Resolución de problemas de administración del sistema en Oracle® Solaris 11.2

Referencia: E53850-02
Septiembre de 2014

ORACLE®

Contenido

Uso de esta documentación

- **Descripción general**: describe los temas de Resolución de problemas en plataformas SPARC y x86.
- **Destinatarios**: administradores del sistema que usan la versión 11 de Oracle Solaris.
- **Conocimientos necesarios**: experiencia en la administración de sistemas UNIX.

Biblioteca de documentación del producto

En la biblioteca de documentación (http://www.oracle.com/pls/topic/lookup?ctx=E56339), se incluye información de última hora y problemas conocidos para este producto.

Acceso a My Oracle Support

Los clientes de Oracle tienen acceso a soporte electrónico por medio de My Oracle Support. Para obtener más información, visite http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info o, si tiene alguna discapacidad auditiva, visite http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs.

Comentarios

Envíenos comentarios acerca de esta documentación mediante http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CAPÍTULO 1

Resolución de problemas de caídas del sistema

En este capítulo, se describe cómo prepararse para una caída del sistema y cómo resolver caídas del sistema en el sistema operativo Oracle Solaris.

En este capítulo se abordan los siguientes temas:

Novedades en archivos de volcado por caída en Oracle Solaris 11.2

En esta sección, se describen los cambios para gestionar archivos de volcado por caída en esta versión de Oracle Solaris.

Los archivos de volcado por caída se reestructuran

En esta versión, los archivos de volcado por caída del núcleo se dividen en varios nuevos archivos según su contenido para realizar análisis iniciales de forma más rápida y activar mayor granularidad en la configuración. Para obtener información, consulte "Archivos reestructurados" [9].

Los archivos de volcado por caída se guardan en el directorio `/var/crash`

En el sistema operativo Oracle Solaris 11, los archivos de volcado por caída se guardan en el directorio `/var/crash`. Este cambio se presentó originalmente en la versión de Oracle Solaris 10 1/13 y se incluye en todas las versiones de Oracle Solaris 11.

Acerca de las caídas del sistema

Las caídas del sistema pueden producirse debido a errores de software, problemas de E/S y mal funcionamiento del hardware. Si se produce una caída del sistema, se mostrará un mensaje de error en la consola y, a continuación, se escribirá una copia de la memoria física correspondiente en el dispositivo de volcado. El sistema se reiniciará automáticamente. Cuando se reinicia el sistema, se ejecuta el comando `savecore` para recuperar los datos del dispositivo de volcado y escribir en el directorio `savecore` los archivos de volcado por caída guardados. Estos archivos guardados proporcionan información muy valiosa para ayudar a diagnosticar el problema.

Nota - El término *volcado por caída* hace referencia al resultado general de este proceso, que incluye el conjunto de archivos de volcado por caída, dónde se encuentran, y cómo estos archivos se organizan y se formatean.

Archivos de volcado por caída del sistema

El comando `savecore`se ejecuta automáticamente después de una caída del sistema para recuperar la información del volcado por caída del dispositivo de volcado y escribe la información en un conjunto de archivos. Posteriormente, el comando `savecore` se puede invocar en el mismo sistema o en un sistema distinto para ampliar los archivos comprimidos de volcado por caída.

Nota - En ocasiones, los archivos de volcado por caída pueden confundirse con los archivos *core*, que son imágenes de aplicaciones de usuario que se escriben cuando la aplicación finaliza de modo anormal.

Los archivos de volcado por caída se guardan en un directorio predefinido, el directorio predeterminado es `/var/crash/`. En versiones anteriores, los archivos de volcado por caída se

sobrescribían después del reinicio del sistema, a menos que activara manualmente el sistema para que guarde las imágenes de la memoria física en un archivo de volcado por caída. Ahora, el guardado de archivos de volcado por caída está activado de manera predeterminada.

Archivos reestructurados

En la versión Oracle Solaris 11.2, se han reestructurado los archivos de volcado por caída del núcleo. El contenido de estos archivos se divide en varios nuevos archivos según su contenido para realizar análisis iniciales de forma más rápida y activar mayor granularidad en la configuración. Se acceder a los archivos y estudiarlos con mayor facilidad.

Los volcados por caída del núcleo se almacenaban anteriormente en los archivos siguientes:

- `vmdump.N`
- `unix.N`
- `vmcore.N`

Los datos y metadatos de las páginas de núcleo almacenadas en `vmdump.N` y `vmcore.N` en formato comprimido y descomprimido, respectivamente.

A partir de la versión Oracle Solaris 11.2, la información sobre el volcado por caída se escribe en el conjunto de archivos `vmdump-`*`section`*`.`*`n`*. El valor de section es el nombre de una sección del archivo que contiene un tipo específico de información de volcado. El valor *n* es un número entero que aumenta cada vez que se ejecuta `savecore`para copiar un volcado por caída y cada vez que se encuentra un nuevo volcado por caída en el dispositivo de volcado. Entre los posibles archivos se incluyen:

`vmdump-proc.N`	Archivo de volcado con páginas de proceso comprimido
`vmdump-zfs.N`	Archivo de volcado con metadatos ZFS comprimidos
`vmdump-other.N`	Archivo de volcado con otras páginas

Para obtener más información, consulte las páginas del comando man `dumpadm`(1M) y `savecore`(1M).

Los comandos `dumpadm` y `savecore`

Las utilidades dumpadm y savecore, configuran y gestionan la creación de un volcado por caída de la siguiente manera:

Durante el inicio del sistema, se invoca el comando `dumpadm` mediante el servicio `svc:/system/dumpadm:default` a fin de configurar los parámetros de volcado por caída. Inicializa el dispositivo de volcado y el contenido del volcado mediante la interfaz `/dev/dump`.

Nota - En la versión Oracle Solaris 11.2, el comando dumpadm tiene nuevas opciones para especificar el contenido de volcado, imprimir cálculos de espacio en disco y producir resultados analizables. Consulte “Modificación de la configuración de volcados por caída” [12].

Cuando se completa la configuración del volcado, la secuencia de comandos `savecore` busca la ubicación del directorio del archivo de volcado por caída. Luego, se invoca `savecore` para comprobar si existen volcados por caída y para comprobar el contenido del archivo `minfree` en el directorio de volcado por caída. Los archivos de volcado por caída del sistema, generados por el comando `savecore`, se guardan de manera predeterminada.

Los datos del volcado se almacenan en un formato comprimido en el dispositivo de volcado. Las imágenes de volcado por caída del núcleo pueden ocupar 4 Gbytes o más. La compresión de los datos representa un volcado más rápido y una menor cantidad de espacio en el disco requerida para el dispositivo de volcado.

Cuando un dispositivo de volcado dedicado, no el área de swap, es parte de la configuración de volcado, el guardado de archivos de volcado por caída se ejecuta en segundo plano. Si un sistema se está iniciando, no espera a que se complete el comando `savecore` para pasar al siguiente paso. En los sistemas con memorias de gran tamaño, el sistema puede estar disponible antes de que finalice `savecore`.

El comando `savecore -L` permite a un administrador obtener un volcado por caída de un sistema operativo Oracle Solaris en ejecución. Este comando está diseñado para resolver los problemas de un sistema en ejecución mediante la toma de una instantánea de la memoria durante un estado erróneo, como un problema de rendimiento temporal o cuando se interrumpe el servicio. Si el sistema está activo y todavía puede ejecutar algunos comandos, puede ejecutar el comando `savecore -L` para guardar una instantánea del sistema en el dispositivo de volcado e inmediatamente escribir los archivos de volcado por caída en el directorio `savecore`. Debido a que el sistema aún está en ejecución, sólo puede utilizar el comando `savecore -L` si ha configurado un dispositivo de volcado dedicado.

Para obtener más información, consulte “Modificación de la configuración de volcados por caída” [12], `dumpadm`(1M) y las páginas del comando man `savecore`(1M).

Configuración del sistema para volcados por caída

En esta sección, se describen las tareas para gestionar los procedimientos de volcado por caída para su sistema.

Tenga en cuenta los siguientes puntos cuando trabaje con información sobre la caída del sistema:

- Debe asumir el rol `root` para acceder y gestionar información sobre caídas del sistema. Consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".
- No desactive la opción de guardado de archivos de volcado por caída del sistema en el sistema. Los archivos de volcado por caída del sistema proporcionan una manera muy útil de determinar los motivos de la caída del sistema.
- Los volúmenes ZFS dedicados se utilizan para las áreas de intercambio y volcado. Después de una instalación, es posible que necesite ajustar el tamaño de los dispositivos de intercambio y volcado o que posiblemente deba volver a crear los volúmenes de intercambio y volcado. Para obtener instrucciones, consulte "Gestión de los dispositivos de intercambio y volcado ZFS" de "Gestión de sistemas de archivos ZFS en Oracle Solaris 11.2 ".

Para personalizar los procesos de volcado por caída del sistema antes de se produzca una caída del sistema, consulte lo siguiente:

- "Visualización de la configuración de volcado por caída actual" [11]
- "Modificación de la configuración de volcados por caída" [12]
- "Desactivación o activación de guardado de volcados por caída" [14]

Visualización de la configuración de volcado por caída actual

Para mostrar la configuración actual de volcado por caída, asuma el rol root y ejecute el comando `dumpadm` sin argumentos.

```
# dumpadm
 Dump content: kernel pages
       Dump device: /dev/zvol/dsk/rpool/dump (dedicated)
Savecore directory: /var/crash
  Savecore enabled: yes
   Save compressed: on
```

Este ejemplo de salida muestra la siguiente configuración:

- El contenido del volcado incluye las páginas de la memoria del núcleo.
- La memoria del núcleo se vuelca en un dispositivo de volcado dedicado, `/dev/zvol/dsk/rpool/dump`.
- Los archivos de volcado por caída del sistema se guardan en el directorio `/var/crash`.
- El guardado de archivos de volcado por caída está activado.
- Los volcados por caída se deben guardar en formato comprimido.

Modificación de la configuración de volcados por caída

Para modificar la configuración de volcado por caída, asuma el rol root y use el comando `dumpadm`.

La sintaxis del comando `dumpadm` es la siguiente:

```
#  /usr/sbin/dumpadm [-nuy] [-c content-type] [-d dump-device] [-m mink | minm | min%]
[-s savecore-dir] [-r root-dir] [-z on | off]
```

-c *content-type*
: Especifica el tipo de datos que componen el volcado. Han cambiado los valores de esta opción para la versión Oracle Solaris 11.2. Use `kernel` para volcar únicamente la páginas de la memoria del núcleo, `all` para volcar todas las páginas de la memoria, `curproc` para volcar la memoria del núcleo y las páginas de la memoria del proceso cuyo subproceso estaba en ejecución cuando se produjo la caída, `allproc` para volcar todas las páginas de la memoria del núcleo y todas las páginas del proceso o `zfs` para volcar todas las páginas del núcleo que almacenan metadatos de ZFS. El contenido predeterminado del volcado incluye la memoria del núcleo.

  Consulte los siguientes ejemplos de la opción -c:

  ```
  # dumpadm -c kernel
  # dumpadm -c +zfs
  # dumpadm -c -zfs
  # dumpadm -c curproc+zfs
  ```

-d *dump-device*
: Especifica el dispositivo que almacena los datos de volcado temporalmente cuando cae el sistema. El dispositivo de volcado principal es el dispositivo de volcado predeterminado. Si el dispositivo de volcado no es el área de intercambio, `savecore` se ejecuta en segundo plano, lo que agiliza el proceso de inicio.

-e
: Imprime el cálculo de espacio en disco necesario para almacenar el volcado por caída comprimido. El valor se calcula mediante la configuración actual y mediante el sistema actualmente en ejecución.

-m *min*k | *min*m | *min*%
: Especifica el espacio libre mínimo que debe estar disponible en el disco para el guardado de archivos de volcado por caída mediante la creación de un archivo `minfree` en el directorio `savecore` actual. Este parámetro se puede especificar en Kbytes (`mink`), Mbytes (`minm`) o en porcentaje de tamaño del sistema de archivos (`min%`). Si no se configuró un espacio libre mínimo, el valor predeterminado es 1 Mbyte.

El comando `savecore` consulta este archivo antes de escribir los archivos de volcado por caída. Si la escritura de los archivos de volcado por caída redujera la cantidad de espacio libre por debajo del umbral `minfree` debido al tamaño, no se escribirán los archivos de volcado y se registrará un mensaje de error. Para obtener información sobre la recuperación en esta situación, consulte "Guardado de datos cuando el directorio de volcado por caída está completo" [19].

`-n` — Especifica que no debe ejecutarse `savecore` cuando se reinicia el sistema. No se recomienda esta configuración de volcado. Si la información sobre la caída del sistema se escribe en el dispositivo de swap y `savecore` no está activado, se sobrescribe la información sobre el volcado por caída cuando el sistema comienza el swap.

`-p` — Produce resultados que la máquina puede analizar.

`-s` *savecore-dir* — Especifica un directorio alternativo para almacenar archivos de volcado por caída. En Oracle Solaris 11, en el directorio por defecto es `/var/crash`.

`-u` — Realiza la actualización forzosa de la configuración de volcado del núcleo en función del contenido del archivo `/etc/dumpadm.conf`.

`-y` — Modifica la configuración de volcado para que, al reiniciarse el sistema, se ejecute automáticamente el comando `savecore`, que es el valor predeterminado de esta configuración de volcado.

`-z on` | `off` — Modifica la configuración de volcado para controlar el funcionamiento del comando `savecore` al reiniciarse el sistema. La configuración `on` permite el guardado del archivo del núcleo central en un formato comprimido. La configuración `off` descomprime automáticamente el archivo de volcado por caída. Debido a que los archivos de volcado por caída pueden ser de gran tamaño y, por lo tanto, si se guardaran en un formato comprimido, se necesitaría menos espacio en el sistema de archivos, la configuración predeterminada es `on`.

EJEMPLO 1-1 Modificación de una configuración de volcado por caída

En este ejemplo, se realiza el volcado de toda la memoria en el dispositivo de volcado dedicado, `/dev/zvol/dsk/rpool/dump`, y el espacio libre mínimo que debe estar disponible después de guardar los archivos de volcado por caída corresponde al 10% del espacio del sistema de archivos.

```
# dumpadm
      Dump content: kernel pages
       Dump device: /dev/zvol/dsk/rpool/dump (dedicated)
```

```
Savecore directory: /var/crash
  Savecore enabled: yes
   Save compressed: on

# dumpadm -c all -d /dev/zvol/dsk/rpool/dump -m 10%
       Dump content: all pages
       Dump device: /dev/zvol/dsk/rpool/dump (dedicated)
Savecore directory: /var/crash (minfree = 5697105KB)
  Savecore enabled: yes
   Save compressed: on
```

Desactivación o activación de guardado de volcados por caída

Atención - Oracle Solaris recomienda no desactivar el guardado de volcados por caída. Los volcados por caída proporcionan una manera muy útil para determinar qué provoca la caída del sistema.

Con el rol root, tiene la capacidad para activar o desactivar el guardado de volcados de por caída:

```
# dumpadm -n | -y
```

`-n` Desactiva el guardado de volcados por caída

`-y` Activa el guardado de volcados por caída

EJEMPLO 1-2 Desactivación del guardado de volcados por caída

En este ejemplo, se muestra cómo desactivar el guardado de volcados por caída en el sistema.

```
# Dump content: all pages
       Dump device: /dev/zvol/dsk/rpool/dump (dedicated)
Savecore directory: /var/crash (minfree = 5697105KB)
  Savecore enabled: no
   Save compressed: on
```

EJEMPLO 1-3 Activación del guardado de volcados por caída

En este ejemplo, se muestra cómo activar el guardado de volcado por caída en el sistema.

```
# dumpadm -y
      Dump content: all pages
       Dump device: /dev/zvol/dsk/rpool/dump (dedicated)
Savecore directory: /var/crash (minfree = 5697105KB)
  Savecore enabled: yes
   Save compressed: on
```

Resolución de problemas después de la caída de un sistema

Si se produce la caída de un sistema Oracle Solaris, deberá proporcionar a su proveedor de servicios toda la información posible, incluidos la información general del sistema y la información específica proporcionada en los archivos de volcado por caída.

Para solucionar problemas de un volcado por caída existente, consulte lo siguiente:

Qué hacer si el sistema se bloquea

En la siguiente lista, se describe la información más importante para recordar en el caso de un bloqueo del sistema:

1. Anote los mensajes de la consola del sistema.
   - Se se produce la caída de un sistema, volver a ejecutarlo probablemente será su inquietud principal. Sin embargo, antes de reiniciar el sistema, debe examinar la pantalla de la consola para ver los mensajes. Estos mensajes pueden ayudar a comprender la causa del bloqueo. Incluso si el sistema se reinicia automáticamente, y los mensajes de la consola no aparecen en la pantalla, podría revisar estos mensajes. Para ello, vea el log de los errores del sistema (archivo `/var/adm/messages`). Para obtener más información sobre la visualización de los archivos del log de los errores del sistema, consulte Cómo ver los mensajes del sistema [42].
   - Si experimenta caídas frecuentes y no puede determinar la causa, recopile toda la información que pueda de la consola del sistema o del archivo `/var/adm/messages` y téngala a mano para que la examine un representante de servicio al cliente. Para obtener una lista completa de la información sobre resolución de problemas para recopilar información para el proveedor de servicios, consulte "Lista de comprobación para resolución de problemas de caídas del sistema" [17].
2. Verifique si se generó un volcado por caída del sistema después del bloqueo del sistema.

Atención - No elimine información importante sobre la caída del sistema antes de enviarla al representante de servicio al cliente.

3. Si no puede iniciar el sistema después de una caída del sistema, consulte "Cierre e inicio de un sistema para fines de recuperación" de "Inicio y cierre de sistemas Oracle Solaris 11.2 " para obtener más instrucciones.

Análisis de la información de volcado por caída

Puede examinar las estructuras de control, las tablas activas, las imágenes de la memoria de un núcleo del sistema caído o en ejecución, y otra información sobre la operación del núcleo mediante la utilidad `mdb`, como se describe en el siguiente procedimiento.

Nota - El siguiente procedimiento proporciona sólo un ejemplo limitado de cómo usar la utilidad `mdb`. Para poder usar la utilidad `mdb` con todo su potencial, se requiere un conocimiento detallado sobre el núcleo y ello excede el alcance de este manual. Para obtener más información sobre el uso de esta utilidad, consulte la página del comando man `mdb`(1).

▼ Cómo examinar la información de volcado por caída

1. **Asuma el rol de usuario `root`.**

   Consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

2. **Pase al directorio en el que se ha guardado la información de volcado por caída.**

   Por ejemplo:

   ```
   # cd /var/crash
   ```

   Si no está seguro de la ubicación del volcado por caída, use el comando `dumpadm` para determinar el lugar en el que el sistema tiene configurado almacenar los archivos de volcado por caída del núcleo. Por ejemplo:

   ```
   # /usr/sbin/dumpadm
         Dump content: kernel pages
          Dump device: /dev/zvol/dsk/rpool/dump (dedicated)
   Savecore directory: /var/crash
     Savecore enabled: yes
      Save compressed: on
   ```

3. **Examine el volcado por caída mediante el uso de la utilidad de depurador modular (`mdb`).**

   ```
   # /usr/bin/mdb [-k] crashdump-file
   ```

`-k`	Especifica el modo de depuración del núcleo considerando que el archivo es un archivo de volcado por caída del sistema operativo.
crashdump-file	Especifica el archivo de volcado por caída del sistema operativo.

   Por ejemplo:

```
# /usr/bin/mdb -K vmcore.0
```

Este comando también se puede especificar de la siguiente manera:

```
# /usr/bin/mdb -k 0
```

4. **Muestre el estado de caída del sistema.**

```
> ::status
   .
   .
   .
> ::system
   .
   .
   .
```

Para usar el comando `::system dcmd` al examinar el volcado por caída del núcleo, el archivo del núcleo debe ser un archivo de volcado por caída del núcleo y se debe haber especificado la opción `-k` al iniciar la utilidad `mdb`.

5. **Salga de la utilidad `mdb`.**

```
> $quit
```

ejemplo 1-4 Análisis de la información de volcado por caída

Este ejemplo muestra el resultado de la utilidad `mdb`, que incluye la información del sistema e identifica los valores ajustables definidos en este archivo `/etc/system` del sistema.

```
# cd /var/crash
# /usr/bin/mdb -k unix.0
Loading modules: [ unix krtld genunix ip nfs ipc ptm ]
> ::status
debugging crash dump /dev/mem (64-bit) from ozlo
operating system: 5.10 Generic sun4v
> ::system
set ufs_ninode=0x9c40 [0t40000]
set ncsize=0x4e20 [0t20000]
set pt_cnt=0x400 [0t1024]
> $q
```

Lista de comprobación para resolución de problemas de caídas del sistema

Responda las preguntas de la siguiente lista de comprobación para ayudar a aislar el problema del sistema y para prepararse para realizar la consulta a los proveedores de asistencia.

Elemento	Sus datos
¿Se encuentra disponible un volcado por caída del sistema?	
Identifique la versión del sistema operativo y los niveles adecuados de la versión de la aplicación de software.	
Identifique el hardware del sistema.	
Incluir la salida de `prtdiag` para sistemas SPARC. Incluya el resultado de Explorer para otros sistemas.	
¿Se encuentran instalados los parches? Si es así, incluya el resultado de `showrev -p`.	
¿Es posible reproducir el problema? Esto es importante porque un caso de prueba que pueda reproducirse resulta esencial para la depuración de problemas realmente complejos. Mediante la reproducción del problema, el proveedor de servicios puede crear núcleos con instrumentación especial para activar, diagnosticar y corregir el error.	
¿Tiene el sistema algún controlador de terceros? Los controladores se ejecutan en el mismo espacio de direcciones que el núcleo, con todos los mismos privilegios, por lo que pueden producir bloqueos si tienen errores.	
¿Qué estaba haciendo el sistema antes de bloquearse? Si el sistema estaba haciendo algo poco común, como ejecutar una nueva prueba de esfuerzo o gestionar una carga más grande que lo normal, eso puede haber provocado el bloqueo.	
¿Había algún mensaje de la consola que fuera inusual justo antes del bloqueo del sistema? En ocasiones, el sistema muestra signos de problemas antes de bloquearse; esta información suele resultar útil.	
¿Agregó algún parámetro al archivo `/etc/system`? A veces, los parámetros de ajuste, como aumentar los segmentos de memoria compartida para que el sistema trate de asignar más de lo que tiene, pueden causar el bloqueo del sistema.	
¿El problema empezó hace poco? Si es así, verifique si el inicio de los problemas coinciden con algún cambio realizado en el sistema; por ejemplo, controladores nuevos, software nuevo, un cambio en la carga de trabajo, una actualización de CPU o una ampliación de memoria.	

Guardado de datos cuando el directorio de volcado por caída está completo

Si se produce la caída del sistema, y no hay espacio disponible en el directorio `savecore` y desea guardar información crítica de volcado por caída del sistema, use uno de los siguientes métodos.

Después de reiniciar el sistema, inicie sesión con el rol root . Elimine los archivos de volcado por caída existentes que ya se han enviado a su proveedor de servicios del directorio `savecore`.

Nota - El directorio savecore es normalmente `/var/crash`.

Como alternativa, después de reiniciar el sistema, inicie sesión con el rol root. Ejecute manualmente el comando `savecore` y especifique un directorio alternativo que tenga espacio suficiente en el disco:

```
# savecore directory
```

Gestión de incidentes con Oracle Enterprise Manager Ops Center

Si es necesario gestionar incidentes para sistemas operativos, servidores y dispositivos de almacenamiento físicos y virtuales de un centro de datos, en lugar de supervisar incidentes sólo en los sistemas individuales, se pueden usar las soluciones completas de gestión de sistemas disponibles en Oracle Enterprise Manager Ops Center.

Enterprise Manager Ops Center le permite configurar alertas que le indican si una parte de su centro de datos no está funcionando como se esperaba, y le permite gestionar estos informes e intentar reparaciones.

Para obtener información, consulte http://www.oracle.com/pls/topic/lookup?ctx=oc122.

♦ ♦ ♦ CAPÍTULO 2

Resolución de problemas cuando un sistema se bloquea o se produce un error al reiniciar

En este capítulo, se describen las acciones que puede realizar cuando un sistema se bloquea o si tiene problemas para reiniciar un sistema.

En este capítulo, se aborda la siguiente información:

Qué hacer si se produce un error al reiniciar

Si el sistema no se reinicia por completo o si se reinicia, pero luego se vuelve a bloquear, quizás haya un problema de software o hardware que esté impidiendo que el sistema se inicie correctamente.

Motivo por el cual el sistema no se inicia	Cómo resolver el problema
El sistema no puede encontrar `/platform/`uname -m`/kernel/sparcv9/unix`.	Es posible que tenga que cambiar la configuración de `boot-device` de la PROM en un sistema basado en SPARC. Para obtener información sobre cómo cambiar el dispositivo de inicio predeterminado, consulte "Visualización y configuración de atributos de inicio" de "Inicio y cierre de sistemas Oracle Solaris 11.2 ".
El archivo de inicio de Oracle Solaris está dañado. O bien, el servicio del archivo de inicio SMF falló. Se muestra un mensaje de error si ejecuta el comando `svcs -x`.	Cree un segundo entorno de inicio, que es una copia de seguridad del entorno de inicio principal. En el caso de que el entorno de inicio principal no se pueda iniciar, inicie la copia de seguridad del entorno de inicio. Como alternativa, puede iniciar desde el soporte activo de CD o USB.
Hay una entrada que no es válida en el archivo `/etc/passwd`.	Para obtener información sobre cómo recuperarse desde un archivo `passwd` no válido, consulte "Cómo iniciar desde un medio para resolver una contraseña de usuario

Motivo por el cual el sistema no se inicia	Cómo resolver el problema
	root desconocida" de "Inicio y cierre de sistemas Oracle Solaris 11.2 ".
El cargador de inicio x86 (GRUB) está dañado. O bien, el menú de GRUB falta o está dañado.	Para obtener información acerca de un cargador de inicio x86 dañado o un menú GRUB dañado o faltante, consulte "Cómo iniciar desde un medio para resolver un problema con la configuración de GRUB que impide el inicio del sistema" de "Inicio y cierre de sistemas Oracle Solaris 11.2 ".
Hay un problema de hardware con un disco u otro dispositivo.	Compruebe las conexiones de hardware: ■ Asegúrese de que el equipo esté enchufado. ■ Asegúrese de que todos los conmutadores estén correctamente establecidos. ■ Revise todos los conectores y los cables, incluidos los cables Ethernet. ■ Si todos estos pasos fallan, apague el sistema, espere entre 10 y 20 segundos y, luego, vuelva a encenderlo.

Si el problema no se resuelve con ninguna de las sugerencias anteriores, póngase en contacto con el proveedor de servicios local.

Qué hacer si ha olvidado la contraseña del usuario root o no se puede iniciar el sistema

Si olvida la contraseña `root` o experimenta otro problema que evita que el sistema se inicie, realice lo siguiente:

- Detenga el sistema.
- Siga las instrucciones en "Cómo iniciar desde un medio para resolver una contraseña de usuario root desconocida" de "Inicio y cierre de sistemas Oracle Solaris 11.2 ".
- Si la contraseña `root` es el problema, elimínela del archivo `/etc/shadow`.
- Reinicie el sistema.
- Inicie sesión y establezca la contraseña `root`.

Qué hacer si el sistema se cuelga

Un sistema puede congelarse o colgarse en lugar de bloquearse por completo si algún proceso de software se detiene. Siga estos pasos para efectuar la recuperación de un sistema colgado.

1. Determine si el sistema está ejecutando un entorno de ventanas y siga estas sugerencias. Si el problema no se resuelve con estas sugerencias, vaya al paso 2.

- Asegúrese de que el puntero se encuentre en la ventana en la que escribe los comandos.
- Presione Control-q en caso de que el usuario haya presionado por accidente las teclas Control-s, que congelan la pantalla. Control-s congela solamente la ventana, no toda la pantalla. Si una ventana se congela, intente utilizar otra ventana.
- Si es posible, inicie sesión de manera remota desde otro sistema de la red. Utilice el comando `pgrep` para buscar el proceso que está colgado. Si parece que el sistema de ventanas está colgado, identifique el proceso y termínelo.

2. Presione **Control-**\ para forzar el cierre del programa en ejecución y (probablemente) escribir un archivo `core`.
3. Presione **Control-c** para interrumpir el programa que podría estar en ejecución.
4. Inicie sesión de manera remota e intente identificar y terminar el proceso que cuelga el sistema.
5. Inicie sesión de manera remota, asuma el rol `root` y, luego, vuelva a iniciar el sistema.
6. Si el sistema sigue sin responder, genere un volcado por caída y vuelva a iniciar.
   Para obtener información sobre cómo forzar un volcado por caída e iniciar, consulte “Provocación de un volcado por caída y un reinicio del sistema” de “Inicio y cierre de sistemas Oracle Solaris 11.2 ”.
7. Si el sistema sigue sin responder, apáguelo, espere aproximadamente un minuto y, luego, enciéndalo de nuevo.
8. Si no puede lograr que el sistema responda de ninguna manera, póngase en contacto con el proveedor de servicios local para obtener ayuda.

♦ ♦ ♦ CAPÍTULO 3

Resolución de problemas del sistema de archivos

En este capítulo, se describe cómo solucionar problemas del sistema de archivos, incluidos los siguientes:

Qué hacer si el sistema de archivos se llena

Cuando el sistema de archivos root (/) o cualquier otro sistema de archivos se llenan, aparece el siguiente mensaje en la ventana de la consola:

```
.... file system full
```

Hay varios motivos por los que un sistema de archivos se puede llenar. En las siguientes secciones, se describen varios escenarios para la recuperación de un sistema de archivos lleno.

El sistema de archivos se llenó porque se creó un archivo o directorio grande

Motivo del error	Cómo resolver el problema
Alguien copió accidentalmente un archivo o directorio en una ubicación incorrecta. Esto también sucede cuando una aplicación se bloquea y registra un archivo `core` grande en el sistema de archivos.	Inicie sesión y asuma el rol `root`; luego, use el comando `ls -tl` en el sistema de archivos específico para identificar el archivo grande que se acaba de crear y eliminarlo.

El sistema de archivos TMPFS está lleno porque el sistema se quedó sin memoria

Motivo del error	Cómo resolver el problema
Esto puede ocurrir si TMPFS intenta escribir más de lo que se permite o si algunos procesos actuales utilizan mucha memoria.	Para obtener información sobre la recuperación a partir de mensajes de error relacionados con tmpfs, consulte la página del comando man tmpfs(7FS).

Qué hacer si las ACL de los archivos se pierden después de copiar o restaurar

Motivo del error	Cómo resolver el problema
Si se copian o restauran archivos o directorios con ACL en el directorio /tmp, los atributos de las ACL se pierden. Por lo general, el directorio /tmp se encuentra montado como sistema de archivos temporal, que no admite los atributos del sistema de archivos UFS, como las ACL.	Copie o restaure los archivos en el directorio /var/tmp.

Resolución de problemas de acceso a archivos

A menudo, cuando los usuarios tienen problemas, recurren a un administrador del sistema en busca de ayuda, por ejemplo si no pueden acceder a un programa, un archivo o un directorio al que antes sí podían.

Siempre que tenga un problema de esta clase, investigue una de las tres siguientes posibilidades:

- Puede que la ruta de búsqueda del usuario haya cambiado o que los directorios en la ruta de búsqueda no se encuentren en el orden correcto.
- Puede que el archivo o el directorio no tengan la propiedad o los permisos adecuados.
- Puede que la configuración de un sistema al que se accede mediante la red haya cambiado.

Este capítulo describe brevemente cómo reconocer los problemas de cada una de estas tres áreas y se sugieren posibles soluciones.

Resolución de problemas con rutas de búsqueda (`Command not found`)

Un mensaje `Command not found` indica una de las siguientes situaciones:

- El comando no está disponible en el sistema.
- El directorio del comando no está en la ruta de búsqueda.

Para solucionar un problema de la ruta de búsqueda, necesita saber el nombre de ruta del directorio donde el comando se encuentra almacenado.

Si se encuentra la versión incorrecta del comando, hay un directorio que tiene un comando con el mismo nombre en la ruta de búsqueda. En este caso, puede que el directorio correspondiente se encuentre más adelante en la ruta de búsqueda o que directamente no se encuentre en ninguna parte.

Puede mostrar la ruta de búsqueda actual con el comando `echo $PATH`.

Utilice el comando `type` para determinar si está ejecutando la versión incorrecta del comando. Por ejemplo:

```
$ type acroread
acroread is /usr/bin/acroread
```

▼ Cómo diagnosticar y corregir problemas de ruta de búsqueda

1. **Visualice la ruta de búsqueda actual a fin de verificar que el directorio para el comando no esté en la ruta ni esté mal escrito.**

   ```
   $ echo $PATH
   ```

2. **Compruebe lo siguiente:**

   - ¿Es correcta la ruta de búsqueda?
   - ¿Está enumerada la ruta de búsqueda antes que otras rutas de búsqueda donde se encuentra otra versión del comando?
   - ¿Se encuentra el comando en una de las rutas de búsqueda?

   Si es necesario corregir la ruta, vaya al paso 3. De lo contrario, vaya al paso 4.

3. **Agregue la ruta al archivo correspondiente, como se muestra en la siguiente tabla.**

Shell	Archivo	Sintaxis	Notas de tabla
bash y ksh93	$HOME/.profile	$ PATH=*$HOME/bin:/sbin:/usr/local /bin ...* $ export PATH	Los nombres de ruta se separan con dos puntos.

4. Active la ruta nueva como se muestra a continuación:

Shell	Ubicación de la ruta	Comando para activar la ruta
bash y ksh93	.profile	. $HOME/.profile
	.login	hostname$ source $HOME/.login

5. Verifique la ruta nueva.

$ **which** *command*

ejemplo 3-1 Diagnóstico y corrección de problemas de ruta de búsqueda

En este ejemplo, se muestra que el ejecutable `mytool` no está en ninguno de los directorios de la ruta de búsqueda con el comando `type`.

```
$ mytool
 -bash: mytool: command not found
 $ type mytool
 -bash: type: mytool: not found
 $ echo $PATH
 /usr/bin:
 $ vi $HOME/.profile
 (Add appropriate command directory to the search path)
 $ . $HOME/.profile
 $ mytool
```

Si no puede encontrar un comando, consulte la página del comando man para la ruta de directorio.

Cambio de propiedades de grupo y archivo

Con frecuencia, las propiedades de los archivos y los directorios cambian porque un superusuario edita los archivos como administrador. Al crear directorios principales para los usuarios nuevos, asegúrese de asignarles la propiedad del archivo punto (`.`) en el directorio principal. Si los usuarios no tienen la propiedad de "`.`", no pueden crear archivos en su directorio principal.

También pueden surgir problemas de acceso cuando cambia la propiedad del grupo o cuando un grupo del que un usuario es miembro se suprime de la base de datos `/etc/group`.

Para obtener información sobre cómo cambiar los permisos o la propiedad de un archivo al que no puede acceder, consulte el Capítulo 1, “Control de acceso a archivos” de “Protección y verificación de la integridad de archivos en Oracle Solaris 11.2 ”.

Resolución de problemas de acceso a archivos

Si los usuarios no pueden acceder a archivos o directorios a los que antes podían acceder, es probable que la propiedad o los permisos de los archivos o directorios se hayan modificado.

Detección de problemas con el acceso de red

Si los usuarios tienen problemas con el comando de copia remota `rcp` para copiar archivos en la red, puede que los directorios y los archivos del sistema remoto tengan acceso restringido mediante la definición de permisos. También se pueden ocasionar problemas si el sistema remoto y el sistema local no están configurados para permitir el acceso.

Consulte “Estrategias para resolución de problemas de NFS” de “Gestión de sistemas de archivos de red en Oracle Solaris 11.2 ” para obtener información sobre problemas con el acceso a red y problemas con el acceso a sistemas mediante AutoFS.

♦ ♦ ♦ CAPÍTULO 4

Preparación para posibles fallos de proceso mediante archivos del núcleo central

En este capítulo, se describe cómo configurar las especificaciones para los archivos del núcleo central que produce un sistema cuando un proceso falla y cómo examinar estos archivos del núcleo central después de un fallo.

A continuación, se muestra una lista con la información que se incluye en este capítulo:

Acerca de fallos del proceso y archivos del núcleo central

Cuando un proceso o una aplicación finalizan de modo anormal, el sistema genera automáticamente un conjunto de archivos. Este proceso se puede describir como un *volcado del núcleo central*. Los archivos que se crean son *archivos del núcleo central*. Un archivo del núcleo central es una copia de disco del contenido del espacio de la dirección del proceso en el momento de su terminación, junto con información adicional sobre el estado del proceso. Normalmente, los archivos del núcleo central se producidos tras una terminación anormal de un proceso resultante de un error en la aplicación correspondiente. Un archivo de núcleo central proporciona información muy útil para uso en el diagnóstico del problema que causa el fallo del proceso. Consulte "Parámetros para la creación del archivo del núcleo central" [32].

Como parte de la administración del sistema en curso, puede usar el comando `coreadm` para controlar las especificaciones de creación de los archivos del núcleo central. Por ejemplo, puede usar el comando `coreadm` para configurar un sistema a fin de que todos los archivos del núcleo central del proceso se ubiquen en un solo directorio del sistema, de modo que pueda realizar un seguimiento de los problemas con facilidad. Consulte "Administración de las especificaciones del archivo del núcleo central" [34].

Cuando un proceso finaliza de modo anormal, puede inspeccionar los archivos del núcleo central que se crean mediante un depurador como el comando `mdb` o mediante una herramienta de `proc`. Consulte "Examen de archivos del núcleo central tras un fallo de proceso" [37].

Parámetros para la creación del archivo del núcleo central

Cuando un proceso falla, el sistema intenta crear hasta dos archivos del núcleo central para cada proceso mediante un patrón de nombre de archivo del núcleo central global y un patrón de nombre de archivo del núcleo central por proceso para crear cada nombre de archivo del núcleo central archivos del núcleo central. El comando `coreadm` controla estos patrones de nombres y especifica la ubicación de los archivos del núcleo central. En esta sección, se describen algunos de los parámetros de ruta y de nombre de archivo. Para obtener una descripción completa de los procesos de volcado de núcleo central, consulte la página del comando man `core`(4). Para obtener una descripción completa de las opciones de `coreadm`, consulte la página del comando man `coreadm`(1M).

Rutas configurables de los archivos del núcleo central

Cuando un proceso finaliza de modo anormal, genera un archivo del núcleo central en el directorio actual de manera predeterminada. Si la ruta del archivo del núcleo central global está activada, todos los procesos finalizados de modo anormal pueden generar dos archivos: uno se genera en el directorio de trabajo actual y otro, en la ubicación del archivo del núcleo central global. Las rutas de los archivos que se usan son parámetros configurables.

Dos rutas configurables del archivo `core` se pueden activar o desactivar de manera independiente de la siguiente manera:

- Una ruta del archivo del núcleo central por proceso, la cual está activada y asignada al archivo `core` de manera predeterminada. Cuando está activada, la ruta del archivo del núcleo central por proceso permite que se genere un archivo `core` cuando el proceso finaliza de modo anormal. Un proceso nuevo hereda la ruta por proceso del proceso principal correspondiente.

  El propietario del proceso es propietario del archivo del núcleo central por proceso que se genera, y cuenta con permisos de lectura y escritura. Sólo el usuario propietario puede ver este archivo.
- Una ruta del archivo del núcleo central global, que está desactivada y asignada al archivo `core` de manera predeterminada. Si está activada, mediante la ruta del archivo del núcleo central global, se genera un archivo del núcleo central *adicional* con el mismo contenido que el archivo del núcleo central por proceso.

  Cuando se genera, un archivo de núcleo central global es propiedad del usuario root, que cuenta con permisos de lectura y escritura *exclusivos* para usuario root. Los usuarios sin privilegios no pueden ver este archivo.

Nota - De manera predeterminada, un proceso `setuid` no genera archivos del núcleo central mediante la ruta global ni la ruta por proceso.

Nombres ampliados de archivos del núcleo central

El nombre de un archivo de núcleo central contiene campos con información acerca del proceso con fallo. Para obtener una descripción completa de los campos de nombre de archivo de núcleo central, consulte la página del comando man `coreadm`(1M). Esta sección se concentra en las variables globales.

Si un directorio global de archivos `core` está activado, es posible distinguir los archivos `core` entre sí mediante las variables descritas en la siguiente tabla.

`%d`	Nombre de directorio de archivo ejecutable (hasta un máximo de `MAXPATHLEN` caracteres)
`%f`	Nombre de archivo ejecutable (hasta un máximo de `MAXCOMLEN` caracteres)
`%g`	ID de grupo efectivo
`%m`	Nombre del equipo (`uname -m`)
`%n`	Nombre del nodo del sistema (`uname -n`)
`%p`	ID de proceso
`%t`	Valor decimal de tiempo (2)
`%u`	ID de usuario efectivo
`%z`	Nombre de la zona en la que se ejecuta el proceso (`zonename`)
`%%`	% literal

Por ejemplo, supongamos que `/var/core/core.%f.%p` está configurado como la ruta del archivo del núcleo central global. Si un proceso `sendmail` con PID `12345` finaliza de modo anormal, produce `/var/core/core.sendmail.12345` como archivo `core`.

Mejora del rendimiento de volcado de archivos del núcleo central

Puede mejorar el rendimiento del volcado del archivo del núcleo central en un sistema mediante la exclusión de algunas partes de la imagen binaria del proceso de volcado de núcleo central. Al introducir el comando `coreadm` para personalizar las especificaciones de volcado del núcleo central, puede especificar la exclusión, por ejemplo, de asignaciones de DISM o asignaciones de ISM, o de una memoria compartida System V de un volcado de núcleo central. Para obtener instrucciones, consulte la página del comando man `coreadm`(1M).

Administración de las especificaciones del archivo del núcleo central

Puede gestionar los archivos del núcleo central de la siguiente manera:

Visualización de la configuración de volcado del núcleo central actual

Use el comando `coreadm` sin opciones para visualizar la configuración de volcado del núcleo central actual.

```
$ coreadm
              global core file pattern:
     global core file content: default
       init core file pattern: core
       init core file content: default
            global core dumps: disabled
      per-process core dumps: enabled
     global setid core dumps: disabled
per-process setid core dumps: disabled
     global core dump logging: disabled
```

Configuración de patrón de nombre de archivo del núcleo central

Es posible configurar un patrón de nombre de archivo del núcleo central de manera global, según la zona o por proceso. Además, puede configurar los valores predeterminados por proceso que se mantienen después de reiniciar el sistema.

Por ejemplo, puede usar el siguiente comando `coreadm` para definir el patrón de archivo del núcleo central por proceso para todos los procesos iniciados por el proceso `init`. Esta configuración se aplica a todos los procesos que no han sustituido explícitamente el patrón

predeterminado del archivo del núcleo central. Dicha configuración se mantiene después de cada reinicio del sistema.

```
# coreadm -i /var/core/core.%f.%p
```

Puede usar el siguiente comando `coreadm` para definir el patrón de nombre de archivo del núcleo central por proceso para todos los procesos:

```
# coreadm -p /var/core/core.%f.%p $$
```

Los símbolos `$$` representan un marcador de posición para el ID de proceso del shell que se ejecuta actualmente. Todos los procesos secundarios heredan el patrón de nombre de archivo del núcleo central por proceso.

```
Here's another example:

$ coreadm -p $HOME/corefiles/%f.%p $$
```

Como alternativa, asuma el rol `root` y defina un patrón de nombre de archivo global:

```
# coreadm -g /var/corefiles/%f.%p
```

Después de definir un patrón de nombre de archivo del núcleo central, ya sea por proceso o global, deberá activarse con el comando `coreadm -e`.

Puede configurar el patrón de nombre de archivo del núcleo central para todos los procesos que se ejecutan durante la sesión de inicio de un usuario si coloca el comando en un archivo de inicialización de usuario, por ejemplo, `.profile`.

Activación de rutas de archivos

Puede activar una ruta de archivo del núcleo central global o por proceso.

- Para activar una ruta del núcleo central por proceso, asuma el rol root y escriba el siguiente comando:

  ```
  # coreadm -e process
  ```

  Si desea verificar la configuración, visualice la ruta de archivo del núcleo central del proceso actual:

  ```
  # coreadm $$
  1180:   /home/kryten/corefiles/%f.%p
  ```

- Para activar una ruta de archivo de núcleo central global, asuma el rol root y escriba el siguiente comando:

  ```
  # coreadm -e global -g /var/core/core.%f.%p
  ```

  Si desea verificar la configuración, visualice la ruta de archivo del núcleo central del proceso actual:

```
# coreadm
       global core file pattern: /var/core/core.%f.%p
     global core file content: default
       init core file pattern: core
       init core file content: default
            global core dumps: enabled
       per-process core dumps: enabled
      global setid core dumps: disabled
 per-process setid core dumps: disabled
     global core dump logging: disabled
```

Activación de programas `setuid` para generar archivos del núcleo central

Puede usar el comando `coreadm` para activar o desactivar los programas `setuid` a fin de generar archivos del núcleo central para todos los procesos del sistema, o por proceso, mediante la configuración de las siguientes rutas:

- Si la opción `setuid` global está activada, una ruta del archivo del núcleo central global permite que todos los programas `setuid` de un sistema generen archivos `core`.
- Si la opción `setuid` por proceso está activada, una ruta del núcleo central por proceso permite que determinados procesos `setuid` generen archivos `core`.

De manera predeterminada, ambos indicadores están desactivados. Por motivos de seguridad, la ruta del archivo del núcleo central global debe ser un nombre de ruta completo que empiece con `/`. Si el usuario root desactiva los archivos del núcleo central por proceso, los usuarios individuales no pueden obtener archivos del núcleo central.

Los archivos del núcleo central `setuid` son propiedad del usuario root, el cual dispone de permisos de lectura y escritura exclusivos. Los usuarios comunes no pueden acceder a estos archivos, aunque el proceso que generó el archivo del núcleo central `setuid` sea propiedad de un usuario común.

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

Reversión a la configuración predeterminada de archivos del núcleo central

Como usuario root, ejecute uno de los siguientes comandos para desactivar la ruta de archivo del núcleo central y elimine el patrón de nombre de archivo del núcleo central:

- Para configuración de archivos del núcleo central global:

  ```
  # coreadm -d global -g ""
  ```

Nota - "" es una cadena vacío sin espacios.

- Para configuración de archivos del núcleo central por proceso:

  ```
  # coreadm -d process -g ""
  ```

  La opción -d desactiva la ruta de archivo del núcleo central. La opción -gcon variable de cadena vacía elimina el patrón de nombre de archivo de núcleo central. Se restablece la configuración predeterminada original de la ruta de archivos del núcleo central y el patrón de nombre de archivos del núcleo central.

Corrección de parámetros obsoletos de archivos del núcleo central

Mensaje de Error

```
NOTICE: 'set allow_setid_core = 1' in /etc/system is obsolete
NOTICE: Use the coreadm command instead of 'allow_setid_core'
```

Causa

Hay un parámetro obsoleto que permite la generación de archivos del núcleo central `setuid` en el archivo `/etc/system`.

Solución

Elimine `allow_setid_core=1` del archivo `/etc/system`. Luego, utilice el comando `coreadm` para activar las rutas de archivos del núcleo central `setuid` globales.

Examen de archivos del núcleo central tras un fallo de proceso

Las herramientas de `proc` le permiten examinar los archivos del núcleo central del proceso y los procesos activos. Las herramientas de `proc` son utilidades que pueden manipular funciones del sistema de archivos `/proc`.

Es posible aplicar las herramientas `/usr/proc/bin/pstack`, `pmap`, `pldd`, `pflags` y `pcred` a los archivos del núcleo central si se especifica el nombre del archivo del núcleo central en la línea

de comandos mediante un proceso similar al que se utiliza para especificar un ID de proceso para estos comandos.

Para obtener más información acerca del uso de las herramientas de `proc` para examinar archivos del núcleo central, consulte `proc`(1).

EJEMPLO 4-1 Análisis de archivos del núcleo central con herramientas de `proc`

```
$ ./a.out
Segmentation Fault(coredump)
$ /usr/proc/bin/pstack ./core
core './core' of 19305: ./a.out
 000108c4 main     (1, ffbef5cc, ffbef5d4, 20800, 0, 0) + 1c
 00010880 _start   (0, 0, 0, 0, 0, 0) + b8
```

♦ ♦ ♦ CAPÍTULO 5

Gestión de logs del sistema y mensajes

En este capítulo, se tratan la visualización y la gestión de los logs del sistema y de los mensajes del sistema.

En este capítulo, se aborda la siguiente información:

Registro ampliado del sistema con `rsyslogd`

Esta versión de Oracle Solaris incluye la opción de instalar y usar el servicio `rsrsyslog` para gestionar el registro del sistema. `rsyslog` es una implementación confiable y ampliada del daemon `syslog` con un diseño modular que admite varias funciones, por ejemplo, filtrado, Protocolo de control de transmisión (TCP), cifrado e indicadores de hora y fecha de alta precisión, así como control de salida.

El servicio SMF de syslog servicio, svc:/system/system-log:default, continúa siendo el servicio de registro predeterminado. Para usar el servicio `rsyslog`, debe instalar el paquete de `rsyslog` y activar el servicio `rsyslog`.

▼ Instalación y activación de `rsyslog`

1. **Puede comprobar si el paquete de `rsyslog` ya está instalado en el sistema. Para ello, intente activar el servicio de la siguiente manera:**

```
root@pcclone: ~# svcadm enable svc:/system/system-log:rsyslog
```

Si el paquete de rsyslog no está instalado, aparece el siguiente mensaje:

```
svcadm: Pattern 'svc:/system/system-log:rsyslog' doesn't match any instance.
```

2. **Si el paquete `rsyslog` no está instalado, instálelo.**

```
root@pcclone:~# pkg install rsyslog
           Packages to install:  3
            Services to change:  1
       Create boot environment: No
Create backup boot environment: No

DOWNLOAD                                  PKGS         FILES    XFER (MB)   SPEED
Completed                                  3/3         68/68      1.7/1.7  354k/s

PHASE                                          ITEMS
Installing new actions                       147/147
Updating package state database                 Done
Updating package cache                           0/0
Updating image state                            Done
Creating fast lookup database                   Done
```

3. **Confirme que existe una instancia de `rsyslog`.**

```
root@pcclone:~# svcs -a | grep "system-log"
disabled       18:27:16 svc:/system/system-log:rsyslog
online         18:27:21 svc:/system/system-log:default
```

Esta salida confirma que la instancia de `rsyslog` existe, pero que está desactivada.

4. **Cambie al servicio `rsyslog`.**

```
root@pcclone:~# svcadm disable svc:/system/system-log:default
root@pcclone:~# svcadm enable svc:/system/system-log:rsyslog
root@pcclone:~# svcs -xv

These commands disable the default service, enable rsyslog and report on status.
```

Pasos siguientes Una vez que `rsyslog` esté instalado y activado, puede configurar en `syslog` en `/etc/rsyslog.conf`.

Gestión de mensajes del sistema

En las siguientes secciones, se describen las funciones de mensajes del sistema en Oracle Solaris.

Visualización de los mensajes del sistema

Los mensajes del sistema se muestran en el dispositivo de la consola. El texto de la mayoría de los mensajes del sistema se ve así:

`[ID` *msgid facility*`.]`

Por ejemplo:

```
[ID 672855 kern.notice] syncing file systems...
```

Si el mensaje se originó en el núcleo, se muestra el nombre del módulo del núcleo. Por ejemplo:

```
Oct 1 14:07:24 mars ufs: [ID 845546 kern.notice] alloc: /: file system full
```

Cuando se produce la caída de un sistema, es posible que se muestre un mensaje como el siguiente en la consola del sistema:

`panic:` *error message*

En ocasiones, puede que aparezca el siguiente mensaje en lugar del mensaje de aviso grave:

```
Watchdog reset !
```

El daemon del registro, `syslogd`, registra automáticamente varias advertencias y errores en los archivos de mensajes. De manera predeterminada, muchos de estos mensajes del sistema se muestran en la consola del sistema y se almacenan en el directorio `/var/adm`. Puede establecer dónde se almacenan estos mensajes mediante la configuración del log de mensajes del sistema. Para obtener más información, consulte “Personalización del log de mensajes del sistema” [43]. Estos mensajes pueden alertar sobre problemas del sistema, como si un dispositivo está a punto de fallar.

El directorio `/var/adm` contiene varios archivos de mensajes. Los mensajes más recientes están en el archivo `/var/adm/messages` (y en `messages.*`) y los más viejos están en el archivo `messages.3`. Cuando transcurre un tiempo (en general, cada diez días), se crea un nuevo archivo `messages`. El nombre del archivo `messages.0` se cambia a `messages.1`, el nombre del archivo `messages.1` se cambia a `messages.2` y el de `messages.2` se cambia a `messages.3`. El archivo actual `/var/adm/messages.3` fue suprimido.

Dado que el directorio `/var/adm` almacena archivos grandes que contienen mensajes, volcados por caída y otros datos, este directorio puede consumir mucho espacio del disco. Para evitar que el directorio `/var/adm` alcance un tamaño excesivo, y a fin de garantizar que los futuros volcados por caída puedan guardarse, debe eliminar los archivos innecesarios con periodicidad. Puede automatizar esta tarea con el archivo `crontab`. Para obtener más información sobre cómo automatizar esta tarea, consulte “Eliminación de archivos de volcado” de “Gestión de dispositivos en Oracle Solaris 11.2 ” y Capítulo 4, “Programación de tareas del sistema” de “Gestión del rendimiento, los procesos y la información del sistema en Oracle Solaris 11.2 ”.

▼ Cómo ver los mensajes del sistema

- **Visualice los mensajes recientes que se hayan generado a raíz de un reinicio o un bloqueo del sistema con el comando `dmesg`.**

```
$ dmesg
```

Asimismo, utilice el comando `more` para visualizar una pantalla de mensajes por vez.

```
$ more /var/adm/messages
```

ejemplo 5-1 Visualización de los mensajes del sistema

El siguiente ejemplo muestra el resultado del comando `dmesg` en el sistema Oracle Solaris 10.

```
$ dmesg
Mon Sep 13 14:33:04 MDT 2010
Sep 13 11:06:16 sr1-ubrm-41 svc.startd[7]: [ID 122153 daemon.warning] ...
Sep 13 11:12:55 sr1-ubrm-41 last message repeated 398 times
Sep 13 11:12:56 sr1-ubrm-41 svc.startd[7]: [ID 122153 daemon.warning] ...
Sep 13 11:15:16 sr1-ubrm-41 last message repeated 139 times
Sep 13 11:15:16 sr1-ubrm-41 xscreensaver[25520]:  ,,,
Sep 13 11:15:16 sr1-ubrm-41 xscreensaver[25520]: ...
Sep 13 11:15:17 sr1-ubrm-41 svc.startd[7]: [ID 122153 daemon.warning]...
.
.
.
```

Véase también Para obtener más información, consulte la página del comando man `dmesg`(1M).

Rotación del log del sistema

Los archivos de registro del sistema se rotan con el comando `logadm` a partir de una entrada en el archivo root `crontab`. La secuencia de comandos `/usr/lib/newsyslog` ya no se utiliza.

La rotación del registro del sistema se define en el archivo `/etc/logadm.conf`. Este archivo incluye entradas de rotación de registro para procesos como `syslogd`. Por ejemplo, una entrada en el archivo `/etc/logadm.conf` especifica que el archivo `/var/log/syslog` se rota semanalmente, salvo que esté vacío. El archivo `syslog` más reciente se convierte en `syslog.0`, el siguiente archivo más reciente se convierte en `syslog.1` y así sucesivamente. Se guardan ocho registros previos de `syslog`.

El archivo `/etc/logadm.conf` también contiene la indicación de la hora en que se realizó la última rotación del registro.

Puede utilizar el comando `logadm` para personalizar el registro del sistema y para agregar registros adicionales en el archivo `/etc/logadm.conf` según sea necesario.

Por ejemplo, para rotar el acceso a Apache y los logs de errores, utilice los siguientes comandos:

```
# logadm -w /var/apache/logs/access_log -s 100m
# logadm -w /var/apache/logs/error_log -s 10m
```

En este ejemplo, el archivo de Apache `access_log` se rota cuando alcanza un tamaño de 100 MB, con un sufijo de `.0`, `.1` y así sucesivamente. Se mantienen 10 copias del archivo `access_log` anterior. El archivo `error_log` se rota cuando alcanza un tamaño de 10 MB, con los mismos sufijos y números de copias que el archivo `access_log`.

Las entradas de `/etc/logadm.conf` de los ejemplos anteriores sobre rotación de registros de Apache son similares a la siguiente:

```
# cat /etc/logadm.conf
.
.
.
/var/apache/logs/error_log -s 10m
/var/apache/logs/access_log -s 100m
```

Para obtener más información, consulte `logadm`(1M).

Si desea conceder a los usuarios que no sean usuarios root, el privilegio del mantenimiento de los archivos log, puede otorgar Mantenimiento del registro como un perfil de derechos para ese usuario. Puede otorgar los derechos mediante el uso de la opción `-P` con el comando `useradd` para nuevos usuarios o el comando `usermod` para un usuario existente. Para obtener instrucciones, consulte las páginas del comando man `useradd`(1M) y `usermod`(1M).

Personalización del log de mensajes del sistema

Puede capturar mensajes de error adicionales generados por varios procesos del sistema mediante la modificación del archivo `/etc/syslog.conf`. De manera predeterminada, el archivo `/etc/syslog.conf` ubica muchos mensajes de procesos del sistema en el archivo `/var/adm/messages`. Los mensajes de bloqueo e inicio también se almacenan ahí. Para ver los mensajes de `/var/adm`, consulte Cómo ver los mensajes del sistema [42].

El archivo `/etc/syslog.conf` tiene dos columnas separadas por fichas:

facility.level ... action

facility.level — La *utilidad* o fuente del sistema del mensaje o la condición. Puede ser una lista de utilidades separadas por comas. Los valores de las utilidades se muestran en la Tabla 5-1, “Utilidades de origen para mensajes `syslog.conf`”. El *nivel* indica la gravedad o prioridad de la condición

que se registra. Los niveles de prioridad se muestran en la Tabla 5-2, “Niveles de prioridad para mensajes de `syslog.conf`”.

No incluya dos entradas para la misma utilidad en la misma línea si las entradas son para distintas prioridades. Al establecer una prioridad en el archivo syslog, se indica que todos los mensajes con al menos esa prioridad se registrarán y el último mensaje tendrá precedencia. Para una utilidad o un nivel determinados, `syslogd` hace coincidir todos los mensajes para ese nivel y todos los niveles superiores.

action El campo de acción indica a dónde se reenvían los mensajes.

El siguiente ejemplo muestra líneas de ejemplo de un archivo `/etc/syslog.conf` predeterminado.

```
user.err                                /dev/sysmsg
user.err                                /var/adm/messages
user.alert                              `root, operator'
user.emerg                              *
```

Esto significa que los siguientes mensajes de usuario se registran automáticamente:

- Los errores de usuario se imprimen en la consola y también se registran en el archivo `/var/adm/messages`.
- Los mensajes de usuario que exigen una acción inmediata (`alert`) se envían a los usuarios `root` y a los usuarios `operator`.
- Los mensajes de emergencia de usuario se envían a los usuarios individuales.

Nota - La colocación de entradas en líneas separadas puede hacer que los mensajes se registren como deshabilitados si el destino del registro se encuentra especificado más de una vez en el archivo `/etc/syslog.conf`. Tenga en cuenta que puede especificar varios selectores en una entrada de una sola línea, separados con punto y coma.

Los orígenes de condiciones de error más habituales se muestran en la siguiente tabla. Las prioridades más habituales se muestran en la Tabla 5-2, “Niveles de prioridad para mensajes de `syslog.conf`” en orden de gravedad.

TABLA 5-1 Utilidades de origen para mensajes `syslog.conf`

Origen	Descripción
`kern`	El núcleo
`auth`	Autenticación
`daemon`	Todos los daemons
`mail`	Sistema de correo
`lp`	Sistema de trabajos en cola
`user`	Procesos de usuario

Nota - El número de utilidades `syslog` que se pueden activar en el archivo `/etc/syslog.conf` es ilimitado.

TABLA 5-2 Niveles de prioridad para mensajes de `syslog.conf`

Prioridad	Descripción
`emerg`	Emergencias del sistema
`alert`	Errores que requieren corrección inmediata
`crit`	Errores críticos
`err`	Otros errores
`info`	Mensajes informativos
`debug`	Resultado utilizado para la depuración
`ninguno`	Esta configuración no registra el resultado

▼ Cómo personalizar el registro de mensajes del sistema

1. **Asuma el rol `root` o un rol con la autorización `solaris.admin.edit/etc/syslog.conf` asignada.**

   Consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

2. **Use el comando `pfedit` para editar el archivo `/etc/syslog.conf`. Para ello, agregue o modifique los orígenes de los mensajes, las prioridades y las ubicaciones de los mensajes según la sintaxis que se describe en `syslog.conf`(4).**

   ```
   $ pfedit /etc/syslog.conf
   ```

3. **Guarde los cambios.**

ejemplo 5-2 Personalización del registro de mensajes del sistema

La utilidad de muestra `/etc/syslog.conf` `user.emerg` envía mensajes de emergencia de usuario al usuario `root` *y* a los usuarios individuales.

```
user.emerg                                      `root, *'
```

Activación remota de mensajería de consola

Las siguientes funciones de la consola son nuevas y mejoran la capacidad de resolver problemas de sistemas remotos:

- El comando `consadm` permite seleccionar un dispositivo serie como consola *auxiliar* (o remota). Con el comando `consadm`, un administrador del sistema puede configurar uno o más puertos de serie para mostrar los mensajes de la consola redireccionados y alojar sesiones de `sulogin` cuando el sistema pasa por los niveles de ejecución. Esta función le permite acceder a un puerto de serie con un módem para controlar los mensajes de la consola y participar en las transiciones de estado `init`. Para obtener más información, consulte `sulogin`(1M) y los procedimientos paso a paso que se establecen a continuación.

  Aunque se puede iniciar una sesión en un sistema con un puerto configurado como consola auxiliar, fundamentalmente, es un dispositivo de salida que muestra información que también se incluye en la consola predeterminada. Si las secuencias de comandos de inicio u otras aplicaciones leen y escriben en la consola predeterminada, la entrada de escritura se muestra en todas las consolas auxiliares, pero la entrada es de sólo lectura desde la consola predeterminada. Para obtener más información sobre el uso del comando `consadm` durante una sesión de inicio interactiva, consulte "Directrices para usar el comando `consadm` durante una sesión de inicio interactiva" [47].
- Ahora, el resultado de la consola se compone de un núcleo y de los mensajes de `syslog` que se escribieron en un nuevo pseudodispositivo, `/dev/sysmsg`. Además, los mensajes de inicio de la secuencia de comandos `rc` se escriben en `/dev/msglog`. Antes, todos estos mensajes se escribían en `/dev/console`.

  Debe cambiar las secuencias de comandos que dirigen el resultado de la consola de `/dev/console` a `/dev/msglog` si desea ver los mensajes de la secuencia de comandos que se muestran en las consolas auxiliares. Los programas que hacen referencia a `/dev/console` deben modificarse específicamente para usar `syslog()` o `strlog()` si desea que los mensajes se redireccionen a un dispositivo auxiliar.
- El comando `consadm` ejecuta un daemon para controlar los dispositivos de las consolas auxiliares. Cualquier dispositivo de visualización designado como consola auxiliar que desconecta, cuelga o pierde el portador se elimina de la lista de dispositivos de la consola auxiliar y deja de estar activo. La activación de una o más consolas auxiliares no desactiva la visualización de mensajes en la consola predeterminada. Los mensajes se siguen mostrando en `/dev/console`.

Uso de mensajes de la consola auxiliar durante las transiciones de nivel de ejecución

Tenga en cuenta lo siguiente cuando use mensajes de la consola auxiliar durante las transiciones de nivel de ejecución:

- La entrada no puede provenir de una consola auxiliar si se espera la entrada de usuarios para una secuencia de comandos `rc` que se ejecuta en el inicio del sistema. La entrada debe proceder de la consola predeterminada.
- El programa `sulogin`, que se invoca mediante `init` para que se solicite la contraseña de usuario root cuando se realizan transiciones entre los niveles de ejecución, se modificó

para que se solicite la contraseña de usuario root a cada dispositivo auxiliar, además del dispositivo de la consola predeterminada.

- El usuario nunca debe invocar directamente `sulogin`. El usuario debe tener `solaris.system.maintenance authorization` para usar esta utilidad.
- Cuando el sistema se encuentra en modo de usuario único y una o varias consolas auxiliares se activan mediante el comando `consadm`, se ejecuta una sesión de inicio de consola en el primer dispositivo a fin de proporcionar la contraseña de usuario root correcta al indicador `sulogin`. Cuando se recibe la contraseña correcta desde un dispositivo de consola, `sulogin` desactiva la entrada de todos los demás dispositivos de consola.
- Se muestra un mensaje en la consola predeterminada y las otras consolas auxiliares cuando una de las consolas asume privilegios de un usuario único. Este mensaje indica qué dispositivo aceptó una contraseña de usuario root correcta y se convirtió en consola. Si se pierde el portador en la consola auxiliar que ejecuta el shell de usuario único, una de las dos acciones siguientes puede ocurrir:
  - Si la consola auxiliar representa un sistema en el nivel de ejecución 1, el sistema continúa con el nivel de ejecución predeterminado.
  - Si la consola auxiliar representa un sistema en el nivel de ejecución S, el sistema muestra el mensaje `ENTER RUN LEVEL (0-6, s or S):` en el dispositivo en que los comandos `init s` o `shutdown` se habían introducido desde el shell. Si tampoco hay ningún portador en ese dispositivo, tendrá que restablecer el portador y escribir el nivel de ejecución correcto. Los comandos `init` o `shutdown` no vuelven a mostrar el indicador de nivel de ejecución.
- Si inició sesión en un sistema que utiliza un puerto de serie, y se emiten los comandos `init` o `shutdown` para realizar la transición a otro nivel de ejecución, la sesión de inicio se pierde, sin importar si el dispositivo es la consola auxiliar o no lo es. Esta situación es idéntica a las versiones sin las capacidades de la consola auxiliar.
- Después de que se selecciona un dispositivo como consola auxiliar con el comando `consadm`, éste continúa siendo la consola auxiliar hasta que el sistema vuelve a iniciarse o la consola auxiliar ya no está seleccionada. Igualmente, el comando `consadm` incluye una opción que permite definir un dispositivo como consola auxiliar en cualquier reinicio del sistema. (Consulte el procedimiento siguiente para obtener instrucciones paso a paso).

Directrices para usar el comando `consadm` durante una sesión de inicio interactiva

Si desea ejecutar una sesión de inicio interactiva mediante el inicio de sesión con un terminal que está conectado a un puerto serie y, a continuación, utilizar el comando `consadm` para ver los mensajes de la consola desde el terminal, tenga en cuenta el siguiente comportamiento:

- Si utiliza el terminal para una sesión de inicio interactiva mientras la consola auxiliar está activa, los mensajes de la consola se envían a los dispositivos `/dev/sysmsg` o `/dev/msglog`.

- Mientras introduce comandos en el terminal, la entrada se dirige a su sesión interactiva en lugar de a la consola predeterminada (`/dev/console`).
- Si ejecuta el comando `init` para cambiar los niveles de ejecución, el software de la consola remota cierra su sesión interactiva y ejecuta el programa `sulogin`. En este punto, se acepta únicamente la entrada del terminal y se la trata como si proviniera de un dispositivo de consola. Esto permite introducir la contraseña al programa `sulogin`, como se describe en "Uso de mensajes de la consola auxiliar durante las transiciones de nivel de ejecución" [46].

  A continuación, si introduce la contraseña correcta en el terminal (auxiliar), la consola auxiliar ejecuta una sesión interactiva `sulogin` y bloquea la consola predeterminada y cualquier consola auxiliar que genere conflicto. Esto significa que el terminal básicamente funciona como la consola del sistema.
- Desde aquí puede cambiar al nivel de ejecución 3 o ir a otro nivel de ejecución. Si cambia los niveles de ejecución, `sulogin` se ejecuta de nuevo en todos los dispositivos de consola. Si sale o especifica que el sistema debe alcanzar el nivel de ejecución 3, todas las consolas auxiliares pierden su capacidad para proporcionar entrada. Vuelven a funcionar como dispositivos de visualización para los mensajes de la consola.

  A medida que el sistema va cambiando de nivel, debe proporcionar la información a las secuencias de comandos `rc` en el dispositivo de consola predeterminado. Una vez que el sistema alcanza el nivel, el programa `login` se ejecuta en los puertos de serie, y se puede volver a iniciar una sesión interactiva. Si designó el dispositivo como consola auxiliar, seguirá teniendo mensajes de la consola en el terminal, pero todas las entradas del terminal se dirigen a su sesión interactiva.

▼ Cómo activar una consola auxiliar (remota)

El daemon `consadm` no empieza a controlar el puerto hasta que agrega la consola auxiliar con el comando `consadm`. Como función de seguridad, los mensajes de la consola sólo se vuelven a dirigir hasta que se descarta el portador o se anula la selección del dispositivo de consola auxiliar. Esto significa que el portador debe establecerse en el puerto antes de poder utilizar correctamente el comando `consadm`.

Para obtener más información sobre la activación de una consola auxiliar, consulte la página del comando man `consadm`(1m).

1. **Inicie sesión en el sistema y asuma el rol `root`.**

   Consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

2. **Active la consola auxiliar.**

   ```
   # consadm -a devicename
   ```

3. **Compruebe que la conexión actual sea la consola auxiliar.**

```
# consadm
```

ejemplo 5-3 Activación de una consola auxiliar (remota)

```
# consadm -a /dev/term/a
# consadm
 /dev/term/a
```

▼ Cómo mostrar una lista de consolas auxiliares

1. **Inicie sesión en el sistema y asuma el rol `root`.**

   Consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Seleccione uno de los siguientes pasos:**

   a. **Muestre la lista de consolas auxiliares.**

   ```
   # consadm
   /dev/term/a
   ```

   b. **Muestre la lista de consolas auxiliares persistentes.**

   ```
   # consadm -p
   /dev/term/b
   ```

▼ Cómo activar la consola auxiliar (remota) en los reinicios del sistema

1. **Inicie sesión en el sistema y asuma el rol `root`.**

   Consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Active la consola auxiliar en los reinicios del sistema.**

   `# consadm -a -p` *devicename*

   Así se agrega el dispositivo a la lista de consolas auxiliares persistentes.

3. **Compruebe que el dispositivo se haya agregado a la lista de consolas auxiliares persistentes.**

```
# consadm
```

ejemplo 5-4 Activación de una consola auxiliar (remota) en los reinicios del sistema

```
# consadm -a -p /dev/term/a
# consadm
/dev/term/a
```

▼ Cómo desactivar una consola auxiliar (remota)

1. **Inicie sesión en el sistema y asuma el rol `root`.**

   Consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Seleccione uno de los siguientes pasos:**

   a. **Desactivar la consola auxiliar.**

      ```
      # consadm -d devicename
      ```

      O

   b. **Desactive la consola auxiliar y elimínela de la lista de consolas auxiliares persistentes.**

      ```
      # consadm -p -d devicename
      ```

3. **Verifique que la consola auxiliar se haya desactivado.**

   ```
   # consadm
   ```

ejemplo 5-5 Desactivación de una consola auxiliar (remota)

```
# consadm -d /dev/term/a
# consadm
```

Índice

V