarios, visite la dirección:

`http://www.sun.com/hwdocs/feedback`

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

Guía de administración del servidor Netra T2000, número de referencia 819-7336-10.

CAPÍTULO 1

Consola del sistema

Este capítulo explica cómo acceder a la consola del sistema para habilitar la gestión y administración remotas. El capítulo está dividido en las siguientes secciones:

Comunicación con la consola del sistema

El administrador necesita una manera de interactuar con el servidor en un nivel bajo, a fin de configurar el comportamiento de E/S básico y el arranque del servidor. La consola del sistema permite al administrador realizar estas tareas utilizando comandos especiales. Además, la consola del sistema muestra mensajes de información, de estado y de error generados por el firmware durante el encendido y el funcionamiento del servidor. Después de iniciar el entorno operativo, la consola muestra mensajes de Solaris y acepta comandos de Solaris.

El servidor dispone de dos puertos de E/S dedicados para la consola del sistema:

- SC SERIAL MGT
- SC NET MGT

Puerto serie de gestión

El puerto serie de gestión (SC SERIAL MGT) es la conexión predeterminada de la consola del sistema. Este puerto utiliza un conector RJ-45 en una conexión serie. Para la comunicación con el controlador del sistema mediante este puerto se requieren los siguientes parámetros serie:

- 9600 baudios
- 8 bits

- Sin paridad
- 1 bit de parada
- Sin protocolo de enlace

Los dispositivos serie que se pueden comunicar con el puerto serie de gestión son:

- Servidor de terminales
- Línea TIP conectada a otro sistema de Sun™
- Terminal alfanumérico o un dispositivo similar

Como es una conexión serie, sólo puede haber comunicación entre dos dispositivos. Esta restricción limita el acceso y ofrece un enlace más seguro entre el administrador y el servidor.

El puerto serie de gestión no es un puerto serie de propósito general. Está dedicado al controlador del sistema. Si desea utilizar un dispositivo periférico en serie, conéctelo al puerto serie de 9 patillas estándar que se encuentra en el panel posterior del servidor. El entorno operativo Solaris reconoce este puerto como TTYA, tal como está etiquetado.

Comunicación con el puerto serie de gestión

▼ Para acceder a la consola del sistema mediante un servidor de terminales

1. **Establezca la conexión física entre el puerto serie de gestión y el servidor de terminales.**

   El puerto serie de gestión del servidor es de tipo DTE (terminal de datos). Compruebe que las patillas del puerto serie del servidor coinciden con las del servidor de terminales que va a utilizar.

   - Si la asignación de señales del puerto serie de gestión del servidor coincide con la del puerto RJ-45 del servidor de terminales, dispone de dos opciones de conexión:
     - Conectar un cable de interfaz serie multifibra directamente al servidor.
     - Conectar el cable serie multifibra a un panel de conexiones y utilizar el cable recto (suministrado por Sun) para conectar el panel de conexiones al servidor.
   - Si la asignación de señales del puerto serie de gestión del servidor *no* coincide con la del puerto RJ-45 del servidor de terminales, tendrá que construir un cable cruzado. La TABLA 1-1 muestra la asignación de señales para el cable cruzado.

TABLA 1-1 Correspondencias entre las patillas para la conexión con un servidor de terminales típico mediante un cable cruzado

Patilla del puerto serie (conector RJ-45) del servidor	Patilla del puerto serie del servidor de terminales
Patilla 1 (RTS)	Patilla 1 (CTS)
Patilla 2 (DTR)	Patilla 2 (DSR)
Patilla 3 (TXD)	Patilla 3 (RXD)
Patilla 4 (señal de tierra)	Patilla 4 (señal de tierra)
Patilla 5 (señal de tierra)	Patilla 5 (señal de tierra)
Patilla 6 (RXD)	Patilla 6 (TXD)
Patilla 7 (DSR /DCD)	Patilla 7 (DTR)
Patilla 8 (CTS)	Patilla 8 (RTS)

2. **Abra una sesión de terminal en el dispositivo de conexión y escriba:**

```
% telnet dirección-IP-servidor-terminales  número-puerto
```

Por ejemplo, en el caso de un servidor conectado al puerto 10000 de un servidor de terminales cuya dirección IP sea 192.20.30.10, debería escribir:

```
% telnet 192.20.30.10 10000
```

▼ Para acceder a la consola del sistema mediante la conexión TIP

1. **Conecte el cable serie RJ-45 y, si es necesario, el adaptador DB-9 o DB-25 suministrado.**

   El cable y el adaptador permiten establecer la conexión entre el puerto serie de otro sistema Sun (normalmente TTYB) y el puerto serie de gestión situado en el panel posterior del servidor.

2. **Asegúrese de que el archivo** `/etc/remote` **del sistema Sun contenga una entrada de** `hardwire`**.**

   Consulte la TABLA 1-2.

TABLA 1-2 Entradas de `hardwire` en el archivo `/etc/remote`

Puerto serie	Entrada de `hardwire`
`ttya`	`hardwire:\` `:dv=/dev/term/a:br#9600:el=^C^S^Q^U^D:ie=%$:oe=^D:`
`ttyb`	`hardwire:\` `:dv=/dev/term/b:br#9600:el=^C^S^Q^U^D:ie=%$:oe=^D:`

3. **Desde una ventana de terminal del sistema Sun, escriba:**

```
% tip hardwire
```

   El sistema Sun responde con el siguiente mensaje:

```
connected
```

   El servidor y el sistema de Sun se están comunicando.

▼ Para acceder a la consola del sistema mediante un terminal alfanumérico

1. **Conecte un extremo del cable serie al puerto serie del terminal alfanumérico.**

   Utilice un cable serie cruzado o un cable serie RJ-45 y el adaptador correspondiente (null modem). Conecte el cable al puerto serie del terminal.

2. **Conecte el otro extremo del cable serie al puerto serie de gestión del servidor.**

3. **Encienda el terminal alfanumérico.**

4. **Configure el terminal para recibir los datos con la siguiente configuración:**

   - 9600 baudios
   - 8 bits
   - Sin paridad
   - 1 bit de parada
   - Sin protocolo de enlace

   Consulte la documentación entregada con el terminal para obtener información sobre la forma de configurarlo y utilizarlo.

Puerto de gestión de red

El puerto de gestión de red (SC NET MGT) permite la comunicación con el controlador del sistema mediante la red Ethernet existente. Es un puerto 10/100BASE-T con una dirección IP exclusiva distinta de la dirección IP del servidor. Como en el caso del puerto serie de gestión, el puerto de gestión de red está dedicado al controlador del sistema. A diferencia del puerto serie de gestión, admite hasta ocho sesiones simultáneas del controlador del sistema. Por lo tanto, se requiere un estricto control del acceso al controlador del sistema.

Antes de poder utilizar el puerto de gestión de red, es necesario asignarle la dirección IP exclusiva por medio del puerto serie de gestión. Puede asignar una dirección IP estática o configurar el controlador del sistema para que encuentre una dirección IP dinámica, utilizando DHCP.

Nota – Los centros de procesamiento de datos (CPD) suelen dedicar una subred a la administración de sistemas. Si la configuración de su CPD responde a este modelo, conecte el puerto de gestión de red a esta subred.

▼ Para activar el puerto de gestión de red

1. **Conecte un cable Ethernet al puerto de gestión de red.**
2. **Abra una sesión del controlador del sistema a través del puerto serie de gestión.**
   Consulte "Comunicación con el puerto serie de gestión" en la página 2.
3. **Escriba uno de los comandos siguientes:**
   - **Si la red utiliza direcciones IP estáticas, especifique:**

```
sc> setsc if_network true
sc> setsc netsc_ipaddr dirección-ip
sc> setsc netsc_ipnetmask dirección-ip
sc> setsc netsc_ipgateway dirección-ip
```

   - **Si la red utiliza DHCP, escriba:**

```
sc> setsc netsc_dhcp true
```

4. **Reinicie el controlador del sistema para que la nueva configuración tenga efecto:**

```
sc> resetsc
```

5. **Una vez que el sistema se reinicie, utilice el comando `shownetwork` para verificar la configuración de red:**

```
sc> shownetwork
```

6. **Salga de la sesión del controlador del sistema.**

```
sc> console
```

Si quiere establecer la conexión a través del puerto de gestión de red, utilice el comando `telnet` para indicar la dirección IP especificada en el paso 3 de la sección "Para activar el puerto de gestión de red" en la página 5.

Cambio de consola

La conexión a la consola del controlador del sistema proporciona acceso al shell de ALOM, al entorno operativo Solaris, y a la consola de OpenBoot PROM.

En esta sección se describen los procedimientos para desplazarse entre:

- ALOM (indicador `sc>`)
- El entorno operativo Solaris (indicador `#`)
- OpenBoot PROM (indicador `ok`)

Estos procedimientos se resumen en la FIGURA 1-1.

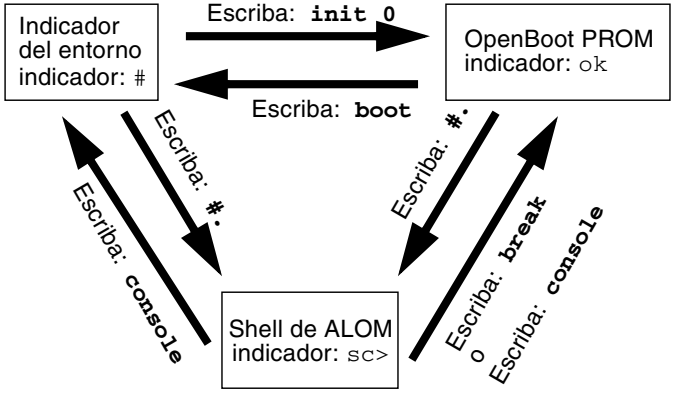

FIGURA 1-1 Procedimientos de navegación entre consolas

Indicador sc> de ALOM

ALOM se ejecuta con independencia del servidor y del estado de la alimentación del sistema. Al conectar el servidor a la alimentación de CA, ALOM se inicia de inmediato y empieza a supervisar el sistema.

Nota – Para ver los mensajes de inicio generados por ALOM, es preciso conectar un terminal alfanumérico al puerto serie de gestión *antes* de conectar los cables de alimentación de CA al servidor.

La presencia del indicador `sc>` significa que se está interaccionando con ALOM directamente. Es el primer indicador que aparece al iniciar la sesión en el sistema a través de cualquiera de los puertos de gestión e independientemente del estado de la alimentación del sistema.

Nota – Al acceder a ALOM por primera vez y ejecutar un comando de administración, el controlador obliga a crear una contraseña (asociada al nombre de usuario predeterminado `admin`) para posteriores accesos. Tras esta configuración inicial, aparecerá un mensaje solicitando la introducción de un nombre y una contraseña cada vez que acceda a ALOM.

Para obtener más información sobre ALOM, consulte el Capítulo 2.

▼ Para obtener el indicador ALOM desde la consola de Solaris

- **Cuando esté conectado con la consola de Solaris, escriba la secuencia de escape para que la consola pase al indicador de ALOM.**

  La secuencia de escape predeterminada es `#.` (almohadilla punto).

  Por ejemplo, si la secuencia de escape es la predeterminada (`#.`), puede escribir:

```
# #.
sc>
```

Nota – A diferencia del ejemplo, no aparecerá `#`.

Si escribe el primer carácter de la secuencia de escape, transcurrirá un segundo antes de que el carácter aparezca en la pantalla. Durante este intervalo, debe escribir el segundo carácter de la secuencia de escape. Si la secuencia de escape se escribe dentro del intervalo de un segundo, aparece el indicador `sc>`. Cualquier carácter escrito después del segundo carácter de escape se agrega al indicador `sc>`.

Si el segundo carácter de escape no es correcto o escribe después del intervalo de un segundo, todos los caracteres aparecerán junto al indicador original.

▼ Para ver el indicador ALOM desde OpenBoot PROM

- **Escriba la secuencia de caracteres de escape.**

  La secuencia de escape predeterminada es `#.` (almohadilla punto).

```
{2} ok #.
sc>
```

Nota – A diferencia del ejemplo, no aparecerá `#`.

▼ Para conectarse a la consola de Solaris desde el indicador ALOM

- **Utilice el comando `console` desde el indicador ALOM.**
  - Si se está ejecutando el software Solaris en el sistema, aparece el indicador de Solaris:

```
sc>console
#
```

  - Si el sistema está en OpenBoot PROM, aparece el indicador de OpenBoot PROM:

```
sc>console
{2} ok
```

  - Si el servidor está en modo de espera, se genera el siguiente mensaje:

```
sc>console
Solaris is not active
```

Nota – El comando `console` intenta primero una conexión con la consola de Solaris. Si no está disponible la consola, el comando `console` intenta una conexión con OpenBoot PROM. Si el intento no tiene éxito, aparece este mensaje: `Solaris is not active`.

Indicador `ok` de OpenBoot PROM

Un servidor con el sistema operativo Solaris instalado funciona con distintos *niveles de ejecución*. La mayor parte del tiempo, el servidor opera en los niveles de ejecución 2 o 3, que son los estados multiusuario con acceso al sistema completo y los recursos de red. A veces es posible manejar el sistema en el nivel de ejecución 1, que es un estado de administración con un solo usuario. Pero el estado operativo más bajo es el de nivel 0, un estado en el que se puede apagar el sistema sin riesgos.

Cuando un servidor se encuentra en el nivel de ejecución 0, aparece el indicador `ok`, que significa que el sistema está controlado por el firmware de OpenBoot.

Para obtener más información sobre OpenBoot PROM, consulte el Capítulo 3.

▼ Para ver el indicador de OpenBoot desde el indicador de ALOM

- **Escriba el comando** `break`**.**

```
sc> break
{2} ok
```

▼ Para ver el indicador de OpenBoot cuando se ejecute el entorno operativo Solaris

- **Escriba el comando** `init 0` **en el indicador de Solaris.**

```
# init 0
{1} ok
```

▼ Para poner fin a una sesión si está conectado al controlador del sistema a través del puerto serie

- Si está en la consola de Solaris o en OpenBoot PROM, escriba la secuencia de escape para ir al indicador de ALOM y, a continuación, termine la sesión del indicador de ALOM. Para ello escriba `logout` y pulse la tecla Intro:

```
sc>logout
```

- Si está conectado a través de un servidor de terminal, utilice el comando del servidor de terminal para desconectarse.
- Si estableció la conexión con un comando `tip`, escriba la secuencia de salida `tip ~.` (es decir, ~ seguido por un punto):

```
~.
```

▼ Para poner fin a una sesión si está conectado al controlador del sistema a través de una conexión de red

1. **Si está en el indicador de Solaris o en OpenBoot PROM, escriba la secuencia de escape para ir al indicador de ALOM.**
2. **Termine la sesión del indicador de ALOM con el comando** `logout`**.**

   La sesión remota se termina automáticamente:

```
sc>logout
Connection closed by foreign host.
%
```

CAPÍTULO 2

Advanced Lights Out Manager

Este capítulo describe la utilización de Advanced Lights Out Manager (ALOM) para la administración remota del servidor. Entre los temas se incluyen:

Se puede obtener más información acerca de ALOM en *Advanced Lights Out Manager CMT v1.2 Guide*, 819-7133-10.

Descripción de ALOM

Características de ALOM

ALOM es un controlador de sistema que está preinstalado en el servidor y que se encuentra disponible al instalar y encender el sistema. Mediante una interfaz de la línea de comandos, puede personalizar ALOM según su instalación específica. A continuación, podrá supervisar y controlar el servidor, ya sea en la red o a través de un servidor de terminal mediante el puerto de gestión serie exclusivo del servidor.

Información suministrada por ALOM

En la TABLA 2-1 se enumeran algunos de los componentes que ALOM puede supervisar en el servidor.

TABLA 2-1 Componentes que ALOM supervisa

Componente supervisado	Información proporcionada
Unidades de disco	Si cada ranura contiene una unidad y si ésta indica un estado correcto.
Ventiladores	Velocidad del ventilador y si los ventiladores indican un estado correcto.
Temperaturas de las CPU	Si una CPU está presente, la temperatura medida en la CPU y los posibles estados de advertencia o fallo térmico.
Temperatura del chasis del sistema	Temperatura ambiente del sistema, así como cualquier advertencia de problema térmico o condición de fallo.
Fusibles	Si los fusibles se han fundido.
Panel frontal del servidor	Posición del conmutador giratorio del sistema y estado de los LED.
Voltajes	Si los voltajes están dentro de los intervalos de funcionamiento.

Nota – Aunque se aconseja la utilización de fuentes de alimentación redundantes, si sólo un conector de CC alimenta al servidor alimentado con CC, ALOM podría generar ocasionalmente el siguiente mensaje:
`SC Alert: env_log_event unsupported event`

Uso de ALOM

El software de ALOM se suministra listo para utilizarse y puede admitir múltiples usuarios. No obstante, sólo un usuario a la vez puede emitir comandos que requieran permisos de escritura. Los demás usuarios únicamente podrán emitir comandos de sólo lectura.

Se puede conectar con ALOM de dos formas:

- Utilice el comando `telnet` para efectuar la conexión con ALOM mediante la conexión Ethernet incorporada en el puerto NET MGT.
- Conecte un dispositivo serie, tal como un terminal ASCII o un puerto de un servidor de terminal, al puerto SERIAL MGT.

▼ Para configurar la contraseña inicial

Al encender el servidor por primera vez, ALOM comienza automáticamente a supervisar el sistema y a mostrar la salida a la consola del sistema utilizando una cuenta predeterminada y preconfigurada que se denomina `admin` y que tiene todos (`cuar`) los permisos. Por cuestiones de seguridad, se debe establecer la contraseña de administración.

1. **Conéctese físicamente al puerto de gestión serie de ALOM y establezca una conexión.**

   Los parámetros de comunicación son los siguientes:

   - 9600 baudios
   - 8 bits de datos
   - Sin paridad
   - 1 bit de parada
   - Dúplex total
   - Sin protocolo de enlace

2. **Inicie la sesión en el indicador de ALOM. Escriba:**

```
#.
SC>
```

   Es decir:

   a. **Mantenga pulsada la tecla Mayús y pulse la tecla 3.**

   b. **Pulse la tecla de punto.**

   c. **Pulse la tecla Intro.**

   Se muestra el indicador `sc>` (indicador de ALOM).

3. **Escriba el comando** `password`**.**

```
sc> password
```

4. **Escriba la contraseña y vuelva a escribirla.**

   La contraseña se crea y se requerirá para todas las conexiones posteriores con ALOM.

   Si no se conecta antes de que ALOM entre en el tiempo de espera, ALOM cambia a la consola del sistema y presenta el siguiente mensaje:

```
Enter #. to return to ALOM.
```

Comandos del shell de ALOM

En las tablas siguientes se enumeran algunos de los comandos del shell de ALOM más comunes y se describen brevemente sus funciones.

Muchos comandos del shell de ALOM se pueden ejecutar desde la interfaz de línea de comandos de Solaris, utilizando para ello el comando `scadm`. Por ejemplo:

```
# scadm loghistory
```

Consulte la página del comando man `scadm` para obtener más información.

Comandos de configuración

Los comandos de configuración de ALOM establecen o muestran la configuración de distintos aspectos del sistema.

TABLA 2-2 Comandos de configuración de ALOM

Comando	Resumen	Ejemplo
`password`	Permite cambiar la contraseña de acceso del usuario actual.	`sc> password`
`setdate` *mmddHHMMaaaa*	Establece la fecha y la hora cuando no se está ejecutando el sistema operativo gestionado.	`sc> setdate 091321451999` `MON SEP 13 21:45:00 1999 UTC`
`setdefaults [-y] [-a]`	Restablece los parámetros de configuración predeterminados de ALOM. La opción `-y` permite omitir la pregunta de confirmación. La opción `-a` restablece la información de usuario a los valores predeterminados de fábrica (sólo una cuenta admin).	`sc> setdefaults -a`
`setsc` *valor parámetro*	Establece el *parámetro* especificado de ALOM en el *valor* asignado.	`sc> setsc netsc_ipaddr 1.2.3.4`
`setupsc`	Ejecuta la secuencia de comandos (script) interactiva, que permite definir las variables de configuración de ALOM.	`sc> setupsc`

TABLA 2-2 Comandos de configuración de ALOM *(continuación)*

Comando	Resumen	Ejemplo
`showdate`	Muestra la fecha configurada en ALOM. La hora del sistema operativo Solaris y de ALOM están sincronizadas, pero la de ALOM se expresa en UTC (Tiempo universal coordinado) en lugar de en la hora local.	`sc>` **`showdate`** `MON SEP 13 21:45:00 1999 UTC`
`showplatform [-v]`	Muestra información sobre la configuración del hardware del sistema e indica si está en servicio. La opción `-v` muestra información detallada acerca de los componentes visualizados.	`sc>` **`showplatform`**
`showsc [-v]` *parámetro*	Muestra el valor actual de los *parámetros* de configuración de la memoria de acceso aleatorio no volátil (NVRAM). La opción `-v` es necesaria para mostrar toda la información sobre la versión.	`sc>` **`showsc sys_autorestart`** `xir`
`showusers [-g` *líneas*`]`	Presenta una lista de los usuarios que tienen abierta una sesión de ALOM. La pantalla de este comando tiene un formato similar al del comando `who` de UNIX. La opción `-g` hace una pausa en la visualización después del número de líneas especificado en *líneas*.	`sc>` **`showusers -g 10`**
`useradd` *nombre_usuario*	Permite agregar una cuenta de usuario a ALOM.	`sc>` **`useradd newuser`**
`userdel [-y]` *nombre_usuario*	Permite suprimir una cuenta de usuario de ALOM. La opción `-y` permite omitir la pregunta de confirmación.	`sc>` **`userdel newuser`**
`userpassword` *nombre_usuario*	Permite establecer o cambiar una cuenta de usuario.	`sc>` **`userpassword newuser`**
`userperm` *nombre_usuario* `[c][u][a][r]`	Permite establecer el nivel de permiso de las cuentas de usuario.	`sc>` **`userperm newuser cr`**
`usershow` [*nombre_usuario*]	Muestra una lista de todas las cuentas de usuario, con sus niveles de permiso, e indica si tienen contraseñas asignadas.	`sc>` **`usershow newuser`**

Comandos de FRU

Los comandos de FRU de ALOM pueden mostrar las FRU instaladas.

TABLA 2-3 Comandos de FRU de ALOM

Comando	Resumen	Ejemplo
`removefru PS0|PS1`	Indica si se puede intercambiar en marcha una fuente de alimentación.	`sc>` **`removefru PS0`**
`showfru`	Muestra información acerca de las FRU (unidades sustituibles de campo) de un servidor.	`sc>` **`showfru`**

Comandos de registro

Los comandos de registro de ALOM muestran las memorias intermedias de eventos de ALOM y de salida de la consola.

TABLA 2-4 Comandos de registro de ALOM

Comando	Resumen	Ejemplo
`consolehistory [-b` *líneas*`|-e` *líneas*`] [-g` *líneas*`] [-v] [boot|run]`	Muestra los bufers de salida de la consola del servidor. La opción `-v` muestra el contenido del archivo de registro especificado.	`sc>` **`consolehistory boot -b 10`**
`showlogs [-b` *líneas*`|-e` *líneas*`] [-g` *líneas*`] [-v]`	Presenta el historial de todos los eventos registrados en el búfer de eventos de ALOM.	`sc>` **`showlogs -b 100`**

Comandos de estado y control

Los comandos de estado y control de ALOM permiten realizar tareas habitualmente manuales con el servidor de forma remota.

TABLA 2-5 Comandos de estado y control de ALOM

Comando	Resumen	Ejemplo
`bootmode [skip_diag | diag | reset_nvram | normal | bootscript="`*cadena*`"]`	Controla el método de arranque del servidor a través del firmware de OpenBoot PROM.	`sc>` **`bootmode reset_nvram`** `sc>` **`reset`**
`break [-y] [-c]`	Coloca el servidor del sistema en OpenBoot PROM o `kadb`.	`sc>` **`break`**
`clearasrdb`	Quita todas las entradas de la lista negra de `asr-db`.	`sc>` **`clearasrdb`**

TABLA 2-5 Comandos de estado y control de ALOM *(continuación)*

Comando	Resumen	Ejemplo
`clearfault` *UUID*	Elimina los fallos detectados por el host manualmente. *UUID* es el ID exclusivo del fallo que se va a eliminar.	`sc>` **`clearfault 1234`**
`console [-f]`	Establece conexión con la consola del sistema. La opción `-f` fuerza el bloqueo de escritura de la consola para un usuario sobre los demás.	`sc>` **`console`**
`disablecomponent` *asrkey*	Agrega un componente a la lista negra de `asr-db`, donde *asrkey* es el componente que se va a deshabilitar.	`sc>` **`disablecomponent MB/CMP0/CH3/R1/D1`**
`enablecomponent` *asrkey*	Quita un componente de la lista negra de asr-db, donde *asrkey* es el componente que se va a habilitar.	`sc>` **`enablecomponent MB/CMP0/CH3/R1/D1`**
`flashupdate [-s` *dirección_IP* `-f` *nombre_ruta*`] [-v]`	Actualiza el firmware de ALOM. Este comando descarga en ALOM imágenes del firmware `main` (principal) y de `bootmon`.	`sc>` **`flashupdate -s 1.2.3.4 -f /usr/platform/SUNW,Netra210/lib/images/alommainfw`**
`powercycle [-f]`	Realiza un `apagado` seguido de un `encendido`. La opción `-f` provoca con `poweroff` el cierre de sesión inmediato; sin ella, el comando ejecuta el cierre de sistema predeterminado.	`sc>` **`powercycle`**
`poweroff [-y] [-f]`	Interrumpe la alimentación principal del servidor. La opción `-y` permite omitir la pregunta de confirmación. La opción `-f` fuerza un apagado inmediato.	`sc>` **`poweroff`**
`poweron [-c] [`*FRU*`]`	Conecta la alimentación principal al servidor o a una determinada FRU.	`sc>` **`poweron HDD1`**
`reset [-y] [-x] [-c]`	Restaura el hardware del servidor. La opción `-x` genera el equivalente de un XIR (reinicio iniciado externamente). La opción `-y` permite omitir la pregunta de confirmación.	`sc>` **`reset -x`**
`setalarm critical|major|minor|user on|off`	Activa o desactiva la alarma y el LED asociado.	`sc>` **`setalarm critical on`**
`setkeyswitch [-y] normal | stby | diag | locked`	Establece el interruptor de seguridad virtual. La opción `-y` permite omitir el mensaje de confirmación cuando se define el interruptor de seguridad virtual en `stby`.	`sc>` **`setkeyswitch diag`**
`setlocator on|off`	Activa (on) o desactiva (off) el LED localizador del servidor. Esta función sólo está disponible en servidores equipados con LED de localización.	`sc>` **`setlocator on`**

TABLA 2-5 Comandos de estado y control de ALOM *(continuación)*

Comando	Resumen	Ejemplo
`showcomponent`	Muestra los componentes del sistema y su estado actual. El comando `showcomponent` puede no mostrar todos los DIMM de la lista negra.	`sc>` **`showcomponent`**
`showfaults [-v]`	Muestra los fallos del sistema actuales. La opción `-v` proporciona la salida con mensajes completos.	`sc>` **`showfaults`**
`showenvironment`	Muestra información sobre el estado del entorno del servidor. Esta información incluye las temperaturas del sistema, el estado de las fuentes de alimentación, el estado de los LED del panel frontal, el estado de las unidades de disco, el estado de los ventiladores, el estado de los sensores de corriente y voltaje y la posición del conmutador giratorio.	`sc>` **`showenvironment`**
`showkeyswitch`	Muestra el estado del interruptor de seguridad virtual.	`sc>` **`showkeyswitch`**
`showlocator`	Muestra el estado actual del LED localizador (on u off). Esta función sólo está disponible en servidores equipados con LED de localización.	`sc>` **`showlocator`** `Locator LED is ON`
`shownetwork [-v]`	Muestra la configuración actual de la red. La opción `-v` muestra información adicional acerca de la red, incluida información acerca del servidor DHCP.	`sc>` **`shownetwork`**

Otros comandos de ALOM

En la TABLA 2-6 se enumeran otros comandos de ALOM.

TABLA 2-6 Otros comandos de ALOM

Comando	Resumen	Ejemplo
`help`	Muestra una lista de todos los comandos de ALOM, o de un determinado comando, con su sintaxis y una descripción breve del funcionamiento de cada uno de ellos.	`sc>` **`help poweron`**
`logout`	Cierra la sesión de shell de ALOM.	`sc>` **`logout`**
`resetsc [-y]`	Reinicia ALOM. La opción `-y` permite omitir la pregunta de confirmación.	`sc>` **`resetsc`**

Tareas básicas de ALOM

Después de iniciar sesión en ALOM como `admin` y especificar la contraseña de `admin`, podrá efectuar diversas tareas administrativas comunes:

▼ Para reiniciar ALOM

Esto reinicia el software de ALOM. Reinicie ALOM tras modificar sus parámetros o si deja de responder por algún motivo.

- **En el indicador `sc>`, escriba `resetsc`.**

▼ Para cambiar entre la consola del sistema y ALOM

- **Para pasar de la consola al indicador `sc>` de ALOM, escriba `#.` (almohadilla punto).**
- **Para cambiar del indicador `sc>` a la consola, escriba el comando `console`.**

▼ Para controlar el LED de localización

- **Para activar y desactivar el LED, utilice el comando `setlocator`.**
- **Para conocer el estado del LED, utilice el comando `showlocator`.**

  El LED también se puede controlar en el indicador de superusuario de Solaris utilizando el comando `locator`.

▼ Para reiniciar el servidor

1. **Escriba el comando** `poweroff`**.**

   Aparece este mensaje:

```
SC Alert: Host system has shut down.
```

2. **Escriba el comando** `poweron`**.**

▼ Para visualizar información del entorno relativa al servidor

ALOM puede mostrar la temperatura del sistema, el estado de las unidades de disco, el estado de la fuente de alimentación y el ventilador, el estado de los LED del panel frontal, la posición del conmutador giratorio, el estado de los sensores de corriente y voltaje y de las alarmas, etc.

- **Para visualizar información del entorno, utilice el comando** `showenvironment`**.**

▼ Para reconfigurar ALOM a fin de que utilice el puerto Ethernet (NET MGT)

De forma predeterminada, ALOM utiliza el puerto de gestión serie (SERIAL MGT) para comunicarse con un dispositivo serie. Si lo desea, puede reconfigurar ALOM para que utilice el puerto de gestión de red Ethernet (NET MGT); así podrá conectarse a ALOM mediante el comando `telnet`.

Nota – ALOM admite solamente redes de 10 Mbits.

Para configurar el software de ALOM para comunicarse mediante el puerto NET MGT, deberá especificar los valores de las variables de la interfaz de red. La secuencia `setupsc` permite realizar esta tarea.

1. **Ejecute la secuencia** `setupsc`**. Escriba:**

```
sc> setupsc
```

Al hacerlo, se inicia la secuencia de comandos de configuración (script). Responda a las preguntas de la secuencia. La secuencia solicitará:

```
Do you wish to configure the enabled interfaces [y]?
```

2. **Escriba** `y`**.**

La secuencia solicitará:

```
Should the SC network interface be enabled?
```

3. **Escriba** `true` **o pulse Intro para habilitar la interfaz de red.**

Esto define el valor de la variable `if_network`.

4. **Proporcione valores para las siguientes variables de la secuencia:**
   - `if_modem` (especifique `false`)
   - `netsc_dhcp` (`true` o `false`)
   - `netsc_ipaddr` (dirección IP)
   - `netsc_ipnetmask` (máscara de red)
   - `netsc_ipgateway` (dirección IP)
   - `netsc_tpelinktest` (`true` o `false`)
5. **Una vez configuradas las variables de la interfaz de red, escriba Ctrl-Z para guardar los cambios y salir de la secuencia** `setupsc`**.**
6. **Reinicie ALOM. Escriba:**

```
sc> resetsc
```

▼ Para agregar cuentas de usuario de ALOM

No pueden añadirse más de 15 usuarios diferentes a ALOM.

1. **Cree una cuenta de usuario de ALOM. Escriba:**

```
sc> useradd nombre_usuario
```

2. **Asigne una contraseña a esta cuenta. Escriba:**

```
sc> userpassword nombre_usuario
New password:
Re-enter new password:
```

3. **Asigne permisos a esta cuenta. Escriba:**

```
sc> userperm nombre_usuario cuar
```

donde *cuar* representa los permisos `cuar`.

4. **Para verificar cuentas y sus permisos, utilice el comando** `usershow`**.**

▼ Para eliminar una cuenta de usuario de ALOM

- **Para borrar una cuenta de usuario de ALOM, escriba:**

```
sc> userdel nombre_usuario
```

Nota – No se puede eliminar la cuenta `admin` predeterminada de ALOM.

▼ Para iniciar una sesión en ALOM

1. **Establezca una conexión con ALOM.**
2. **Cuando la conexión esté establecida, escriba** `#.` **(almohadilla punto) como secuencia de escape de la consola del sistema.**
3. **Escriba el nombre de usuario y la contraseña de ALOM.**

▼ Para cambiar una contraseña de ALOM

- **Para cambiar su contraseña, utilice el comando** `password`**.**
- **Para cambiar una contraseña de cuenta de usuario, utilice el comando** `userpassword` *nombre_usuario***.**

▼ Para configurar las alertas por correo electrónico

Nota – Es posible configurar alertas por correo electrónico de hasta ocho usuarios. También puede definir un nivel de alertas para cada dirección de correo electrónico.

---

1. **Compruebe que ALOM esté configurado para utilizar el puerto de gestión Ethernet (NET MGT) y que las variables de interfaz de red estén configuradas.**

   Consulte "Para reconfigurar ALOM a fin de que utilice el puerto Ethernet (NET MGT)" en la página 20.

2. **Configure las alertas por correo electrónico y el servidor de correo. Escriba:**

```
sc> setsc if_emailalerts true
sc> setsc mgt_mailhost dirección_IP1,...
```

3. **Configure cada uno de los destinatarios de las alertas. Escriba:**

```
sc> setsc mgt_mailalert dirección_correo_electrónico nivel_alerta
```

   donde:

   - *dirección_correo_electrónico* tiene el formato `nombre_usuario_correo_electrónico@dominio_correo`
   - *nivel_alerta* es `1` para alerta crítica, `2` para alerta principal y `3` para alerta secundaria

4. **Repita el** paso 3 **para cada uno de los destinatarios de las alertas.**

   Las alertas de correo electrónico de ALOM aparecen con el siguiente formato:

   `$HOSTID $EVENT $TIME $CUSTOMERINFO $HOSTNAME` *mensaje*

▼ Para hacer una copia de seguridad de la configuración de ALOM

Es conveniente crear de forma periódica un archivo de copia de seguridad en un sistema remoto que almacene los parámetros de configuración de ALOM.

- **Como superusuario, abra una ventana de terminal y escriba:**

```
# /usr/platform/SUNW,Netra210/sbin/scadm show > nombre_archivo_remoto
# /usr/platform/SUNW,Netra210/sbin/scadm usershow >
nombre_archivo_remoto
```

Utilice nombres de archivo significativos, que contengan el nombre del servidor que ALOM controla. Más adelante puede recurrir a este archivo para, en caso necesario, restablecer la configuración.

▼ Para visualizar la versión de ALOM

- **Para visualizar la versión de ALOM, escriba:**

```
sc> showsc version
Advanced Lights Out Manager v1.6
```

CAPÍTULO 3

OpenBoot PROM

Este capítulo describe el funcionamiento, los métodos de visualización y la configuración de OpenBoot PROM. Entre los temas se incluyen:

Descripción de OpenBoot PROM

OpenBoot PROM es el firmware de bajo nivel que permite al servidor iniciar el entorno operativo Solaris. Cuando se ejecuta Solaris, OpenBoot PROM lleva el control del servidor al entorno operativo Solaris. Bajo determinadas condiciones, OpenBoot PROM vuelve a obtener el control del servidor. A continuación, se muestra una lista de las circunstancias en que el firmware de OpenBoot obtiene el control:

- Cuando se pone el sistema bajo el control del firmware de forma deliberada para ejecutar los comandos del firmware. Esta situación tiene importancia para el administrador, ya que en ocasiones tendrá que obtener el indicador `ok`.
- En principio, el sistema se pone bajo el control del firmware OpenBoot antes de la instalación del sistema operativo.
- Cuando la variable de configuración `auto-boot?` de OpenBoot se define con el valor `false`, el sistema presenta el indicador `ok` al iniciarse.
- Cuando el sistema operativo se detiene, el sistema pasa al nivel de ejecución 0 de forma normal.
- Si el sistema operativo deja de funcionar, el servidor devuelve el control al firmware OpenBoot.

- Durante el proceso de inicio, cuando se produce un problema serio con el hardware que impide la ejecución del sistema operativo, el sistema devuelve el control al firmware OpenBoot.
- Cuando se produce un problema grave con el hardware durante la ejecución del servidor, el sistema operativo pasa al nivel de ejecución 0 de forma normal.

Antes de obtener el indicador `ok`

Nota – El acceso al indicador `ok` hace que se suspenda la ejecución de Solaris. Antes de suspender la ejecución del sistema operativo, debería hacer una copia de seguridad de los archivos, advertir a los usuarios del cierre inminente y detener el sistema mediante el procedimiento normal.

Precaución – Al acceder al indicador `ok` desde un servidor en funcionamiento, se está suspendiendo la ejecución de Solaris y poniendo el sistema bajo el control del firmware. Cualquier proceso del sistema operativo que se estuviese ejecutando también queda suspendido y *su estado posiblemente sea irrecuperable*.

Los comandos que se ejecutan desde el indicador `ok` pueden afectar al estado del sistema. Esto significa que no siempre es posible reanudar la ejecución del sistema operativo en el punto en que se suspendió. Aunque el comando `go` reanuda la ejecución en la mayoría de las circunstancias, en general, lo habitual es que necesite reiniciar el servidor para volver al sistema operativo cada vez que acceda al indicador `ok`.

Visualización del indicador `ok`

Hay varias formas de llegar hasta el indicador `ok`. Son las siguientes, por orden de preferencia:

- Cierre normal
- ALOM Comandos `break` y `console`
- Las teclas Stop-A o la tecla Break
- Reinicio manual del sistema

Nota – Tenga presente que, si pone el servidor bajo el control del firmware de OpenBoot, podría bloquear el sistema al ejecutar ciertos comandos de este firmware (como `probe-scsi`, `probe-scsi-all` o `probe-ide`).

Cierre normal

La forma recomendada de acceder al indicador `ok` es cerrar la sesión del sistema operativo ejecutando el comando apropiado (por ejemplo, los comandos `shutdown`, `init` o `uadmin`) tal y como se describe en la documentación de Solaris. También se puede utilizar el botón de encendido del sistema para iniciar un cierre normal.

El cierre normal del sistema evita la pérdida de datos, permite avisar a los usuarios con antelación y provoca mínima interrupción de la actividad. Normalmente es posible realizar este tipo de cierre sin problemas, siempre que Solaris se esté ejecutando y el hardware no haya sufrido ninguna avería grave.

También se puede realizar un cierre normal del sistema desde el indicador de comandos de ALOM.

Comandos `break` o `console`

La ejecución del comando `break` desde el indicador `sc>` pone al servidor bajo el control del firmware de OpenBoot. Si ya se ha detenido el sistema operativo, es posible usar el comando `console` en lugar de `break` para acceder al indicador `ok`.

Las teclas Stop-A o la tecla Break

Cuando resulta imposible o inadecuado cerrar el sistema de forma normal, se puede acceder al indicador `ok` escribiendo la secuencia de teclas Stop-A desde el teclado de Sun. Si tiene un terminal alfanumérico conectado al servidor, pulse la tecla Break.

Nota – Estas formas de acceder al indicador `ok` sólo funcionarán si la consola del sistema se ha dirigido al puerto apropiado.

Reinicio manual del sistema

Precaución – El reinicio manual del servidor provoca la pérdida de los datos de estado del sistema y debe utilizarse sólo como último recurso. Cuando se efectúa el reinicio, se pierde la información de estado, lo que impide rastrear la causa del problema hasta que éste vuelve a producirse.

Para reiniciar el servidor, utilice los comandos `poweron` y `poweroff` o el comando `reset` del ALOM. El uso de estos comandos hace que se pierda la coherencia del sistema y la información de estado. El reinicio manual del servidor puede dañar sus sistemas de archivos, aunque el comando `fsck` suele restaurarlos. Utilice este método únicamente cuando no quede otra solución.

▼ Para visualizar el indicador `ok`

1. **Decida qué método necesita utilizar para entrar en el indicador `ok`.**
2. **Siga las instrucciones adecuadas de la** TABLA 3-1**.**

TABLA 3-1 Métodos de visualizar el indicador `ok`

Método	Procedimiento
Cierre normal de Solaris	Desde un shell o la ventana de una utilidad de comandos, ejecute el comando de cierre adecuado (por ejemplo, `shutdown` o `init 0`) según se describe en los documentos de administración de sistemas Solaris.
Teclas Stop-A o tecla Break	• Desde un teclado Sun directamente conectado al servidor, pulse a la vez las teclas Stop y A. • Pulse la tecla Break desde un terminal alfanumérico configurado para acceder a la consola del sistema.
Comandos `break` y `console` de ALOM	Desde el indicador `sc>`, escriba el comando `break`. A continuación, ejecute el comando `console`, siempre que haya detenido la ejecución del sistema operativo y el servidor se encuentre bajo el control del firmware de OpenBoot.
Reinicio manual del sistema	1. Sitúese en el indicador `sc>` y escriba: `sc>` **`bootmode bootscript="setenv auto-boot? false"`** 2. Pulse Intro. 3. A continuación, escriba: `sc>` **`reset`**

Variables de configuración de OpenBoot PROM

▼ Para cambiar una variable de configuración de OpenBoot PROM

- **Utilice el comando** `setenv`**.**

  Por ejemplo:

```
ok setenv diag-switch? true
```

  Este ejemplo habilita los diagnósticos.

  La TABLA 3-2 contiene una descripción de las variables del firmware de OpenBoot almacenadas en la memoria no volátil del sistema. Dichas variables se imprimen aquí en el mismo orden con el que aparecen al ejecutar el comando `showenv`.

TABLA 3-2 Variables de configuración de OpenBoot almacenadas en la tarjeta de configuración del sistema

Variable	Valores posibles	Valor predeterminado	Descripción
`local-mac-address?`	`true, false`	`true`	Si tiene el valor `true`, los controladores de red utilizan su propia dirección MAC y no la dirección MAC del servidor.
`fcode-debug?`	`true, false`	`false`	Si tiene el valor `true`, se incluyen los nombres de campo en el código FCode de controladores de dispositivos conectables.
`scsi-initiator-id`	`0-15`	`7`	ID SCSI del controlador SCSI conectado en serie.
`oem-logo?`	`true, false`	`false`	Si tiene el valor `true`, se utiliza el logotipo del fabricante del equipo, de lo contrario, se utiliza el logotipo de Sun.
`oem-banner?`	`true, false`	`false`	Si tiene el valor `true`, se utiliza la pantalla de presentación del fabricante del equipo.
`ansi-terminal?`	`true, false`	`true`	Si tiene el valor `true`, se habilita la emulación de terminales ANSI.
`screen-#columns`	`0-n`	`80`	Establece el número de columnas de la pantalla.

TABLA 3-2 Variables de configuración de OpenBoot almacenadas en la tarjeta de configuración del sistema *(continuación)*

Variable	Valores posibles	Valor predeterminado	Descripción
screen-#rows	0-n	34	Establece el número de filas de la pantalla.
ttya-rts-dtr-off	true, false	false	Si tiene el valor true, el sistema operativo no utiliza las señales rts (request-to-send) ni dtr (data-transfer-ready) en el puerto serie de gestión.
ttya-ignore-cd	true, false	true	Si tiene el valor true, el sistema operativo hace caso omiso de la detección de portadora en el puerto serie de gestión.
ttya-mode	9600,8,n,1,-	9600,8,n,1,-	Puerto serie de gestión (velocidad de baudios, bits, paridad, parada, protocolo de negociación). El puerto serie de gestión sólo funciona con los valores predeterminados.
output-device	virtual-console, screen	virtual-console	Dispositivo de salida durante el encendido.
input-device	virtual-console, keyboard	virtual-console	Dispositivo de entrada durante el encendido.
auto-boot-on-error?	true, false	false	Si tiene el valor true, el sistema se inicia automáticamente tras un error.
load-base	0-n	16384	Dirección.
auto-boot?	true, false	true	Si tiene el valor true, el sistema arranca automáticamente tras encenderse o reiniciarse.
boot-command	*nombre-variable*	boot	Acción que sigue al comando boot.
boot-file	*nombre-variable*	none	Archivo desde el que se efectúa el inicio del sistema si diag-switch? tiene el valor false.
boot-device	*nombre-variable*	disk net	Dispositivos desde los cuales se efectúa el inicio del sistema si diag-switch? tiene el valor false.
use-nvramrc?	true, false	false	Si tiene el valor true, ejecuta los comandos de NVRAMRC durante el inicio del servidor.
nvramrc	*nombre-variable*	none	Secuencia de comandos que se ejecuta si use-nvramrc? tiene el valor true.
security-mode	none, command, full	none	Nivel de seguridad del firmware.
security-password	*nombre-variable*	none	Contraseña de seguridad del firmware si security-mode no tiene el valor none (nunca visualizada). *No debe definirse directamente.*

TABLA 3-2 Variables de configuración de OpenBoot almacenadas en la tarjeta de configuración del sistema *(continuación)*

Variable	Valores posibles	Valor predeterminado	Descripción
`security-#badlogins`	*nombre-variable*	`none`	Número de intentos fallidos de introducción de la contraseña de seguridad.
`diag-switch?`	`true, false`	`false`	Si tiene el valor `true`: 1. El nivel de detalle de los mensajes de OpenBoot se establece en el máximo. 2. Después de una petición de inicio de `boot`, se inicia `diag-file` desde `diag-device`. Si tiene el valor `false`: 1. El nivel de detalle de los mensajes de OpenBoot se establece en el mínimo. 2. Después de una petición de inicio de `boot`, se inicia `boot-file` desde `boot-device`.
`error-reset-recovery`	`boot, sync, none`	`boot`	Comando que debe ejecutarse después de un reinicio del sistema provocado por un error.
`network-boot-arguments`	[*protocolo*,] [*clave=valor,*]	`none`	Argumentos que utilizará la PROM para el inicio de red. El valor predeterminado es una cadena vacía. `network-boot-arguments` sirve para especificar el protocolo de inicio (RARP/DHCP) que debe utilizarse y una amplia variedad de datos sobre el sistema que pueden emplearse en el proceso. Para obtener más información, consulte la página del comando man de `eeprom` (1M) del manual de referencia de Solaris.

Procedimientos de urgencia de OpenBoot

La introducción de teclados USB (Universal Serial Bus) en los nuevos sistemas Sun ha provocado la necesidad de cambiar algunos procedimientos de urgencia de OpenBoot. En concreto, los comandos `Stop-N`, `Stop-D` y `Stop-F`, que estaban disponibles en otros tipos de teclados, ya no se pueden utilizar en sistemas con teclados USB. Si está habituado a utilizar las funciones de los otros tipos de teclados, en esta sección encontrará los procedimientos de urgencia equivalentes disponibles en los teclados USB.

Función Stop-A

La secuencia de teclas Stop-A (cancelar) se comporta de forma similar a la de los sistemas con teclados estándar, salvo por el hecho de que no funciona durante los segundos posteriores al reinicio del servidor. También es posible utilizar el comando `break` del ALOM para realizar esa función. Para obtener más información, consulte "Cambio de consola" en la página 6.

Función Stop-N

La función Stop-N no está disponible, aunque puede emularse realizando el procedimiento siguiente, siempre que la consola del sistema esté configurada para acceder a ella a través de los puertos de gestión serie o de red.

▼ Para restablecer los valores predeterminados de configuración de OpenBoot

1. **Inicie la sesión en ALOM.**

   Consulte "Cambio de consola" en la página 6.

2. **Escriba el comando siguiente:**

```
sc> bootmode reset_nvram
sc> bootmode bootscript="setenv auto-boot? false"
sc>
```

Nota – Si no se ejecutan los comandos `poweroff` y `poweron` o el comando `reset` en un plazo de 10 minutos, el servidor hace caso omiso del comando `bootmode`.

Es posible ejecutar el comando `bootmode` sin argumentos para ver el valor que tiene definido.

```
sc> bootmode
Bootmode: reset_nvram
Expires WED SEP 09 09:52:01 UTC 2005
bootscript="setenv auto-boot? false"
```

3. **Para reiniciar el sistema, escriba el siguiente comando:**

```
sc> reset
Are you sure you want to reset the system [y/n]? y
sc>
```

4. **Para ver la salida de la consola durante el inicio del sistema con las variables de configuración de OpenBoot predeterminadas, cambie al modo** `console`**.**

```
sc> console

ok
```

5. **Escriba** `set-defaults` **para descartar los posibles valores personalizados de IDPROM y recuperar los valores predeterminados de todas las variables de configuración de OpenBoot.**

Función Stop-F

Esta función no está disponible en sistemas con teclados USB.

Función Stop-D

La secuencia de teclas Stop-D (diagnóstico) no está disponible en sistemas con teclados USB, aunque se puede obtener un funcionamiento muy parecido configurando el selector virtual con el valor `diag` mediante el comando `setkeyswitch` de ALOM.

CAPÍTULO 4

Tareas básicas de administración

Este capítulo describe los indicadores de estado y las tareas básicas que se realizan para la administración del sistema. Entre los temas se incluyen:

Indicadores de estado

El sistema tiene indicadores LED asociados al servidor y a varios componentes. Los indicadores del estado del servidor se encuentran en la cubierta y se repiten en el panel posterior. Los componentes con indicadores LED para transmitir el estado son la tarjeta de alarma de contacto seco, las fuentes de alimentación, el puerto Ethernet y las unidades de disco duro.

Entre los temas que se tratan en esta sección se incluyen:

Interpretación de los LED de estado

El comportamiento de los LED del servidor es conforme con la norma SIS (Status Indicator Standard) del instituto americano de normalización (American National Standards Institute o ANSI). El comportamiento estándar de los LED se describe en la TABLA 4-1.

TABLA 4-1 Comportamiento de los LED y significado

Comportamiento del LED	Significado
Apagado	La condición representada por el color no es verdadera.
Continuamente iluminado	La condición representada por el color es verdadera.
Parpadeo continuo	El sistema está funcionando en un nivel mínimo y está listo para reanudar el funcionamiento completo.
Parpadeo lento	Se está produciendo una actividad transitoria o una nueva actividad representada por el color.
Parpadeo rápido	El sistema necesita atención.
Destello paralelo a la actividad	Está teniendo lugar una actividad paralela a la frecuencia de los destellos (por ejemplo, la actividad de la unidad de disco).

Los LED tienen diferentes significados asignados que se describen en la TABLA 4-2.

TABLA 4-2 Comportamiento de los LED y significados asignados

Color	Comportamiento	Definición	Descripción
Blanco	Apagado	Estado continuo	
	Parpadeo rápido	Secuencia repetida de 4 Hz, intervalos equivalentes de apagado y encendido.	Este indicador ayuda a localizar una carcasa, una placa o un subsistema en particular (por ejemplo, el LED de localización).
Azul	Apagado	Estado continuo	
	Continuamente iluminado	Estado continuo	Si el azul está encendido, es posible realizar una operación de mantenimiento en el componente aplicable sin consecuencias negativas (por ejemplo, el LED de extracción segura).
Amarillo/ ámbar	Apagado	Estado continuo	
	Parpadeo lento	Secuencia repetida de 1 Hz, intervalos equivalentes de apagado y encendido.	Este indicador señala nuevas situaciones de fallo. Se requiere el mantenimiento (por ejemplo, el LED de servicio).
	Continuamente iluminado	Estado continuo	El indicador ámbar permanece encendido hasta que se realiza la operación de mantenimiento y el sistema reanuda su funcionamiento normal.

TABLA 4-2 Comportamiento de los LED y significados asignados *(continuación)*

Color	Comportamiento	Definición	Descripción
Verde	Apagado	Estado continuo	
	Parpadeo continuo	Secuencia repetida que consiste en un breve destello (0,1 s) seguido de un largo periodo apagado (2,9 s).	El sistema se está ejecutando en un nivel mínimo y está listo para reanudar el funcionamiento normal (por ejemplo, el LED de actividad del sistema).
	Continuamente iluminado	Estado continuo	Estado normal; el sistema o el componente funciona sin necesidad de que intervenga el servicio técnico.
	Parpadeo lento		Se está produciendo un evento transitorio (temporal) para el que no se necesita indicación de actividad proporcional o no es factible.

Indicadores de estado de la cubierta del servidor

La FIGURA 4-1 muestra la ubicación de los indicadores de la cubierta y la TABLA 4-3 proporciona información sobre los indicadores del estado del servidor.

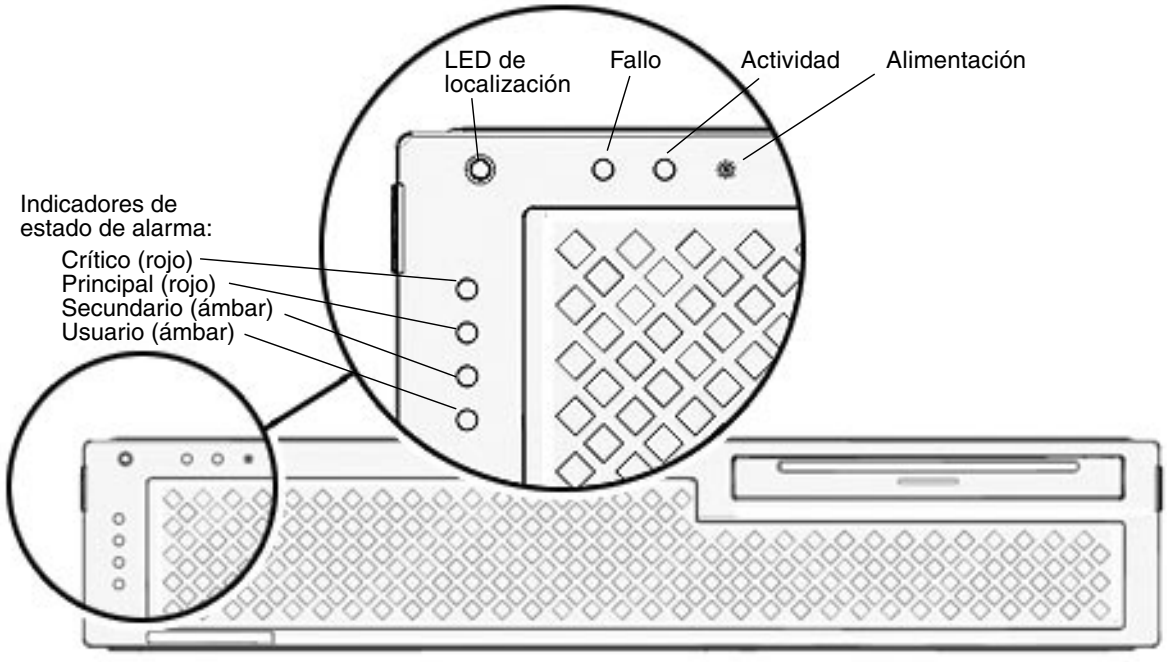

FIGURA 4-1 Ubicación de los indicadores de la cubierta de alarma y estado del servidor

TABLA 4-3 Indicadores de estado de la cubierta del servidor

Indicador	Color del LED	Estado del LED	Estado del componente
LED de localización	Blanco	Encendido	El servidor se identifica con el comando `locator` de superusuario o `setlocator` de ALOM.
		Apagado	Estado normal
Fallo	Ámbar	Encendido	El servidor ha detectado un problema y requiere la atención del personal de servicio.
		Apagado	El servidor no ha detectado errores.
Actividad	Verde	Encendido	El servidor se enciende y ejecuta el sistema operativo Solaris.
		Apagado	O no hay alimentación o no se está ejecutando el software Solaris.

Puede comprobar el estado y encender y apagar el LED de localización desde el indicador de superusuario o de ALOM. En la TABLA 4-4 se enumeran los comandos.

TABLA 4-4 Comandos del LED de localización

Indicador	Estado	Encender	Apagar
Superusuario	`# /usr/sbin/locator`	`# /usr/sbin/locator -n`	`# /usr/sbin/locator -f`
ALOM	`sc> showlocator`	`sc> setlocator on`	`sc> setlocator off`

Indicadores de estado de alarma

La tarjeta de alarma de contacto seco dispone de cuatro indicadores LED compatibles con ALOM situados verticalmente en la cubierta (FIGURA 4-1). La TABLA 4-5 contiene información acerca de los indicadores de alarma y los estados de alarma de contacto seco. Para obtener más información sobre los indicadores de alarma, consulte el documento *Advanced Lights Out Manager CMT v1.2 Guide,* 819-7133-10.

TABLA 4-5 Indicadores de alarma y estado de alarma de contacto seco

Etiquetas de indicador y relé	Color del indicador	Estado de la aplicación o del servidor	Condición o acción	Estado del indicador de actividad	Estado del indicador de alarma	Relé NC§ Estado	Relé NO** Estado	Comentarios
Crítico (`Alarm0`)	Rojo	Estado del servidor (Encendido o apagado y sistema operativo Solaris funcional o no funcional)	Sin entrada de alimentación	Apagado	Apagado	Cerrado	Abierto	Estado predeterminado
			Sistema apagado	Apagado	Apagado‡	Cerrado	Abierto	Alimentación de entrada conectada
			El sistema se enciende, el sistema operativo Solaris no está totalmente cargado	Apagado	Apagado‡	Cerrado	Abierto	Estado transitorio
			SO Solaris cargado satisfactoriamente	Encendido	Apagado	Abierto	Cerrado	Estado de funcionamiento normal
			Tiempo de espera de vigilancia agotado	Apagado	Encendido	Cerrado	Abierto	Estado transitorio, rearrancar SO Solaris
			Apagado del SO Solaris iniciado por el usuario*	Apagado	Apagado‡	Cerrado	Abierto	Estado transitorio
			Se ha perdido la alimentación de entrada	Apagado	Apagado	Cerrado	Abierto	Estado predeterminado
			El usuario apaga la alimentación	Apagado	Apagado‡	Cerrado	Abierto	Estado transitorio
		Estado de aplicación	El usuario activa (`on`†) la alarma crítica	--	Encendido	Cerrado	Abierto	Fallo crítico detectado
			El usuario desactiva (`off`†) la alarma crítica	--	Apagado	Abierto	Cerrado	Fallo crítico resuelto
Principal (`Alarm1`)	Rojo	Estado de aplicación	El usuario activa (`on`†) la alarma principal	--	Encendido	Abierto	Cerrado	Fallo principal detectado
			El usuario desactiva (`off`†) la alarma principal	--	Apagado	Cerrado	Abierto	Fallo principal resuelto

TABLA 4-5 Indicadores de alarma y estado de alarma de contacto seco *(continuación)*

Etiquetas de indicador y relé	Color del indicador	Estado de la aplicación o del servidor	Condición o acción	Estado del indicador de actividad	Estado del indicador de alarma	Relé NC§ Estado	Relé NO** Estado	Comentarios
Secundario (`Alarm2`)	Ámbar	Estado de aplicación	El usuario activa (`on`†) la alarma secundaria	--	Encendido	Abierto	Cerrado	Fallo secundario detectado
			El usuario desactiva (`off`†) la alarma secundaria	--	Apagado	Cerrado	Abierto	Fallo secundario resuelto
Usuario (`Alarm3`)	Ámbar	Estado de aplicación	El usuario activa (`on`†) la alarma de usuario	--	Encendido	Abierto	Cerrado	Fallo de usuario detectado
			El usuario desactiva (`off`†) la alarma de usuario	--	Apagado	Cerrado	Abierto	Fallo de usuario resuelto

* El usuario puede apagar el sistema mediante comandos como `init0` e `init6`. Estos comandos no desconectan la alimentación del sistema.

† Tras determinar las condiciones del fallo, el usuario puede conectar la alarma mediante la API de alarma de la plataforma Solaris o la interfaz de línea de comandos de ALOM.

‡ La implementación de este estado de indicador de alarma puede variar.

§ Estado NC significa estado normalmente cerrado. Este estado representa el modo predeterminado de los contactos de relé en estado normalmente cerrado.

** Estado NO significa estado normalmente abierto. Este estado representa el modo predeterminado de los contactos de relé en estado normalmente abierto.

Cuando el usuario activa una alarma, se muestra un mensaje en la consola. Por ejemplo, cuando se activa la alarma crítica se muestra el siguiente mensaje en la consola:

```
SC Alert: CRITICAL ALARM is set
```

En ciertos casos, al activarse una alarma crítica no se enciende el indicador de alarma asociado. Esta implementación es susceptible de variar en próximas versiones.

Selección de un dispositivo de arranque

El dispositivo de arranque del sistema está especificado por la variable de configuración `boot-device` de OpenBoot. El valor predeterminado de esta variable es `disk net`. Este valor hace que el firmware primero intente iniciar el sistema desde el disco duro y, si no lo consigue, lo intente desde la interfaz Gigabit Ethernet NET0 de la placa.

En este procedimiento se da por supuesto que está familiarizado con el firmware OpenBoot y que sabe cómo acceder al entorno de OpenBoot. Para obtener más información, consulte "OpenBoot PROM" en la página 25.

Si quiere que el arranque se realice desde un dispositivo distinto, realice el siguiente procedimiento.

▼ Para seleccionar un dispositivo de arranque

1. **Obtenga el indicador `ok`.**

   Consulte "Para visualizar el indicador `ok`" en la página 28.

2. **Cuando aparezca el indicador `ok`, escriba:**

   ```
   ok setenv boot-device identificador-dispositivo
   ```

   donde *identificador-dispositivo* es uno de los siguientes:

   - `cdrom`: indica la unidad de almacenamiento óptico
   - `disk`: indica el disco de arranque del sistema (el valor predeterminado es el disco interno 0).
   - `disk0`: indica el disco interno 0.
   - `disk1`: indica el disco interno 1.
   - `disk2`: indica el disco interno 2.
   - `disk3`: indica el disco interno 3.
   - `net`, `net0`, `net1`, `net2`, `net3`: indican las interfaces de red.
   - *ruta de acceso completa*: indica el dispositivo o la interfaz de red mediante el nombre de la ruta de acceso.

Nota – Solaris sustituye la variable `boot-device` por la ruta de acceso completa, no por el alias. Si selecciona la variable `boot-device` con un valor que no sea el predeterminado, Solaris especifica la ruta de acceso completa al dispositivo de arranque.

Nota – También puede especificar el nombre del programa que se debe iniciar, así como el modo en que funcionará dicho programa. Para obtener más información, consulte el documento *OpenBoot 4.x Command Reference Manual* en la colección *OpenBoot Collection AnswerBook* correspondiente a la versión de Solaris en uso.

Si desea seleccionar una interfaz de red distinta de la interfaz Ethernet de la placa como dispositivo de inicio predeterminado, indique la ruta de acceso de cada interfaz escribiendo:

```
ok show-devs
```

El comando `show-devs` presenta una lista de los dispositivos del sistema junto con la ruta de acceso de cada dispositivo PCI.

Nota – Para arrancar desde una interfaz de red, debe tener un servidor de arranque disponible en la red.

Desconfiguración y reconfiguración de dispositivos

Para poder efectuar inicios del sistema en modo degradado, el firmware de ALOM proporciona el comando `disablecomponent`, que permite desconfigurar dispositivos de forma manual. Este comando crea una entrada en la base de datos ASR, con el dispositivo en cuestión marcado como deshabilitado. Cualquier dispositivo marcado como `disabled` (debido a una deshabilitación manual o realizada por el firmware del sistema) se suprime de la descripción de la máquina antes de pasarla a otras capas del firmware del sistema tales como la de OpenBoot PROM.

▼ Para desconfigurar un dispositivo de forma manual

1. **Acceda al indicador de ALOM.**

   Consulte "Cambio de consola" en la página 6.

2. **Sitúese en el indicador** `sc>` **y escriba:**

```
sc> disablecomponent clave-asr
```

donde, *clave-asr* es uno de los identificadores de dispositivo citados en la TABLA 4-6.

Nota – En lo que se refiere a los identificadores de dispositivo, el sistema no diferencia entre mayúsculas y minúsculas. Pueden escribirse de cualquiera de las dos formas.

TABLA 4-6 Identificadores de dispositivo y dispositivos

Identificadores de dispositivo	Dispositivos
`MB/CMP`*número-cpu*`/P`*número-bloque*	Bloque de CPU (número: 0-31)
`PCIE`*número-ranura*	Ranura PCI-E (número: 0-2)
`PCIX`*número-ranura*	PCI-X (número: 0-1):
`IOBD/PCIEa`	Componente PCI-E A (`/pci@780`)
`IOBD/PCIEb`	Componente PCI-E B (`/pci@7c0`)
`TTYA`	Puerto serie DB9
`MB/CMP0/CH`*número-canal*`/R`*número-rango*`/D`*número-dimm*	Módulos DIMM

▼ Para reconfigurar un dispositivo de forma manual

1. **Acceda al indicador de ALOM.**

   Consulte "Cambio de consola" en la página 6.

2. **Sitúese en el indicador** `sc>` **y escriba:**

```
sc> enablecomponent clave-asr
```

donde, *clave-asr* es cualquier identificador de dispositivo citado en la TABLA 4-6.

Nota – En lo que se refiere a los identificadores de dispositivo, el sistema no diferencia entre mayúsculas y minúsculas. Pueden escribirse de cualquiera de las dos formas.

El comando `enablecomponent` de ALOM puede utilizarse para reconfigurar cualquier dispositivo que se haya desconfigurado previamente con el comando `disablecomponent`.

Visualización de la información de errores del sistema

El software de ALOM permite ver los errores válidos del sistema. El comando `showfaults` muestra el ID de error, el dispositivo FRU afectado y el mensaje de error en la salida estándar. `showfaults` presenta también los resultados de las pruebas POST.

▼ Para ver la información de errores del sistema

1. **Acceda al indicador de ALOM.**

   Consulte "Cambio de consola" en la página 6.

2. **Sitúese en el indicador `sc>` y escriba:**

```
sc> showfaults -v
```

Por ejemplo:

```
sc> showfaults
   ID FRU       Fault
    0 FT0.FM2   SYS_FAN at FT0.FM2 has FAILED.
```

Si se añade la opción –v, también indica la hora:

```
sc> showfaults -v
   ID Time              FRU         Fault
    0 MAY 20 10:47:32   FT0.FM2     SYS_FAN at FT0.FM2 has FAILED.
```

Software de acceso multirruta

El software de acceso multirruta permite definir y controlar rutas físicas redundantes de acceso a dispositivos de E/S tales como las redes y los dispositivos de almacenamiento. Si la ruta de acceso a un dispositivo deja de estar disponible, el software puede desviar los datos automáticamente a una ruta alternativa para mantener la disponibilidad. Esta capacidad se denomina *failover automático*

(tolerancia a fallos). Para aprovechar las capacidades que ofrece este software, es preciso configurar el servidor con componentes de hardware redundantes, como interfaces de red redundantes o dos adaptadores de bus del sistema conectados a una misma matriz de almacenamiento de dos puertos.

Para el servidor, existen tres tipos de software multirruta disponibles:

- IP Network Multipathing de Solaris, que proporciona funciones de acceso multirruta y-balanceo de carga para las interfaces de red IP.
- VERITAS Volume Manager (VxVM), cuya función Dynamic Multipathing (DMP) proporciona rutas redundantes y balanceo de carga en el acceso a los discos para optimizar la velocidad de E/S.
- Sun StorEdge™ Traffic Manager es una arquitectura totalmente integrada en Solaris (desde la versión Solaris 8) que permite acceder a los dispositivos de E/S a través de diferentes interfaces de la controladora del sistema desde una sola instancia del dispositivo de E/S.

Para obtener instrucciones sobre cómo configurar y administrar el software IP Network Multipathing de Solaris, consulte el documento *IP Network Multipathing Administration Guide* suministrado con la versión de Solaris en uso.

Para obtener información sobre VxVM y su función DMP, consulte la documentación suministrada con el software VERITAS Volume Manager.

Si precisa información sobre el software Sun StorEdge Traffic Manager, consulte la documentación de Solaris.

Almacenamiento de la información de las unidades FRU

▼ Para guardar la información en las PROM de las unidades FRU disponibles

1. **Acceda al indicador de ALOM.**

   Consulte "Cambio de consola" en la página 6.

2. **Sitúese en el indicador `sc>` y escriba:**

```
setfru -c datos
```

Recuperación automática del sistema

Recuperación automática del sistema (ASR) consta de funciones de autocomprobación y una función de configuración automática para detectar fallos en componentes del hardware y quitarlos de la configuración. Si se habilita esta característica, el servidor puede reanudar su funcionamiento después de experimentar ciertos errores o fallos de hardware no graves.

Si ASR supervisa un componente y el servidor puede funcionar sin él, se reiniciará automáticamente en caso de fallo o error de dicho componente. Esta función evita que un componente de hardware defectuoso cause el cierre de todo el sistema o errores continuos en el servidor.

Si se detecta un fallo durante la secuencia de encendido, el componente defectuoso se inhabilita. Si el sistema puede funcionar sin él, la secuencia de arranque prosigue.

Para la admisión de la función de arranque reducido, el firmware de OpenBoot utiliza la interfaz de cliente 1275 (por medio del árbol de dispositivos) para marcar un dispositivo como *failed* (fallo) o *disabled* (deshabilitado) mediante la creación de la propiedad de estado apropiada en el nodo correspondiente del árbol de dispositivos. El sistema operativo Solaris no activa los controladores de los subsistemas marcados como failed (fallo) o disabled (deshabilitado).

Mientras el componente defectuoso sea eléctricamente inactivo (no provoque errores aleatorios o ruido de señal, por ejemplo), el sistema se reinicia automáticamente y reanuda su funcionamiento al tiempo que se efectúa una llamada de mantenimiento.

Después de sustituir el dispositivo en estado *failed* o *disabled* por uno nuevo, el firmware de OpenBoot modifica automáticamente el estado del mismo en el siguiente rearranque.

Nota – ASR no se habilita hasta que el usuario la activa. Consulte "Para habilitar ASR" en la página 48.

Opciones de autoarranque

El conmutador `auto-boot?` controla si el firmware debe arrancar automáticamente el sistema operativo después de cada reinicio. El valor predeterminado es `true`.

El conmutador `auto-boot-on-error?` controla si el sistema debe intentar efectuar un arranque reducido en caso de detectar un fallo en un subsistema. La configuración predeterminada para `auto-boot-on-error?` es `false`. Tanto `auto-boot?` como `auto-boot-on-error?` se deben establecer en `true` para permitir un arranque reducido automático.

▼ Para habilitar el arranque reducido automático

1. **Obtenga el indicador `ok`.**
   Consulte "Para visualizar el indicador `ok`" en la página 28.
2. **Escriba:**

```
ok setenv auto-boot? true
ok setenv auto-boot-on-error? true
```

Nota – El sistema no efectuará un arranque reducido en respuesta a un error irrecuperable y grave, aunque la opción esté activada. Para ver ejemplos de errores irrecuperables y graves, consulte la sección "Resumen de gestión de errores" en la página 47.

Resumen de gestión de errores

La gestión de errores durante la secuencia de encendido puede clasificarse en tres categorías que se resumen en la tabla siguiente:

- Si las pruebas de diagnóstico de POST y OpenBoot no detectan ningún error, el sistema intentará arrancar si `auto-boot?` es `true`.
- Si las pruebas de diagnóstico de POST y OpenBoot no detectan ningún error no fatal, el sistema intentará arrancar cuando `auto-boot?` sea `true` y `auto-boot-on-error?` sea también `true`. Entre los casos de errores leves se incluyen los siguientes:
  - Error del subsistema SAS. En este caso se precisa una ruta de acceso al disco de arranque alternativa. Para obtener más información, consulte "Software de acceso multirruta" en la página 44.
  - Error de la interfaz Ethernet.
  - Error de la interfaz USB.
  - Error de la interfaz serie.
  - Error de la tarjeta PCI.
  - Error de la memoria. Si falla un módulo DIMM, el firmware desconfigurará todo el banco lógico asociado al módulo defectuoso. Es preciso que haya otro banco lógico en buen estado de funcionamiento en el sistema para poder intentar un inicio en modo degradado.

Nota – Si las pruebas de diagnóstico de POST y OpenBoot detectan un error no grave asociado al dispositivo de arranque normal, el firmware de OpenBoot desconfigurará automáticamente el dispositivo defectuoso y probará con el siguiente dispositivo especificado en la variable de configuración `boot-device`.

- Si las pruebas de diagnóstico de POST y OpenBoot detectan un error grave, el sistema no se iniciará independientemente de los valores de `auto-boot?` o `auto-boot-on-error?` Entre los casos de errores irrecuperables se incluyen los siguientes:
  - Error en todas las CPU
  - Error en todos los bancos de memoria lógicos
  - Error de CRC (comprobación de redundancia cíclica) en la memoria RAM flash
  - Error crítico de los datos de configuración de la PROM de FRU (field-replaceable unit)
  - Error crítico de un ASIC (circuito integrado para aplicaciones específicas)

▼ Para habilitar ASR

1. **Obtenga el indicador `ok`.**

   Consulte "Para visualizar el indicador `ok`" en la página 28.

2. **Configure el sistema para ASR. Escriba:**

```
ok setenv diag-switch? true
ok setenv auto-boot? true
ok setenv auto-boot-on-error? true
```

3. **Habilite ASR. Escriba:**

```
ok reset-all
```

   El sistema almacena permanentemente los cambios de los parámetros y arranca automáticamente.

▼ Para deshabilitar ASR

1. **Obtenga el indicador `ok`.**

   Consulte "Para visualizar el indicador `ok`" en la página 28.

2. **Desconfigure los modos de diagnóstico. Escriba:**

```
ok setenv diag-switch? false
```

3. **Deshabilite ASR. Escriba:**

```
ok reset-all
```

El sistema almacena permanentemente los cambios de los parámetros y arranca automáticamente.

Actualización del firmware

La actualización o instalación de una versión anterior del firmware se realiza con el comando `flashupdate` en el indicador de ALOM. El comando `flashupdate` actualiza las PROM flash en el controlador del sistema y la placa base del sistema. El comando `flashupdate` requiere que el puerto de gestión de red esté conectado a una red adecuada. Este puerto se debe configurar para que reconozca un servidor FTP externo que contenga las imágenes del nuevo firmware que va a descargar.

Para utilizar el comando `flashupdate` es necesario conocer los siguientes datos:

- Dirección IP del servidor de FTP desde el que se va a descargar la imagen del firmware
- Ruta de acceso en que la imagen está almacenada
- Nombre de usuario y contraseña, para escribirlos en los indicadores

Si no dispone de esta información, solicítela al administrador de la red.

La sintaxis del comando `flashupdate` es:

`flashupdate [-s` *dirección_IP* `-f` *nombre_ruta*`] [-v]`

donde:

- `-s` *IPaddr* es la dirección IP de un servidor FTP que tiene la imagen del firmware
- `-f` *ruta_acceso* es la ruta de acceso completa al archivo de imagen del firmware.
- `-v` produce la salida del mensaje completo sobre el progreso de la descarga y la actualización

---

Nota – El comando `flashupdate` no puede recuperar imágenes flash de una URL HTTP segura y protegida mediante ID de usuario y contraseña. Se muestra el mensaje `flashupdate: failed, URL does not contain required file:` *archivo*, aunque es posible que el archivo exista.

Precaución – No interrumpa la ejecución del comando `flashupdate`. Si cancela el comando `flashupdate`, el controlador del sistema pasa al modo de un solo usuario y sólo puede tener acceso a él desde el puerto serie.

▼ Para actualizar el firmware del servidor

1. **Encienda el servidor.**
2. **Acceda al indicador de ALOM.**

   Consulte "Cambio de consola" en la página 6.
3. **Actualice el firmware:**

```
sc> flashupdate -s IPaddr -f ruta_acceso
```

   Por ejemplo (sustituyendo `123.45.67.89` por una dirección IP válida):

```
sc> flashupdate -s 123.45.67.89 -f
/net/server/sysfw/System_Firmware-6_0_0-Netra_T2000.bin

SC Alert: System poweron is disabled.
```

4. **Cuando lo solicite el sistema, escriba el nombre de usuario y la contraseña.**

   Por ejemplo:

```
Username: nombre_usuario
Password: contraseña
```

   El nombre de usuario y la contraseña están basados en el nombre de usuario y contraseña de UNIX o LDAP, no de ALOM.

   Después de escribir el nombre de usuario y la contraseña, el proceso de descarga continúa y aparecen líneas de puntos en la pantalla.

   Por ejemplo:

```
.....................................................................
.....................................................................
.....................................
```

   Una vez finalizada la descarga, ALOM muestra el mensaje:

```
Update complete. Reset device to use new software.

SC Alert: SC firmware was reloaded
```

5. **Escriba el comando `resetsc` para restaurar ALOM:**

```
sc> resetsc
Are you sure you want to reset the SC [y/n]? y
User Requested SC Shutdown
```

Nota – Si quiere omitir el mensaje de confirmación, utilice la opción `-y` con el comando `resetsc`. Si `resetsc` se ejecuta desde una sesión Telnet, ésta finalizará al reiniciar el controlador. La salida del comando de reinicio aparecerá a través del puerto serie de gestión del controlador del sistema.

El controlador del sistema se reinicia, ejecuta las pruebas de diagnóstico y vuelve a presentar el indicador de inicio de sesión.

CAPÍTULO 5

Seguridad del servidor

En este capítulo se proporciona información importante sobre la seguridad del sistema, se detallan recomendaciones de seguridad y se analiza la minimización de dominios. Además, se hace referencia a las características de la seguridad del entorno operativo Solaris.

El capítulo está dividido en las siguientes secciones:

Directrices de seguridad

A continuación encontrará algunas medidas de seguridad que debe tener en cuenta:

- Asegúrese de que todas las contraseñas cumplen las directrices de seguridad.
- Cambie las contraseñas regularmente.
- Inspeccione los archivos de registro regularmente por si existen irregularidades.

La acción de configurar un sistema para limitar el acceso no autorizado se denomina *blindaje*. Existen varios pasos en la configuración que pueden ayudar a blindar el sistema. Los siguientes pasos son directrices para la configuración del sistema:

- Realice modificaciones de seguridad inmediatamente después de actualizar el firmware de las aplicaciones del controlador del sistema y del entorno operativo en tiempo real de Sun Fire™ (RTOS), y antes de configurar o instalar cualquier dominio de Sun Fire.
- Intente, en general, restringir el acceso al entorno operativo en tiempo real del controlador del sistema.
- Limite el acceso físico a los puertos serie.
- Tenga en cuenta que debe reiniciar el sistema, en función de los cambios de configuración.

Definición de la contraseña de la consola

Las únicas restricciones aplicables a las contraseñas de la consola del controlador del sistema están relacionadas con el conjunto de caracteres ASCII y el emulador terminal en uso. El controlador del sistema utiliza el algoritmo MD5 para generar un código hash de la contraseña introducida. Por lo tanto, todos los caracteres introducidos se tienen en cuenta.

El requisito de que la contraseña tenga una longitud mínima de 16 caracteres favorece el uso de contraseñas formadas por varias palabras en lugar de por una sola. Las contraseñas deberían estar formadas por una combinación de caracteres en minúscula, mayúscula, numéricos y de puntuación. Para obtener más información sobre cómo establecer la contraseña de la consola, consulte *Guía de instalación del servidor Netra T2000*, 819-7361-10.

Uso de la configuración predeterminada del protocolo SNMP

El protocolo SNMP (del inglés Simple Network Management Protocol, protocolo simple de administración de redes) se utiliza normalmente para controlar y administrar dispositivos y servidores en red. De forma predeterminada, el protocolo SNMP está desactivado.

Nota – Para utilizar el software de Sun Management Center es necesario utilizar el protocolo SNMP. Sin embargo, puesto que el controlador del sistema no es compatible con una versión segura del protocolo SNMP, no debe activarlo a menos que tenga que utilizar el software de Sun Management Center.

Reinicio del controlador de sistema después de realizar modificaciones

▼ Para reiniciar el controlador del sistema

Es necesario reiniciar el controlador del sistema si aparece un mensaje en la consola similar al siguiente:

```
Rebooting the SC is required for changes in network settings to
take effect.
```

1. **Escriba** `resetsc -y` **para reiniciar el controlador del sistema.**

   El controlador del sistema se puede reiniciar a la vez que se está ejecutando el dominio de Solaris.

2. **Utilice el comando** `shownetwork` **para comprobar que las modificaciones de la red se han realizado.**

   Para obtener más información sobre el uso de Sun Security Toolkit para crear configuraciones seguras en servidores que ejecuten el entorno operativo Solaris, visite el siguiente sitio web:

   `http://www.sun.com/software/security/jass`

Selección de un tipo de conexión remota

Los servicios SSH y telnet del controlador del sistema están desactivados de forma predeterminada.

Habilitación de SSH

Si el controlador del sistema se encuentra en una red de uso general, puede garantizar el acceso remoto seguro al controlador del sistema mediante SSH en lugar de telnet. El servicio SSH cifra los datos que se transfieren entre el host y el cliente. SSH proporciona mecanismos de autenticación que identifican tanto a los host como a los usuarios, lo que permite establecer conexiones seguras entre sistemas conocidos. El servicio telnet no es seguro, ya que el protocolo de telnet transmite información, incluidas las contraseñas, sin cifrar.

Nota – El servicio SSH no debe utilizarse con los protocolos FTP, HTTP, SYSLOG o SNMPv1. Estos protocolos no son seguros y se deben utilizar con precaución en las redes de uso general.

El controlador del sistema proporciona ciertas funciones de SSH, pero sólo es compatible con las solicitudes de cliente la versión 2 de SSH (SSH v2). En la TABLA 5-1 se identifican los distintos atributos del servidor SSH y se describe cómo se gestionan los atributos en este subconjunto. Los parámetros de los atributos no se pueden configurar.

TABLA 5-1 Atributos del servidor SSH

Atributo	Valores de ejemplo	Comentario
`Protocol`	`2`	Admite sólo SSH v2
`Port`	`22`	Puerto de escucha
`ListenAddress`	`0.0.0.0`	Admite varias direcciones IP
`AllowTcpForwarding`	`no`	No compatible con el reenvío de puerto
`RSAAuthentication`	`no`	Autenticación de clave pública no activada
`PubkeyAuthentication`	`no`	Autenticación de clave pública no activada
`PermitEmptyPasswords`	`yes`	Autenticación de contraseña controlada por el controlador del sistema
`MACs`	`hmac-sha1,hmac-md5`	Implantación del servidor SSH igual que la del entorno operativo Solaris 9
`Ciphers`	`aes128-cbc,blowfish-cbc,3des-cbc`	Implantación del servidor SSH igual que la del entorno operativo Solaris 9

▼ Para activar SSH

- **Para activar SSH, escriba:**

```
sc> setupsc
```

Se le pide que introduzca los parámetros de conexión y la configuración de red.

Por ejemplo:

```
sc> setupsc

Network Configuration
---------------------
Is the system controller on a network? [yes]:
Use DHCP or static network settings? [static]:
Hostname [hostname]:
IP Address [xxx.xxx.xxx.xxx]:
Netmask [xxx.xxx.xxx.x]:
Gateway [xxx.xxx.xxx.xxx]:
DNS Domain [xxxx.xxx.xxx]:
Primary DNS Server [xxx.xxx.xxx.xx]:
Secondary DNS Server [xxx.xxx.xx.x]:
Connection type (ssh, telnet, none) [ssh]:

Rebooting the SC is required for changes in the above network
settings to take effect.
lom>
```

Características no admitidas por SSH

El servidor SSH de este servidor no es compatible con las siguientes características:

- Ejecución de línea de comandos remota
- Comando `scp` (programa de copia segura)
- Comando `sftp` (programa de transferencia de archivos segura)
- Reenvío de puerto
- Autenticación de usuarios por clave
- Clientes SSH v1

Si intenta utilizar cualquiera de las características anteriores, se genera un mensaje de error. Por ejemplo, si escribe el siguiente comando:

```
# ssh SCHOST showboards
```

Se generan los siguientes mensajes:

- En el cliente SSH:

```
Connection to SCHOST closed by remote host.
```

- En la consola del controlador del sistema:

```
[0x89d1e0] sshdSessionServerCreate: no server registered
           for showboards
[0x89d1e0] sshd: Failed to create sshdSession
```

Cambio de las claves de host SSH

Es una buena medida de seguridad obtener periódicamente nuevas claves de host. Si tiene la sospecha de que la privacidad puede haberse puesto en peligro, puede utilizar el comando `ssh-keygen` para volver a generar las claves de host del sistema.

Las claves de host, una vez generadas, sólo se pueden reemplazar, pero no eliminar sin recurrir al comando `setdefaults`. Para activar las claves de host que se acaban de generar, se debe reiniciar el servidor SSH ejecutando el comando `restartssh` o reiniciando el sistema. Para obtener más información sobre los comandos `ssh-keygen` y `restartssh` (con ejemplos), consulte la publicación *Sun Fire Entry-Level Midrange System Controller Command Reference Manual*, 819-1268-10.

Nota – También puede utilizar el comando `ssh-keygen` para ver host la huella digital de la clave de host en el controlador del sistema.

Consideraciones adicionales sobre seguridad

Acceso al shell del entorno operativo en tiempo real por medio de secuencias especiales de clave

Mientras se está iniciando el controlador del sistema, se puede especificar secuencias especiales de claves a través de la conexión en serie. Estas secuencias de claves poseen capacidades especiales si se introducen en el puerto serie en los primeros 30 segundos después de reiniciar el controlador del sistema.

Las capacidades especiales de estas secuencias de claves se desactivan automáticamente pasados 30 segundos después de que aparezca el mensaje de copyright de Sun. Una vez desactivadas las capacidades, las secuencias de claves funcionan como claves de control normales.

Dado que la seguridad del controlador del sistema se puede poner en peligro en caso de acceso no autorizado al shell del entorno operativo en tiempo real, debe controlar el acceso a los puertos serie del controlador.

Minimización de dominios

Una manera de fortalecer la seguridad de los servidores es limitar la instalación del software a los requisitos mínimos esenciales. Al limitar el número de componentes de software instalados en cada dominio (lo que se denomina *minimización de dominios*), se reduce el riesgo de fallos de seguridad que podrían aprovechar posibles intrusos.

Para obtener información detallada y con ejemplos sobre la minimización, consulte el artículo *Minimizing Domains for Sun Fire V1280, 6800, 12K, and 15K Systems* (en dos partes) disponible *en* línea en:

`http://www.sun.com/security/blueprints`

Seguridad del entorno operativo Solaris

Para obtener más información sobre la seguridad del entorno operativo Solaris, consulte las siguientes publicaciones y artículos:

- *Solaris Security Best Practices:* disponible en línea en:

  `http://www.sun.com/software/security/blueprints`
- *Solaris Security Toolkit*: disponible en línea en:

  `http://www.sun.com/software/security/jass`

CAPÍTULO 6

Administración de los volúmenes de discos

En este capítulo se describen los conceptos relativos a la tecnología RAID (matriz redundante de discos independientes), y la forma de configurar y administrar volúmenes de discos RAID utilizando el controlador de discos SCSI (SAS) integrado en la placa del servidor.

Este capítulo incluye las siguientes secciones:

Requisitos de RAID

Para configurar y utilizar volúmenes de discos RAID en el servidor, es necesario que instale los parches ID 119850-12 y 122165-01. Estos parches están disponibles para su descarga en

`http://www.sunsolve.com`

Los procedimientos de instalación de los parches se incluyen en los archivos README que los acompañan.

Nota – Para ver la información más reciente sobre los parches para este servidor, consulte las notas del producto sobre el servidor, disponibles en:
`http://www.sun.com/documentation`

Volúmenes de discos

Desde la perspectiva del controlador de discos integrado en la placa del servidor, los *volúmenes de discos* son discos lógicos que incluyen uno o varios discos físicos completos.

Una vez creado un volumen, el sistema operativo lo utiliza y mantiene como si se tratase de un solo disco. Al proporcionar esta capa de gestión de volumen lógico, el sistema operativo supera las restricciones impuestas por los dispositivos de disco físico.

El controlador de discos integrado en la placa del servidor permite crear un total de dos volúmenes RAID por hardware y configurarlos como volúmenes de dos discos RAID 1 (duplicación en espejo integrada o IM), o bien volúmenes de dos, tres o cuatro discos RAID 0 (segmentación integrada o IS).

Nota – Debido a la inicialización de volúmenes que se produce en el controlador de discos cuando se crea un volumen nuevo, se desconocen propiedades de éste tales como la geometría y el tamaño. Los volúmenes RAID creados con el controlador de hardware deben configurarse y etiquetarse utilizando el comando `format`(1M) antes de utilizarse con el sistema operativo Solaris. Consulte "Para configurar y etiquetar un volumen RAID" en la página 71, o la página del comando man de `format` (1M) para obtener más información.

No es posible efectuar migración de volúmenes (reasignar todos los discos del volumen RAID de un chasis a otro). Si es necesario realizar esta operación, póngase en contacto con el servicio técnico de Sun.

Tecnología RAID

La tecnología RAID permite construir un volumen lógico compuesto por varios discos físicos con el fin de proporcionar redundancia de datos, mayor rendimiento o ambas cosas a la vez. El controlador de discos integrado en la placa del servidor permite crear volúmenes RAID 0 y RAID 1.

En esta sección se explican las configuraciones RAID admitidas por el controlador de discos:

- Segmentación (striping) integrada o volúmenes IS (RAID 0)
- Duplicación en espejo (mirroring) integrada o IM (RAID 1)

Segmentación integrada (RAID 0)

En los volúmenes segmentados, el volumen se distribuye entre dos o más discos físicos y los datos se van escribiendo secuencialmente en los discos que componen volumen (lo que en inglés se denomina *striping*).

Los volúmenes segmentados proporcionan una unidad lógica (LUN) cuya capacidad es equivalente a la suma de todos los discos que la componen. Por ejemplo, un volumen IS de tres discos formado por unidades de disco de 72 GB tendrá 216 GB de capacidad.

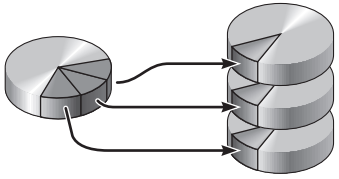

FIGURA 6-1 Representación gráfica de la segmentación de discos

Precaución – No existe redundancia de datos en la configuración de volúmenes IS. Por tanto, si un disco falla, el volumen entero deja de funcionar y los datos se pierden. Si un volumen IS se borra de forma manual, todos sus datos se pierden.

Los volúmenes IS tienden a proporcionar mejor rendimiento que los volúmenes IM o los discos independientes. Bajo determinadas cargas de trabajo, especialmente en cargas de escritura o mixtas de lectura y escritura, las operaciones de E/S se realizan antes porque cada bloque secuencial se escribe por turnos en cada disco del volumen.

Duplicación en espejo integrada (RAID 1)

La duplicación en espejo (RAID 1) es una técnica que utiliza la redundancia de datos, en que dos copias completas de todos los datos se almacenan en dos discos independientes, como forma de protección contra la pérdida de información o posibles errores de los discos. Un volumen lógico se duplica en dos discos diferentes.

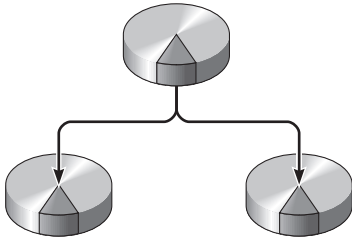

FIGURA 6-2 Representación gráfica de la duplicación de discos en espejo

Ambos discos se actualizan siempre que el sistema operativo escribe en un volumen con duplicación en espejo. Los discos se mantienen en todo momento exactamente con la misma información. Cuando el sistema operativo necesita leer los datos, lo hace desde el disco que se encuentra más accesible en ese momento, lo cual puede mejorar el rendimiento de las operaciones de lectura.

Precaución – La creación de volúmenes RAID con el controlador de discos de la placa destruye todos los datos de los discos que componen el volumen. El procedimiento de inicialización de volúmenes del controlador de discos reserva una porción de cada disco físico para metadatos y otra información interna utilizada por el controlador. Una vez inicializado el volumen, éste puede configurarse y etiquetarse con el comando `format`(1M). Después de hacerlo, puede empezar a utilizarse en Solaris.

Operaciones de RAID de hardware

El controlador SAS del servidor permite efectuar segmentación y duplicación de discos en espejo mediante la utilidad `raidctl` de Solaris.

Un volumen RAID creado por hardware con `raidctl` se comporta de forma ligeramente distinta a otro creado con el software de administración de volúmenes. En el volumen creado mediante software, cada dispositivo tiene su propia entrada en el árbol de dispositivos virtuales y las operaciones de lectura y escritura se realizan en ambos dispositivos virtuales. En los volúmenes RAID por hardware, sólo aparece un dispositivo en el árbol de dispositivos. Los discos que componen el volumen son invisibles para el sistema operativo y sólo se accede a ellos mediante el controlador SAS.

Números de ranura y nombres de dispositivo de los discos sin RAID

Para realizar un procedimiento de sustitución de discos en marcha, es necesario conocer el nombre del dispositivo físico o lógico de la unidad que se va a instalar o extraer. Si el sistema detecta un error de disco, es posible que aparezcan en la consola del sistema mensajes sobre discos que dan problemas o que están fuera de servicio. Esta información también se registra en los archivos `/var/adm/messages`.

Normalmente, estos mensajes de error identifican la unidad de disco duro defectuosa por su nombre de dispositivo físico (por ejemplo, `/devices/pci@1f,700000/scsi@2/sd@1,0`) o su nombre de dispositivo lógico (por ejemplo, `c0t1d0`). Asimismo, algunas aplicaciones pueden hacer referencia también al número de ranura del disco (de 0 a 3).

Puede utilizar la TABLA 6-1 para asociar los números de ranura de los discos internos al nombre de dispositivo físico de cada unidad de disco duro.

TABLA 6-1 Número de ranura de los discos físicos y nombres de los dispositivos físicos y lógicos

Número de ranura de disco	Nombre de dispositivo lógico*	Nombre de dispositivo físico
Ranura 0	`c0t0d0`	`/devices/pci@780/pci@0/pci@9/scsi@0/sd@0,0`
Ranura 1	`c0t1d0`	`/devices/pci@780/pci@0/pci@9/scsi@0/sd@1,0`

* En función del número y el tipo de controladores de disco que se hayan instalado, es posible que los dispositivos lógicos aparezcan con un nombre distinto en su sistema.

▼ Para crear un volumen con duplicación en espejo

1. **Compruebe qué unidad de disco duro corresponde a cada nombre de dispositivo lógico y físico.**

   Consulte "Números de ranura y nombres de dispositivo de los discos sin RAID" en la página 64.

   Para verificar qué tipo de configuración RAID de hardware hay en el sistema, escriba:

```
# raidctl
No RAID volumes found.
```

   En el ejemplo anterior se indica que no existe ningún volumen RAID. Otro posible caso:

```
# raidctl
RAID    Volume  RAID            RAID            Disk
Volume  Type    Status          Disk            Status
-----------------------------------------------------------
c0t0d0  IM      OK              c0t0d0          OK
                                c0t1d0          OK
```

   En este ejemplo, sólo se ha habilitado un volumen IM. Está completamente sincronizado y en línea.

   El controlador SAS integrado en la placa del servidor puede configurar dos volúmenes RAID como máximo. Antes de crear un volumen, asegúrese de que los discos que lo componen estén disponibles y que no existan ya dos volúmenes.

   Los valores proporcionados en la columna `RAID Status` se describen a continuación:

   - `OK`: el volumen RAID se encuentra conectado y totalmente sincronizado.

- RESYNCING: los datos entre el disco principal y el disco secundario de un volumen IM se están sincronizando.
- DEGRADED: un disco del volumen tiene un fallo o está desconectado.
- FAILED: el volumen se debe borrar y reinicializar. Esto puede producirse si se pierde uno de los discos de un volumen IS o se pierden ambos discos de un volumen IM.

Los valores proporcionados en la columna Disk Status se describen a continuación:

- OK: la unidad está conectada y funciona correctamente.
- FAILED, MISSING o OFFLINE: el disco tiene alguna cuestión de hardware o de configuración que precisa atención.

Por ejemplo, un IM cuyo disco secundario se ha extraído del chasis aparece como:

```
# raidctl
RAID    Volume  RAID            RAID            Disk
Volume  Type    Status          Disk            Status
-----------------------------------------------------
c0t0d0  IM      DEGRADED        c0t0d0          OK
                                c0t1d0          MISSING
```

Consulte la página del comando man de raidctl(1M) para obtener más información sobre el estado de los volúmenes y los discos.

Nota – En función del número y el tipo de controladores de disco que se hayan instalado, es posible que los dispositivos lógicos aparezcan con un nombre distinto en su sistema.

---

2. **Escriba el comando siguiente:**

```
# raidctl -c principal secundario
```

La creación de un volumen RAID es interactiva de forma predeterminada. Por ejemplo:

```
# raidctl -c c0t0d0 c0t1d0
Creating RAID volume c0t0d0 will destroy all data on member disks,
proceed
(yes/no)? yes
Volume 'c0t0d0' created
#
```

Como alternativa, también puede utilizar la opción `-f` para forzar la creación del volumen si conoce con certeza los discos que lo integran y tiene la seguridad de que sus datos pueden perderse sin problemas. Por ejemplo:

```
# raidctl -f -c c0t0d0 c0t1d0
Volume 'c0t0d0' created
#
```

Cuando se crea el duplicado RAID en espejo, el disco secundario (en este caso, `c0t1d0`) desaparece del árbol de dispositivos de Solaris.

3. **(Opcional) Para comprobar el estado de un duplicado RAID, escriba el comando siguiente:**

```
# raidctl
RAID    Volume  RAID          RAID          Disk
Volume  Type    Status        Disk          Status
------------------------------------------------------------
c0t0d0  1M      RESYNCING     c0t0d0        OK
                              c0t1d0        OK
```

En el ejemplo anterior se indica que el duplicado RAID aún se está resincronizando con la unidad de disco secundaria.

En el ejemplo siguiente, el duplicado RAID está completamente sincronizado y en línea.

```
# raidctl
RAID    Volume  RAID            RAID            Disk
Volume  Type    Status          Disk            Status
-----------------------------------------------------
c0t0d0  IM      OK              c0t0d0          OK
                                c0t1d0          OK
```

El controlador de discos sincroniza los volúmenes IM de uno en uno. Si se crea un segundo volumen IM antes de que haya finalizado la sincronización del primero, el primero de ellos indicará el estado de RAID `RESYNCING` y el segundo mostrará el estado `OK`. Una vez sincronizado el primer volumen, su estado cambiará a `OK` y empezará automáticamente la sincronización del segundo volumen, que ahora mostrará el estado `RESYNCING`.

Con la configuración RAID 1 (duplicación de discos en espejo), todos los datos se duplican en ambas unidades de disco. Si una de ellas falla, sustitúyala por otra en buen estado y recupere los datos a partir del disco duplicado. Para obtener instrucciones al respecto, consulte "Para realizar una operación de conexión en marcha de un disco duplicado en espejo-" en la página 76.

Para obtener más información sobre la utilidad `raidctl`, consulte la página del comando man de `raidctl`(1M).

▼ Para crear un volumen con el dispositivo de arranque predeterminado duplicado

Debido a la inicialización de volúmenes que se produce en el controlador de discos cada vez que se crea un volumen nuevo, es preciso configurar y etiquetar el volumen con la utilidad `format`(1M) antes de empezar a usarlo en Solaris (consulte "Para configurar y etiquetar un volumen RAID" en la página 71). Como consecuencia de esta limitación, `raidctl`(1M) bloquea la creación de cualquier volumen RAID por hardware si alguno de los discos integrantes tiene un sistema de archivos montado.

En esta sección se explica el procedimiento necesario para crear un volumen RAID por hardware que contenga el dispositivo de arranque predeterminado. Dado que este dispositivo siempre tiene un sistema de archivos montado cuando se inicia, es preciso utilizar una forma de arranque alternativa en cuyo entorno se creará el volumen. El medio alternativo sugerido es una imagen de instalación en red en el modo de un solo usuario. Consulte *Solaris 10 Installation Guide* para obtener información sobre cómo configurar y utilizar las instalaciones basadas en red.

1. **Determine cuál de los discos es el dispositivo de arranque predeterminado.**

   Desde el indicador `ok` de OpenBoot, ejecute el comando `printenv` y, si es necesario, el comando `devalias` para identificar el dispositivo de arranque predeterminado. Por ejemplo:

```
ok printenv boot-device
boot-device =         disk

ok devalias disk
disk                  /pci@780/pci@0/pci@9/scsi@0/disk@0,0
```

2. **Ejecute el comando** `boot net -s`**.**

```
ok boot net -s
```

3. **Una vez iniciado el sistema, use la utilidad** `raidctl(1M)` **para crear un volumen duplicado por hardware cuyo disco principal sea el dispositivo de arranque predeterminado.**

   Consulte "Para crear un volumen con duplicación en espejo" en la página 65. Por ejemplo:

```
# raidctl -c c0t0d0 c0t1d0
Creating RAID volume c0t0d0 will destroy all data on member disks,
proceed
(yes/no)? yes
Volume  c0t0d0  created
#
```

   Ahora el volumen se puede instalar con el sistema operativo Solaris utilizando cualquier método admitido. El volumen RAID `c0t0d0` creado por hardware aparece como un disco para el programa de instalación de Solaris.

Nota – En función del número y el tipo de controladores de disco que se hayan instalado, es posible que los dispositivos lógicos aparezcan con un nombre distinto en su sistema.

▼ Para crear un volumen con segmentación

1. **Compruebe qué unidad de disco duro corresponde a cada nombre de dispositivo lógico y físico.**

   Consulte "Números de ranura y nombres de dispositivo de los discos sin RAID" en la página 64.

2. **(Opcional) Para verificar la configuración RAID actual, escriba:**

```
# raidctl
No RAID volumes found.
```

   En el ejemplo anterior se indica que no existe ningún volumen RAID.

Nota – En función del número y el tipo de controladores de disco que se hayan instalado, es posible que los dispositivos lógicos aparezcan con un nombre distinto en su sistema.

---

3. **Escriba el comando siguiente:**

```
# raidctl -c -r 0 disco1 disco2 ...
```

   La creación de un volumen RAID es interactiva de forma predeterminada. Por ejemplo:

```
# raidctl -c -r 0 c0t1d0 c0t2d0 c0t3d0
Creating RAID volume c0t1d0 will destroy all data on member disks,
proceed
(yes/no)? yes
Volume 'c0t1d0' created
#
```

   Cuando se crea un volumen RAID segmentado, las otras unidades de disco que lo componen (en este caso, `c0t2d0` y `c0t3d0`) desaparecen del árbol de dispositivos de Solaris.

   Como alternativa, también se puede utilizar la opción `-f` para forzar la creación del volumen si se conocen con certeza los discos que lo integran y se tiene la seguridad de que sus datos pueden perderse sin problemas. Por ejemplo:

```
# raidctl -f -c -r 0 c0t1d0 c0t2d0 c0t3d0
Volume 'c0t1d0' created
#
```

4. **(Opcional) Para comprobar el estado de un volumen RAID segmentado, escriba el comando siguiente:**

```
# raidctl
RAID    Volume  RAID            RAID            Disk
Volume  Type    Status          Disk            Status
-----------------------------------------------------------
c0t1d0  IS      OK              c0t1d0          OK
                                c0t2d0          OK
                                c0t3d0          OK
```

En este ejemplo se indica que el volumen RAID segmentado está en línea y en funcionamiento.

En la configuración RAID 0 (segmentación o striping de discos), no se duplican los datos en las distintas unidades de disco. Los datos se van escribiendo por turno rotatorio en los discos que componen el volumen. Si se pierde un disco, se pierden todos los datos del volumen. Por este motivo, RAID 0 no puede utilizarse para garantizar la integridad ni la disponibilidad de los datos, pero sí para incrementar el rendimiento de las operaciones de escritura en determinadas situaciones.

Para obtener más información sobre la utilidad `raidctl`, consulte la página del comando man de `raidctl`(1M).

▼ Para configurar y etiquetar un volumen RAID

Después de crear un volumen RAID con `raidctl`, utilice la función `format`(`1M`) para configurarlo y etiquetarlo antes de proceder a usarlo con el sistema operativo Solaris.

1. **Inicie la utilidad** `format`**.**

```
# format
```

`format` puede generar mensajes indicando que la actual etiqueta del volumen que va a cambiar está dañada. Puede hacer caso omiso de estos mensajes sin riesgo.

2. **Seleccione el nombre del disco que representa el volumen RAID que ha configurado.**
   En este ejemplo, `c0t2d0` es el nombre lógico del volumen.

```
# format
Searching for disks...done
AVAILABLE DISK SELECTIONS:
        0. c0t0d0 <SUN72G cyl 14084 alt 2 hd 24 sec 424>
           /pci@780/pci@0/pci@9/scsi@0/sd@0,0
        1. c0t1d0 <SUN72G cyl 14084 alt 2 hd 24 sec 424>
           /pci@780/pci@0/pci@9/scsi@0/sd@1,0
        2. c0t2d0 <SUN72G cyl 14084 alt 2 hd 24 sec 424>
           /pci@780/pci@0/pci@9/scsi@0/sd@2,0
Specify disk (enter its number): 2
selecting c0t2d0
[disk formatted]
FORMAT MENU:
         disk       - select a disk
         type       - select (define) a disk type
         partition  - select (define) a partition table
         current    - describe the current disk
         format     - format and analyze the disk
         fdisk      - run the fdisk program
         repair     - repair a defective sector
         label      - write label to the disk
         analyze    - surface analysis
         defect     - defect list management
         backup     - search for backup labels
         verify     - read and display labels
         save       - save new disk/partition definitions
         inquiry    - show vendor, product and revision
         volname    - set 8-character volume name
         !<cmd>     - execute <cmd>, then return
         quit
```

3. **Ejecute el comando** `type` **en el indicador de** `format>` **y seleccione 0 (cero) para configurar el volumen de forma automática.**

   Por ejemplo:

```
format> type

AVAILABLE DRIVE TYPES:
         0. Auto configure
         1. DEFAULT
         2. SUN72G
         3. SUN72G
         4. other
Specify disk type (enter its number)[3]: 0
c0t2d0: configured with capacity of 68.23GB
<LSILOGIC-LogicalVolume-3000 cyl 69866 alt 2 hd 16 sec 128>
selecting c0t2d0
[disk formatted]
```

4. **Utilice el comando** `partition` **para *particionar* el volumen según la configuración que desee.**

   Consulte la página del comando man de `format(1M)` para obtener más información.

5. **Escriba la nueva etiqueta en el disco utilizando el comando** `label`**.**

```
format> label
Ready to label disk, continue? yes
```

6. **Compruebe si la nueva etiqueta se ha escrito utilizando el comando** `disk` **para ver la lista de discos.**

```
format> disk

AVAILABLE DISK SELECTIONS:
        0. c0t0d0 <SUN72G cyl 14084 alt 2 hd 24 sec 424>
           /pci@780/pci@0/pci@9/scsi@0/sd@0,0
        1. c0t1d0 <SUN72G cyl 14084 alt 2 hd 24 sec 424>
           /pci@780/pci@0/pci@9/scsi@0/sd@1,0
       2. c0t2d0 <LSILOGIC-LogicalVolume-3000 cyl 69866 alt 2 hd
16 sec 128>
           /pci@780/pci@0/pci@9/scsi@0/sd@2,0
Specify disk (enter its number)[2]:
```

Nota – Ahora, observe que el dispositivo `c0t2d0` indica el tipo `LSILOGIC-LogicalVolume`.

---

7. **Salga de la utilidad** `format`**.**

   Ahora puede empezar a usar el volumen en Solaris.

Nota – En función del número y el tipo de controladores de disco que se hayan instalado, es posible que los dispositivos lógicos aparezcan con un nombre distinto en su sistema.

▼ Para borrar un volumen RAID

1. **Compruebe qué unidad de disco duro corresponde a cada nombre de dispositivo lógico y físico.**

   Consulte "Números de ranura y nombres de dispositivo de los discos sin RAID" en la página 64.

2. **Determine el nombre del volumen RAID. Escriba el comando siguiente:**

```
# raidctl
RAID    Volume  RAID            RAID            Disk
Volume  Type    Status          Disk            Status
-----------------------------------------------------------
c0t0d0  IM      OK              c0t0d0          OK
                                c0t1d0          OK
```

   En este ejemplo, el volumen RAID es `c0t1d0`.

Nota – En función del número y el tipo de controladores de disco que se hayan instalado, es posible que los dispositivos lógicos aparezcan con un nombre distinto en su sistema.

---

3. **Para borrar el volumen, escriba el siguiente comando:**

```
# raidctl -d volumen-duplicado
```

Por ejemplo:

```
# raidctl -d c0t0d0
RAID Volume 'c0t0d0' deleted
```

Si el volumen RAID es del tipo IS, la supresión es interactiva, por ejemplo:

```
# raidctl -d c0t0d0
Deleting volume c0t0d0 will destroy all data it contains, proceed
(yes/no)? yes
Volume 'c0t0d0' deleted.
#
```

Si se borra un volumen IS, se pierden todos los datos que contiene. Como alternativa, puede usar la opción `-f` para forzar la supresión si sabe con certeza que no volverá a necesitar ni el volumen ni sus datos. Por ejemplo:

```
# raidctl -f -d c0t0d0
Volume 'c0t0d0' deleted.
#
```

4. **Para comprobar si se ha borrado la matriz RAID, escriba este comando:**

```
# raidctl
```

Por ejemplo:

```
# raidctl
No RAID volumes found
```

Para obtener más información, consulte la página del comando man de `raidctl`(1M).

▼ Para realizar una operación de conexión en marcha de un disco duplicado en espejo-

1. **Compruebe qué unidad de disco duro corresponde a cada nombre de dispositivo lógico y físico.**

   Consulte "Números de ranura y nombres de dispositivo de los discos sin RAID" en la página 64.

   Si el estado del disco es FAILED, significa que se puede extraer la unidad de disco e introducir una nueva. Una vez hecho, el nuevo disco debería presentar el estado OK y el volumen debería mostrar RESYNCING.

2. **Para comprobar si un disco ha fallado, escriba el comando siguiente:**

```
# raidctl
```

   Por ejemplo:

```
# raidctl
RAID    Volume  RAID            RAID            Disk
Volume  Type    Status          Disk            Status
-----------------------------------------------------------
c0t1d0  IM      DEGRADED        c0t1d0          OK
                                c0t2d0          FAILED
```

   En este ejemplo se indica que el duplicado está funcionando en modo degradado debido a un fallo del disco `c0t2d0`.

Nota – En función del número y el tipo de controladores de disco que se hayan instalado, es posible que los dispositivos lógicos aparezcan con un nombre distinto en su sistema.

---

3. **Extraiga la unidad de disco según se explica en el manual de servicio del servidor.**

   No hay necesidad de ejecutar ningún comando de software para poner la unidad fuera de servicio cuando ha fallado.

4. **Instale una unidad de disco nueva según se explica en el manual de servicio del servidor.**

   La utilidad de RAID restablece automáticamente los datos en el disco.

5. **Para comprobar el estado de un volumen RAID reconstruido, escriba el comando siguiente:**

```
# raidctl
```

Por ejemplo:

```
# raidctl
RAID    Volume  RAID            RAID            Disk
Volume  Type    Status          Disk            Status
-----------------------------------------------------------
c0t1d0  IM      RESYNCING       c0t1d0          OK
                                c0t2d0          OK
```

En este ejemplo se indica que el volumen RAID `c0t1d0` se está resincronizando.

Si vuelve a ejecutar el comando unos minutos después, indicará que el duplicado RAID ha terminado de resincronizarse y que vuelve a estar en servicio:

```
# raidctl
RAID    Volume  RAID            RAID            Disk
Volume  Type    Status          Disk            Status
-----------------------------------------------------------
c0t1d0  IM      OK              c0t1d0          OK
                                c0t2d0          OK
```

Para obtener más información, consulte la página del comando man de `raidctl`(1M).

▼ Para realizar una operación de sustitución en marcha de un disco no duplicado

1. **Compruebe qué unidad de disco duro corresponde a cada nombre de dispositivo lógico y físico.**

   Consulte "Números de ranura y nombres de dispositivo de los discos sin RAID" en la página 64.

   Asegúrese de que no haya ninguna aplicación o proceso accediendo al disco duro.

2. **Vea el estado de los dispositivos SCSI.**

   Para ello, escriba el comando siguiente:

```
# cfgadm -al
```

   Por ejemplo:

```
# cfgadm -al
Ap_Id           Type         Receptacle   Occupant      Condition
c0              scsi-bus     connected    configured    unknown
c0::dsk/c0t0d0  disk         connected    configured    unknown
c0::dsk/c0t1d0  disk         connected    configured    unknown
c0::dsk/c0t2d0  disk         connected    configured    unknown
c0::dsk/c0t3d0  disk         connected    configured    unknown
c1              scsi-bus     connected    configured    unknown
c1::dsk/c1t0d0  CD-ROM       connected    configured    unknown
usb0/1          unknown      empty        unconfigured  ok
usb0/2          unknown      empty        unconfigured  ok
usb1/1.1        unknown      empty        unconfigured  ok
usb1/1,2        unknown      empty        unconfigured  ok
usb1/1,3        unknown      empty        unconfigured  ok
usb1/1,4        unknown      empty        unconfigured  ok
usb1/2          unknown      empty        unconfigured  ok
#
```

Nota – En función del número y el tipo de controladores de disco que se hayan instalado, es posible que los dispositivos lógicos aparezcan con un nombre distinto en su sistema.

Las opciones `-al` presentan el estado de todos los dispositivos SCSI, incluidos los buses y los dispositivos USB. (En este ejemplo, no hay ningún dispositivo USB conectado al sistema.)

Observe que, aunque se pueden utilizar los comandos `cfgadm install_device` y `cfgadm remove_device` de Solaris para realizar el procedimiento de conexión de un disco duro en marcha, dichos comandos generan el siguiente mensaje de error cuando se ejecutan con un bus que contiene el disco del sistema:

```
# cfgadm -x remove_device c0::dsk/c0t1d0
Removing SCSI device: /devices/pci@1f,4000/scsi@3/sd@1,0
This operation will suspend activity on SCSI bus: c0
Continue (yes/no)? y
dev = /devices/pci@780/pci@0/pci@9/scsi@0/sd@1,0
cfgadm: Hardware specific failure: failed to suspend:
     Resource              Information
------------------  -------------------------
/dev/dsk/c0t0d0s0   mounted filesystem "/"
/dev/dsk/c0t0d0s6   mounted filesystem "/usr"
```

Esta advertencia se genera porque los citados comandos tratan de detener la actividad del bus SCSI (SAS), pero el firmware del servidor se lo impide. Se puede hacer caso omiso de este mensaje del servidor sin riesgo, pero el siguiente procedimiento evita que aparezca del todo.

3. **Suprima la unidad de disco del árbol de dispositivos.**

   Para hacerlo, escriba el siguiente comando:

```
# cfgadm -c unconfigure Id-punto-conexión
```

   Por ejemplo:

```
# cfgadm -c unconfigure c0::dsk/c0t3d0
```

   En este ejemplo, se suprime `c0t3d0` del árbol de dispositivos. El LED de extracción segura (azul) se enciende.

4. **Compruebe si el dispositivo se ha borrado del árbol de dispositivos.**

   Para ello, escriba el comando siguiente:

```
# cfgadm -al
Ap_Id           Type         Receptacle   Occupant      Condition
c0              scsi-bus     connected    configured    unknown
c0::dsk/c0t0d0  disk         connected    configured    unknown
c0::dsk/c0t1d0  disk         connected    configured    unknown
c0::dsk/c0t2d0  disk         connected    configured    unknown
c0::dsk/c0t3d0  unavailable  connected    configured    unknown
c1              scsi-bus     connected    unconfigured  unknown
c1::dsk/c1t0d0  CD-ROM       connected    configured    unknown
usb0/1          unknown      empty        unconfigured  ok
usb0/2          unknown      empty        unconfigured  ok
usb1/1.1        unknown      empty        unconfigured  ok
usb1/1,2        unknown      empty        unconfigured  ok
usb1/1,3        unknown      empty        unconfigured  ok
usb1/1,4        unknown      empty        unconfigured  ok
usb1/2          unknown      empty        unconfigured  ok
#
```

   Observe que, ahora, el dispositivo `c0t3d0` está `unavailable` (no disponible) y `unconfigured` (desconfigurado). El LED de extracción segura de la unidad de disco correspondiente se ilumina.

5. **Extraiga la unidad de disco según se explica en el manual de servicio del servidor.**

   El LED de extracción segura (azul) se apaga al extraer la unidad.

6. **Instale una unidad de disco nueva según se explica en el manual de servicio del servidor.**

7. **Configure la nueva unidad de disco.**

   Para ello, escriba el comando siguiente:

```
# cfgadm -c configure Id-punto-conexión
```

   Por ejemplo:

```
# cfgadm -c configure c1::dsk/c0t3d0
```

   El LED de actividad (verde) parpadea cuando el nuevo disco de `c1t3d0` se añade al árbol de dispositivos.

8. **Compruebe si la unidad de disco duro nueva se ha agregado al árbol de dispositivos.**
   Para ello, escriba el comando siguiente:

```
# cfgadm -al
Ap_Id           Type         Receptacle   Occupant      Condition
c0              scsi-bus     connected    configured    unknown
c0::dsk/c0t0d0  disk         connected    configured    unknown
c0::dsk/c0t1d0  disk         connected    configured    unknown
c0::dsk/c0t2d0  disk         connected    configured    unknown
c0::dsk/c0t3d0  disk         connected    configured    unknown
c1              scsi-bus     connected    configured    unknown
c1::dsk/c1t0d0  CD-ROM       connected    configured    unknown
usb0/1          unknown      empty        unconfigured  ok
usb0/2          unknown      empty        unconfigured  ok
usb1/1.1        unknown      empty        unconfigured  ok
usb1/1,2        unknown      empty        unconfigured  ok
usb1/1,3        unknown      empty        unconfigured  ok
usb1/1,4        unknown      empty        unconfigured  ok
usb1/2          unknown      empty        unconfigured  ok
#
```

   Ahora, el dispositivo `c0t3d0` aparece como configurado.

APÉNDICE **A**

Modo para aplicaciones del mecanismo de vigilancia

En este apéndice se proporciona información sobre el modo para aplicaciones del mecanismo de vigilancia del servidor. Está dividido en las siguientes secciones, que ayudan a configurar y utilizar el mecanismo de vigilancia y a programar la Alarma 3:

Nota – Una vez que el mecanismo de vigilancia para aplicaciones entra en funcionamiento, es necesario reiniciar el entorno operativo Solaris para que vuelva al temporizador predeterminado (no programable) y al comportamiento predeterminado de los indicadores LED (sin la Alarma 3).

Descripción del modo para aplicaciones del mecanismo de vigilancia

El mecanismo de vigilancia detecta el bloqueo del sistema, además del bloqueo y fallo de las aplicaciones, en el caso de que ocurran. Consiste en un temporizador que se reinicia continuamente por las aplicaciones del usuario, siempre que el entorno operativo y las aplicaciones se estén ejecutando.

Cuando una aplicación está rearmando el mecanismo de vigilancia, puede ocurrir una caducidad por lo siguiente:

- Fallo de la aplicación que rearma el mecanismo de vigilancia.
- Bloqueo o fallo del subproceso de rearmado en la aplicación.
- Bloqueo del sistema.

Cuando se está ejecutando el mecanismo de vigilancia del sistema, la caducidad se produce si el sistema se bloquea, o específicamente, si se bloquea el gestor de interrupciones del reloj.

El mecanismo de vigilancia del sistema es el modo predeterminado. Si no se inicia el mecanismo de vigilancia de las aplicaciones, se utiliza el modo del sistema.

El modo para aplicaciones permite lo siguiente:

- Configurar el mecanismo de vigilancia: se puede configurar y utilizar en las aplicaciones que se ejecutan en el host para detectar los problemas graves y hacer que las aplicaciones se recuperen automáticamente.
- Programar la Alarma 3: para generar esta alarma en el caso de ocurrir problemas críticos en las aplicaciones.

El comando `setupsc` de ALOM puede utilizarse para configurar *sólo* la recuperación del mecanismo de vigilancia del sistema:

```
sc> setupsc
```

La configuración del controlador del sistema debe ser la siguiente:

```
SC POST diag Level [off]:
Host Watchdog [enabled]:
Rocker Switch [enabled]:
Secure Mode [off]:

PROC RTUs installed: 0
PROC Headroom quantity (0 to disable, 4 MAX) [0]:
```

La configuración de recuperación del mecanismo de vigilancia para las aplicaciones se realiza con los códigos de control de E/S (IOCTL) que se envían al controlador `ntwdt`.

Limitaciones del mecanismo de vigilancia

Las limitaciones del modo del mecanismo de vigilancia incluyen:

- Cuando el controlador del sistema detecta la caducidad del mecanismo de vigilancia, intenta recuperar el dominio una sola vez; no habrá más intentos si falla esta primera recuperación.
- Si el mecanismo de vigilancia para aplicaciones está activado y accede a OpenBoot PROM ejecutando el comando `break>` desde el indicador `sc` del controlador del sistema, el temporizador del mecanismo de vigilancia se desactiva automáticamente.

Nota – Aparece un mensaje en la consola para recordarle que el mecanismo de vigilancia, para el controlador del sistema, se ha desactivado.

  Sin embargo, al acceder otra vez al entorno operativo Solaris, el mecanismo de vigilancia seguirá activado según lo detecta el entorno operativo. Para que el controlador del sistema y el entorno operativo Solaris detecten el mismo estado, es necesario que active o desactive el mecanismo de vigilancia en el modo para aplicaciones.

- Si efectúa una operación de reconfiguración dinámica (DR) en que se elimina una tarjeta del sistema que contiene memoria permanente (memoria de kernel), tendrá que desactivar el modo para aplicaciones del mecanismo de vigilancia antes de empezar la reconfiguración dinámica, y volver a activarlo una vez terminada. Esto es necesario porque el software de Solaris pasa a un estado quiescente todas las E/S del sistema y desactiva todas las interrupciones durante la eliminación de memoria permanente. Como resultado, el firmware del controlador del sistema y el software de Solaris no se comunican durante la operación de reconfiguración dinámica. Tenga en cuenta que esta limitación no afecta a la adición dinámica de memoria, ni a la eliminación de tarjetas que no contengan memoria permanente. En estos casos, el modo para aplicaciones del mecanismo de vigilancia puede ejecutarse a la vez que la operación de reconfiguración dinámica.

  Puede ejecutar el siguiente comando para buscar las tarjetas del sistema que contienen memoria permanente (memoria de kernel):

  ```
  sc> cfgadm -lav | grep -i permanent
  ```

- Si el entorno operativo Solaris se bloquea en las condiciones siguientes, el firmware del controlador del sistema no puede detectar el bloqueo del software de Solaris:
  - El modo para aplicaciones del mecanismo de vigilancia está activado.
  - El mecanismo de vigilancia no está activado.
  - El usuario no rearma el mecanismo de vigilancia.

- El mecanismo de vigilancia proporciona un control parcial del inicio. Además, el mecanismo de vigilancia para aplicaciones sirve para controlar el reinicio del dominio.

  Sin embargo, no controla el reinicio del dominio en estos casos:

  - Después de una operación de encendido en frío.
  - Recuperación de un dominio bloqueado o con fallo.

  En el caso de recuperación de un dominio bloqueado o con error, el error del arranque no se detecta y no se efectúan intentos de recuperación.
- El modo para aplicaciones del mecanismo de vigilancia no controla el inicio de las aplicaciones. Con este modo activado, si una aplicación falla y no se inicia, no se detecta el error y no se intenta su recuperación.

Utilización del controlador `ntwdt`

Para utilizar esta nueva función del mecanismo de vigilancia para aplicaciones, es necesario instalar el controlador `ntwdt`. Para activar y controlar el modo para aplicaciones del mecanismo de vigilancia, también es necesario programar el mecanismo de vigilancia del sistema utilizando los códigos de control IOCTL `LOMIOCDOG`*xxx*, explicados en "Descripción de la API de usuario" en la página 87.

Si el controlador `ntwdt`, en vez del controlador del sistema, reinicia el entorno operativo Solaris después de una caducidad del mecanismo de vigilancia, se utiliza el valor de la propiedad siguiente del archivo de configuración del controlador `ntwdt` (`ntwdt.conf`):

```
ntwdt-boottimeout="600";
```

En caso de aviso grave o caducidad del mecanismo de vigilancia, el controlador `ntwdt` reprograma el tiempo de espera del mecanismo de vigilancia en el valor indicado en esta propiedad.

Asigne un valor que represente un intervalo de tiempo mayor que el necesario para reiniciar y efectuar un volcado de bloqueo del sistema. Si el valor especificado no es lo bastante amplio, el controlador del sistema reinicia el host cuando el reinicio está activado. Tenga en cuenta que el reinicio del controlador del sistema ocurre sólo una vez.

Descripción de la API de usuario

El controlador `ntwdt` proporciona una interfaz de programación de aplicaciones utilizando los códigos de control IOCTL. Es necesario abrir el nodo del dispositivo `/dev/ntwdt` antes de enviar los códigos de control para el mecanismo de vigilancia.

Nota – Está permitida una sola instancia de `open()` en `/dev/ntwdt`. Más de una instancia de `open()` generará el siguiente mensaje de error: `EAGAIN - The driver is busy, try again`.

Puede utilizar los siguientes códigos IOCTL con el mecanismo de vigilancia:

- `LOMIOCDOGTIME`
- `LOMIOCDOGCTL`
- `LOMIOCDOGPAT`
- `LOMIOCDOGSTATE`
- `LOMIOCALCTL`
- `LOMIOCALSTATE`

Uso del mecanismo de vigilancia

Configuración del periodo de tiempo de espera

El código de control `LOMIOCDOGTIME` establece el periodo de tiempo de espera del mecanismo de vigilancia. Este código programa el hardware del mecanismo de vigilancia con el periodo de tiempo especificado. Es necesario establecer el periodo de tiempo de espera (`LOMIOCDOGTIME`) antes de activar el temporizador del mecanismo de vigilancia (`LOMIOCDOGCTL`).

El argumento es un apuntador de un número entero sin signo. Este número entero mantiene el tiempo de espera del mecanismo de vigilancia en múltiplos de 1 segundo. Se puede especificar un periodo de tiempo de espera entre 1 segundo y 180 minutos.

Si la función del mecanismo de vigilancia está activada, el tiempo de espera se reinicia de inmediato y surte efecto el nuevo valor. Se muestra un error (EINVAL) cuando el periodo de tiempo de espera es inferior a 1 segundo o superior a 180 minutos.

Nota – El código `LOMIOCDOGTIME` no es para uso general. Si se configura el tiempo de espera del mecanismo de vigilancia en un valor demasiado bajo, el sistema puede recibir un reinicio del hardware cuando las funciones de reinicio y del mecanismo de vigilancia están activadas. Si el tiempo de espera es muy corto, la aplicación del usuario se debe ejecutar con una prioridad más alta (por ejemplo, como un subproceso en tiempo real) y se tiene que rearmar con mayor frecuencia para evitar una caducidad no prevista.

Activación o desactivación del mecanismo de vigilancia

El código de control `LOMIOCDOGCTL` activa o desactiva el mecanismo de vigilancia, además de activar o desactivar la función de reinicio. Consulte "Búsqueda y definición de estructuras de datos" en la página 89 para obtener los valores correctos del temporizador del mecanismo de vigilancia.

El argumento es un apuntador a la estructura `lom_dogctl_t`. Esta estructura se describe detalladamente en "Búsqueda y definición de estructuras de datos" en la página 89.

Utilice el miembro `reset_enable` para activar o desactivar la función de reinicio del sistema. Utilice el miembro `dog_enable` para activar o desactivar la función del mecanismo de vigilancia. Se muestra un error (EINVAL) si el mecanismo de vigilancia está desactivado, pero la función de reinicio está activada.

Nota – Si no se ejecuta `LOMIOCDOGTIME` para configurar el tiempo de espera antes de este código de control, el mecanismo de vigilancia *no* estará activado en el hardware.

Rearmado del mecanismo de vigilancia

El código de control `LOMIOCDOGPAT` rearma el mecanismo de vigilancia para que el temporizador empiece a contar desde el principio, es decir, desde el valor especificado con el código `LOMIOCDOGTIME`. Este código no requiere argumentos. Cuando el mecanismo de vigilancia está activado, este código debe funcionar a intervalos regulares más cortos que el tiempo de espera del mecanismo de vigilancia, o de lo contrario, caducará.

Obtención del estado del mecanismo de vigilancia

El código de control `LOMIOCDOGSTATE` obtiene el estado del mecanismo de vigilancia y de la función de reinicio, además de recuperar el periodo de tiempo de espera. Si no se ejecutó `LOMIOCDOGSTATE` para configurar el tiempo de espera antes de este código de control, el mecanismo de vigilancia no estará activado en el hardware.

El argumento es un apuntador a la estructura `lom_dogstate_t`, que se describe detalladamente en "Búsqueda y definición de estructuras de datos" en la página 89. Los miembros de la estructura se utilizan para mantener el estado actual de los circuitos de reinicio, y el periodo de tiempo de espera, del mecanismo de vigilancia. No se trata del periodo de tiempo restante antes de que se active el mecanismo de vigilancia.

El código `LOMIOCDOGSTATE` únicamente requiere que se invoque `open()` con éxito. Este código de control se puede ejecutar las veces que sea necesario una vez que se haya invocado `open()` y no requiere que se ejecuten previamente otros códigos `DOG`.

Búsqueda y definición de estructuras de datos

Todas las estructuras de datos y los códigos de control IOCTL están definidos en `lom_io.h`, disponible en el paquete `SUNWlomu`.

Las estructuras de datos para el temporizador del mecanismo de vigilancia son las siguientes:

- La estructura de datos del estado del mecanismo de vigilancia y reinicio:

CÓDIGO EJEMPLO A-1 Estructura de datos de estado del mecanismo de vigilancia y reinicio

```
typedef struct {
        int reset_enable; /* reset enabled if non-zero */
        int dog_enable; /* watchdog enabled if non-zero */
        uint_t dog_timeout; /* Current watchdog timeout */
} lom_dogstate_t;
```

- La estructura de datos del control del mecanismo de vigilancia y reinicio:

CÓDIGO EJEMPLO A-2 Estructura de datos de control del mecanismo de vigilancia y reinicio

```
typedef struct {
        int reset_enable; /* reset enabled if non-zero */
        int dog_enable; /* watchdog enabled if non-zero */
} lom_dogctl_t;
```

Programa de ejemplo del mecanismo de vigilancia

El siguiente ejemplo es un programa para el temporizador del mecanismo de vigilancia.

CÓDIGO EJEMPLO A-3 Programa de ejemplo del mecanismo de vigilancia

```
#include <sys/types.h>
#include <fcntl.h>
#include  <unistd.h>
#include  <sys/stat.h>
#include <lom_io.h>

int main() {
    uint_t timeout = 30; /* 30 seconds */
    lom_dogctl_t dogctl;
    int fd;

    dogctl.reset_enable = 1;
    dogctl.dog_enable = 1;

    fd = open("/dev/ntwdt", O_EXCL);

    /* Set timeout */
    ioctl(fd, LOMIOCDOGTIME, (void *)&timeout);

    /* Enable watchdog */
    ioctl(fd, LOMIOCDOGCTL, (void *)&dogctl);

    /* Keep patting */
    while (1) {
       ioctl(fd, LOMIOCDOGPAT, NULL);
       sleep (5);
    }
    return (0);
}
```

Programación de la Alarma 3

La Alarma 3 se encuentra disponible en el entorno operativo Solaris, con independencia del modo en que se utilice el mecanismo de vigilancia. La Alarma 3 (encendido y apagado de la alarma del sistema) ha sido redefinida (consulte la TABLA A-1).

Configure el valor de la Alarma 3 utilizando el código de control `LOMIOCALCTL`. La Alarma 3 se programa con el mismo método que sirve para establecer y cancelar las alarmas 1 y 2.

En la siguiente tabla se muestra el comportamiento de la Alarma 3:

TABLA A-1 Comportamiento de la Alarma 3

	Alarma 3	**Relé**	**LED del sistema (verde)**
Apagado del sistema	Encendido	COM -> NC	Apagado
Encendido del sistema/LOM	Encendido	COM -> NC	Apagado
Solaris ejecutándose	Apagado	COM -> NO	Encendido
Solaris no ejecutándose	Encendido	COM -> NC	Apagado
Caducidad WDT del host	Encendido	COM -> NC	Apagado
Encendida por usuario	Encendido	COM -> NC	Apagado
Apagada por usuario	Apagado	COM -> NO	Encendido

donde:

- COM es la línea común
- NC significa normalmente cerrado
- NO significa normalmente abierto

Resumen de los datos de la tabla:

- Alarma3 encendida = Transmisión(COM->NC), LED del sistema apagado
- Alarma3 apagada = Transmisión(COM->NO), LED del sistema encendido

Cuando la Alarma 3 (o alarma del sistema) está programada, puede comprobarla utilizando el comando `showalarm` y el argumento `system`.

Por ejemplo:

```
sc> showalarm system
system alarm is on
```

La estructura de datos utilizada en los códigos de control LOMIOCALCTL y LOMIOCALSTATE es la siguiente:

CÓDIGO EJEMPLO A-4 Estructura de datos de los códigos de control LOMIOCALCTL y LOMIOCALSTATE

```
#include <fcntl.h>
#include <lom_io.h>

#define LOM_DEVICE  "/dev/lom"
#define ALARM_OFF 0
#define ALARM_ON 1

int main() {
    int fd, ret;
    lom_aldata_t ald;
    ald.alarm_no = ALARM_NUM_3;
     ald.state = ALARM_OFF;

     fd = open(LOM_DEVICE, O_RDWR);
     if (fd == -1) {
     printf("Error opening device: %s\n", LOM_DEVICE);
       return (1);
    }

    /* Set Alarm3 to on state */
    ald.state = ALARM_ON;
     ioctl(fd, LOMIOCALCTL, (void *)&ald);

     /* Get Alarm3 state */
    ioctl(fd, LOMIOCALSTATE, (char *)&ald);
     printf("alarm %d state :%d:\n", ald.alarm_no, ald.state);

     /* Set Alarm3 to off state */
     ald.state = ALARM_OFF;
    ioctl(fd, LOMIOCALCTL, (char *)&ald);

     /* Get Alarm3 state */
    ioctl(fd, LOMIOCALSTATE, (char *)&ald);
    printf("alarm %d state :%d:\n", ald.alarm_no, ald.state);

    close (fd);
    return (0);
}
```

Mensajes de error del mecanismo de vigilancia

La TABLA A-2 describe los mensajes de error que pueden aparecer y su significado.

TABLA A-2 Mensajes de error del mecanismo de vigilancia

Mensaje	Significado
EAGAIN	Se ha intentado abrir más de una instancia de `open()` en `/dev/ntwdt`.
EFAULT	Se ha especificado una dirección de espacio de usuario no válida.
EINVAL	Se ha solicitado un comando de control que no existe o se han introducido parámetros no válidos.
EINTR	Se ha interrumpido un proceso que esperaba el cambio de estado de un componente.
ENXIO	El controlador no está instalado en el sistema.

APÉNDICE **B**

Interfaz de programación de aplicaciones (API) de salida de relés de alarma

En este apéndice se incluye un programa de ejemplo que ilustra cómo efectuar las operaciones de `get` (obtener) o `set` (establecer) en el estado de las alarmas. La aplicación puede utilizar `LOMIOCALSTATE ioctl` para obtener el estado de cada alarma y `LOMIOCALCTL ioctl` para establecer el valor de cada una de ellas individualmente. Para obtener más información sobre los indicadores de alarma, consulte "Indicadores de estado de alarma" en la página 38.

CÓDIGO EJEMPLO B-1 Programa de ejemplo para efectuar `get` y `set` en el estado de las alarmas

```
#include <sys/types.h>
#include <string.h>
#include <stdlib.h>
#include <sys/unistd.h>
#include <fcntl.h>
#include "lom_io.h"

#define ALARM_INVALID   -1
#define LOM_DEVICE  "/dev/lom"

static void usage();
static void get_alarm(const char *alarm);
static int set_alarm(const char *alarm, const char *alarmval);
static int parse_alarm(const char *alarm);
static int lom_ioctl(int ioc, char *buf);
static char *get_alarmval(int state);
static void get_alarmvals();


main(int argc, char *argv[])
{
```

CÓDIGO EJEMPLO B-1 Programa de ejemplo para efectuar `get` y `set` en el estado de las alarmas *(continuación)*

```
        if (argc < 3) {
                usage();
                if (argc == 1)
                        get_alarmvals();
                exit(1);
        }

        if (strcmp(argv[1], "get") == 0) {
                if (argc != 3) {
                        usage();
                        exit(1);
                }
                        get_alarm(argv[2]);
        }
        else
        if (strcmp(argv[1], "set") == 0) {
                if (argc != 4) {
                        usage();
                        exit(1);
                }
                set_alarm(argv[2], argv[3]);
        } else {
                usage();
                exit(1);
        }
}

static void
usage()
{
        printf("usage: alarm [get|set] [crit|major|minor|user] [on|off]\n");
}

static void
get_alarm(const char *alarm)
{
        ts_aldata_t     ald;
        int altype = parse_alarm(alarm);
        char *val;

        if (altype  == ALARM_INVALID) {
                usage();
                exit(1);
        }

        ald.alarm_no = altype;
```

CÓDIGO EJEMPLO B-1 Programa de ejemplo para efectuar `get` y `set` en el estado de las alarmas *(continuación)*

```
        ald.alarm_state = ALARM_OFF;

        lom_ioctl(LOMIOCALSTATE, (char *)&ald);

        if ((ald.alarm_state != ALARM_OFF) &&
                        (ald.alarm_state != ALARM_ON)) {
                printf("Invalid value returned: %d\n", ald.alarm_state);
                exit(1);
        }

        printf("ALARM.%s = %s\n", alarm, get_alarmval(ald.alarm_state));
}

static int
set_alarm(const char *alarm, const char *alarmstate)
{
        ts_aldata_t     ald;
        int alarmval = ALARM_OFF, altype = parse_alarm(alarm);

        if (altype  == ALARM_INVALID) {
                usage();
                exit(1);
        }

        if (strcmp(alarmstate, "on") == 0)
                alarmval = ALARM_ON;
        else
        if (strcmp(alarmstate, "off") == 0)
                alarmval = ALARM_OFF;
        else {
                usage();
                exit(1);
        }

        ald.alarm_no = altype;
        ald.alarm_state = alarmval;

        if (lom_ioctl(LOMIOCALCTL, (char *)&ald) != 0) {
                printf("Setting ALARM.%s to %s failed\n", alarm, alarmstate);
                return (1);
        } else {
                printf("Setting ALARM.%s successfully set to %s\n", alarm,
alarmstate);
                return (1);
        }
}
```

CÓDIGO EJEMPLO B-1 Programa de ejemplo para efectuar `get` y `set` en el estado de las alarmas *(continuación)*

```
static int
parse_alarm(const char *alarm)
{
        int altype;

        if (strcmp(alarm, "crit") == 0)
                altype = ALARM_CRITICAL;
        else
        if (strcmp(alarm, "major") == 0)
                altype = ALARM_MAJOR;
        else
        if (strcmp(alarm, "minor") == 0)
                altype = ALARM_MINOR;
        else
        if (strcmp(alarm, "user") == 0)
                altype = ALARM_USER;
        else {
                printf("invalid alarm value: %s\n", alarm);
                altype = ALARM_INVALID;
        }

        return (altype);

}

static int
lom_ioctl(int ioc, char *buf)
{
        int fd, ret;

        fd = open(LOM_DEVICE, O_RDWR);

        if (fd == -1) {
                printf("Error opening device: %s\n", LOM_DEVICE);
                exit(1);
        }

        ret = ioctl(fd, ioc, (void *)buf);

        close (fd);

        return (ret);
}

static char *
get_alarmval(int state)
{
```

CÓDIGO EJEMPLO B-1 Programa de ejemplo para efectuar `get` y `set` en el estado de las alarmas *(continuación)*

```
        if (state == ALARM_OFF)
                return ("off");
        else
        if (state == ALARM_ON)
                return ("on");
        else
                return (NULL);
}
static void
get_alarmvals()
{
        get_alarm("crit");
        get_alarm("major");
        get_alarm("minor");
        get_alarm("user");
}
```

Índice

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U