Gestión de auditoría en Oracle® Solaris 11.2

Referencia: E53973
Julio de 2014

Contenido

Uso de esta documentación

Gestión de auditoría en Oracle® Solaris 11.2 documenta la función de auditoría de Oracle Solaris.

- **Descripción general**: describe cómo administrar la auditoría en un sistema o en una red de sistemas Oracle Solaris.
- **Destinatarios**: los administradores del sistema que deben implementar la seguridad en la empresa.
- **Conocimiento requerido**: estar familiarizado con terminología y conceptos de seguridad.

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

Acerca de la auditoría en Oracle Solaris

El subsistema de auditoría de Oracle Solaris mantiene un registro de cómo se está utilizando el sistema. El servicio de auditoría incluye herramientas para ayudar con el análisis de los datos de auditoría.

En este capítulo, se presenta cómo funciona la auditoría en el Oracle Solaris:

Para obtener sugerencias de planificación, consulte el Capítulo 2, Planificación de la auditoría. Si desea conocer los procedimientos para configurar la auditoría en su sitio, consulte los capítulos siguientes:

Para obtener información de referencia, consulte el Capítulo 7, Referencia sobre auditoría.

Novedades del servicio de auditoría de Oracle Solaris

En esta sección, se destaca información para los clientes existentes sobre nuevas funciones importantes del servicio de auditoría de Oracle Solaris.

- Los registros de auditoría de un sistema Oracle Solaris se pueden conectar a Oracle Audit Vault and Database Firewall, que luego se puede utilizar para obtener información sobre los eventos auditados en los sistemas Oracle Solaris.

- Los archivos de configuración de auditoría `audit_class`, `audit_event` y `audit_warn`tienen dos atributos de paquete definidos. El atributo `preserve=renamenew` permite que los archivos se modifiquen, y las modificaciones se retienen en las actualizaciones de paquetes y en las correcciones de paquetes. El atributo `overlay=allow` permite que los archivos sean reemplazados por archivos en paquetes que crea un cliente.

¿Qué es la auditoría?

La auditoría es la recopilación de datos sobre el uso de los recursos del sistema. Los datos de auditoría proporcionan un registro de los eventos del sistema relacionados con la seguridad. Estos datos se pueden utilizar para asignar responsabilidad para acciones que ocurren en un host.

La auditoría correcta comienza con dos funciones de seguridad: identificación y autenticación. En cada inicio de sesión, después de que un usuario proporciona un nombre de usuario y la autenticación PAM (módulo de autenticación conectable) se realiza correctamente, se genera un *ID de usuario de auditoría* único e inmutable y se lo asocia con el usuario, y se genera un ID de sesión de auditoría único y se lo asocia con el proceso del usuario. El ID de sesión de auditoría es heredado por cada proceso que se inicia durante esa sesión de inicio de sesión. Cuando un usuario cambia a otro usuario, a todas las acciones del usuario se les realiza un seguimiento con el mismo ID de usuario de auditoría. Para obtener más detalles sobre cómo cambiar la identidad, consulte la página del comando man `su`(1M). Tenga en cuenta que, de manera predeterminada, ciertas acciones como el inicio y cierre del sistema siempre se auditan.

El servicio de auditoría hace que lo siguiente sea posible:

- Supervisión de eventos relacionados con la seguridad que ocurren en el host
- Registro de los eventos en una pista de auditoría de toda la red
- Detección de uso incorrecto o actividad no autorizada
- Revisión de patrones de acceso e historiales de acceso de personas y objetos
- Detección de intentos para eludir los mecanismos de protección
- Detección de uso ampliado de privilegio que se produce cuando un usuario cambia la identidad

Nota - Para mantener la seguridad, no todos los eventos auditados se pueden ver, por ejemplo, las contraseñas modificadas. Para obtener más información, consulte “Registros de auditoría y tokens de auditoría” [15].

Conceptos y terminología de auditoría

Los siguientes términos se usan para describir el servicio de auditoría. Algunas definiciones incluyen enlaces a descripciones más completas.

clase de auditoría

Una agrupación de eventos de auditoría. Las clases de auditoría proporcionan una forma de seleccionar un grupo de eventos que se van a auditar.

Para obtener más información, consulte "Clases de auditoría y preselección" [14] y las páginas del comando man `audit_flags`(5), `audit_class`(4) y `audit_event`(4).

sistema de archivos de auditoría

Un repositorio de archivos de auditoría en formato binario.

Para obtener más información, consulte "Logs de auditoría" [17] y la página del comando man `audit.log`(4).

evento de auditoría

Una acción del sistema relacionada con la seguridad que se puede auditar. Para una mayor facilidad de selección, los eventos se agrupan en clases de auditoría.

Para obtener más información, consulte "Eventos de auditoría" [13] y la página del comando man `audit_event`(4).

indicador de auditoría

Una clase de auditoría que se proporciona como un argumento para un comando o palabra clave. Un indicador puede estar precedido de un signo más o signo menos para indicar que la clase se audita para determinar si es correcta (+) o tiene fallos (-). Un signo de intercalación (^) indica que no se debe auditar una clase correcta (^+) o que no se debe auditar una clase con fallos (^-).

Para obtener más información, consulte la página del comando man `audit_flags`(5) y "Sintaxis de la clase de auditoría" [120].

complemento de auditoría

Un módulo que transfiere los registros de auditoría de la cola a una ubicación especificada. El complemento `audit_binfile` crea archivos de auditoría binarios. Los archivos de auditoría binarios incluyen la pista de auditoría, que está almacenada en sistemas de archivos de auditoría. El complemento `audit_remote` envía registros de auditoría binarios a un repositorio remoto. El complemento `audit_syslog` realiza un resumen de todos los registros de auditoría en los registros `syslog`.

Para obtener más información, consulte "Módulos de complemento de auditoría" [16] y las páginas del comando man de módulo, `audit_binfile`(5), `audit_remote`(5) y `audit_syslog`(5).

política de auditoría	Un conjunto de opciones de auditoría que puede activar o desactivar en el sitio. Puede especificar si determinados tipos de datos de auditoría se deben registrar y si desea suspender las acciones auditables cuando la cola de auditoría está llena. Para obtener más información, consulte “Comprensión de la política de auditoría” [35] y la página del comando man `auditconfig`(1M).
registro de auditoría	Datos de auditoría que se recopilan en la cola de auditoría. Un registro de auditoría describe un único evento de auditoría. Cada registro de auditoría se compone de tokens de auditoría. Para obtener más información, consulte “Registros de auditoría y tokens de auditoría” [15] y la página del comando man `audit.log`(4).
token de auditoría	Un campo de un evento o registro de auditoría. Cada token de auditoría describe un atributo de un evento de auditoría, como un usuario, un grupo, un programa u otro objeto. Para obtener más información, consulte “Formatos de token de auditoría” [127] y la página del comando man `audit.log`(4).
pista de auditoría	Una colección de uno o más archivos de auditoría que almacenan los datos de auditoría de todos los sistemas auditados que utilizan el complemento predeterminado, `audit_binfile`. Para obtener más información, consulte “Pista de auditoría” [125].
auditoría local	Recopilación de registros de auditoría que se generan en el sistema local. Los registros se pueden generar en la zona global, en las zonas no globales o en ambos lugares. Para obtener más información, consulte “Módulos de complemento de auditoría” [16].
selección posterior	La elección de qué eventos de auditoría se deben examinar en la pista de auditoría. El complemento activo predeterminado, `audit_binfile` , crea la pista de auditoría. Una herramienta de selección posterior, el comando `auditreduce`, selecciona registros de la pista de auditoría. Para obtener más información, consulte las páginas del comando man `auditreduce`(1M) y `praudit`(1M).
preselección	La elección de qué clases de auditoría se deben supervisar. Los eventos de auditoría de clases de auditoría preseleccionadas se recopilan en la cola de auditoría. Las clases de auditoría que no se preseleccionan no se auditan, por lo que sus eventos no aparecen en la cola.

Para obtener más información, consulte “Clases de auditoría y preselección” [14] y las páginas del comando man `audit_flags`(5) y `auditconfig`(1M).

objeto público

Un archivo que es propiedad del usuario `root` y que todos pueden leer. Por ejemplo, los archivos en el directorio `/etc` y el directorio `/usr/bin` son objetos públicos. Los objetos públicos no se auditan en eventos de sólo lectura. Por ejemplo, incluso si la clase de auditoría `file_read` (`fr`) está preseleccionada, la lectura de objetos públicos no se audita. Puede sustituir el valor predeterminado cambiando la opción de política de auditoría `public`.

auditoría remota

Servidor de auditoría remota (Audit Remote Server, ARS) que recibe y almacena los registros de auditoría de un sistema que se está auditando y se configura con un complemento `audit_remote` activo. Para distinguir un sistema auditado de un ARS, se puede hacer referencia al sistema auditado como “sistema auditado localmente”.

Para obtener más información, consulte las opciones `-setremote` en la página del comando man `auditconfig`(1M) y en “Servidor de auditoría remoto” [121].

Eventos de auditoría

Los eventos de auditoría representan acciones que se pueden auditar en un sistema. Los eventos de auditoría se muestran en el archivo `/etc/security/audit_event`. Cada evento de auditoría está conectado a una llamada del sistema o comando de usuario, y está asignado a una o más clases de auditoría. Para obtener una descripción del formato del archivo `audit_event`, consulte la página del comando man `audit_event`(4).

Por ejemplo, el evento de auditoría `AUE_EXECVE` audita la llamada del sistema `execve()`. El comando `auditrecord -e execve` muestra esta entrada:

```
# auditrecord -e execve
execve
system call execve              See execve(2)
event ID    23                  AUE_EXECVE
class       ps,ex               (0x0000000040100000)
header
path
[attribute]                 omitted on error
[exec_arguments]            output if argv policy is set
[exec_environment]          output if arge policy is set
subject
[use_of_privilege]
```

`return`

Cuando preselecciona la clase de auditoría `ps` o la clase de auditoría `ex`, entonces cada llamada del sistema `execve()` se registra en la cola de auditoría.

La auditoría maneja eventos *atribuibles* y *no atribuibles*. La política de auditoría divide los eventos en *síncronos* y *asíncronos*, de la siguiente manera:

- **Eventos atribuibles**: eventos que se pueden atribuir a un usuario. La llamada del sistema `execve()` se puede atribuir a un usuario, por lo tanto, se considera un evento atribuible. Todos los eventos atribuibles son eventos síncronos.
- **Eventos no atribuibles**: eventos que ocurren en el nivel de interrupción del núcleo o antes de que un usuario sea autenticado. La clase de auditoría `na` maneja los eventos de auditoría que no son atribuibles. Por ejemplo, el inicio del sistema es un evento no atribuible. La mayoría de los eventos no atribuibles son eventos asíncronos. Sin embargo, los eventos no atribuibles que tienen procesos asociados, como un inicio de sesión fallido, son eventos síncronos.
- **Eventos síncronos**: eventos que están asociados con un proceso en el sistema. La mayoría de los eventos del sistema son eventos síncronos.
- **Eventos asíncronos**: eventos que no están asociados con ningún proceso, por lo que no hay ningún proceso disponible para bloquear y más tarde iniciar. Los eventos de salida y entrada de la PROM, y de inicio del sistema inicial son ejemplos de eventos asíncronos.

Además de los eventos de auditoría que define el servicio de auditoría, las aplicaciones de terceros pueden generar eventos de auditoría. Los números de evento de auditoría de 32768 a 65535 están disponibles para aplicaciones de terceros. Los proveedores necesitan ponerse en contacto con sus representantes de Oracle Solaris para reservar números de evento y obtener acceso a las interfaces de auditoría.

Clases de auditoría y preselección

Cada uno de los eventos de auditoría pertenece a una *clase de auditoría*. Las clases de auditoría son contenedores prácticos para un gran número de eventos de auditoría. Cuando se *preselecciona* una clase para auditar, todos los eventos de esa clase se registran en la cola de auditoría. Por ejemplo, cuando preselecciona la clase de auditoría `ps`, se registran `execve()`, `fork ()` y otras llamadas del sistema.

Puede preseleccionar para eventos de un sistema y para eventos iniciados por un usuario concreto.

- **Preselección en todo el sistema:** especifique los valores predeterminados en todo el sistema para auditoría mediante las opciones `-setflags` y `-setnaflags` para el comando `auditconfig`.

Nota - Si la política `perzone` está establecida, se pueden especificar las clases de auditoría predeterminadas en cada zona. Para la auditoría `perzone`, los valores predeterminados son para toda la zona y no para todo el sistema.

- **Preselección específica del usuario:** especifique diferencias de valores predeterminados de auditoría en todo el sistema para usuarios individuales mediante la configuración de los indicadores de auditoría para el usuario. Los comandos `useradd`, `roleadd`, `usermod` y `rolemod` ubican el atributo de seguridad `audit_flags` en la base de datos `user_attr`. El comando `profiles` ubica indicadores de auditoría para los perfiles de derechos en la base de datos `prof_attr`.

  La máscara de preselección de auditoría determina las clases de eventos que se auditarán para un usuario. Para obtener una descripción de la máscara de preselección de usuario, consulte “Características del proceso de auditoría” [124]. Para conocer los indicadores de auditoría configurados que se utilizan, consulte “Orden de búsqueda para derechos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

Las clases de auditoría se definen en el archivo `/etc/security/audit_class`. Cada entrada contiene la máscara de auditoría para la clase, el nombre para la clase y un nombre descriptivo para la clase. Por ejemplo, las definiciones de clase `lo` y `ps` aparecen en el archivo `audit_class`, de la siguiente manera:

```
0x0000000000001000:lo:login or logout
0x0000000000100000:ps:process start/stop
```

Las clases de auditoría incluyen dos clases globales: `all` y `no`. Las clases de auditoría se describen en la página del comando man `audit_class`(4). Para la lista de clases, lea el archivo `/etc/security/audit_class`.

La asignación de eventos de auditoría a clases es configurable. Puede eliminar eventos de una clase, agregar eventos a una clase y crear una nueva clase para colocar eventos seleccionados. Para conocer el procedimiento, consulte Cómo cambiar una pertenencia a clase de un evento de auditoría [58]. Para ver los eventos que se asignan a una clase, utilice el comando `auditrecord -c` *clase*.

Registros de auditoría y tokens de auditoría

Cada *registro de auditoría* registra la aparición de un único evento auditado. El registro incluye información, como quién realizó la acción, qué archivos fueron afectados, qué acción se intentó realizar y dónde y cuándo ocurrió la acción. El siguiente ejemplo muestra un registro de auditoría `login` con tres tokens: `header`, `subject` y `return`:

```
header,69,2,login - local,,example_system,2010-10-10 10:10:10.020 -07:00
subject,jdoe,jdoe,staff,jdoe,staff,1210,4076076536,69 2 example_system
```

```
return,success,0
```

El tipo de información que se guarda para cada uno de los eventos de auditoría se define mediante un conjunto de *tokens de auditoría*. Cada vez que un registro de auditoría se crea para un evento, el registro contiene algunos de los tokens o todos los tokens que se definen para el evento. La naturaleza del evento determina qué tokens se registran. En el ejemplo anterior, cada línea empieza con el nombre del token de auditoría. El contenido del token de auditoría sigue al nombre del token. Juntos, los tokens de auditoría `header`, `subject` y `return` componen el registro de auditoría `login - local`. Para mostrar los tokens que componen un registro de auditoría, utilice el comando `auditrecord -e` *event*.

Nota - El contenido y los cambios de contenido de los archivos con el atributo del sistema `sensitive` no se incluyen en el registro de auditoría. Este atributo garantiza que nadie pueda acceder a información confidencial, como contraseñas, PIN, claves, etc., en archivos específicos. Para obtener más información, consulte la página del comando man `pfedit`(1M).

Para obtener una descripción detallada de la estructura de cada token de auditoría con un ejemplo de salida de `praudit`, consulte “Formatos de token de auditoría” [127]. Para obtener una descripción de la cadena binaria de tokens de auditoría, consulte la página del comando man `audit.log`(4).

Módulos de complemento de auditoría

Los módulos de complemento de auditoría dirigen los registros de auditoría de la cola de auditoría a un archivo o repositorio. Al menos un complemento debe estar activo. De manera predeterminada, el complemento `audit_binfile` está activo. Se configuran complementos con el comando `auditconfig -setplugin` *plugin-name*.

El servicio de auditoría proporciona los siguientes complementos:

- Complemento `audit_binfile`: maneja la entrega de la cola de la auditoría a los archivos de auditoría binarios. Para obtener más información, consulte la página del comando man `audit.log`(4).
- Complemento `audit_remote`: maneja la entrega segura de registros de auditoría binarios de la cola de auditoría a un servidor remoto configurado. El complemento `audit_remote` utiliza la biblioteca `libgss()` para autenticar el servidor. La transmisión está protegida para privacidad e integridad.
- Complemento `audit_syslog`: maneja la entrega de registros seleccionados de la cola de auditoría a los registros `syslog`.

Para obtener información sobre cómo configurar un complemento, consulte la página del comando man `auditconfig`(1M). Para ver ejemplos de configuración de complementos,

consulte las tareas en “Configuración de logs de auditoría” [75]. Para obtener información sobre los complementos, consulte las páginas del comando man `audit_binfile`(5), `audit_remote`(5) y `audit_syslog`(5).

Logs de auditoría

Los registros de auditoría se recopilan en registros de auditoría. El servicio de auditoría proporciona tres modos de salida para los registros de auditoría.

- Los registros que se denominan *archivos de auditoría* almacenan registros de auditoría en formato binario. El conjunto de archivos de auditoría de un sistema o sitio proporciona un registro de auditoría completo. El registro de auditoría completo se denomina *pista de auditoría*. Estos registros se crean mediante el complemento `audit_binfile` y pueden ser revisados por los comandos `praudit` y `auditreduce` de selección posterior.
- El complemento `audit_remote` envía registros de auditoría a un repositorio remoto. El repositorio es responsable de mantener una pista de auditoría y de suministrar herramientas de selección posterior.
- La utilidad `syslog` recopila y almacena resúmenes de texto del registro de auditoría. Un registro `syslog` no está completo. El siguiente ejemplo muestra una entrada `syslog` para un registro de auditoría `login`:

```
Oct 10  10:10:20 example_system auditd: [ID 6472 audit.notice] \
login - login ok session 4076172534 by root as root:other
```

Un sitio puede configurar la auditoría para recopilar registros de auditoría en todos los formatos. Puede configurar los sistemas en su sitio para que usen el modo binario localmente, para que envíen archivos binarios a un repositorio remoto y para usar el modo `syslog`. En la siguiente tabla, se comparan registros de auditoría binarios con registros de auditoría `syslog`.

TABLA 1-1 Comparación de registros de auditoría binarios, remotos y `syslog`

Característica	Registros binarios y remotos	Registros `syslog`
Protocolo	Binario: escribe en el sistema de archivos Remoto: envía a un repositorio remoto	Utiliza UDP para el registro remoto
Tipo de datos	Binarios	Texto
Longitud de registro	Sin límite	Hasta 1024 caracteres por registro de auditoría
Ubicación	Binaria: almacenados en un `zpool` en el sistema Remota: repositorio remoto	Se almacenan en una ubicación que se especifica en el archivo `syslog.conf`
Cómo configurar	Binario: se define el atributo `p_dir` en el complemento `audit_binfile`	Se activa el complemento `audit_syslog` y se configura el archivo `syslog.conf`

Característica	Registros binarios y remotos	Registros `syslog`
	Remoto: se define el atributo `p_hosts` en el complemento `audit_remote` y se hace que se active el complemento	
Cómo leer	Binario: normalmente, en modo de lote, salida del explorador en XML	En tiempo real o se buscan mediante secuencias de comandos creadas para `syslog`
	Remoto: el repositorio dicta el procedimiento	Salida de texto sin formato
Integridad	Se garantiza que estén completos y que aparezcan en el orden correcto	No se garantiza que estén completos
Indicación de hora	Hora universal coordinada (UTC)	Hora en el sistema que se audita

Para obtener más información sobre complementos y registros de auditoría, consulte lo siguiente:

- Página del comando man `audit_binfile`(5)
- Página del comando man `audit_syslog`(5)
- Página del comando man `audit.log`(4)
- Cómo asignar espacio de auditoría para la pista de auditoría [80]
- Cómo configurar registros de auditoría `syslog` [89]

Acerca de los registros binarios

Los registros binarios proporcionan la mayor seguridad y cobertura. La salida binaria cumple con los requisitos de las certificaciones de seguridad, como los requisitos de auditoría Common Criteria (http://www.commoncriteriaportal.org/).

El complemento `audit_binfile` escribe los registros en un sistema de archivos que tiene protección para no ser vistos. En un único sistema, todos los registros binarios se recopilan y se muestran en orden. La indicación de hora del UTC en registros binarios permite realizar una comparación exacta cuando los sistemas en una pista de auditoría se distribuyen entre zonas horarias. El comando `praudit -x` permite ver los registros en un explorador, en XML. También puede utilizar secuencias de comandos para analizar la salida XML.

El complemento `audit_remote` escribe registros de auditoría en un repositorio remoto. El repositorio maneja el almacenamiento y la selección posterior.

Acerca de los registros de auditoría `syslog`

En contraste, es posible que los registros `syslog` proporcionen una mayor comodidad y flexibilidad. Por ejemplo, puede recopilar los datos de `syslog` de un gran variedad de orígenes. Además, al supervisar eventos `audit.notice` en el archivo `syslog.conf`, la utilidad `syslog`

registra un resumen de registros de auditoría con la indicación de hora actual. Puede utilizar las mismas herramientas de análisis y de gestión que ha desarrollado para mensajes `syslog` de una gran variedad de orígenes, incluidos estaciones de trabajo, servidores, cortafuegos y enrutadores. Los registros se pueden consultar en tiempo real y se pueden almacenar en un sistema remoto.

Si usa `syslog.conf` para almacenar registros de auditoría de manera remota, está protegiendo los datos del registro para evitar que los modifique o suprima un agresor. Sin embargo, tenga en cuenta los siguientes inconvenientes para el modo `syslog`.

- Los registros son susceptibles a ataques de red, como denegación de servicio y direcciones de origen suplantadas.
- El protocolo UDP puede eliminar paquetes o puede entregar paquetes que no funcionan.
- El límite de 1.024 caracteres para las entradas `syslog` puede provocar que algunos registros de auditoría se trunquen en el log.
- En un único sistema, no se recopilan todos los registros de auditoría, y es posible que estos no se muestren en orden.
- En cada registro de auditoría, se registran la fecha y la hora del sistema local. Por lo tanto, no puede basarse en el registro de hora para construir una pista de auditoría para varios sistemas.

Almacenamiento y gestión de la pista de auditoría

Cuando el complemento `audit_binfile` está activo, un *sistema de archivos de auditoría* mantiene los archivos de auditoría en formato binario. Una instalación típica utiliza el sistema de archivos `/var/audit` y puede usar sistemas de archivos adicionales. El contenido de todos los sistemas de archivos de auditoría compone la *pista de auditoría*. Los registros de auditoría se almacenan en estos sistemas de archivos en el siguiente orden:

- **Sistema de archivos de auditoría primario:** el sistema `/var/audit`, el sistema de archivos predeterminado para archivos de auditoría de un sistema
- **Sistemas de archivos de auditoría secundarios:** sistemas de archivos donde los archivos de auditoría para un sistema se ubican según el criterio del administrador

Los sistemas de archivos se especifican como argumentos para el atributo `p_dir` del complemento `audit_binfile`. Un sistema de archivos no se utiliza hasta que un sistema de archivos que está antes en la lista esté lleno. Para ver un ejemplo con una lista de las entradas del sistema de archivos, consulte Cómo crear sistemas de archivos ZFS para archivos de auditoría [76].

Colocar los archivos de auditoría en el directorio raíz de auditoría predeterminado ayuda al revisor de auditoría cuando revisa la pista de auditoría. El comando `auditreduce` usa el directorio raíz de auditoría para encontrar todos los archivos en la pista de auditoría. El directorio raíz de auditoría predeterminado es `/var/audit`.

Puede utilizar las siguientes opciones con el comando `auditreduce`:

- La opción `-M` para el comando `auditreduce` se puede utilizar a fin de especificar archivos de auditoría de un equipo específico.
- La opción `-S` se puede utilizar para especificar un sistema de archivos de auditoría diferente.

Para obtener ejemplos del uso del comando `auditreduce`, consulte Cómo fusionar archivos de auditoría de la pista de auditoría [102]. Para obtener más información, consulte la página del comando man `auditreduce`(1M).

El servicio de auditoría proporciona comandos para combinar y filtrar archivos de la pista de auditoría. El comando `auditreduce` puede fusionar archivos de auditoría de la pista de auditoría. El comando también puede filtrar archivos para localizar eventos particulares. El comando `praudit` lee los archivos binarios. Las opciones para el comando `praudit` ofrecen una salida que es adecuada para las secuencias de comandos y para la presentación del explorador.

Indicaciones de hora confiables

Al fusionar registros de auditoría de varios sistemas, la fecha y la hora en esos sistemas deben ser exactas. De manera similar, al enviar registros de auditoría a un sistema remoto, el sistema de registro y sistema de repositorio deben tener relojes precisos. El protocolo de hora de red (NTP) mantiene relojes del sistema precisos y coordinados. Para obtener más información, consulte el Capítulo 3, “Servicios relacionados con el tiempo” de “Introducción a los servicios de red de Oracle Solaris 11.2 ” y la página del comando man `xntpd` (1M).

Gestión de un repositorio remoto

Una vez que se configura el complemento `audit_remote`, un repositorio remoto recibe los registros de auditoría. El ARS proporciona un receptor para los registros de auditoría. Los registros de auditoría pasan al ARS mediante una conexión protegida y se pueden almacenar de forma similar a como se almacenan localmente. Para configurar un ARS, consulte Cómo configurar un repositorio remoto para los archivos de auditoría [85]. Para obtener una descripción del ARS, consulte la página del comando man “Servidor de auditoría remoto” [121] and the `ars`(5).

¿Cómo se relaciona la auditoría con la seguridad?

La auditoría ayuda a detectar posibles brechas de seguridad al revelar patrones sospechosos o anómalos del uso del sistema. La auditoría también proporciona un medio para rastrear acciones

sospechosas de un usuario concreto, lo que sirve como elemento de disuasión. Es decir, es menos probable que los usuarios que saben que sus actividades se están auditando intenten realizar actividades maliciosas.

Para proteger un sistema informático, especialmente un sistema en una red, se requieren mecanismos que controlan las actividades antes de que comiencen los procesos del sistema o del usuario. La seguridad requiere herramientas que supervisan las actividades a medida que se producen. También requiere informes de actividades después de que las actividades ocurren.

Establezca la opción S en los parámetros de auditoría antes de que los usuarios inicien sesión o se inicien procesos del sistema, porque la mayoría de las actividades de auditoría incluyen la supervisión de eventos actuales y el registro de eventos que cumplen con parámetros especificados. Cómo el servicio de auditoría supervisa e informa estos eventos se trata detalladamente en el Capítulo 2, Planificación de la auditoría y en el Capítulo 3, Gestión del servicio de auditoría.

La auditoría no puede evitar que los piratas informáticos entren de manera no autorizada. Sin embargo, el servicio de auditoría puede informar, por ejemplo, que un usuario específico realizó acciones específicas a una hora y en una fecha concretas. El informe de auditoría puede identificar al usuario por ruta de entrada y nombre de usuario. Dicha información se puede informar de inmediato en su terminal y en un archivo para su análisis posterior. Por lo tanto, el servicio de auditoría proporciona datos que ayudan a determinar lo siguiente:

- Cómo se comprometió la seguridad del sistema
- Qué espacios de bucle se deben cerrar para garantizar el nivel de seguridad deseado

¿Cómo funciona la auditoría?

La auditoría genera registros de auditoría cuando se producen eventos especificados. Habitualmente, los eventos que generan registros de auditoría incluyen los siguientes:

- Inicio y cierre del sistema
- Inicio y cierre de sesión
- Creación o destrucción de proceso, o creación o destrucción de subproceso
- Apertura, cierre, creación, destrucción o cambio de nombre de objetos
- Uso de derechos
- Acciones de identificación y de autenticación
- Cambios de permiso por un proceso o usuario
- Acciones administrativas, como la instalación de un paquete
- Aplicaciones específicas de sitio

Los registros de auditoría se generan a partir de tres orígenes:

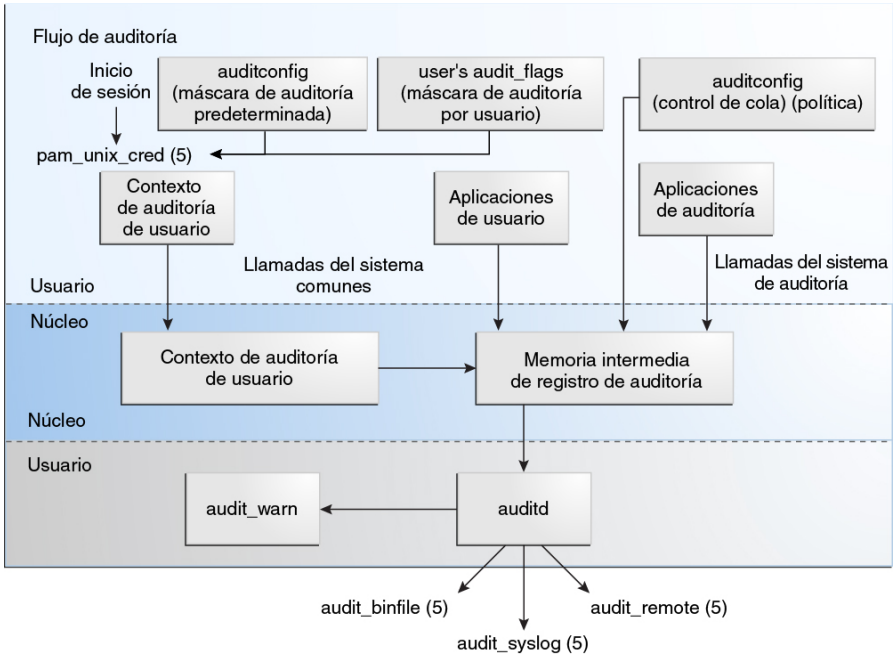
- Por una aplicación
- Como resultado de un evento asíncrono de auditoría
- Como resultado de una llamada del sistema de proceso

Una vez que la información de evento pertinente se ha capturado, la información se formatea en un registro de auditoría. En cada registro de auditoría, se incluye información que identifica el evento, qué generó el evento, la hora del evento y otra información relevante. Este registro se coloca en una cola de auditoría y se envía a los *complementos* activos para su almacenamiento. Al menos un complemento debe estar activo, aunque todos los complementos pueden estar activos. Los complementos se describen en "¿Cómo se configura la auditoría?" [22] y en "Módulos de complemento de auditoría" [16].

¿Cómo se configura la auditoría?

Durante la configuración del sistema, *preselecciona* las clases de registros de auditoría que desea supervisar. También puede ajustar el grado de auditoría que se realiza para usuarios individuales. En la siguiente figura, se muestran los detalles del flujo de auditoría en Oracle Solaris.

FIGURA 1-1 Flujo de auditoría



Después de que los datos de auditoría se recopilan en el núcleo, los complementos distribuyen los datos a las ubicaciones adecuadas.

- El complemento `audit_binfile` ubica registros de auditoría binarios en el sistema de archivos `/var/audit`. De manera predeterminada, el complemento `audit_binfile` está activo. Las herramientas de selección posterior permiten examinar partes interesantes de la pista de auditoría.

  Los archivos de auditoría se pueden almacenar en una o más agrupaciones ZFS. Estas agrupaciones pueden estar en diferentes sistemas y en redes diferentes pero que estén relacionadas. La recopilación de archivos de auditoría que están enlazados se considera una *pista de auditoría*.
- El complemento `audit_remote` envía registros de auditoría binarios a través de un enlace protegido a un repositorio remoto.
- El complemento `audit_syslog` envía resúmenes de texto de registros de auditoría a la utilidad `syslog`.

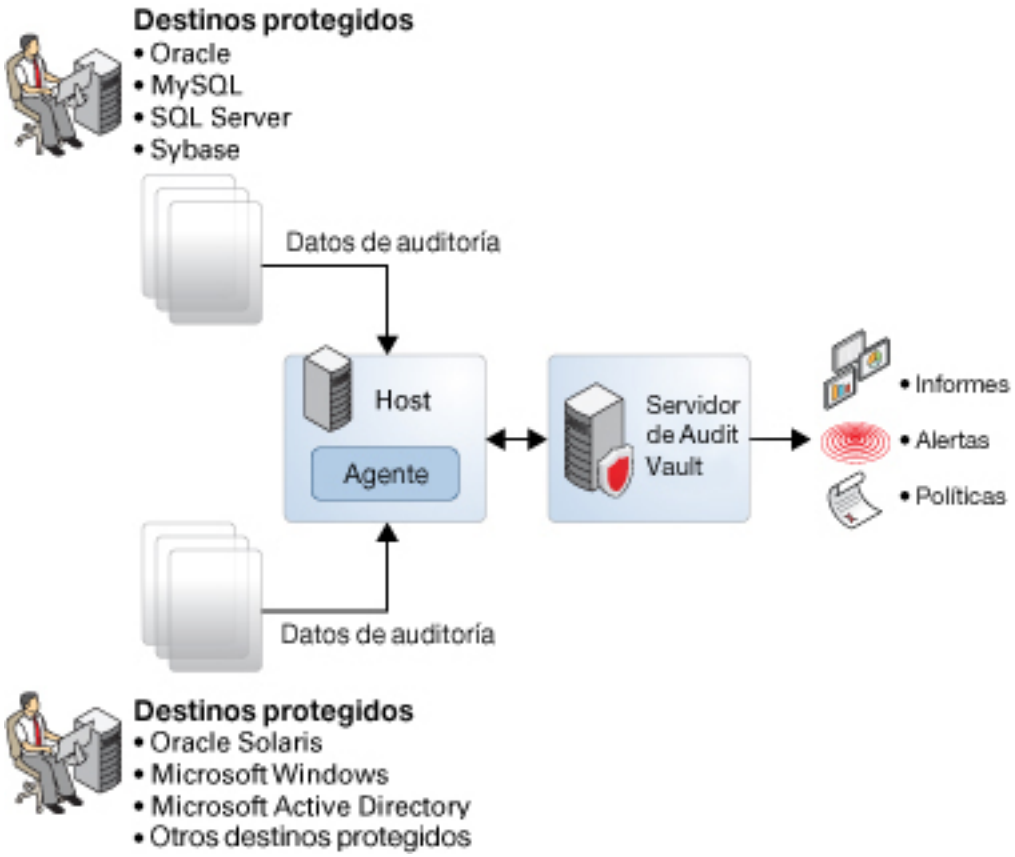
Los sistemas que instalan zonas no globales pueden auditar todas las zonas de forma idéntica desde la zona global. Estos sistemas también se pueden configurar para recopilar diferentes registros en las zonas no globales. Para obtener más información, consulte “Auditoría y Oracle Solaris Zones” [119].

Uso de Oracle Audit Vault and Database Firewall para el almacenamiento y el análisis de registros de auditoría

Los registros de auditoría de un sistema Oracle Solaris se pueden conectar a Oracle Audit Vault and Database Firewall versión 12.1.0.0. Oracle Audit Vault and Database Firewall automatiza la consolidación y la supervisión de datos de auditoría de bases de datos de Oracle y que no pertenecen a Oracle. A continuación, Oracle Audit Vault and Database Firewall se puede utilizar para análisis e informes de eventos auditados en los sistemas Oracle Solaris. Para obtener más información, consulte Oracle Audit Vault and Database Firewall (http://www.oracle.com/technetwork/products/audit-vault/overview/index.html).

En la siguiente figura, se muestra cómo Oracle Audit Vault and Database Firewall recopila registros de auditoría de Oracle Solaris desde los destinos seguros designados. Un destino seguro es cualquier sistema que almacena datos o registros de auditoría.

FIGURA 1-2 Oracle Solaris y Audit Vault



Un host se designa para ejecutar el agente de AV que se comunica con Oracle Audit Vault and Database Firewall. El agente permite que Oracle Audit Vault and Database Firewall reciba y procese datos de auditoría de destinos seguros. El agente lee los registros de auditoría de una pista de auditoría designada en el destino seguro. Estos registros de auditoría están codificados en formato binario nativo. El agente convierte los datos a un formato analizable por Oracle Audit Vault and Database Firewall. Oracle Audit Vault and Database Firewall recibe los datos y genera informes para los administradores y los gestores de seguridad según sea necesario.

El agente se puede instalar en un destino seguro en lugar de un host o sistema distinto. También se pueden configurar varios hosts con agentes para que se conecten al servidor de Audit Vault. Sin embargo, cuando registre los destinos seguros, indique un host específico con el que el servidor de AV se deba comunicar para obtener los datos de auditoría.

Para configurar Oracle Audit Vault and Database Firewall a fin de que acepte registros de auditoría de los destinos seguros de Oracle Solaris y que no pertenecen a Oracle Solaris, asegúrese de que el agente esté instalado y activado en el sistema host designado. Para obtener más información, consulte Oracle Audit Vault and Database Firewall documentation (http://www.oracle.com/technetwork/products/audit-vault/documentation/index.html).

Auditoría en un sistema con Oracle Solaris Zones

Una zona es un entorno de sistema operativo virtualizado que se crea dentro de una única instancia del Sistema operativo Oracle Solaris. El servicio de auditoría realiza la auditoría de la totalidad del sistema, incluidas las actividades en las zonas. Un sistema que ha instalado zonas no globales puede ejecutar un solo servicio de auditoría para auditar todas las zonas de manera idéntica o puede ejecutar un servicio de auditoría por zona, incluida la zona global.

Los sitios que cumplen con las siguientes condiciones pueden ejecutar un solo servicio de auditoría:

- El sitio requiere una pista de auditoría de única imagen.
- Las zonas no globales se utilizan como contenedores de aplicaciones. Las zonas forman parte de un dominio administrativo. Es decir, ninguna zona no global tiene archivos personalizados de servicio de nombres.

  Si todas las zonas en un sistema están dentro de un dominio administrativo, la política de auditoría `zonename` se puede utilizar para distinguir eventos de auditoría configurados en zonas distintas.
- Los administradores desean una baja sobrecarga de auditoría. El administrador de la zona global audita todas las zonas de manera idéntica. Además, el daemon de auditoría de la zona global presta servicio a todas las zonas en el sistema.

Los sitios que cumplen con las siguientes condiciones pueden ejecutar un servicio de auditoría por zona:

- El sitio no requiere una pista de auditoría de única imagen.
- Las zonas no globales tienen archivos personalizados de servicio de nombres. Esos dominios administrativos separados, normalmente, funcionan como servidores.
- Los administradores de zonas individuales desean controlar la auditoría en las zonas que administran. En la auditoría por zona, los administradores de zonas pueden decidir activar o desactivar la auditoría para la zona que administran.

Las ventajas de la auditoría por zona son una pista de auditoría personalizada para cada zona y la capacidad de desactivar la auditoría según la zona. Estas ventajas pueden ser contrarrestadas por la sobrecarga administrativa. Cada administrador de zona debe administrar la auditoría. Cada zona ejecuta su propio daemon de auditoría y tiene su propia cola de auditoría y sus propios registros de auditoría. Estos registros de auditoría se deben gestionar.

♦ ♦ ♦ CAPÍTULO 2

Planificación de la auditoría

En este capítulo, se describe cómo planificar la personalización del servicio de auditoría para su instalación de Oracle Solaris:

- “Conceptos de planificación para la auditoría” [27]
- “Planificación para auditoría” [30]
- “Comprensión de la política de auditoría” [35]
- “Control de costos de auditoría” [38]
- “Auditoría eficaz” [40]

Para obtener una descripción general de la auditoría, consulte el Capítulo 1, Acerca de la auditoría en Oracle Solaris. Si desea conocer los procedimientos para configurar la auditoría en su sitio, consulte los capítulos siguientes:

- Capítulo 3, Gestión del servicio de auditoría
- Capítulo 4, Supervisión de actividades del sistema
- Capítulo 5, Cómo trabajar con datos de auditoría
- Capítulo 6, Análisis y resolución de problemas del servicio de auditoría

Para obtener información de referencia, consulte el Capítulo 7, Referencia sobre auditoría.

Conceptos de planificación para la auditoría

Desea ser selectivo sobre los tipos de actividades que se auditan. Al mismo tiempo, desea recopilar información de auditoría útil. También debe planificar cuidadosamente a quién auditar y qué auditar. Si utiliza el complemento `audit_binfile` predeterminado, los archivos de auditoría pueden crecer rápidamente y llenar el espacio disponible, por lo que debe asignar suficiente espacio en disco.

Planificación de la pista de auditoría de un solo sistema

Nota - La implementación de la pista de auditoría de un solo sistema se aplica sólo al complemento `audit_binfile`.

Los sistemas dentro de un único dominio administrativo pueden crear una pista de auditoría de imagen de sistema único.

Para crear la pista de auditoría de la imagen de un solo sistema para un sitio, cumpla los siguientes requisitos:

- Utilice el mismo servicio de nombres para todos los sistemas.

  Para una interpretación correcta de los registros de auditoría, los archivos `passwd`, `group` y `hosts` deben ser coherentes.
- Configure el servicio de auditoría de manera idéntica en todos los sistemas. Para obtener información sobre la visualización y la modificación de la configuración del servicio, consulte la página del comando man `auditconfig`(1M).
- Utilice los mismos archivos `audit_warn`, `audit_event` y `audit_class` para todos los sistemas.

Consulte Cómo planificar a quién y qué auditar [30] para conocer consideraciones adicionales para activar la auditoría en los sistemas.

Planificación de la auditoría en zonas

Si su sistema contiene zonas no globales, las zonas se pueden auditar cuando se audita la zona global, o el servicio de auditoría para cada zona no global se puede configurar, activar y desactivar por separado. Por ejemplo, puede auditar sólo las zonas no globales sin auditar la zona global.

Para ver una explicación de las compensaciones, consulte “Auditoría en un sistema con Oracle Solaris Zones” [25].

Están disponibles las siguientes opciones al implementar la auditoría en zonas.

Implementación de un servicio de auditoría para todas las zonas

Auditar todas las zonas de manera idéntica puede crear una pista de auditoría de una sola imagen. Una pista de auditoría de imagen única se produce cuando utiliza `audit_binfile` o

el complemento `audit_remote`, y todas las zonas en un sistema son parte de un solo dominio administrativo. Los registros de auditoría se pueden comparar fácilmente porque los registros en cada zona están preseleccionados con valores de configuración idénticos.

Esta configuración trata todas las zonas como parte de un sistema. La zona global ejecuta el único servicio de auditoría en un sistema y recopila registros de auditoría para cada zona. Se personalizan los archivos `audit_class` y `audit_event` sólo en la zona global y, a continuación, se copian estos archivos en cada zona no global.

Utilice las siguientes directrices al configurar un único servicio de auditoría para todas las zonas.

- Utilice el mismo servicio de nombres para cada zona.

Nota - Si los archivos de servicio de nombres están personalizados en zonas no globales y la política `perzone` no está establecida, se requiere el uso cuidadoso de herramientas de auditoría para seleccionar registros utilizables. Un ID de usuario en una zona puede hacer referencia a un usuario diferente del mismo ID en una zona diferente.

- Permita que los registros de auditoría incluyan el nombre de la zona.

  Para colocar el nombre de zona como parte del registro de auditoría, establezca la política `zonename` en la zona global. El comando `auditreduce` podrá seleccionar luego los eventos de auditoría por zona de la pista de auditoría. Para obtener un ejemplo, consulte la página del comando man `auditreduce`(1M).

Para planificar una pista de auditoría de imagen única, consulte Cómo planificar a quién y qué auditar [30]. Comience con el primer paso. El administrador de la zona global también debe dejar a un lado el almacenamiento, como se describe en Cómo planificar espacio en el disco para los registros de auditoría [33].

Implementación de un servicio de auditoría por zona

Opte por configurar la auditoría por zona si diferentes zonas usan diferentes bases de datos de servicio de nombres o si los administradores de zonas desean controlar la auditoría en sus zonas.

Nota - Para auditar zonas no globales, se debe establecer la política `perzone`, pero el servicio de auditoría no tiene que estar activado en la zona global. La auditoría de la zona no global se configura y el servicio de auditoría se activa y desactiva independientemente de la zona global.

- Cuando se configura la auditoría por zona, se establece la política de auditoría `perzone` en la zona global. Si la auditoría por zona se establece antes de que se inicie por primera vez la zona no global, la auditoría comienza en el primer inicio de la zona. Para establecer una política de auditoría, consulte Cómo configurar la auditoría por zona [71].

- Cada administrador de zona configura la auditoría para la zona.

  Un administrador de zona no global puede establecer todas las opciones de política excepto `perzone` y `ahlt`.
- Cada administrador de zona puede activar o desactivar la auditoría en la zona.
- Para generar registros que puedan rastrearse a sus respectivas zonas de origen durante la revisión, establezca la política de auditoría `zonename`.

Nota - En la auditoría por zona, si el complemento `audit_binfile` está activo, cada administrador de zona también debe reservar el almacenamiento para cada zona, como se describe en Cómo planificar espacio en el disco para los registros de auditoría [33]. Para obtener instrucciones adicionales sobre planificación, consulte Cómo planificar a quién y qué auditar [30].

Planificación para auditoría

El siguiente mapa de tareas hace referencia a las tareas principales necesarias para planificar el espacio en disco y los eventos que se deben registrar.

TABLA 2-1 Mapa de tareas de planificación para auditoría

Tarea	Más instrucciones
Determinar a quién y qué auditar	Cómo planificar a quién y qué auditar [30]
Planificar espacio de almacenamiento para la pista de auditoría	Cómo planificar espacio en el disco para los registros de auditoría [33]
Planificar la transmisión de la pista de auditoría a un servidor remoto	Cómo prepararse para transmitir los registros de auditoría al almacenamiento remoto [34]

▼ Cómo planificar a quién y qué auditar

Antes de empezar Si implementa zonas no globales, consulte “Planificación de la auditoría en zonas” [28] antes de utilizar este procedimiento.

1. **Determine la política de auditoría.**

   De manera predeterminada, sólo la política `cnt` está activa.

   Utilice el comando `auditconfig -lspolicy` para ver una descripción de opciones de políticas disponibles.

   - Para ver los efectos de las opciones de política, consulte “Comprensión de la política de auditoría” [35].

- Para el efecto de la política `cnt`, consulte “Políticas de auditoría para eventos síncronos y asíncronos” [123].
- Para establecer una política de auditoría, consulte Cómo cambiar la política de auditoría [51].

2. **Determine si desea modificar asignaciones de evento-clase.**

   En la mayoría de las situaciones, la asignación predeterminada es suficiente. Sin embargo, si agrega nuevas clases, cambia las definiciones de clase o determina que un registro de una llamada del sistema específica no es útil, es posible que desee modificar asignaciones de evento-clase.

   Para obtener un ejemplo, consulte Cómo cambiar una pertenencia a clase de un evento de auditoría [58].

3. **Determine las clases de auditoría que se van preseleccionar.**

   La mejor hora para agregar clases de auditoría o cambiar las clases predeterminadas es antes de que los usuarios inicien sesión en el sistema.

   Las clases de auditoría que preselecciona con las opciones `-setflags` y `-setnaflags` para el comando `auditconfig` se aplican a todos los usuarios y procesos. Puede preseleccionar una clase para comprobar si es correcta, si tiene fallos o ambas cosas.

   Para la lista de clases de auditoría, lea el archivo `/etc/security/audit_class`.

4. **Determine modificaciones de usuario para preselecciones en todo el sistema.**

   Si ha decidido que algunos usuarios se deben auditar de manera diferente en el sistema, puede modificar el atributo de seguridad `audit_flags` para usuarios individuales o para un perfil de derechos. La máscara de preselección de usuario se modifica para los usuarios cuyos indicadores de auditoría se definen explícitamente o a quienes se les asigna un perfil de derechos con indicadores de auditoría explícitos.

   Para conocer el procedimiento, consulte Cómo configurar las características de auditoría de un usuario [47]. Para conocer los indicadores de auditoría que están vigentes, consulte “Orden de búsqueda para derechos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

5. **Decida cómo gestionar el alias de correo electrónico `audit_warn`.**

   La secuencia de comandos `audit_warn` se ejecuta siempre que el sistema de auditoría detecta una situación que requiere atención administrativa. De manera predeterminada, la secuencia de comandos `audit_warn` envía un correo electrónico al alias `audit_warn` y envía un mensaje a la consola.

   Para configurar el alias, consulte Cómo configurar el alias de correo electrónico `audit_warn` [55].

6. **Decidida en qué formato y dónde recopilar registros de auditoría.**

Dispone de tres opciones.

- De manera predeterminada, los registros de auditoría binarios se almacenan localmente. El directorio de almacenamiento predeterminado es `/var/audit`. Para más opciones de configuración del complemento `audit_binfile`, consulte Cómo crear sistemas de archivos ZFS para archivos de auditoría [76].
- Envíe registros de auditoría binarios a un repositorio protegido remoto mediante el complemento `audit_remote`. Debe tener un receptor para los registros. Para conocer los requisitos, consulte “Gestión de un repositorio remoto” [20]. Para conocer el procedimiento, consulte Cómo enviar archivos de auditoría a un repositorio remoto [83].
- Envíe resúmenes de registros de auditoría a `syslog` utilizando el complemento `audit_syslog`. Para conocer el procedimiento, consulte Cómo configurar registros de auditoría `syslog` [89].

  Para una comparación de formatos `syslog` y binarios, consulte “Logs de auditoría” [17].

7. Determine cuándo advertir al administrador sobre la reducción de espacio en disco.

Nota - Este paso se aplica sólo al complemento `audit_binfile`.

Cuando el espacio en disco en un sistema de archivos de auditoría está por debajo del porcentaje de espacio libre mínimo, o límite dinámico, el servicio de auditoría cambia al siguiente directorio de auditoría disponible. A continuación, el servicio envía una advertencia de que el límite variable se ha excedido.

Para ver cómo definir un porcentaje de espacio libre mínimo, consulte el Ejemplo 4-7, “Definición de un límite variable para advertencias”.

8. Decida la acción que se llevará a cabo cuando todos los directorios de auditoría estén completos.

Nota - Este paso se aplica sólo al complemento `audit_binfile`.

En la configuración predeterminada, el complemento `audit_binfile` está activo y la política `cnt` está establecida. En esta configuración, cuando la cola de auditoría de núcleo está completa, el sistema sigue funcionando. El sistema cuenta los registros de auditoría que se descartan, pero no registra los eventos. Para mayor seguridad, puede desactivar la política `cnt` y activar la política `ahlt`. La política `ahlt` detiene el sistema cuando un evento asíncrono no se puede ubicar en la cola de auditoría.

Sin embargo, si la cola `audit_binfile` está completa y la cola para otro complemento activo no está completa, entonces la cola del núcleo seguirá enviando registros al complemento que no está completo. Cuando la cola `audit_binfile` pueda aceptar registros nuevamente, el servicio de auditoría volverá a enviarlos allí.

Para ver una explicación de las opciones de política `cnt` y `ahlt`, consulte “Políticas de auditoría para eventos síncronos y asíncronos” [123]. Para ver cómo configurar estas opciones de política, consulte el Ejemplo 3-10, “Configuración de la opción de política de auditoría `ahlt`”.

Nota - La política `cnt` o `ahlt` no se activa si la cola para al menos un complemento está aceptando registros de auditoría.

Planificación del espacio en el disco para los registros de auditoría

El complemento `audit_binfile` crea una pista de auditoría. La pista de auditoría requiere espacio de archivo dedicado. Este espacio debe estar disponible y debe ser seguro. El sistema utiliza el sistema de archivos `/var/audit` para almacenamiento inicial. Puede configurar sistemas de archivos de auditoría adicionales para los archivos de auditoría. El siguiente procedimiento trata los problemas que debe resolver cuando planifica el almacenamiento de la pista de auditoría.

▼ Cómo planificar espacio en el disco para los registros de auditoría

Antes de empezar Si implementa zonas no globales, siga las instrucciones de “Planificación de la auditoría en zonas” [28] antes de utilizar este procedimiento.

En este procedimiento, se presupone que se utiliza el complemento `audit_binfile`.

1. **Determine cuánta auditoría necesita el sitio.**

   Equilibre las necesidades de seguridad del sitio con la disponibilidad de espacio en disco para la pista de auditoría.

   Para obtener indicaciones acerca de cómo reducir los requisitos de espacio manteniendo la seguridad del sitio y cómo diseñar el almacenamiento de auditoría, consulte “Control de costos de auditoría” [38] y “Auditoría eficaz” [40].

   Para obtener pasos prácticos, consulte “Volumen grande de registros de auditoría” [110], Cómo comprimir archivos de auditoría en un sistema de archivos dedicado [66] y el Ejemplo 5-4, “Combinación y reducción de archivos de auditoría”.

2. **Determine qué sistemas se van a auditar y configure sus sistemas de archivos de auditoría.**

   Cree una lista de todos los sistemas de archivos de auditoría que se van a utilizar. Para obtener directrices de configuración, consulte “Almacenamiento y gestión de la pista de auditoría” [19]

y la página del comando man auditreduce(1M). Para especificar los sistemas de archivos de auditoría, consulte Cómo asignar espacio de auditoría para la pista de auditoría [80].

3. **Sincronice los relojes en todos los sistemas.**
   Para obtener más información, consulte “Indicaciones de hora confiables” [20].

Preparación para transmitir los registros de auditoría al almacenamiento remoto

El complemento `audit_remote` envía la pista de auditoría binaria a un ARS en el mismo formato que el complemento `audit_binfile` escribe en los archivos de auditoría locales. El complemento `audit_remote` utiliza la biblioteca `libgss` para autenticar el ARS y un mecanismo GSS-API para proteger la transmisión con privacidad e integridad. Como referencia, consulte “¿Qué es el servicio Kerberos?” de “Gestión de Kerberos y otros servicios de autenticación en Oracle Solaris 11.2 ” y “Utilidades de Kerberos” de “Gestión de Kerberos y otros servicios de autenticación en Oracle Solaris 11.2 ”.

El único mecanismo GSS-API que se admite actualmente es `kerberosv5`. Para obtener más información, consulte la página del comando man mech(4).

▼ Cómo prepararse para transmitir los registros de auditoría al almacenamiento remoto

Nota - Si dispone de un dominio Kerberos configurado con un servidor de auditoría remoto (ARS) identificado y todos los sistemas auditados dentro del dominio, puede omitir este procedimiento. Los pasos para configurar el ARS y los sistemas auditados se incluyen en Cómo configurar un repositorio remoto para los archivos de auditoría [85] y Cómo enviar archivos de auditoría a un repositorio remoto [83].

Para verificar si se configuró un dominio Kerberos, emita el siguiente comando. La salida de ejemplo indica que Kerberos no está instalado en el sistema.

```
# pkg info system/security/kerberos-5
pkg: info: no packages matching these patterns are installed on the system.
```

Antes de empezar En este procedimiento, se presupone que se utiliza el complemento `audit_remote`.

1. **Instale el paquete del KDC (Centro de distribución de claves) maestro.**
   Puede utilizar el sistema que actuará como ARS o puede utilizar un sistema cercano. El ARS envía una cantidad considerable de tráfico de autenticación al KDC principal.

```
# pkg install pkg:/system/security/kerberos-5
```

En el KDC maestro, se usan los comandos `kdcmgr` y `kadmin` de Kerberos para gestionar el dominio. Para obtener más información, consulte las páginas del comando man `kdcmgr`(1M) y `kadmin`(1M).

2. **En cada sistema auditado que enviará registros de auditoría al ARS, instale el paquete KDC principal.**

```
# pkg install pkg:/system/security/kerberos-5
```

Este paquete incluye el comando `kclient`. En estos sistemas, ejecuta el comando `kclient` para conectarse con el KDC. Para obtener más información, consulte la página del comando man `kclient`(1M).

3. **Sincronice los relojes en el dominio de KDC.**

Si el sesgo de reloj es demasiado grande entre los sistemas auditados y el ARS, el intento de conexión fallará. Después de establecer una conexión, la hora local del ARS determina los nombres de los archivos de auditoría almacenados, como se describe en “Convenciones de nombres de archivos de auditoría binarios” [125].

Para obtener más información sobre los relojes, consulte “Indicaciones de hora confiables” [20].

Comprensión de la política de auditoría

La política de auditoría determina las características de los registros de auditoría para el sistema local. Puede utilizar el comando `auditconfig` para establecer estas políticas. Para obtener más información, consulte la página del comando man `auditconfig`(1M).

La mayoría de las opciones de política de auditoría están desactivadas de manera predeterminada para minimizar los requisitos de almacenamiento y las demandas de procesamiento del sistema. Estas opciones son propiedades del servicio de auditoría y determinan las políticas que están vigentes en el inicio del sistema. Para obtener más información, consulte la página del comando man `auditconfig`(1M).

Utilice la siguiente tabla para determinar si las necesidades de su sitio justifican la sobrecarga adicional que se genera como resultado de la activación de una o más opciones de política de auditoría.

TABLA 2-2 Efectos de opciones de política de auditoría

Nombre de la política	Descripción	Consideraciones de políticas
`ahlt`	Esta política se aplica sólo a eventos asíncronos. Cuando está desactivada, esta política permite que se complete el evento sin que se haya generado un registro de auditoría. Cuando está activada, esta política detiene el sistema cuando la cola de auditoría está completa. La intervención administrativa es necesaria para limpiar la cola de auditoría, liberar espacio para los registros de auditoría y reiniciar. Esta política sólo puede activarse en la zona global. La política afecta todas las zonas.	Se prefiere la opción desactivada cuando la disponibilidad del sistema es más importante que la seguridad. Se prefiere la opción activada en un entorno donde la seguridad es primordial. Para obtener más detalles, consulte “Políticas de auditoría para eventos síncronos y asíncronos” [123].
`arge`	Cuando está desactivada, esta política omite variables de entorno de un programa ejecutado del registro de auditoría `execve`. Cuando está activada, esta política agrega variables de entorno de un programa ejecutado al registro de auditoría `execve`. Los registros de auditoría resultantes contienen más detalles que cuando esta política está desactivada.	La opción desactivada recopila mucho menos información que la opción activada. Para una comparación, consulte Cómo auditar todos los comandos por usuarios [60]. Se prefiere la opción activada cuando se audita a unos pocos usuarios. La opción también resulta útil cuando no está seguro acerca de las variables de entorno que se utilizan en programas en la clase de auditoría `ex`.
`argv`	Cuando está desactivada, esta política omite argumentos de un programa ejecutado del registro de auditoría `execve`. Cuando está activada, esta política agrega argumentos de un programa ejecutado al registro de auditoría `execve`. Los registros de auditoría resultantes contienen más detalles que cuando esta política está desactivada.	La opción desactivada recopila mucho menos información que la opción activada. Para una comparación, consulte Cómo auditar todos los comandos por usuarios [60]. Se prefiere la opción activada cuando se audita a unos pocos usuarios. La opción también resulta útil cuando tiene motivos para creer que programas poco usuales se ejecutan en la clase de auditoría `ex`.
`cnt`	Cuando está desactivada, esta política bloquea un usuario o una aplicación para que no se ejecute. El bloqueo ocurre cuando los registros de auditoría no se pueden agregar a la pista de auditoría porque la cola de auditoría está completa. Cuando está activada, esta política permite que se complete el evento sin que se haya generado un registro de auditoría. La política mantiene un recuento de registros de auditoría que se descartan.	Se prefiere la opción desactivada en un entorno donde la seguridad es primordial. Se prefiere la opción activada cuando la disponibilidad del sistema es más importante que la seguridad. Para obtener más detalles, consulte “Políticas de auditoría para eventos síncronos y asíncronos” [123].
`group`	Cuando está desactivada, esta política no agrega una lista de grupos a los registros de auditoría. Cuando está activada, esta política agrega una lista de grupos a cada registro de auditoría como un token especial.	La opción desactivada normalmente satisface los requisitos de seguridad del sitio. Se prefiere la opción activada cuando necesita auditar los grupos suplementarios a los que pertenece el sujeto.
`path`	Cuando está desactivada, esta política registra en un registro de auditoría una ruta como máximo que se utiliza durante una llamada del sistema.	La opción desactivada ubica como máximo una ruta en un registro de auditoría.

Nombre de la política	Descripción	Consideraciones de políticas
	Cuando está activada, esta política registra cada ruta que se utiliza junto con un evento de auditoría para cada registro de auditoría.	La opción activada introduce cada nombre de archivo o ruta que se utiliza durante una llamada del sistema en el registro de auditoría como un token `path`.
`perzone`	Cuando está desactivada, esta política mantiene una única configuración de auditoría para un sistema. Un servicio de auditoría se ejecuta en la zona global. Los eventos de auditoría en zonas específicas se pueden ubicar en el registro de auditoría si el token de auditoría `zonename` estaba preseleccionado. Cuando está activada, esta política mantiene una configuración de auditoría, una cola de auditoría y registros de auditoría independientes para cada zona. Un servicio de auditoría se ejecuta en cada zona. Esta política se puede activar sólo en la zona global.	La opción desactivada es útil cuando no tiene una razón en especial para mantener un registro de auditoría, una cola y un daemon independientes para cada zona. La opción activada es útil cuando no puede supervisar el sistema eficazmente mediante un examen simple de registros de auditoría con el token de auditoría `zonename`.
`public`	Cuando está desactivada, esta política no agrega eventos de sólo lectura de objetos públicos a la pista de auditoría cuando la lectura de archivos está preseleccionada. Las clases de auditoría que contienen eventos de sólo lectura incluyen `fr`, `fa` y `cl`. Cuando está activada, esta política registra todos los eventos de auditoría de sólo lectura de objetos públicos si una clase de auditoría apropiada está preseleccionada.	La opción desactivada normalmente satisface los requisitos de seguridad del sitio. La opción activada rara vez es útil.
`seq`	Cuando está desactivada, esta política no agrega un número de secuencia a cada registro de auditoría. Cuando está activada, esta política agrega un número de secuencia a cada registro de auditoría. El token `sequence` contiene el número de secuencia.	La opción desactivada es suficiente si la auditoría se ejecuta sin problemas. Se prefiere la opción activada cuando la política `cnt` está activada. La política `seq` le permite determinar cuándo se descartan los datos. Como alternativa, puede utilizar el comando `auditstat` para ver registros descartados.
`trail`	Cuando está desactivada, esta política no agrega un token `trailer` a los registros de auditoría. Cuando está activada, esta política agrega un token `trailer` a cada registro de auditoría.	La opción desactivada crea un registro de auditoría más pequeño. La opción activada marca claramente el final de cada registro de auditoría con un token `trailer`. El token `trailer` se suele utilizar con el token `sequence`. El token `trailer` facilita la recuperación de pistas de auditoría dañadas.
`zonename`	Cuando está desactivada, esta política no incluye un token `zonename` en los registros de auditoría. Cuando está activada, esta política incluye un token `zonename` en cada registro de auditoría.	La opción desactivada es útil cuando no necesita hacer un seguimiento del comportamiento de auditoría por zonas. La opción activada es útil si desea aislar y comparar un comportamiento de auditoría entre

Nombre de la política	Descripción	Consideraciones de políticas
		zonas mediante la selección posterior de registros según la zona.

Control de costos de auditoría

Debido a que la auditoría consume recursos del sistema, debe controlar el grado de detalle que se registra. Cuando decide lo que se debe auditar, tenga en cuenta los siguientes costos de auditoría:

- Costo de mayor tiempo de procesamiento
- Costo de análisis de datos de auditoría

Si utiliza el complemento predeterminado, `audit_binfile`, también debe considerar el costo de almacenamiento de datos de auditoría.

Costo de mayor tiempo de procesamiento de datos de auditoría

El costo de mayor tiempo de procesamiento es el menos significativo de los costos de auditoría. La auditoría, por lo general, no se produce durante tareas de cálculos intensivos, como procesamiento de imágenes, cálculos complejos, etc. Si utiliza el complemento `audit_binfile`, los administradores de auditoría pueden mover las tareas de selección posterior del sistema auditado a sistemas que se dedican a analizar datos de auditoría. Finalmente, a menos que los sucesos del núcleo estén seleccionados previamente, el servicio de auditoría no tiene ningún impacto medible en el rendimiento del sistema.

Costo de análisis de datos de auditoría

El costo de análisis es más o menos proporcional a la cantidad de datos de auditoría que se recopilan. El costo de análisis incluye el tiempo que se necesita para fusionar y revisar los registros de auditoría.

Para los registros recopilados por el complemento `audit_binfile`, el costo también incluye el tiempo que se necesita para archivar los registros y sus bases de datos de servicios de nombres admitidas, y mantener los registros en un lugar seguro. Las bases de datos admitidas incluyen `groups`, `hosts` y `passwd`.

Cuantos menos registros se generan, menor es el tiempo que se necesita para analizar la pista de auditoría. Las secciones, “Costo de almacenamiento de datos de auditoría” [39] y

“Auditoría eficaz” [40] describen maneras de auditar de manera eficaz. La auditoría eficaz reduce la cantidad de datos de auditoría al tiempo que se sigue proporcionando suficiente cobertura para lograr los objetivos de seguridad del sitio.

Costo de almacenamiento de datos de auditoría

Si utiliza el complemento `audit_binfile`, el costo de almacenamiento es el costo más significativo para la auditoría. La cantidad de datos de auditoría depende de lo siguiente:

- Número de usuarios
- Número de sistemas
- Cantidad de uso
- Grado de rastreabilidad y responsabilidad necesario

Debido a que estos factores varían de sitio en sitio, ninguna fórmula puede predeterminar la cantidad de espacio en disco que se debe destinar al almacenamiento de datos de auditoría. Utilice la siguiente información como guía:

- Comprenda las clases de auditoría.

  Antes de configurar la auditoría, debe comprender los tipos de eventos que las clases contienen. Puede cambiar las asignaciones de evento-clase de auditoría para optimizar la recopilación de registros de auditoría.
- Preseleccione las clases de auditoría con cuidado para reducir el volumen de registros que se generan.

  La auditoría completa, es decir, con la clase `all`, llena el espacio en disco rápidamente. Incluso una simple tarea, como compilar un programa podría generar un archivo de auditoría de gran tamaño. Un programa de tamaño moderado podría generar miles de registros de auditoría en menos de un minuto.

  Por ejemplo, si se omite la clase de auditoría `file_read`, `fr`, puede reducir significativamente el volumen de auditoría. Si selecciona auditar operaciones fallidas, sólo a veces puede reducir el volumen de auditoría. Por ejemplo, si realiza una auditoría de operaciones fallidas `file_read`, `-fr`, puede generar muchos menos registros que si realiza una auditoría de todos los eventos `file_read`.
- Si utiliza el complemento `audit_binfile`, la gestión eficiente de archivos de auditoría es también importante. Por ejemplo, puede comprimir un sistema de archivos ZFS dedicado a archivos de auditoría.
- Desarrolle una filosofía de auditoría para su sitio.

  Base la filosofía en medidas como el nivel de rastreabilidad que su sitio requiere y los tipos de usuarios que administra.

Auditoría eficaz

Las siguientes técnicas lo pueden ayudar a lograr los objetivos de seguridad de su organización y al mismo tiempo auditar de manera más eficaz.

- Para la mayor cantidad de clases de auditoría posible, sólo preseleccione aquellas clases para usuarios y roles, y no para todo el sistema.
- Audite de manera aleatoria sólo un determinado porcentaje de usuarios a la vez.
- Si el complemento `audit_binfile` está activo, reduzca los requisitos de espacio en disco para archivos de auditoría filtrando, fusionando y comprimiendo los archivos. Desarrolle procedimientos para archivar los archivos, para transferir los archivos a soportes extraíbles y para almacenar los archivos fuera de línea.
- Supervise los datos de auditoría en tiempo real para comportamientos poco usuales.
  - Complemento `audit_syslog`: puede ampliar las herramientas de análisis y de gestión que ya haya desarrollado para gestionar los registros de auditoría en archivos `syslog`.
  - Complemento `audit_binfile`: puede configurar procedimientos para supervisar la pista de auditoría para ciertas actividades. Puede escribir una secuencia de comandos para impulsar un aumento automático de la auditoría de determinados usuarios o determinados sistemas en respuesta a la detección de eventos poco usuales.

    Por ejemplo, puede escribir una secuencia de comandos que haga lo siguiente:

    1. Controla la creación de archivos de auditoría en los sistemas auditados.
    2. Procese los archivos de auditoría con el comando `tail`.

       La conducción de la salida del comando `tail -0f` mediante el comando `praudit` pueden producir un flujo de registros de auditoría a medida que los registros se generan. Para obtener más información, consulte la página del comando man `tail`(1).
    3. Analice este flujo para tipos de mensajes poco usuales u otros indicadores y entregue el análisis al auditor.

       De manera alternativa, la secuencia de comandos se puede utilizar para desencadenar respuestas automáticas.
    4. Supervise constantemente los sistemas de archivos de auditoría en busca de nuevos archivos de auditoría `not_terminated`.
    5. Termine procesos `tail` pendientes cuando no se esté escribiendo en los archivos.

♦ ♦ ♦ CAPÍTULO 3

Gestión del servicio de auditoría

En este capítulo, se proporcionan procedimientos que lo ayudarán a configurar y gestionar la auditoría en un sistema Oracle Solaris. En este capítulo, se tratan las siguientes tareas:

- "Configuración predeterminada del servicio de auditoría" [41]
- "Configuración del servicio de auditoría" [44]
- "Personalización de lo que se audita" [59]
- "Configuración del servicio de auditoría en zonas" [68]
- "Ejemplo: configuración de auditoría de Oracle Solaris" [72]

Además, en los siguientes capítulos, se describen otras tareas de gestión de auditoría:

- Capítulo 4, Supervisión de actividades del sistema
- Capítulo 5, Cómo trabajar con datos de auditoría
- Capítulo 6, Análisis y resolución de problemas del servicio de auditoría

Para obtener una descripción general del servicio de auditoría, consulte el Capítulo 1, Acerca de la auditoría en Oracle Solaris. Para obtener sugerencias de planificación, consulte el Capítulo 2, Planificación de la auditoría. Para obtener información de referencia, consulte el Capítulo 7, Referencia sobre auditoría.

Configuración predeterminada del servicio de auditoría

El servicio de auditoría tiene una configuración predeterminada y comienza a funcionar correctamente de manera inmediata en la zona global después de instalar Oracle Solaris 11.2. No se necesita ninguna acción adicional para activar o configurar el servicio a fin de que se pueda utilizar. Con su configuración predeterminada, el servicio de auditoría registra las siguientes operaciones:

- Operaciones de inicio y cierre de sesión
- Uso del comando `su`
- Operaciones de bloqueo y desbloqueo de pantalla

Dado que la configuración predeterminada del servicio no tiene ningún impacto sobre el rendimiento del sistema, no es necesario desactivar el servicio por motivos de rendimiento.

Siempre y cuando tenga los derechos adecuados en relación con la auditoría, como los del perfil de derechos de revisión de auditoría, podrá revisar los logs de auditoría. Los logs se almacenan en `/var/audit/`*hostname*. Puede ver estos archivos mediante los comandos `praudit` y `auditreduce`. Para obtener más información, consulte “Visualización de datos de pista de auditoría” [93].

Las siguientes secciones de este capítulo proporcionan instrucciones para la personalización de la configuración del servicio de auditoría, en caso de que la configuración predeterminada no sea suficiente para satisfacer sus necesidades.

Visualización de los valores predeterminados del servicio de auditoría

El servicio de auditoría está regulado por los siguientes parámetros:

- Clases de eventos atribuibles y no atribuibles
- Política de auditoría
- Complementos de auditoría
- Controles de colas

Para mostrar los valores predeterminados del servicio de auditoría, se suele utilizar el subcomando `auditconfig -get*`. Este subcomando muestra la configuración actual del parámetro que está representado por el asterisco (*), como `-getflags` `-getpolicy` o `-getqctrl`. Para mostrar información sobre las clases de eventos no atribuibles, utilice el subcomando `auditconfig -getnaflags`.

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

Nota - Para mostrar la configuración del servicio de auditoría, debe convertirse en un administrador que tenga asignado el perfil de derechos de control de auditoría o de configuración de auditoría. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

Los siguientes ejemplos muestran la sintaxis de comando adecuada que se debe utilizar para mostrar los valores predeterminados de configuración de auditoría.

EJEMPLO 3-1 Visualización de clase predeterminada para los eventos

En este ejemplo, se utilizan dos subcomandos para mostrar las clases preseleccionadas para eventos atribuibles y no atribuibles, respectivamente. Para ver qué eventos están asignados a una clase y, por lo tanto, qué eventos se registran, ejecute el comando `auditrecord -c` *clase*.

```
# auditconfig -getflags
active user default audit flags = lo(0x1000,0x1000)
configured user default audit flags = lo(0x1000,0x1000)
```

`lo` es el indicador para la clase de auditoría `login/logout`. El formato de la salida de la máscara es (*success*,*failure*).

```
# auditconfig -getnaflags
active non-attributable audit flags = lo(0x1000,0x1000)
configured non-attributable audit flags = lo(0x1000,0x1000)
```

EJEMPLO 3-2 Visualización de la política de auditoría predeterminada

```
$ auditconfig -getpolicy
configured audit policies = cnt
active audit policies = cnt
```

La política *activa* es la política actual, pero el valor de la política no es almacenado por el servicio de auditoría. La política *configurada* es almacenada por el servicio de auditoría, por lo que la política se restaura al reiniciar el servicio de auditoría.

EJEMPLO 3-3 Visualización de los complementos de auditoría predeterminados

```
$ auditconfig -getplugin
Plugin: audit_binfile
Attributes: p_dir=/var/audit;p_fsize=0;p_minfree=1;

Plugin: audit_syslog (inactive)
Attributes: p_flags=;

Plugin: audit_remote (inactive)
Attributes: p_hosts=;p_retries=3;p_timeout=5;
```

El complemento `audit_binfile` está activo de manera predeterminada.

EJEMPLO 3-4 Visualización de los controles de colas de auditoría

```
$ auditconfig -getqctrl
no configured audit queue hiwater mark
no configured audit queue lowater mark
no configured audit queue buffer size
no configured audit queue delay
active audit queue hiwater mark (records) = 100
active audit queue lowater mark (records) = 10
active audit queue buffer size (bytes) = 8192
active audit queue delay (ticks) = 20
```

El control de colas *activo* es el control de colas que está siendo utilizado actualmente por el núcleo. La cadena `no configured` indica que el sistema está utilizando los valores predeterminados.

Activación y desactivación del servicio de auditoría

El servicio de auditoría está activado de manera predeterminada. Si la política de auditoría `perzone` está configurada, los administradores de zona deben activar, refrescar o desactivar el servicio de auditoría en cada zona no global según lo deseado. Si la política de auditoría `perzone` no está configurada, si se activa, refresca o desactiva el servicio de auditoría de la zona global, esto se aplica a todas las zonas no globales.

Para activar o desactivar el servicio de auditoría, debe convertirse en administrador con el perfil de derechos de control de auditoría asignado. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

Para desactivar el servicio de auditoría, escriba el comando siguiente:

```
# audit -t
```

Para activar el servicio de auditoría, escriba el comando siguiente:

```
# audit -s
```

Para verificar que el servicio de auditoría se esté ejecutando, escriba el siguiente comando:

```
# auditconfig -getcond
audit condition = auditing
```

Si la política de auditoría `perzone` está configurada, debe realizar esta verificación en las zonas no globales en las que se activó la auditoría.

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

Configuración del servicio de auditoría

Antes de activar la auditoría en su red, puede modificar los valores predeterminados para satisfacer los requisitos de auditoría de su sitio. Lo mejor es personalizar la configuración de auditoría lo más posible antes de que los primeros usuarios inicien sesión.

Si ha implementado zonas, puede decidir auditar todas las zonas de la zona global o auditar las zonas no globales individualmente. Para obtener una descripción general, consulte “Auditoría y Oracle Solaris Zones” [119]. Para obtener información sobre planificación,

consulte “Planificación de la auditoría en zonas” [28]. Para obtener información sobre los procedimientos, consulte “Configuración del servicio de auditoría en zonas” [68].

Para configurar el servicio de auditoría, se suelen utilizar los subcomandos `auditconfig`. La configuración que se establece con estos subcomandos se aplica a todo el sistema.

- `auditconfig -get*` muestra la configuración actual del parámetro que está representado por el asterisco (*), como se muestra en los ejemplos de “Visualización de los valores predeterminados del servicio de auditoría” [42].
- `auditconfig -set*` asigna un valor al parámetro que está representado por el asterisco (*), como `-setflags`, `-setpolicy` o `-setqctrl`. Para configurar clases para eventos no atribuibles, utilice el subcomando `auditconfig setnaflags`.

También puede personalizar la auditoría para que se aplique a los usuarios o perfiles, en lugar de a todo el sistema. Las preselecciones de clase de auditoría para cada usuario son especificadas por el atributo de seguridad `audit_flags`. Estos valores específicos de usuario, además de las clases preseleccionadas para el sistema, determinan la máscara de auditoría del usuario, como se describe en “Características del proceso de auditoría” [124].

Mediante la preselección de clases por usuario en lugar de por sistema, a veces, puede reducir el impacto de la auditoría en el rendimiento del sistema. También puede que desee auditar a usuarios específicos de manera ligeramente diferente del sistema.

Para configurar la auditoría que se aplica a los usuarios o perfiles, se utilizan los siguientes comandos:

- `usrattr` muestra el valor `audit_flags` que está configurado para los usuarios. De manera predeterminada, los usuarios sólo se auditan para la configuración en todo el sistema.
- `usermod -K` establece los indicadores que se aplican a los usuarios.
- `profile` establece los indicadores que se aplican a los perfiles.

Para ver una descripción del comando `userattr`, consulte la página del comando man `userattr`(1). Para ver una descripción de la palabra clave `audit_flags`, consulte la página del comando `user_attr`(4).

En el siguiente mapa de tareas, se hace referencia a los procedimientos para configurar la auditoría. Todas las tareas son opcionales.

TABLA 3-1 Mapa de tareas de configuración del servicio de auditoría

Tarea	Descripción	Más instrucciones
Seleccionar los eventos que se han auditado.	Selecciona previamente en todo el sistema clases de auditoría. Si un evento es atribuible, todos los usuarios se auditan para este evento.	Cómo preseleccionar clases de auditoría [46]
Seleccionar los eventos que se van a auditar para usuarios concretos.	Establece diferencias específicas de usuarios para las clases de auditoría en todo el sistema.	Cómo configurar las características de auditoría de un usuario [47]

Tarea	Descripción	Más instrucciones
Especificar la política de auditoría.	Define datos adicionales de auditoría que el sitio necesita.	Cómo cambiar la política de auditoría [51]
Especificar controles de colas.	Modifica el tamaño predeterminado de la memoria intermedia, los registros de auditoría en la cola y el intervalo de escritura de registros de auditoría en la memoria intermedia.	Cómo cambiar controles de colas de auditoría [54]
Crear el alias de correo electrónico `audit_warn`.	Define quién recibe advertencias por correo electrónico cuando el servicio de auditoría necesita atención.	Cómo configurar el alias de correo electrónico `audit_warn` [55]
Configurar logs de auditoría.	Configura la ubicación de los registros de auditoría de cada complemento.	"Configuración de logs de auditoría" [75]
Agregar clases de auditoría.	Reduce el número de registros de auditoría mediante la creación de una nueva clase de auditoría para retener eventos críticos.	Cómo agregar una clase de auditoría [56]
Cambiar asignaciones de evento-clase.	Reduce el número de registros de auditoría mediante el cambio de la asignación de evento-clase.	Cómo cambiar una pertenencia a clase de un evento de auditoría [58]

▼ Cómo preseleccionar clases de auditoría

Preseleccione clases de auditoría que contienen los eventos que desea supervisar. Los eventos que no están en clases preseleccionadas no se registran.

Antes de empezar Debe convertirse en un administrador con el perfil de derechos de configuración de auditoría asignado. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

1. **Determine las clases preseleccionadas actuales.**

```
# auditconfig -getflags
...

# auditconfig -getnaflags
,,,
```

Para obtener una explicación de la salida, consulte "Visualización de los valores predeterminados del servicio de auditoría" [42].

2. **Preseleccione las clases atribuibles.**

```
# auditconfig -setflags lo,ps,fw
user default audit flags = ps,lo,fw(0x101002,0x101002)
```

Este comando audita los eventos en las clases `login/logout`, `process start/stop` y `file write` para determinar si se efectuaron con éxito o fallaron.

Nota - El comando `auditconfig -setflags` *sustituye* la preselección actual, por lo que usted debe especificar todas las clases que desea preseleccionar.

3. **Preseleccione las clases no atribuibles.**

   La clase `na` contiene montajes no atribuibles, de inicio y de PROM, entre otros eventos.

```
# auditconfig -setnaflags lo,na
non-attributable audit flags = lo,na(0x1400,0x1400)
```

   Los argumentos `lo` y `na` son los únicos argumentos útiles de la opción `-setnaflags`.

Nota - El comando `auditconfig -setnaflags` *sustituye* la preselección actual, por lo que usted debe especificar todas las clases que desea preseleccionar.

▼ Cómo configurar las características de auditoría de un usuario

Estas características de auditoría específicas del usuario que se establecen mediante este procedimiento se combinan con las clases preseleccionadas para el sistema. Juntas determinan la máscara de auditoría del usuario, como se describe en “Características del proceso de auditoría” [124].

Antes de empezar Debe asumir el rol `root`. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

1. **(Opcional) Visualice las clases de auditoría que están seleccionadas actualmente para los usuarios existentes.**

   a. **Visualice la lista de usuarios.**

```
# who
adoe    pts/1        Oct 10 10:20 (:0.0)
adoe    pts/2        Oct 10 10:20 (:0.0)
jdoe    pts/5        Oct 12 12:20 (:0.0)
jdoe    pts/6        Oct 12 12:20 (:0.0)
...
```

   b. **Visualice el valor del atributo `audit_flags` para cada usuario.**

```
# userattr audit_flags adoe
# userattr audit_flags jdoe
```

2. **Defina los indicadores de auditoría en la base de datos `user_attr` o `prof_attr`.**

   Por ejemplo, puede crear un perfil de derechos que define los derechos de un subconjunto de sus usuarios. Los usuarios que tengan asignado ese perfil de derechos se auditan de forma idéntica.

   - **Para definir indicadores de auditoría de un usuario, utilice el comando `usermod`.**

     ```
     # usermod -K audit_flags=fw:no jdoe
     ```

     El formato de la palabra clave `audit_flags` es *always-audit*:*never-audit*.

     always-audit — Muestra las clases de auditoría que se van a auditar para este usuario. Las modificaciones a las clases de todo el sistema están precedidas por un signo de intercalación (^). Las clases que se agregan a las clases de todo el sistema no están precedidas por un signo de intercalación.

     never-audit — Muestra las clases de auditoría que nunca se van a auditar para el usuario, incluso si estos eventos de auditoría se auditan en todo el sistema. Las modificaciones a las clases de todo el sistema están precedidas por un signo de intercalación (^).

     Para especificar varias clases de auditoría, separe las clases con comas. Para obtener más información, consulte la página del comando man `audit_flags`(5).

   - **Para definir indicadores de auditoría para un perfil de derechos, utilice el comando `profiles`.**

     ```
     # profiles -p "System Administrator"
     profiles:System Administrator> set name="Audited System Administrator"
     profiles:Audited System Administrator> set always_audit=fw,as
     profiles:Audited System Administrator> end
     profiles:Audited System Administrator> exit
     ```

     Cuando asigna el perfil de derechos de administrador del sistema auditado a un usuario o un rol, ese usuario o rol se audita en busca de esos indicadores, según el orden de búsqueda que se describe en “Orden de búsqueda para derechos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

ejemplo 3-5 Cambio de eventos que se van a auditar para un usuario

En este ejemplo, la máscara de preselección de auditoría para todos los usuarios es la siguiente:

```
# auditconfig -getflags
active user default audit flags = ss,lo(0x11000,0x11000)
configured user default audit flags = ss,lo(0x11000,0x11000)
```

Ningún usuario, excepto el administrador, inicia sesión.

Para reducir el impacto del evento de auditoría `AUE_PFEXEC` en los recursos del sistema, el administrador no audita este evento en el nivel del sistema. En su lugar, el administrador selecciona previamente la clase `pf` para un usuario, `jdoe`. La clase `pf` se crea en el Ejemplo 3-15, "Creación de una clase de auditoría nueva".

```
# usermod -K audit_flags=pf:no jdoe
```

El comando `userattr` muestra la agregación.

```
# userattr audit_flags jdoe
pf:no
```

Cuando el usuario `jdoe` inicia sesión, la máscara de preselección de auditoría de `jdoe` es una combinación de los valores `audit_flags` con los valores predeterminados del sistema. `289` es el PID del shell de inicio de sesión de `jdoe`.

```
# auditconfig -getpinfo 289
audit id = jdoe(1234)
process preselection mask = ss,pf,lo(0x0100000008011000,0x0100000008011000)
terminal id (maj,min,host) = 242,511,example1(192.168.160.171)
audit session id = 103203403
```

ejemplo 3-6 Modificación de excepción de preselección de auditoría para un usuario

En este ejemplo, la máscara de preselección de auditoría para todos los usuarios es la siguiente:

```
# auditconfig -getflags
active user default audit flags = ss,lo(0x11000,0x11000)
configured user default audit flags = ss,lo(0x11000,0x11000)
```

Ningún usuario, excepto el administrador, inicia sesión.

El administrador decide no recopilar eventos `ss` fallidos para el usuario `jdoe`.

```
# usermod -K audit_flags=^-ss:no jdoe
```

El comando `userattr` muestra la excepción.

```
# userattr audit_flags jdoe
^-ss:no
```

Cuando el usuario `jdoe` inicia sesión, la máscara de preselección de auditoría de `jdoe` es una combinación de los valores `audit_flags` con los valores predeterminados del sistema. `289` es el PID del shell de inicio de sesión de `jdoe`.

```
# auditconfig -getpinfo 289
audit id = jdoe(1234)
process preselection mask = +ss,lo(0x11000,0x1000)
terminal id (maj,min,host) = 242,511,example1(192.168.160.171)
```

```
audit session id = 103203403
```

ejemplo 3-7 Auditoría de usuarios seleccionados, sin auditoría en todo el sistema

En este ejemplo, se auditan el inicio de sesión y las actividades de rol de cuatro usuarios seleccionados en el sistema. No se preseleccionan clases de auditoría para el sistema.

En primer lugar, el administrador elimina todos los indicadores en todo el sistema.

```
# auditconfig -setflags no
user default audit flags = no(0x0,0x0)
```

A continuación, el administrador selecciona previamente dos clases de auditoría para los cuatro usuarios. La clase `pf` se crea en el Ejemplo 3-15, “Creación de una clase de auditoría nueva”.

```
# usermod -K audit_flags=lo,pf:no jdoe
# usermod -K audit_flags=lo,pf:no kdoe
# usermod -K audit_flags=lo,pf:no pdoe
# usermod -K audit_flags=lo,pf:no zdoe
```

A continuación, el administrador selecciona previamente la clase `pf` para el rol `root`.

```
# userattr audit_flags root
# rolemod -K audit_flags=lo,pf:no root
# userattr audit_flags root
lo,pf:no
```

Para registrar intrusiones injustificadas, el administrador no cambia la auditoría de inicios de sesión no atribuibles.

```
# auditconfig -getnaflags
active non-attributable audit flags = lo(0x1000,0x1000)
configured non-attributable audit flags = lo(0x1000,0x1000)
```

ejemplo 3-8 Eliminación de indicadores de auditoría de un usuario

En el siguiente ejemplo, el administrador elimina todos los indicadores de auditoría específicos de usuario. Los procesos existentes de usuarios que han iniciado sesión actualmente siguen siendo auditados.

El administrador ejecuta el comando `usermod` con la palabra clave `audit_flags` establecida en ningún valor.

```
# usermod -K audit_flags= jdoe
# usermod -K audit_flags= kdoe
# usermod -K audit_flags= ldoe
```

A continuación, el administrador verifica la eliminación.

```
# userattr audit_flags jdoe
# userattr audit_flags kdoe
```

```
# userattr audit_flags ldoe
```

ejemplo 3-9 Creación de un perfil de derechos para un grupo de usuarios

El administrador desea que todos los perfiles de derechos administrativos del sitio auditen explícitamente la clase `pf`. Para cada perfil de derechos que se va a asignar, el administrador crea una versión específica de sitio en LDAP que incluye indicadores de auditoría.

En primer lugar, el administrador clona un perfil de derechos existente y, luego, cambia el nombre y agrega indicadores de auditoría.

```
# profiles -p "Network Wifi Management" -S ldap
profiles: Network Wifi Management> set name="Wifi Management"
profiles: Wifi Management> set desc="Audited wifi management"
profiles: Wifi Management> set audit_always=pf
profiles: Wifi Management> exit
```

Después de repetir este procedimiento para cada perfil de derechos que se va a utilizar, el administrador enumera la información en el perfil de gestión de Wi-Fi.

```
# profiles -p "Wifi Management" -S ldap info
name=Wifi Management
desc=Audited wifi management
auths=solaris.network.wifi.config
help=RtNetWifiMngmnt.html
always_audit=pf
```

▼ Cómo cambiar la política de auditoría

Puede cambiar la política de auditoría predeterminada para registrar información detallada sobre comandos auditados, para agregar un nombre de zona a cada registro o para satisfacer otros requisitos de seguridad del sitio.

Antes de empezar Debe convertirse en un administrador con el perfil de derechos de configuración de auditoría asignado. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

1. **Visualice la política de auditoría actual.**

   ```
   $ auditconfig -getpolicy
   ...
   ```

   Para obtener una explicación de la salida, consulte “Visualización de los valores predeterminados del servicio de auditoría” [42].

2. **Vea las opciones de política disponibles.**

   ```
   $ auditconfig -lspolicy
   ```

```
policy string    description:
ahlt             halt machine if it can not record an async event
all              all policies for the zone
arge             include exec environment args in audit recs
argv             include exec command line args in audit recs
cnt              when no more space, drop recs and keep a cnt
group            include supplementary groups in audit recs
none             no policies
path             allow multiple paths per event
perzone          use a separate queue and auditd per zone
public           audit public files
seq              include a sequence number in audit recs
trail            include trailer token in audit recs
windata_down     include downgraded window information in audit recs
windata_up       include upgraded window information in audit recs
zonename         include zonename token in audit recs
```

Nota - Las opciones de política `perzone` y `ahlt` solamente se pueden configurar en la zona global. Para que las compensaciones usen una opción de política particular, consulte "Comprensión de la política de auditoría" [35].

3. Active o desactive las opciones de política de auditoría seleccionadas.

```
# auditconfig [ -t ] -setpolicy [prefix]policy[,policy...]
```

`-t` — Opcional. Crea una política *activa* o temporal. Puede definir una política temporal para depurar o para fines de prueba.

Una política temporal permanece vigente hasta que el servicio de auditoría se refresca o hasta que la política es modificada por el comando `auditconfig -setpolicy`.

prefix — Un valor de *prefix* de `+` agrega la lista de políticas a la política actual. Un valor de *prefix* de `-` elimina la lista de políticas de la política actual. Sin un prefijo, la política de auditoría se restablece. Esta opción le permite mantener las políticas de auditoría actuales.

policy — Selecciona la política que se activará o desactivará.

ejemplo 3-10 Configuración de la opción de política de auditoría `ahlt`

En este ejemplo, la seguridad de sitio estricta requiere la política `ahlt`.

```
# auditconfig -setpolicy -cnt
# auditconfig -setpolicy +ahlt
```

El signo más (+) antes de la política `ahlt` agrega la política a la configuración de política actual. Sin el signo más, la política `ahlt` sustituye todas las políticas de auditoría actuales.

ejemplo 3-11 Definición de una política de auditoría temporal

En este ejemplo, está configurada la política de auditoría `ahlt`. Para la depuración, el administrador agrega la política de auditoría `trail` a la política activa (`+trail`) temporalmente (`-t`). La política `trail` ayuda en la recuperación de pistas de auditoría dañadas.

```
$ auditconfig -setpolicy ahlt
$ auditconfig -getpolicy
configured audit policies = ahlt
active audit policies = ahlt
$ auditconfig -t -setpolicy +trail
configured audit policies = ahlt
active audit policies = ahlt,trail
```

El administrador desactiva la política `trail` cuando la depuración finaliza.

```
$ auditconfig -setpolicy -trail
$ auditconfig -getpolicy
configured audit policies = ahlt
active audit policies = ahlt
```

Refrescar el servicio de auditoría ejecutando el comando `audit -s` también elimina esta política temporal, además de otros valores temporales en el servicio de auditoría. Para ver ejemplos de otros valores temporales, consulte Cómo cambiar controles de colas de auditoría [54].

ejemplo 3-12 Configuración de la política de auditoría `perzone`

En este ejemplo, la política de auditoría `perzone` se agrega a la política existente en la zona global. La configuración de la política `perzone` se almacena como una propiedad permanente, por lo que la política `perzone` está en vigor durante la sesión y cuando el servicio de auditoría se reinicia. Para las zonas, la política está disponible en el siguiente inicio de zona.

```
$ auditconfig -getpolicy
configured audit policies = cnt
active audit policies = cnt
$ auditconfig -setpolicy +perzone
$ auditconfig -getpolicy
configured audit policies = perzone,cnt
active audit policies = perzone,cnt
```

ejemplo 3-13 Recopilación de registros de auditoría para auditores externos

En este ejemplo, el administrador está recopilando registros de auditoría para satisfacer los requisitos de auditores externos. El administrador decide utilizar un servidor de auditoría remota (ARS) para recopilar información acerca de las actividades administrativas. El administrador también recopila las acciones que no se pueden atribuir a un usuario, como el inicio.

El administrador configura ARS. Además de la auditoría de la clase `cusa`, el administrador agrega políticas a la configuración de auditoría.

```
# auditconfig -setflags cusa
user default audit flags = ex,xa,ua,as,ss,ap,lo,ft(0x80475080,0x80475080)
# auditconfig -setpolicy ahlt,argv,argeauditconfig # auditconfig -getpolicy
configured audit policies = ahlt,arge,argv
active audit policies = ahlt,arge,argv
# auditconfig -setnaflags lo,na
non-attributable audit flags = lo,na(0x1400,0x1400)
```

Cuando el administrador activa el complemento `audit_remote` y refresca el servicio de auditoría, los registros se recopilan.

▼ Cómo cambiar controles de colas de auditoría

El servicio de auditoría proporciona valores predeterminados para parámetros de cola de auditoría. Puede inspeccionar y cambiar permanente o temporalmente estos valores con el comando `auditconfig`.

Antes de empezar Debe convertirse en un administrador con el perfil de derechos de configuración de auditoría asignado. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

1. **Visualice los valores actuales de los controles de colas de auditoría.**

   ```
   $ auditconfig -getqctrl
   ...
   ```

   Para obtener una explicación de la salida, consulte "Visualización de los valores predeterminados del servicio de auditoría" [42].

2. **Modifique controles de colas de auditoría seleccionados.**

   Para obtener ejemplos y una descripción de los controles de colas de auditoría, consulte la página del comando man `auditconfig`(1M).

   - Para modificar algunos o todos los controles de colas de auditoría, utilice la opción `-setqctrl`.

     # auditconfig [-t] -setqctrl *hiwater lowater bufsz interval*

     Los valores de marca de agua superior (`hiwater`) y de marca de agua inferior (`lowater`) indican en qué punto los procesos se suspenden y reanudan, respectivamente. Los puntos se miden en términos del número de registros de auditoría no entregados. El tamaño de buffer (`bufsz`) se refiere al tamaño del buffer de la cola. `Interval` indica el retraso, medido en número de tics, entre la generación de la salidas de auditoría.

Por ejemplo, establezca el valor *interval* en `10` sin establecer los otros controles.

```
# auditconfig -setqctrl 0 0 0 10
```

- Para modificar un control de colas de auditoría específico, especifique su opción. La opción `-setqdelay` es el equivalente de `-setqctrl 0 0 0` *interval*, como en **`auditconfig -setqdelay 10`**.

```
# auditconfig [ -t ] -setqhiwater value
# auditconfig [ -t ] -setqlowater value
# auditconfig [ -t ] -setqbufsz value
# auditconfig [ -t ] -setqdelay value
```

ejemplo 3-14 Restablecimiento de un control de colas de auditoría al valor predeterminado

El administrador define todos los controles de colas de auditoría y luego regresa el valor *lowater* en el repositorio al valor predeterminado.

```
# auditconfig -setqctrl 200 5 10216 10
# auditconfig -setqctrl 200 0 10216 10
configured audit queue hiwater mark (records) = 200
no configured audit queue lowater mark
configured audit queue buffer size (bytes) = 10216
configured audit queue delay (ticks) = 10
active audit queue hiwater mark (records) = 200
active audit queue lowater mark (records) = 5
active audit queue buffer size (bytes) = 10216
active audit queue delay (ticks) = 10
```

A continuación, el administrador establece el valor *lowater* en el valor predeterminado para la sesión actual.

```
# auditconfig -setqlowater 10
# auditconfig -getqlowater
configured audit queue lowater mark (records) = 10
active audit queue lowater mark (records) = 10
```

▼ Cómo configurar el alias de correo electrónico `audit_warn`

La secuencia de comandos `/etc/security/audit_warn` genera correo que notifica al administrador sobre incidentes de auditoría que podrían requerir atención. Puede personalizar la secuencia de comandos y puede enviar el correo a una cuenta que no sea `root`.

Si la política `perzone` está establecida, el administrador de la zona no global debe configurar el alias de correo `audit_warn` en la zona no global.

Antes de empezar Debe convertirse en un administrador con la autorización `solaris.admin.edit/etc/security/audit_warn` asignada. De manera predeterminada, sólo el rol `root` tiene esta autorización. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

- **Configure el alias de correo electrónico `audit_warn`.**

  Elija una de las siguientes opciones:

  - Reemplace el alias de correo electrónico `audit_warn` con otra cuenta de correo electrónico en la secuencia de comandos `audit_warn`.

    Cambie el alias de correo electrónico `audit_warn` en la línea `ADDRESS` de la secuencia de comandos a otra dirección:

    ```
    #ADDRESS=audit_warn            # standard alias for audit alerts
    ADDRESS=audadmin               # role alias for audit alerts
    ```

    Nota - Para obtener información sobre los efectos de modificar un archivo de configuración de auditoría, consulte “Archivos de configuración de auditoría y empaquetado” [119].

  - Redirija el correo electrónico `audit_warn` a otra cuenta de correo.

    Agregue el alias de correo electrónico `audit_warn` al archivo de alias de correo apropiado. Puede agregar el alias al archivo local `/etc/mail/aliases` o a la base de datos `mail_aliases` en el nombre de espacio. La entrada `/etc/mail/aliases` se parecerá al siguiente ejemplo si las cuentas de correo electrónico `root` y `audadmin` se han agregado como miembros del alias de correo electrónico `audit_warn`:

    ```
    audit_warn: root,audadmin
    ```

    A continuación, ejecute el comando `newaliases` para reconstruir la base de datos de acceso aleatorio para el archivo `aliases`.

    ```
    # newaliases
    /etc/mail/aliases: 14 aliases, longest 10 bytes, 156 bytes total
    ```

▼ Cómo agregar una clase de auditoría

Cuando crea su propia clase de auditoría, puede colocar en ella sólo los eventos de auditoría que desea auditar para su sitio. Esta estrategia puede reducir el número de registros que se recopilan y reducir el ruido en la pista de auditoría.

Al agregar la clase en un sistema, copie el cambio en todos los sistemas que se están auditando. La mejor práctica es crear clases de auditoría antes de que se conecten los primeros usuarios.

Para obtener información sobre los efectos de modificar un archivo de configuración de auditoría, consulte “Archivos de configuración de auditoría y empaquetado” [119].

Sugerencia - En Oracle Solaris, puede crear su propio paquete que contiene archivos y reemplazar los paquetes de Oracle Solaris con archivos personalizados según el sitio. Cuando establece el atributo `preserve` en `true` en su paquete, los subcomandos `pkg`, como verify, fix, revert, etc, se ejecutarán en relación con sus paquetes. Para obtener más información, consulte las páginas del comando man `pkg`(1) y `pkg`(5).

Antes de empezar

Seleccione bits libres para su entrada única. Verifique qué bits están disponibles para que usen los clientes en el archivo `/etc/security/audit_class`.

Debe convertirse en un administrador con la autorización `solaris.admin.edit/etc/security/audit_class` asignada. De manera predeterminada, sólo el rol `root` tiene esta autorización. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

1. **(Opcional) Guarde una copia de seguridad del archivo `audit_class`.**

   ```
   # cp /etc/security/audit_class /etc/security/audit_class.orig
   ```

2. **Agregue las nuevas entradas al archivo `audit_class`.**

   Cada entrada tiene el siguiente formato:

   `0x`*64bitnumber*:*flag*:*description*

   Para obtener una descripción de los campos, consulte la página del comando man `audit_class`(4). Para obtener una lista de clases existentes, lea el archivo `/etc/security/audit_class`.

ejemplo 3-15 Creación de una clase de auditoría nueva

En este ejemplo, se crea una clase para mantener los comandos administrativos que se ejecutan en un rol. La entrada agregada al archivo `audit_class` se muestra a continuación:

```
0x0100000000000000:pf:profile command
```

La entrada crea la clase de auditoría nueva `pf`. El Ejemplo 3-16, “Asignación de eventos de auditoría existentes a una nueva clase” muestra cómo completar la clase de auditoría nueva.

Errores más frecuentes

Si ha personalizado el archivo `audit_class`, asegúrese de que los indicadores de auditoría asignados directamente a los usuarios o los perfiles de derechos sean coherentes con las clases de auditoría nuevas. Se producen errores cuando un valor `audit_flags` no es un subconjunto del archivo `audit_class`.

▼ Cómo cambiar una pertenencia a clase de un evento de auditoría

Puede que desee cambiar la pertenencia a clase de un evento de auditoría para reducir el tamaño de una clase de auditoría existente o para colocar el evento en una clase propia.

Atención - Nunca quite el comentario de eventos en el archivo `audit_event`. Este archivo es utilizado por el comando `praudit` para leer archivos binarios de auditoría. Los archivos de auditoría almacenados pueden contener eventos que se muestran en el archivo.

Cuando reconfigura asignaciones de evento-clase de auditoría en un sistema, copie el cambio en todos los sistemas que se auditan. Lo mejor es cambiar las asignaciones de evento-clase antes de que los primeros usuarios inicien sesión.

Nota - Para obtener información sobre los efectos de modificar un archivo de configuración de auditoría, consulte “Archivos de configuración de auditoría y empaquetado” [119].

Sugerencia - En Oracle Solaris, puede crear su propio paquete que contiene archivos y reemplazar los paquetes de Oracle Solaris con archivos personalizados según el sitio. Cuando establece el atributo `preserve` en `true` en su paquete, los subcomandos `pkg`, como verify, fix, revert, etc, se ejecutarán en relación con sus paquetes. Para obtener más información, consulte las páginas del comando man `pkg`(1) y `pkg`(5).

Antes de empezar Debe convertirse en un administrador con la autorización `solaris.admin.edit/etc/security/audit_event` asignada. De manera predeterminada, sólo el rol `root` tiene esta autorización. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

1. **(Opcional) Guarde una copia de seguridad del archivo `audit_event`.**

   ```
   # cp /etc/security/audit_event /etc/security/audit_event.orig
   ```

2. **Cambie la clase a la que pertenecen los eventos determinados; para esto, cambie la *class-list* de los eventos.**

   Cada entrada tiene el siguiente formato:

   number:*name*:*description*:*class-list*

   number ID del evento de auditoría.

   name Nombre del evento de auditoría.

description	Normalmente, la llamada de sistema o el ejecutable que desencadena la creación de un registro de auditoría.
class-list	Una lista separada por comas de las clases de auditoría.

ejemplo 3-16 Asignación de eventos de auditoría existentes a una nueva clase

En este ejemplo, se asigna un evento de auditoría existente a la nueva clase creada en el Ejemplo 3-15, “Creación de una clase de auditoría nueva”. De manera predeterminada, el evento de auditoría `AUE_PFEXEC` se asigna a varias clases de auditoría. Mediante la creación de la nueva clase, el administrador puede auditar eventos `AUE_PFEXEC` sin auditar los eventos en las otras clases.

```
# grep pf /etc/security/audit_class
0x0100000000000000:pf:profile command
# grep AUE_PFEXEC /etc/security/audit_event
116:AUE_PFEXEC:execve(2) with pfexec enabled:ps,ex,ua,as,cusa
# pfedit /etc/security/audit_event
#116:AUE_PFEXEC:execve(2) with pfexec enabled:ps,ex,ua,as,cusa
116:AUE_PFEXEC:execve(2) with pfexec enabled:pf
# auditconfig -setflags lo,pf
user default audit flags = pf,lo(0x0100000000001000,0x0100000000001000)
```

Personalización de lo que se audita

El siguiente mapa de tareas hace referencia a procedimientos para configurar la auditoría según sus necesidades específicas.

TABLA 3-2 Mapa de tareas de personalización de la auditoría

Tarea	Descripción	Más instrucciones
Auditar todo lo que un usuario hace en el sistema.	Audite uno o más usuarios para cada comando.	Cómo auditar todos los comandos por usuarios [60]
Cambiar los eventos de auditoría que se graban y hacer que el cambio afecte las sesiones existentes.	Actualice la máscara de preselección de un usuario.	Cómo actualizar la máscara de preselección de usuarios con sesión iniciada [63]
Localizar modificaciones en archivos determinados.	Audite las modificaciones en los archivos y, luego, use el comando `auditreduce` para encontrar archivos determinados.	Cómo buscar registros de auditoría de los cambios realizados en archivos específicos [62]
Utilizar menos espacio en el sistema de archivos para archivos de auditoría.	Utilice las cuotas y la compresión ZFS.	Cómo comprimir archivos de auditoría en un sistema de archivos dedicado [66]
Eliminar eventos de auditoría del archivo `audit_event`.	Actualice correctamente el archivo `audit_event`.	Cómo evitar la auditoría de eventos específicos [65]

▼ Cómo auditar todos los comandos por usuarios

Como parte de la política de seguridad del sitio, algunos sitios requieren registros de auditoría de todos los comandos ejecutados por la cuenta `root` y los roles administrativos. Algunos sitios pueden requerir registros de auditoría de todos los comandos por todos los usuarios. Además, los sitios pueden requerir que los argumentos de los comandos y el entorno se registren.

Antes de empezar Para preseleccionar clases de auditoría y definir la política de auditoría, debe tener convertirse en administrador con el perfil de derechos de configuración de auditoría asignado. Para asignar indicadores de auditoría a usuarios, roles y perfiles de derechos, debe asumir el rol `root`.

1. **Visualice la información de evento en el nivel de usuario para las clases `lo` y `ex`.**
   La clase `ex` audita todas las llamadas a las funciones `exec()` y `execve()`.
   La clase `lo` audita los inicios de sesión, los cierres de sesión y los bloqueos de pantalla. La siguiente salida muestra todos los eventos de las clases `ex` y `lo`.

```
% auditconfig -lsevent | grep " lo "
AUE_login                       6152 lo login - local
AUE_logout                      6153 lo logout
AUE_telnet                      6154 lo login - telnet
AUE_rlogin                      6155 lo login - rlogin
AUE_rshd                        6158 lo rsh access
AUE_su                          6159 lo su
AUE_rexecd                      6162 lo rexecd
AUE_passwd                      6163 lo passwd
AUE_rexd                        6164 lo rexd
AUE_ftpd                        6165 lo ftp access
AUE_ftpd_logout                 6171 lo ftp logout
AUE_ssh                         6172 lo login - ssh
AUE_role_login                  6173 lo role login
AUE_newgrp_login                6212 lo newgrp login
AUE_admin_authenticate          6213 lo admin login
AUE_screenlock                  6221 lo screenlock - lock
AUE_screenunlock                6222 lo screenlock - unlock
AUE_zlogin                      6227 lo login - zlogin
AUE_su_logout                   6228 lo su logout
AUE_role_logout                 6229 lo role logout
AUE_smbd_session                6244 lo smbd(1m) session setup
AUE_smbd_logoff                 6245 lo smbd(1m) session logoff
AUE_ClientConnect               9101 lo client connection to x server
AUE_ClientDisconnect            9102 lo client disconn. from x server

% auditconfig -lsevent | egrep " ex |,ex |ex,"
AUE_EXECVE                       23 ex,ps execve(2)
```

2. **Audite las clases `lo` y `ex`.**

   - **Para auditar los roles administrativos de estas clases, modifique los atributos de seguridad de los roles.**

En el siguiente ejemplo, `root` es un rol. El sitio ha creado tres roles: `sysadm`, `auditadm` y `netadm`. Todos los roles se auditan para determinar el éxito y el fallo de eventos en las clases `ex` y `lo`.

```
# rolemod -K audit_flags=lo,ex:no root

# rolemod -K audit_flags=lo,ex:no sysadm

# rolemod -K audit_flags=lo,ex:no auditadm

# rolemod -K audit_flags=lo,ex:no netadm
```

- **Para auditar todos los usuarios de estas clases, establezca los indicadores de todo el sistema.**

  ```
  # auditconfig -setflags lo,ex
  ```

  El resultado es similar al siguiente:

  ```
  header,129,2,AUE_EXECVE,,mach1,2010-10-14 12:17:12.616 -07:00
  path,/usr/bin/ls
  attribute,100555,root,bin,21,320271,18446744073709551615
  subject,jdoe,root,root,root,root,2486,50036632,82 0 mach1
  return,success,0
  ```

3. **Especifique información adicional que se deba registrar sobre el uso de comandos.**

   - **Para registrar los argumentos de comandos, agregue la política `argv`.**

     ```
     # auditconfig -setpolicy +argv
     ```

     El token `exec_args` registra los argumentos de los comandos:

     ```
     header,151,2,AUE_EXECVE,,mach1,2010-10-14 12:26:17.373 -07:00
     path,/usr/bin/ls
     attribute,100555,root,bin,21,320271,18446744073709551615
     exec_args
     ,2,ls,/etc/security
     subject,jdoe,root,root,root,root,2494,50036632,82 0 mach1
     return,success,0
     ```

   - **Para registrar el entorno en el que se ejecuta el comando, agregue la política `arge`.**

     ```
     # auditconfig -setpolicy +arge
     ```

     El token `exec_env` registra el entorno de los comandos:

     ```
     header,1460,2,AUE_EXECVE,,mach1,2010-10-14 12:29:39.679 -07:00
     path,/usr/bin/ls
     ```

```
attribute,100555,root,bin,21,320271,18446744073709551615
exec_args,2,ls,/etc/security
exec_env
,49,MANPATH=/usr/share/man,USER=jdoe,GDM_KEYBOARD_LAYOUT=us,EDITOR=gedit,
LANG=en_US.UTF-8,GDM_LANG=en_US.UTF-8,PS1=#,GDMSESSION=gnome,SESSIONTYPE=1,SHLVL=2,
HOME=/home/jdoe,LOGNAME=jdoe,G_FILENAME_ENCODING=@locale,UTF-8,
PRINTER=example-dbl,...,_=/usr/bin/ls
subject,jdoe,root,root,root,root,2502,50036632,82 0 mach1
return,success,0
```

▼ Cómo buscar registros de auditoría de los cambios realizados en archivos específicos

Si tiene como objetivo registrar las escrituras de los archivos en comparación con un número limitado de archivos, como `/etc/passwd` y los archivos en el directorio `/etc/default`, puede utilizar el comando `auditreduce` para ubicar los archivos.

Antes de empezar

El rol `root` puede realizar cada tarea en este procedimiento.

Si tienen derechos administrativos distribuidos en su organización, tenga en cuenta lo siguiente:

- Un administrador con el perfil de derechos de configuración de auditoría puede ejecutar el comando `auditconfig`.
- Un administrador con el perfil de derechos de revisión de auditoría puede ejecutar el comando `auditreduce`.
- Sólo el rol `root` puede asignar indicadores de auditoría.

Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

1. **Realice uno de los siguientes pasos para auditar cambios en archivos.**

   - Auditoría de la clase `fw`.

     Agregar la clase `fw` a los indicadores de auditoría de un usuario o rol genera menos registros que agregar la clase a la máscara de preselección de auditoría en todo el sistema. Lleve a cabo uno de los pasos siguientes:

     - Agregue la clase `fw` a roles concretos.

       ```
       # rolemod -K audit_flags=fw:no root
       # rolemod -K audit_flags=fw:no sysadm
       # rolemod -K audit_flags=fw:no auditadm
       # rolemod -K audit_flags=fw:no netadm
       ```

     - Agregue la clase `fw` a los indicadores de todo el sistema.

       ```
       # auditconfig -getflags
       ```

```
active user default audit flags = lo(0x1000,0x1000)
configured user default audit flags = lo(0x1000,0x1000)

# auditconfig -setflags lo,fw
user default audit flags = lo,fw(0x1002,0x1002)
```

- Audite escrituras con éxito de archivos.

  Auditar éxitos genera menos registros que auditar fallos y éxitos. Lleve a cabo uno de los pasos siguientes:

  - Agregue la clase `+fw` a roles concretos.

    ```
    # rolemod -K audit_flags=+fw:no root
    # rolemod -K audit_flags=+fw:no sysadm
    # rolemod -K audit_flags=+fw:no auditadm
    # rolemod -K audit_flags=+fw:no netadm
    ```

  - Agregue la clase `+fw` a los indicadores de todo el sistema.

    ```
    # auditconfig -getflags
    active user default audit flags = lo(0x1000,0x1000)
    configured user default audit flags = lo(0x1000,0x1000)

    # auditconfig -setflags lo,+fw
    user default audit flags = lo,+fw(0x1002,0x1000)
    ```

2. **Obtenga los registros de auditoría para archivos específicos mediante el comando `auditreduce`.**

   ```
   # auditreduce -o file=/etc/passwd,/etc/default -O filechg
   ```

   El comando `auditreduce` busca en la pista de auditoría todas las instancias del argumento `file`. El comando crea un archivo binario con el sufijo `filechg` que contiene todos los registros que incluyen la ruta de los archivos de interés. Consulte la página del comando man `auditreduce`(1M) para conocer la sintaxis de la opción `-o file=` *pathname*.

3. **Lea el archivo `filechg` mediante el comando `praudit .`**

   ```
   # praudit *filechg
   ```

▼ Cómo actualizar la máscara de preselección de usuarios con sesión iniciada

Este procedimiento describe cómo auditar usuarios que ya iniciaron sesión en busca de cambios en la máscara de preselección de auditoría en todo el sistema. Por lo general, puede realizar esta tarea indicando a los usuarios que cierren sesión y luego vuelvan a iniciar sesión. Como

alternativa, en un rol que tiene asignado el perfil de derechos de gestión de procesos, se pueden terminar manualmente sesiones activas con el comando `kill`. Las nuevas sesiones heredan la nueva máscara de preselección.

Sin embargo, cerrar sesiones de usuario puede ser poco práctico. Como alternativa, puede utilizar el comando `auditconfig` para cambiar de forma dinámica la máscara de preselección de cada usuario con sesión iniciada.

El siguiente procedimiento presupone que ha cambiado la máscara de preselección de auditoría en todo el sistema de `lo` a `lo,ex` ejecutando el siguiente comando:

```
# auditconfig -setflags lo,ex
```

Antes de empezar Debe convertirse en un administrador con el perfil de derechos de configuración de auditoría asignado. Para finalizar las sesiones de usuario, es necesario que se convierta en administrador con el perfil de derechos de administración de procesos asignado. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

1. **Enumere los usuarios regulares que han iniciado sesión y sus ID de proceso.**

```
# who -a
jdoe  - vt/2         Jan 25 07:56  4:10   1597   (:0)
jdoe  + pts/1        Jan 25 10:10   .     1706   (:0.0)
...
jdoe  + pts/2        Jan 25 11:36  3:41   1706   (:0.0)
```

2. **Para realizar una comparación con posterioridad, visualice la máscara de preselección de cada usuario.**

```
# auditconfig -getpinfo 1706
audit id = jdoe(1234)
process preselection mask = lo(0x1000,0x1000)
terminal id (maj,min,host) = 9426,65559,mach1(192.168.123.234)
audit session id = 103203403
```

3. **Modifique la máscara de preselección apropiada mediante la ejecución de uno o más de los siguientes comandos:**

```
# auditconfig -setpmask 1706 lo,ex          /* for this process */

# auditconfig -setumask jdoe lo,ex          /* for this user */

# auditconfig -setsmask 103203403 lo,ex     /* for this session */
```

4. **Verifique que la máscara de preselección para el usuario haya cambiado.**
Por ejemplo, compruebe un proceso que existía antes de haber cambiado la máscara.

```
# auditconfig -getpinfo 1706
audit id = jdoe(1234)
process preselection mask = ex,lo(0x40001000,0x40001000)
```

```
terminal id (maj,min,host) = 9426,65559,mach1(192.168.123.234)
audit session id = 103203403
```

▼ Cómo evitar la auditoría de eventos específicos

Con fines de mantenimiento, a veces, un sitio quiere evitar que se auditen eventos.

Antes de empezar Debe asumir el rol `root`. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

1. **Cambie la clase del evento a la clase `no`.**

   Nota - Para obtener información sobre los efectos de modificar un archivo de configuración de auditoría, consulte "Archivos de configuración de auditoría y empaquetado" [119].

   Por ejemplo, los eventos 26 y 27 pertenecen a la clase `pm`.

   ```
   ## audit_event file
   ...
   25:AUE_VFORK:vfork(2):ps
   26:AUE_SETGROUPS:setgroups(2):pm
   27:AUE_SETPGRP:setpgrp(2):pm
   28:AUE_SWAPON:swapon(2):no
   ...
   ```

   Cambie estos eventos a la clase `no`.

   ```
   ## audit_event file
   ...
   25:AUE_VFORK:vfork(2):ps
   26:AUE_SETGROUPS:setgroups(2):no
   27:AUE_SETPGRP:setpgrp(2):no
   28:AUE_SWAPON:swapon(2):no
   ...
   ```

   Si la clase `pm` está asiendo auditada actualmente, las sesiones existentes aún auditarán los eventos 26 y 27. Para detener la auditoría de estos eventos, debe actualizar las máscaras de preselección de los usuarios siguiendo las instrucciones de Cómo actualizar la máscara de preselección de usuarios con sesión iniciada [63].

   Atención - Nunca quite el comentario de eventos en el archivo `audit_event`. Este archivo es utilizado por el comando `praudit` para leer archivos binarios de auditoría. Los archivos de auditoría almacenados pueden contener eventos que se muestran en el archivo.

2. **Refresque los eventos del núcleo.**

```
# auditconfig -conf
Configured 283 kernel events.
```

▼ Cómo comprimir archivos de auditoría en un sistema de archivos dedicado

Los archivos de auditoría pueden crecer mucho. Puede establecer un límite superior para el tamaño de un archivo, como se muestra en el Ejemplo 4-3, “Limitación de tamaño de archivo para el complemento `audit_binfile`”. En este procedimiento, se utiliza la compresión para reducir el tamaño.

Antes de empezar Debe convertirse en un administrador al que se le ha asignado perfiles de derechos de gestión de sistemas de archivos ZFS y gestión de almacenamiento ZFS. El último perfil permite crear agrupaciones de almacenamiento. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

1. **Dedique un sistema de archivos ZFS para archivos de auditoría.**
   Para conocer el procedimiento, consulte Cómo crear sistemas de archivos ZFS para archivos de auditoría [76].

2. **Comprima la agrupación de almacenamiento ZFS mediante una de las siguientes opciones.**
   Con ambas opciones, se comprime el sistema de archivos de auditoría. Después de que el servicio de auditoría se refresca, la razón de compresión se muestra.
   En los siguientes ejemplos, la agrupación ZFS `auditp/auditf` es el conjunto de datos.

   - **Utilice el algoritmo de compresión predeterminado.**

     ```
     # zfs set compression=on auditp/auditf
     # audit -s
     # zfs get compressratio auditp/auditf
     NAME           PROPERTY       VALUE  SOURCE
     auditp/auditf  compressratio  4.54x  -
     ```

   - **Utilice un algoritmo de compresión superior.**

     ```
     # zfs set compression=gzip-9 auditp/auditf
     # zfs get compression auditp/auditf
     NAME           PROPERTY     VALUE     SOURCE
     auditp/auditf  compression  gzip-9    local
     ```

     El algoritmo de compresión `gzip-9` genera archivos que ocupan un tercio menos de espacio que el algoritmo de compresión predeterminado, `lzjb`. Para obtener más

información, consulte el Capítulo 5, “Administración de sistemas de archivos ZFS de Oracle Solaris” de “Gestión de sistemas de archivos ZFS en Oracle Solaris 11.2 ”.

3. **Refresque el servicio de auditoría.**

```
# audit -s
```

4. **(Opcional) Verifique la nueva configuración de compresión.**

Por ejemplo, si utiliza el algoritmo de compresión superior, la información será similar a la siguiente:

```
# zfs get compressration auditp/auditf
NAME           PROPERTY       VALUE  SOURCE
auditp/auditf  compressratio  16.89x  -
```

Cómo auditar transferencias de archivos FTP y SFTP

El servicio FTP crea registros de sus transferencias de archivos. El servicio SFTP, que se ejecuta bajo el protocolo `ssh`, puede ser auditado mediante la preselección de la clase de auditoría `ft`. Se pueden auditar los inicios de sesión en ambos servicios.

Nota - Para obtener información sobre cómo registrar comandos y transferencias de archivos del servicio FTP, consulte la página del comando man `proftpd`(8).

Para conocer las opciones de registro disponibles, lea ProFTPD Logging (http://www.proftpd.org/docs/howto/Logging.html).

- **Realice una de las siguientes acciones en función de si desea auditar SFTP o FTP.**

  - Para registrar el acceso a `sftp` y las transferencias de archivos, edite la clase `ft`.

    La clase `ft` incluye las siguientes transacciones SFTP:

```
% auditrecord -c ft
file transfer: chmod ...
file transfer: chown ...
file transfer: get ...
file transfer: mkdir ...
file transfer: put ...
file transfer: remove ...
file transfer: rename ...
file transfer: rmdir ...
```

```
file transfer: session start ...
file transfer: session end ...
file transfer: symlink ...
file transfer: utimes
```

- Para registrar el acceso al servidor FTP, audite la clase `lo`.

  Como indica el siguiente ejemplo de salida, el inicio y cierre de sesión del daemon `proftpd` generan registros de auditoría.

```
% auditrecord -c lo | more
...
FTP server login
program     proftpd             See in.ftpd(1M)
event ID    6165                AUE_ftpd
class       lo                  (0x0000000000001000)
header
subject
[text]                      error message
return

FTP server logout
program     proftpd             See in.ftpd(1M)
event ID    6171                AUE_ftpd_logout
class       lo                  (0x0000000000001000)
header
subject
return
...
```

Configuración del servicio de auditoría en zonas

El servicio de auditoría audita todo el sistema, incluidos los eventos de auditoría en las zonas. Un sistema que tenga zonas no globales instaladas puede auditar todas las zonas de forma idéntica o puede configurar la auditoría por zona. Para obtener más información, consulte “Planificación de la auditoría en zonas” [28].

Cuando se auditan las zonas no globales exactamente como se audita la zona global, los administradores de la zona no global pueden no tener acceso a los registros de auditoría. Además, el administrador de la zona global puede modificar las máscaras de preselección de auditoría de los usuarios en las zonas no globales.

Cuando se auditan las zonas no globales de forma individual, los registros de auditoría están visibles para la zona no global y para la zona global desde el directorio raíz de zonas no globales.

▼ Cómo configurar todas las zonas de forma idéntica para la auditoría

Este procedimiento activa las auditorías de cada zona de forma idéntica. Este método requiere la menor sobrecarga del equipo y la menor cantidad de recursos administrativos.

Antes de empezar Debe asumir el rol `root`. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

1. **Configure la zona global para la auditoría.**

   Complete las tareas en "Configuración del servicio de auditoría" [44], con las siguientes excepciones:

   - No active la política de auditoría `perzone`.
   - Establezca la política `zonename`. Esta política agrega el nombre de la zona a cada registro de auditoría.

     ```
     # auditconfig -setpolicy +zonename
     ```

2. **Si modifica archivos de configuración de auditoría, cópielos de la zona global a cada zona no global.**

   Si modifica el archivo `audit_class` o `audit_event`, cópielo de una de estas dos formas:

   - Puede montar en bucle de retorno los archivos.
   - Puede copiar los archivos.

   La zona no global debe estar en ejecución.

   - **Monte los archivos `audit_class` y `audit_event` cambiados como un sistema de archivos de bucle de retorno (`lofs`).**

     a. **Desde la zona global, detenga la zona no global.**

        ```
        # zoneadm -z non-global-zone halt
        ```

     b. **Cree un montaje en bucle de retorno de sólo lectura para cada archivo de configuración de auditoría que haya modificado en la zona global.**

        ```
        # zonecfg -z non-global-zone
        zone: add fs
        zone/fs: set special=/etc/security/audit-file
        zone/fs: set dir=/etc/security/audit-file
        zone/fs: set type=lofs
        zone/fs: add options [ro,nodevices,nosetuid]
        zone/fs: commit
        ```

```
zone/fs: end
zone: exit
#
```

c. Para que los cambios entren en vigencia, inicie la zona no global.

```
# zoneadm -z non-global-zone boot
```

Más adelante, si modifica un archivo de configuración de auditoría en la zona global, debe reiniciar cada zona para refrescar los archivos montados en bucle de retorno en las zonas no globales.

- **Copie los archivos.**

a. Desde la zona global, muestre el directorio `/etc/security` en cada zona no global.

```
# ls /zone/zonename/root/etc/security/
```

b. Copie los archivos `audit_class` y `audit_event` cambiados en el directorio `/etc/security` de cada zona.

```
# cp /etc/security/audit-file /zone/zonename/root/etc/security/audit-file
```

Más adelante, si cambia uno de estos archivos en la zona global, debe copiar el archivo cambiado a las zonas no globales.

Las zonas no globales se auditan cuando se reinicia el servicio de auditoría en la zona global o cuando las zonas se reinician.

ejemplo 3-17 Montaje de archivos de configuración de auditoría como montajes de bucle de retorno en una zona

En este ejemplo, el administrador del sistema ha modificado los archivos `audit_class` , `audit_event` y `audit_warn`.

El archivo `audit_warn` solamente se lee en la zona global, por lo que no se tiene que montar en las zonas no globales.

En este sistema, `machine1`, el administrador ha creado dos zonas no globales, `machine1-webserver` y `machine1-appserver`. El administrador ha terminado de modificar los archivos de configuración de auditoría. Si el administrador más tarde modifica los archivos, la zona se debe reiniciar para volver a leer los montajes de bucle de retorno.

```
# zoneadm -z machine1-webserver halt
# zoneadm -z machine1-appserver halt
# zonecfg -z machine1-webserver
webserver: add fs
webserver/fs: set special=/etc/security/audit_class
```

```
webserver/fs: set dir=/etc/security/audit_class
webserver/fs: set type=lofs
webserver/fs: add options [ro,nodevices,nosetuid]
webserver/fs: commit
webserver/fs: end
webserver: add fs
webserver/fs: set special=/etc/security/audit_event
webserver/fs: set dir=/etc/security/audit_event
webserver/fs: set type=lofs
webserver/fs: add options [ro,nodevices,nosetuid]
webserver/fs: commit
webserver/fs: end
webserver: exit
#

# zonecfg -z machine1-appserver
appserver: add fs
appserver/fs: set special=/etc/security/audit_class
appserver/fs: set dir=/etc/security/audit_class
appserver/fs: set type=lofs
appserver/fs: add options [ro,nodevices,nosetuid]
appserver/fs: commit
appserver/fs: end
appserver: exit
```

Cuando las zonas no globales se reinician, los archivos `audit_class` y `audit_event` son de sólo lectura en las zonas.

▼ Cómo configurar la auditoría por zona

Este procedimiento permite que distintos administradores de zonas controlen el servicio de auditoría en sus zonas. Para obtener una lista completa de las opciones de políticas, consulte la página del comando man `auditconfig`(1M).

Antes de empezar Para configurar la auditoría, debe convertirse en administrador con el perfil de derechos de configuración de auditoría asignado. Para activar el servicio de auditoría, debe convertirse en administrador con el perfil de derechos de control de auditoría asignado. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

1. **En la zona global, configure la auditoría.**

   a. **Complete las tareas en "Configuración del servicio de auditoría" [44].**

   b. **Agregue la política de auditoría `perzone`. Para el comando, consulte el Ejemplo 3-12, "Configuración de la política de auditoría `perzone`".**

Nota - No es necesario activar el servicio de auditoría en la zona global.

2. **En cada zona no global que planea auditar, configure los archivos de auditoría.**

   a. **Complete las tareas en "Configuración del servicio de auditoría" [44].**

   b. **No configure los valores de auditoría en todo el sistema.**

      Específicamente, no agregue la política `perzone` o `ahlt` al archivo a la zona no global.

3. **Active la auditoría en su zona.**

```
myzone# audit -s
```

ejemplo 3-18 Desactivación de la auditoría en una zona no global

Este ejemplo funciona si está establecida la política de auditoría `perzone`. El administrador de zonas de la zona `noaudit` desactiva la auditoría para dicha zona.

```
noauditzone # auditconfig -getcond
audit condition = auditing
noauditzone # audit -t
noauditzone # auditconfig -getcond
audit condition = noaudit
```

Ejemplo: configuración de auditoría de Oracle Solaris

Esta sección proporciona un ejemplo de cómo configurar e implementar la auditoría de Oracle Solaris. Empieza con la configuración de distintos atributos del servicio de acuerdo con necesidades y requisitos específicos. Después de que la configuración finaliza, el servicio de auditoría se inicia para aplicar los valores de configuración. Cada vez que necesite revisar una configuración de auditoría existente para satisfacer nuevos requisitos, siga la misma secuencia de acciones de este ejemplo:

1. Configure los parámetros de auditoría.
2. Refresque el servicio de auditoría.
3. Verifique la nueva configuración de auditoría.

- En primer lugar, el administrador agrega una política temporal.

```
# auditconfig -t -setpolicy +zonename
# auditconfig -getpolicy
configured audit policies = ahlt,arge,argv,perzone
```

```
active audit policies = ahlt,arge,argv,perzone,zonename
```

- A continuación, el administrador especifica controles de colas.

```
# auditconfig -setqctrl 200 20 0 0
# auditconfig -getqctrl
configured audit queue hiwater mark (records) = 200
configured audit queue lowater mark (records) = 20
configured audit queue buffer size (bytes) = 8192
configured audit queue delay (ticks) = 20
active audit queue hiwater mark (records) = 200
active audit queue lowater mark (records) = 20
active audit queue buffer size (bytes) = 8192
active audit queue delay (ticks) = 20
```

- A continuación, el administrador especifica atributos de complementos.
  - Para el complemento `audit_binfile`, el administrador elimina el valor `qsize`.

```
# auditconfig -getplugin audit_binfile
Plugin: audit_binfile
Attributes: p_dir=/audit/sys1.1,/var/audit;
p_minfree=2;p_fsize=4G;
Queue size: 200
# auditconfig -setplugin audit_binfile  "" 0
# auditconfig -getplugin audit_binfile
Plugin: audit_binfile
Attributes: p_dir=/audit/sys1.1,/var/audit
p_minfree=2;p_fsize=4G;
```

  - Para el complemento `audit_syslog`, el administrador especifica que los eventos de inicio y cierre de sesión con éxito y los archivos ejecutables con fallos se envíen a `syslog`. `qsize` para este complemento se define en 150.

```
# auditconfig -setplugin audit_syslog active p_flags=+lo,-ex 150
# auditconfig -getplugin audit_syslog
auditconfig -getplugin audit_syslog
Plugin: audit_syslog
Attributes: p_flags=+lo,-ex;
Queue size: 150
```

  - El administrador no configura ni usa el complemento `audit_remote`.
- Luego, el administrador refresca el servicio de auditoría y verifica la configuración.
  - La política `zonename` temporal ya no está definida.

```
# audit -s
# auditconfig -getpolicy
configured audit policies = ahlt,arge,argv,perzone
active audit policies = ahlt,arge,argv,perzone
```

  - Los controles de colas permanecen igual.

```
# auditconfig -getqctrl
configured audit queue hiwater mark (records) = 200
configured audit queue lowater mark (records) = 20
configured audit queue buffer size (bytes) = 8192
configured audit queue delay (ticks) = 20
active audit queue hiwater mark (records) = 200
active audit queue lowater mark (records) = 20
active audit queue buffer size (bytes) = 8192
active audit queue delay (ticks) = 20
```

- El complemento `audit_binfile` no tiene un tamaño de cola especificado. El complemento `audit_syslog` tiene un tamaño de cola especificado.

```
# auditconfig -getplugin
Plugin: audit_binfile
Attributes: p_dir=/var/audit;p_fsize=4G;p_minfree=2;

Plugin: audit_syslog
Attributes: p_flags=+lo,-ex;
Queue size: 50
...
```

♦ ♦ ♦ CAPÍTULO 4

Supervisión de actividades del sistema

En este capítulo, se proporcionan procedimientos para ayudarlo a configurar logs de auditoría que le permiten supervisar las actividades del sistema. Además, en los siguientes capítulos, se describen otras tareas de gestión de auditoría:

- Capítulo 3, Gestión del servicio de auditoría
- Capítulo 5, Cómo trabajar con datos de auditoría
- Capítulo 6, Análisis y resolución de problemas del servicio de auditoría

Para obtener una descripción general del servicio de auditoría, consulte el Capítulo 1, Acerca de la auditoría en Oracle Solaris. Para obtener sugerencias de planificación, consulte el Capítulo 2, Planificación de la auditoría. Para obtener información de referencia, consulte el Capítulo 7, Referencia sobre auditoría.

Configuración de logs de auditoría

Hay dos complementos de auditoría, `audit_binfile` y `audit_syslog` , que pueden crear logs de auditoría locales. Las siguientes tareas explican cómo configurar estos logs.

Configuración de logs de auditoría

En el siguiente mapa de tareas, se hace referencia a los procedimientos para configurar registros de auditoría para los distintos complementos. La configuración de los registros para el complemento `audit_binfile` es opcional. Los registros para otros complementos deben ser configurados por un administrador.

TABLA 4-1 Configuración de mapa de tareas de logs de auditoría

Tarea	Descripción	Más instrucciones
Agregar almacenamiento local para el complemento `audit_binfile`	Crea espacio en disco adicional para los archivos de auditoría y los protege con los permisos de archivo	Cómo crear sistemas de archivos ZFS para archivos de auditoría [76]

Tarea	Descripción	Más instrucciones
Asignar almacenamiento para el complemento `audit_binfile`	Identifica directorios para registros de auditoría binarios	Cómo asignar espacio de auditoría para la pista de auditoría [80]
Configurar transmisión por secuencias de registros de auditoría a un sistema remoto	Permite enviar registros de auditoría a un repositorio remoto por medio de un mecanismo protegido	Cómo enviar archivos de auditoría a un repositorio remoto [83]
Configurar almacenamiento remoto para los archivos de auditoría	Le permite recibir los registros de auditoría en un sistema remoto	Cómo configurar un repositorio remoto para los archivos de auditoría [85]
Configurar el almacenamiento para el complemento `audit_syslog`.	Permite transmitir eventos de auditoría en formato de texto a `syslog`.	Cómo configurar registros de auditoría `syslog` [89]

▼ Cómo crear sistemas de archivos ZFS para archivos de auditoría

El procedimiento siguiente muestra cómo crear una agrupación ZFS para los archivos de auditoría, así como los sistemas de archivos y los puntos de montaje correspondientes. De manera predeterminada, el sistema de archivos `/var/audit` contiene archivos de auditoría para el complemento `audit_binfile`.

Antes de empezar Debe convertirse en un administrador al que se le ha asignado perfiles de derechos de gestión de sistemas de archivos ZFS y gestión de almacenamiento ZFS. El último perfil permite crear agrupaciones de almacenamiento. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

1. **Determine la cantidad de espacio en disco que sea necesaria.**

   Asigne, por lo menos, 200 MB de espacio en disco por host. Sin embargo, la cantidad de auditoría que necesita es la que dicta los requisitos de espacio en disco. Los requisitos de espacio en disco pueden ser mucho mayores que los que indica esta figura.

   Nota - La preselección de clases predeterminada crea archivos en `/var/audit` que aumentan en 80 bytes aproximadamente por cada instancia registrada de un evento en la clase `lo`, como un inicio de sesión, un cierre de sesión o una asunción de rol.

2. **Cree una agrupación de almacenamiento ZFS reflejada.**

   El comando `zpool create` crea una agrupación de almacenamiento, es decir, un contenedor para los sistemas de archivos ZFS. Para obtener más información, consulte el Capítulo 1,

"Sistema de archivos ZFS de Oracle Solaris (introducción)" de "Gestión de sistemas de archivos ZFS en Oracle Solaris 11.2 ".

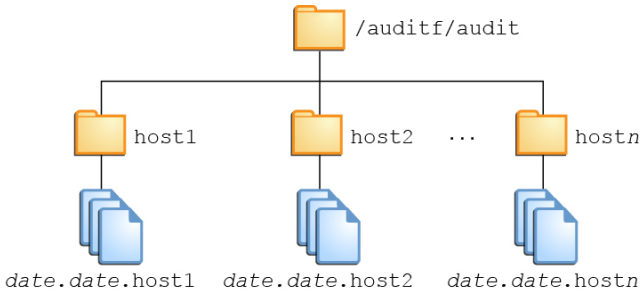
```
# zpool create audit-pool mirror disk1 disk2
```

Por ejemplo, cree la agrupación `auditp` de dos discos, `c3t1d0` y `c3t2d0`, y refléjelos.

```
# zpool create auditp mirror c3t1d0 c3t2d0
```

3. **Cree un sistema de archivos ZFS y un punto de montaje para los archivos de auditoría.**

   Cree el sistema de archivos y el punto de montaje con un comando. En el momento de la creación, se monta el sistema de archivos. Por ejemplo, la siguiente ilustración muestra el almacenamiento de pista de auditoría almacenado por nombre de host.



Nota - Si tiene previsto cifrar el sistema de archivos, debe cifrar el sistema de archivos en el momento de la creación. Si desea ver un ejemplo, consulte el Ejemplo 4-1, "Creación de un sistema de archivos cifrado para archivos de auditoría".

El cifrado requiere gestión. Por ejemplo, una frase de contraseña se requiere en el momento del montaje. Para obtener más información, consulte "Cifrado de sistemas de archivos ZFS" de "Gestión de sistemas de archivos ZFS en Oracle Solaris 11.2 ".

```
# zfs create -o mountpoint=/mountpoint audit-pool/mountpoint
```

Por ejemplo, cree el punto de montaje `/audit` para el sistema de archivos `auditf`.

```
# zfs create -o mountpoint=/audit auditp/auditf
```

4. **Cree un sistema de archivos ZFS para los archivos de auditoría.**

```
# zfs create -p auditp/auditf/system
```

Por ejemplo, cree un sistema de archivos ZFS sin cifrar para el sistema `sys1`.

```
# zfs create -p auditp/auditf/sys1
```

5. **(Opcional) Cree sistemas de archivos adicionales para archivos de auditoría.**

   Un motivo para crear sistemas de archivos adicionales es evitar el desbordamiento de la auditoría. Puede establecer una cuota ZFS por sistema de archivos, como se muestra en el Paso 8. El alias de correo electrónico `audit_warn` le notifica cuando se alcanza cada cuota. Para liberar espacio, puede mover los archivos de auditoría cerrados a un servidor remoto.

   ```
   # zfs create -p auditp/auditf/sys1.1

   # zfs create -p auditp/auditf/sys1.2
   ```

6. **Proteja el sistema de archivos de auditoría principal.**

   Las siguientes propiedades ZFS se establecen en `off` para todos los sistemas de archivos en la agrupación:

   ```
   # zfs set devices=off auditp/auditf

   # zfs set exec=off auditp/auditf

   # zfs set setuid=off auditp/auditf
   ```

7. **Comprima los archivos de auditoría en la agrupación.**

   Normalmente, la compresión está definida en ZFS, en el nivel del sistema de archivos. Sin embargo, debido a que todos los sistemas de archivos de esta agrupación contienen archivos de auditoría, la compresión se establece en el conjunto de datos de nivel superior para la agrupación.

   ```
   # zfs set compression=on auditp
   ```

   Consulte también "Interacciones entre propiedades de compresión, eliminación de datos duplicados y cifrado de ZFS" de "Gestión de sistemas de archivos ZFS en Oracle Solaris 11.2 ".

8. **Defina las cuotas.**

   Puede definir cuotas en el sistema de archivos principal, los sistemas de archivos descendientes o en ambos. Si define una cuota en el sistema de archivos de auditoría principal, las cuotas en los sistemas de archivos descendientes imponen un límite adicional.

   a. **Defina una cuota en el sistema de archivos de auditoría principal.**

      En el siguiente ejemplo, cuando ambos discos en la agrupación `auditp` alcanzan la cuota, la secuencia de comandos `audit_warn` notifica al administrador de la auditoría.

      ```
      # zfs set quota=510G auditp/auditf
      ```

   b. **Defina una cuota en los sistemas de archivos de auditoría descendientes.**

      En el siguiente ejemplo, cuando se alcanza la cuota para el sistema de archivos `auditp/auditf/`*system*, la secuencia de comandos `audit_warn` notifica al administrador de la auditoría.

```
# zfs set quota=170G auditp/auditf/sys1

# zfs set quota=170G auditp/auditf/sys1.1

# zfs set quota=165G auditp/auditf/sys1.2
```

9. **Para una agrupación grande, limite el tamaño de los archivos de auditoría.**

   De manera predeterminada, un archivo de auditoría puede crecer hasta alcanzar el tamaño de la agrupación. Para facilitar la gestión, limite el tamaño de los archivos de auditoría. Consulte Ejemplo 4-3, “Limitación de tamaño de archivo para el complemento `audit_binfile`”.

ejemplo 4-1 Creación de un sistema de archivos cifrado para archivos de auditoría

Para cumplir con los requisitos de seguridad del sitio, el administrador realiza los siguientes pasos:

1. Crea, si es necesario, una nueva agrupación ZFS para almacenar los logs de auditoría cifrados.
2. Genera una clave de cifrado.
3. Crea el sistema de archivos de auditoría con el cifrado activado para almacenar los logs de auditoría y define el punto de montaje.
4. Configura la auditoría para utilizar el directorio de cifrado.
5. Refresca el servicio de auditoría para aplicar los nuevos valores de configuración.

```
# zpool create auditp mirror disk1 disk2

# pktool genkey keystore=file outkey=/filename keytype=aes keylen=256

# zfs create -o encryption=aes-256-ccm \
-o keysource=raw,file:///filename \
-o compression=on -o mountpoint=/audit auditp/auditf

# auditconfig -setplugin audit_binfile p_dir=/audit/

# audit -s
```

Debe hacer una copia de seguridad y proteger el archivo donde se almacena la clave, como *filename* en el ejemplo.

Cuando el administrador crea sistemas de archivos adicionales en el sistema de archivos `auditf`, estos sistemas de archivos descendientes también se cifran.

ejemplo 4-2 Configuración de una cuota en el directorio `/var/audit`

En este ejemplo, el administrador define una cuota en el sistema de archivos de auditoría predeterminado. Cuando se alcanza esta cuota, la secuencia de comandos `audit_warn` advierte al administrador de la auditoría.

```
# zfs set quota=252G rpool/var/audit
```

▼ Cómo asignar espacio de auditoría para la pista de auditoría

En este procedimiento, utilice atributos para el complemento `audit_binfile` con el fin de asignar espacio en disco adicional a la pista de auditoría.

Antes de empezar Debe convertirse en un administrador con el perfil de derechos de configuración de auditoría asignado. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

1. **Determine los atributos para el complemento `audit_binfile`.**

   Lea la sección `OBJECT ATTRIBUTES` de la página del comando man `audit_binfile`(5).

   ```
   # man audit_binfile

   ...
   OBJECT ATTRIBUTES
   The p_dir attribute specifies where the audit files will be created.
   The directories are listed in the order in which they are to be used.

   The p_minfree attribute defines the percentage of free space that the
   audit system requires before the audit daemon invokes the audit_warn
   script.

   The p_fsize attribute defines the maximum size that an audit
   file can become before it is automatically closed and a new
   audit file is opened. ... The format of the p_fsize value can
   be specified as an exact value in bytes or in a human-readable
   form with a suffix of  B,  K, M, G, T, P, E, Z (for bytes,
   kilobytes, megabytes, gigabytes, terabytes,  petabytes, exabytes,
   or zettabytes, respectively). Suffixes of KB, MB, GB, TB, PB, EB,
   and ZB are also accepted.
   ```

2. **Para agregar directorios a la pista de auditoría, especifique el atributo `p_dir`.**

   El sistema de archivos predeterminado es `/var/audit`.

   ```
   # auditconfig -setplugin audit_binfile p_dir=/audit/sys1.1,/var/audit
   ```

El comando anterior establece el sistema de archivos `/audit/sys1.1` como el directorio principal para archivos de auditoría y el sistema de archivos `/var/audit` como el directorio secundario. En este escenario, `/var/audit` es el directorio de último recurso. Para que esta configuración se realice correctamente, el sistema de archivos `/audit/sys1.1` debe existir.

Un sistema de archivos similar se crea en Cómo crear sistemas de archivos ZFS para archivos de auditoría [76].

3. **Refresque el servicio de auditoría.**

   El comando `auditconfig -setplugin` define el valor *configurado*. Este valor es una propiedad del servicio de auditoría, por lo que se restaura cuando el servicio se refresca o se reinicia. El valor configurado se convierte en *activo* cuando el servicio de auditoría se refresca o se actualiza. Para obtener información sobre valores activos y configurados, consulte la página del comando man `auditconfig`(1M).

   ```
   # audit -s
   ```

ejemplo 4-3 Limitación de tamaño de archivo para el complemento `audit_binfile`

En el siguiente ejemplo, el tamaño de un archivo de auditoría binario está establecido en un tamaño específico. El tamaño está especificado en megabytes.

```
# auditconfig -setplugin audit_binfile p_fsize=4M

# auditconfig -getplugin audit_binfile
Plugin: audit_binfile
Attributes: p_dir=/var/audit;p_fsize=4M;p_minfree=1;
```

De manera predeterminada, un archivo de auditoría puede crecer sin límite. Para crear archivos de auditoría más pequeños, el administrador especifica un límite de tamaño de archivo de 4 MB. El servicio de auditoría crea un nuevo archivo cuando se alcanza el límite de tamaño. El límite de tamaño de archivo entra en vigor después de que el administrador refresca el servicio de auditoría.

```
# audit -s
```

ejemplo 4-4 Especificación del tiempo para la rotación de logs

En el siguiente ejemplo, un límite de tiempo se define para un archivo de auditoría. El límite de tiempo se especifica en términos de horas, días, semanas, meses o años.

```
# auditconfig -setplugin audit_binfile "p_age=1w"

# auditconfig -getplugin audit_binfile
Plugin: audit_binfile
Attributes: p_dir=/var/audit;p_age=1w;
```

```
Queue size: 200
```

De manera predeterminada, un archivo de auditoría no tiene ningún límite de tiempo. El archivo permanece abierto indefinidamente hasta que una operación externa provoca una rotación de archivos. El administrador define el límite de tiempo del archivo a una semana, después de la cual se abre un nuevo archivo de auditoría. Para implementar el nuevo límite de tiempo, el administrador refresca el servicio de auditoría.

```
# audit -s
```

ejemplo 4-5 Especificación de varios cambios para un complemento de auditoría

En el siguiente ejemplo, el administrador en un sistema con un alto rendimiento y una agrupación ZFS grande cambia el tamaño de la cola, el tamaño del archivo binario y la advertencia del límite variable para el complemento `audit_binfile`. El administrador permite que los archivos de auditoría crezcan a 4 GB, es advertido cuando queda un 2% de la agrupación ZFS y duplica el tamaño de la cola permitido. El tamaño predeterminado de la cola es la marca de agua superior para la cola de la auditoría del núcleo, `100`, como en `active audit queue hiwater mark (records) = 100`. También se configura el archivo de auditoría para que tenga un límite de tiempo de 2 semanas.

```
# auditconfig -getplugin audit_binfile
Plugin: audit_binfile
Attributes: p_dir=/var/audit;p_fsize=2G;p_minfree=1;

# auditconfig -setplugin audit_binfile \
      "p_minfree=2;p_fsize=4G;p_age=2w" 200

# auditconfig -getplugin audit_binfile
Plugin: audit_binfile
Attributes: p_dir=/var/audit;p_fsize=4G;p_minfree=2;p_age=2w;
Queue size: 200
```

Las especificaciones cambiadas entran en vigor después de que el administrador refresca el servicio de auditoría.

```
# audit -s
```

ejemplo 4-6 Eliminación del tamaño de la cola de un complemento de auditoría

En el siguiente ejemplo, se elimina el tamaño de la cola para el complemento `audit_binfile`.

```
# auditconfig -getplugin audit_binfile
Plugin: audit_binfile
Attributes: p_dir=/var/audit;p_fsize=4G;p_minfree=2;
Queue size: 200

# auditconfig -setplugin audit_binfile "" 0
```

```
# auditconfig -getplugin audit_binfile
Plugin: audit_binfile
Attributes: p_dir=/var/audit;p_fsize=4G;p_minfree=2;
```

Las comillas vacías (`""`) conservan los valores de atributo actuales. Un `0` al final, establece el tamaño de la cola para el complemento en el valor predeterminado.

El cambio en la especificación `qsize` para el complemento entra en vigor después de que el administrador refresca el servicio de auditoría.

```
# audit -s
```

ejemplo 4-7 Definición de un límite variable para advertencias

En este ejemplo, está configurado el nivel mínimo de espacio libre para todos los sistemas de archivos de auditoría, de modo que se emite una advertencia cuando aún queda disponible el 2 % del sistema de archivos.

```
# auditconfig -setplugin audit_binfile p_minfree=2
```

El porcentaje predeterminado es uno (`1`). Para una agrupación ZFS grande, seleccione un porcentaje razonablemente bajo. Por ejemplo, el 10 % de 16 TB es aproximadamente 16 GB, lo que advertiría al administrador de la auditoría cuando queda bastante espacio en disco. Un valor de `2` envía el mensaje `audit_warn` cuando quedan aproximadamente 2 GB de espacio en disco.

El alias de correo electrónico `audit_warn` recibe la advertencia. Para configurar el alias, consulte Cómo configurar el alias de correo electrónico `audit_warn` [55].

Para una agrupación grande, el administrador también limita el tamaño del archivo a 3 GB.

```
# auditconfig -setplugin audit_binfile p_fsize=3G
```

Las especificaciones `p_minfree` y `p_fsize` para el complemento entran en vigor después de que el administrador refresca el servicio de auditoría.

```
# audit -s
```

▼ Cómo enviar archivos de auditoría a un repositorio remoto

En este procedimiento, se utilizan atributos para el complemento `audit_remote` para enviar la pista de auditoría a un repositorio de auditoría remoto. Para configurar un repositorio remoto en un sistema Oracle Solaris, consulte Cómo configurar un repositorio remoto para los archivos de auditoría [85].

Antes de empezar Debe tener un receptor de archivos de auditoría en el repositorio remoto. Debe convertirse en un administrador con el perfil de derechos de configuración de auditoría asignado. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

1. **Determine los atributos para el complemento `audit_remote`.**

   Lea la sección `OBJECT ATTRIBUTES` de la página del comando man `audit_remote`(5).

   ```
   # man audit_remote

   ...
   OBJECT ATTRIBUTES
   The p_hosts attribute specifies the remote servers.
   You can also specify the port number and the GSS-API
   mechanism.

   The p_retries attribute specifies the number of retries for
   connecting and sending data. The default is 3.

   The p_timeout attribute specifies the number of seconds
   in which a connection times out.
   ```

   El puerto predeterminado es el puerto asignado por IANA `solaris_audit`, `16162/tcp`. El mecanismo predeterminado es `kerberos_v5`. El tiempo de espera predeterminado es de `5` s. También puede especificar un tamaño de cola para el complemento.

2. **Para especificar el sistema receptor remoto, utilice el atributo `p_hosts`.**

   En este ejemplo, el sistema receptor utiliza un puerto diferente.

   ```
   # auditconfig -setplugin audit_remote \
        p_hosts=ars.example.com:16088:kerberos_v5
   ```

3. **Especifique otros atributos del complemento que desee cambiar.**

   Por ejemplo, el siguiente comando especifica valores para todos los atributos opcionales:

   ```
   # auditconfig -setplugin audit_remote "p_retries=;p_timeout=3" 300
   ```

4. **Verifique los valores y, a continuación, active el complemento.**

   Por ejemplo, los siguientes comandos especifican y verifican los valores del complemento:

   ```
   # auditconfig -getplugin audit_remote
   Plugin: audit_remote (inactive)
   Attributes: p_hosts=ars.example.com:16088:kerberos_v5;p_retries=5;p_timeout=3;
   Queue size: 300

   # auditconfig -setplugin audit_remote active
   ```

5. **Refresque el servicio de auditoría.**

   El servicio de auditoría lee el cambio de complemento de auditoría después del refrescamiento.

```
# audit -s
```

ejemplo 4-8 Ajuste del tamaño de búfer de cola de auditoría

En este ejemplo, la cola de auditoría está llena detrás del complemento `audit_remote`. Este sistema auditado está configurado para auditar muchas clases y transmite a través de una red lenta, con mucho tráfico. El administrador aumenta el tamaño del búfer del complemento para permitir que la cola de auditoría crezca y no exceda el límite del búfer antes que los registros se eliminen de la cola.

```
audsys1 # auditconfig -setplugin audit_remote "" 1000

audsys1 # audit -s
```

▼ Cómo configurar un repositorio remoto para los archivos de auditoría

En este proceso, puede configurar un sistema remoto, el servidor de auditoría remoto (ARS), para recibir y almacenar los registros de auditoría de uno o más sistemas auditados. A continuación, debe activar el daemon de auditoría en el servidor remoto.

La configuración es doble. En primer lugar, configure los mecanismos de seguridad subyacentes para transportar de modo seguro los datos de auditoría, es decir, configure el KDC. En segundo lugar, se debe configurar el servicio de auditoría en el sistema auditado y el ARS. En este procedimiento, se ilustra un caso con un cliente auditado y un ARS, en el que el ARS y el KDC están en el mismo servidor. Del mismo modo, se pueden configurar escenarios más complejos. Los cuatro primeros pasos describen la configuración del KDC, mientras que el paso final describe la configuración del servicio de auditoría.

Antes de empezar Asegúrese de haber cumplido con lo siguiente:

- Ha asumido el rol de usuario `root`.
- Ha instalado los paquetes Kerberos, como se describe en Cómo prepararse para transmitir los registros de auditoría al almacenamiento remoto [34].
- Trabaja con un administrador que tiene configurado el sistema auditado, como se describe en Cómo enviar archivos de auditoría a un repositorio remoto [83].

1. **Si en su sitio aún no se ha configurado un KDC, configure uno.**

   Necesita un KDC en un sistema que tanto el sistema auditado y el ARS pueden utilizar, un principal de host para cada sistema y un principal de servicio `audit`. El siguiente ejemplo ilustra una estrategia de configuración de KDC:

```
arstore # kdcmgr -a audr/admin -r EXAMPLE.COM create master
```

Este comando usa el principal administrativo `audr/admin` para crear un KDC maestro en el dominio `EXAMPLE.COM`, activa el KDC maestro e inicia el servicio Kerberos.

2. **Verifique que el KDC esté disponible.**

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

```
# kdcmgr status

KDC Status Information
------------------------------------------
svc:/network/security/krb5kdc:default (Kerberos key distribution center)
State: online since Wed Feb 29 01:59:27 2012
See: man -M /usr/share/man -s 1M krb5kdc
See: /var/svc/log/network-security-krb5kdc:default.log
Impact: None.

KDC Master Status Information
------------------------------------------
svc:/network/security/kadmin:default (Kerberos administration daemon)
State: online since Wed Feb 29 01:59:28 2012
See: man -M /usr/share/man -s 1M kadmind
See: /var/svc/log/network-security-kadmin:default.log
Impact: None.

Transaction Log Information
------------------------------------------

Kerberos update log (/var/krb5/principal.ulog)
Update log dump :
Log version # : 1
Log state : Stable
Entry block size : 2048
Number of entries : 13
First serial # : 1
Last serial # : 13
First time stamp : Wed Feb 29 01:59:27 2012
Last time stamp : Mon Mar 5 19:29:28 2012


Kerberos Related File Information
------------------------------------------
(Displays any missing files)
```

3. **Agregue el principal del servicio `audit` al archivo keytab de KDC.**

   Puede agregar el principal escribiendo el comando `kadmin.local` en el sistema KDC. O bien, puede agregar de forma remota el principal mediante el comando `kadmin` y una contraseña. En este ejemplo, el sistema `arstore` está ejecutando el KDC.

```
# kadmin -p audr/admin
```

```
kadmin: addprinc -randkey audit/arstore.example.com@EXAMPLE.COM

kadmin: ktadd audit/arstore.example.com@EXAMPLE.COM
```

4. **En cada sistema auditado, agregue claves.**

   El destinatario y el remitente deben tener claves.

```
enigma # kclient

.. Enter the Kerberos realm:
EXAMPLE.COM

.. KDC hostname for the above realm:
arstore.example.com

.. Will this client need service keys ? [y/n]:
y
```

5. **Configure el servicio de auditoría en el ARS.**

   - **Para crear un grupo que acepta los registros de auditoría de cualquier sistema auditado en el dominio Kerberos, asigne un nombre a un grupo de conexión.**

```
# auditconfig -setremote group create Bank_A
```

     `Bank_A` es un grupo de conexión. Como el atributo `hosts` no está definido, este grupo acepta todas las conexiones, lo que significa que es un grupo *comodín*. Cualquier sistema auditado en este dominio Kerberos cuyo complemento `audit_remote` esté correctamente configurado puede alcanzar este ARS.

   - **Para limitar las conexiones a este grupo, especifique los sistemas auditados que pueden utilizar este repositorio.**

```
# auditconfig -setremote group Bank_A "hosts=enigma.example.com"
```

     El grupo de conexión `Bank_A` ahora sólo acepta conexiones del sistema `enigma`. Una conexión de cualquier otro host se rechaza.

   - **Para evitar que un archivo de auditoría en este grupo sea demasiado grande, establezca un tamaño máximo.**

```
# auditconfig -setremote group Bank_A "binfile_fsize=4GB"

# auditconfig -getremote
Audit Remote Server
Attributes: listen_address=;login_grace_time=30;max_startups=10;listen_port=0;
Connection group: Bank_A (inactive)
Attributes: binfile_dir=/var/audit;binfile_fsize=4GB;binfile_minfree=1;
```

```
hosts=enigma.example.com;
```

6. **Configure el servicio de auditoría en el sistema auditado.**

   Para especificar el ARS, utilice el atributo `p_hosts`.

```
enigma # auditconfig -setplugin audit_remote \
     active p_hosts=arstore.example.com

enigma # auditconfig -getplugin audit_remote
Plugin: audit_remote
Attributes: p_retries=3;p_timeout=5;p_hosts=arstore.example.com;
```

7. **Refresque el servicio de auditoría.**

   El servicio de auditoría lee el cambio de complemento de auditoría después del refrescamiento.

```
# audit -s
```

   El KDC ahora gestiona la conexión entre el sistema auditado `enigma` y el ARS.

ejemplo 4-9 Transmisión por secuencias de registros de auditoría a diferentes ubicaciones de archivos en el mismo ARS

En este ejemplo, se amplía el ejemplo en el procedimiento. El administrador separa los registros de auditoría por host en el ARS mediante la creación de dos grupos de conexión.

Los archivos de auditoría de la transmisión `audsys1` al grupo de conexiones `Bank_A` en este ARS.

```
arstore # auditconfig -setremote group create Bank_A

arstore # auditconfig -setremote group active Bank_A "hosts=audsys1" \
   "hosts=audsys1;binfile_dir=/var/audit/audsys1;binfile_fsize=4M;"
```

Los archivos de auditoría de `audsys2` se transmiten al grupo de conexión `Bank_B`.

```
arstore # auditconfig -setremote group create Bank_B

arstore # auditconfig -setremote group active Bank_B \
"hosts=audsys2;binfile_dir=/var/audit/audsys2;binfile_fsize=4M;"
```

Para facilitar las tareas de mantenimiento, el administrador establece otros valores de atributo de la misma forma.

```
arstore # auditconfig -getremote
Audit Remote Server
Attributes: listen_address=;login_grace_time=30;max_startups=10;listen_port=0;

Connection group: Bank_A
Attributes: binfile_dir=/var/audit/audsys1;binfile_fsize=4M;binfile_minfree=1;
hosts=audsys1
```

```
Connection group: Bank_B
Attributes: binfile_dir=/var/audit/audsys2;binfile_fsize=4M;binfile_minfree=1;
hosts=audsys2
```

ejemplo 4-10 Colocación del ARS en un sistema diferente de KDC

En este ejemplo, el administrador coloca el ARS en un sistema diferente del KDC. En primer lugar, el administrador crea y configura el KDC maestro.

```
kserv # kdcmgr -a audr/admin -r EXAMPLE.COM create master

kserv # kadmin.local -p audr/admin

kadmin: addprinc -randkey \
audit/arstore.example.com@EXAMPLE.COM

kadmin: ktadd -t /tmp/krb5.keytab.audit \
     audit/arstore.example.com@EXAMPLE.COM
```

Después de transmitir de manera segura el archivo `/tmp/krb5.keytab.audit` al ARS, `arstore`, el administrador mueve el archivo a la ubicación correcta.

```
arstore # chown root:root krb5.keytab.audit

arstore # chmod 600 krb5.keytab.audit

arstore # mv krb5.keytab.audit /etc/krb5/krb5.keytab
```

En lugar de volver a escribir el archivo, el administrador también tiene la opción de utilizar el comando `ktutil` en el ARS para fusionar el archivo `krb5.keytab.audit` del KDC con las claves existentes en el archivo `/etc/krb5/krb5.keytab` de `arstore`.

Por último, el administrador genera claves en el sistema auditado.

```
enigma # kclient

.. Enter the Kerberos realm: EXAMPLE.COM

.. KDC hostname for the above realm: kserv.example.com

.. Will this client need service keys ? [y/n]: y
```

▼ Cómo configurar registros de auditoría `syslog`

Puede indicar al servicio de auditoría que copie algunos o todos los registros de auditoría de la cola de auditoría en la utilidad `syslog`. Si registra datos de auditoría binarios y resúmenes de textos, los datos binarios proporcionan un registro completo de auditoría, mientras que los resúmenes filtran los datos para la revisión en tiempo real.

Antes de empezar Para configurar el complemento `audit_syslog`, debe convertirse en un administrador con el perfil de derechos de configuración de auditoría asignado. Para configurar la utilidad `syslog` y crear el archivo `auditlog`, debe asumir el rol `root`.

1. **Seleccione las clases de auditoría que se enviarán al complemento `audit_syslog` y active el complemento.**

   Nota - Las clases de auditoría `p_flags` deben ser preseleccionadas como valores predeterminados del sistema o en los indicadores de auditoría de un usuario o de un perfil de derechos. Los registros no se recopilan para una clase que no está preseleccionada.

   ```
   # auditconfig -setplugin audit_syslog \
        active p_flags=lo,+as,-ss
   ```

2. **Configure la utilidad `syslog`.**

   a. **Agregue una entrada `audit.notice` al archivo `syslog.conf`.**

      La entrada incluye la ubicación del archivo log.

      ```
      # cat /etc/syslog.conf

      …
      audit.notice       /var/adm/auditlog
      ```

   b. **Cree el archivo log.**

      ```
      # touch /var/adm/auditlog
      ```

   c. **Configure los permisos del archivo log en 640.**

      ```
      # chmod 640 /var/adm/auditlog
      ```

   d. **Compruebe qué instancia del servicio system-log se ejecuta en el sistema.**

      ```
      # svcs system-log

      STATE        STIME      FMRI
      online       Nov_27     svc:/system/system-log:default
      disabled     Nov 27     svc:/system/system-log:rsyslog
      ```

   e. **Refresque la información de configuración para la instancia del servicio `syslog` activa.**

      ```
      # svcadm refresh system/system-log:default
      ```

3. **Refresque el servicio de auditoría.**

   El servicio de auditoría lee los cambios en el complemento de auditoría tras el refrescamiento.

```
# audit -s
```

4. **Archive con regularidad los archivos log `syslog`.**

   El servicio de auditoría puede generar muchas salidas. Para gestionar los logs, consulte la página del comando man `logadm`(1M).

ejemplo 4-11 Especificación de clases de auditoría para salida de `syslog`

En el siguiente ejemplo, la utilidad `syslog` recopila un subconjunto de clases de auditoría preseleccionadas. La clase `pf` se crea en el Ejemplo 3-15, “Creación de una clase de auditoría nueva”.

```
# auditconfig -setnaflags lo,na

# auditconfig -setflags lo,ss

# usermod -K audit_flags=pf:no jdoe

# auditconfig -setplugin audit_syslog \
    active p_flags=lo,+na,-ss,+pf
```

Los argumentos del comando `auditconfig` indican al sistema que recopile todos los registros de auditoría de inicio y cierre de sesión, no atribuibles y de cambio de estado del sistema. La entrada del complemento `audit_syslog` indica a la utilidad `syslog` que recopile todos los inicios de sesión, los eventos no atribuibles con éxito y los cambios de estado del sistema con fallos.

Para el usuario `jdoe`, la utilidad binaria recopila llamadas correctas e incorrectas para el comando `pfexec`. La utilidad `syslog` recopila llamadas con éxito al comando `pfexec`.

ejemplo 4-12 Colocación de registros de auditoría `syslog` en un sistema remoto

Puede cambiar la entrada `audit.notice` en el archivo `syslog.conf` para que haga referencia a un sistema remoto. En este ejemplo, el nombre del sistema local es `sys1.1`. El sistema remoto es `remote1`.

```
sys1.1 # cat /etc/syslog.conf

…
audit.notice       @remote1
```

La entrada `audit.notice` en el archivo `syslog.conf` del sistema `remote1` hace referencia al archivo log.

```
remote1 # cat /etc/syslog.conf

…
```

```
audit.notice       /var/adm/auditlog
```

♦ ♦ ♦ CAPÍTULO 5

Cómo trabajar con datos de auditoría

En este capítulo, se proporcionan procedimientos para ayudarle con los datos de auditoría que se generan desde diferentes sistemas locales. En este capítulo, se tratan los siguientes temas:

- “Visualización de datos de pista de auditoría” [93]
- “Gestión de registros de auditoría en sistemas locales” [102]

Además, en los siguientes capítulos, se describen otras tareas de gestión de auditoría:

- Capítulo 3, Gestión del servicio de auditoría
- Capítulo 4, Supervisión de actividades del sistema
- Capítulo 6, Análisis y resolución de problemas del servicio de auditoría

Para obtener una descripción general del servicio de auditoría, consulte el Capítulo 1, Acerca de la auditoría en Oracle Solaris. Para obtener sugerencias de planificación, consulte el Capítulo 2, Planificación de la auditoría. Para obtener información de referencia, consulte el Capítulo 7, Referencia sobre auditoría.

Visualización de datos de pista de auditoría

El complemento predeterminado, `audit_binfile`, crea una pista de auditoría. La pista puede contener grandes cantidades de datos. Las siguientes secciones describen cómo trabajar estos datos.

Visualización de definiciones de registros de auditoría

Para visualizar definiciones de registros de auditoría, utilice el comando `auditrecord`. Las definiciones indican el número de evento de auditoría, la clase de auditoría, la máscara de selección y el formato de registro de un evento de auditoría.

```
% auditrecord -options
```

La salida de la pantalla generada por el comando depende de la opción que se utilice, como se muestra en la siguiente lista parcial.

- La opción -p muestra las definiciones de registros de auditoría de un programa.
- La opción -c muestra las definiciones de registros de auditoría de una clase de auditoría.
- La opción -a muestra una lista de todas las definiciones de eventos de auditoría.

También puede imprimir la salida que se muestra en un archivo.

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

EJEMPLO 5-1 Visualización de las definiciones de registros de auditoría de un programa

En este ejemplo, se muestra la definición de todos los registros de auditoría que se generan mediante el programa `login`. Los programas de inicio de sesión incluyen `rlogin`, `telnet`, `newgrp` y la función de Secure Shell de Oracle Solaris.

```
% auditrecord -p login
...
login: logout
program     various              See login(1)
event ID    6153                 AUE_logout
class       lo                  (0x0000000000001000)
...
newgrp
program     newgrp               See newgrp login
event ID    6212                 AUE_newgrp_login
class       lo                  (0x0000000000001000)
...
rlogin
program     /usr/sbin/login      See login(1) - rlogin
event ID    6155                 AUE_rlogin
class       lo                   (0x0000000000001000)
...
/usr/lib/ssh/sshd
program     /usr/lib/ssh/sshd    See login - ssh
event ID    6172                 AUE_ssh
class       lo                   (0x0000000000001000)
...
telnet login
program     /usr/sbin/login      See login(1) - telnet
event ID    6154                 AUE_telnet
class       lo                   (0x0000000000001000)
…
```

EJEMPLO 5-2 Visualización de definiciones de registros de auditoría de una clase de auditoría

En este ejemplo, se muestran las definiciones de todos los registros de auditoría en la clase `pf` que fue creada en el Ejemplo 3-15, “Creación de una clase de auditoría nueva”.

```
% auditrecord -c pf
pfexec
system call pfexec              See execve(2) with pfexec enabled
event ID    116                 AUE_PFEXEC
class       pf                  (0x0100000000000000)
header
path                    pathname of the executable
path                    pathname of working directory
[privileges]            privileges if the limit or inheritable set are changed
[privileges]            privileges if the limit or inheritable set are changed
[process]               process if ruid, euid, rgid or egid is changed
exec_arguments
[exec_environment]      output if arge policy is set
subject
[use_of_privilege]
return
```

El token `use_of_privilege` se registra siempre que se utiliza un privilegio. Los tokens `privileges` se registran si el conjunto heredable o límite se cambia. El token `process` se registra si un ID se cambia. Ninguna opción de política es necesaria para que estos tokens se incluyan en el registro.

EJEMPLO 5-3 Impresión de definiciones de registros de auditoría en un archivo

En este ejemplo, la opción `-h` se agrega para colocar todas las definiciones de registros de auditoría en un archivo en formato HTML. Cuando visualiza el archivo HTML en un explorador, use la herramienta de búsqueda del explorador para buscar definiciones de registros de auditoría específicas.

```
% auditrecord -ah > audit.events.html
```

Selección de eventos de auditoría que se mostrarán

Como administrador que tiene asignado el perfil de derechos de revisión de auditoría, puede filtrar registros de auditoría para examinarlos mediante el comando `auditreduce`. Este comando puede eliminar los registros menos interesantes a medida que combina los archivos de entrada.

auditreduce -*option argument* **[***optional-file***]**

Donde *argument* es el argumento específico que una opción requiere.

A continuación, se muestra una lista parcial de las opciones de *selección de registros* y sus correspondientes argumentos:

`-c`	Selecciona una clase de auditoría donde *argument* es una clase de auditoría, como `ua`.
`-d`	Selecciona todos los eventos en una fecha determinada. El formato de fecha de *argument* es *aaammdd*. Otras opciones de fecha, como `-b` y `-a`, seleccionan los eventos antes y después de una fecha determinada, respectivamente.
`-u`	Selecciona todos los eventos atribuibles a un usuario determinado. Para esta opción, especifique un nombre de usuario. Otra opción de usuario, `-e`, selecciona todos los eventos atribuibles a un ID de usuario vigente.
`-g`	Selecciona todos los eventos atribuibles a un grupo determinado. Para esta opción, especifique un nombre de grupo.
`-c`	Selecciona todos los eventos de una clase de auditoría preseleccionada. Para utilizar esta opción, especifique un nombre de clase de auditoría.
`-m`	Selecciona todas las instancias de un evento de auditoría determinado.
`-o`	Selecciona por tipo de objeto. Utilice esta opción para seleccionar por archivo, grupo, responsable de archivo, FMRI, PID y otros tipos de objetos.
optional-file	El nombre de un archivo de auditoría.

El comando también utiliza las opciones de *selección de archivos*, que se escriben todas con letras mayúsculas como se muestra en los siguientes ejemplos. Para obtener una lista completa de las opciones, consulte la página del comando man `auditreduce`(1M).

EJEMPLO 5-4 Combinación y reducción de archivos de auditoría

En este ejemplo, sólo se conservan los registros de inicio y cierre de sesión en los archivos de auditoría con más de un mes de antigüedad. El ejemplo asume que la fecha actual es 27 de septiembre. Si necesita recuperar la pista de auditoría completa, puede recuperar la pista del medio de copia de seguridad. La opción `-O` dirige la salida del comando a un archivo denominado `lo.summary`.

```
# cd /var/audit/audit_summary
# auditreduce -O lo.summary -b 20100827 -c lo; compress *lo.summary
```

EJEMPLO 5-5 Copia de los registros de auditoría de un usuario en un archivo de resumen

En este ejemplo, se fusionan los registros en la pista de auditoría que contienen el nombre de un usuario determinado. La opción `-e` busca el usuario vigente. La opción `-u` busca el usuario de inicio de sesión. La opción `-O` dirige la salida al archivo `tamiko`.

```
# cd /var/audit/audit_summary
# auditreduce -e tamiko -O tamiko
```

Puede reducir aún más la información mostrada. En el ejemplo que aparece a continuación, se filtra e imprime lo siguiente en un archivo denominado `tamikolo`.

- Hora de inicio y cierre de sesión del usuario, especificada por la opción `-c`.
- Fecha del 7 de septiembre de 2013, especificada por la opción `-d`. La abreviatura de la fecha es *aaaammdd*.
- Nombre de usuario tamiko, especificado por la opción `-u`.
- Nombre de equipo, especificado por la opción `-M`.

```
# auditreduce -M tamiko -O tamikolo -d 20130907 -u tamiko -c lo
```

EJEMPLO 5-6 Fusión de registros seleccionados en un archivo único

En este ejemplo, los registros de inicio y cierre de sesión de un día determinado se seleccionan de la pista de auditoría. Los registros se fusionan en un archivo de destino. El archivo de destino se escribe en un sistema de archivos que no sea el sistema de archivos que contiene el directorio raíz de auditoría.

```
# auditreduce -c lo -d 20130827 -O /var/audit/audit_summary/logins

# ls /var/audit/audit_summary/*logins
/var/audit/audit_summary/20130827183936.20130827232326.logins
```

Visualización del contenido de los archivos de auditoría binarios

Como administrador que tiene asignado el perfil de derechos de revisión de auditoría, puede ver el contenido de los archivos de auditoría binarios con el comando `praudit`.

```
# praudit options
```

A continuación, se muestra una lista parcial de las opciones. Puede combinar cualquiera de estas opciones con la opción `-l` para mostrar cada registro en una línea.

`-s`	Muestra los registros de auditoría en formato corto, un token por línea.
`-r`	Muestra los registros de auditoría en formato básico, un token por línea.
`-x`	Muestra los registros de auditoría en formato XML, un token por línea. Esta opción es útil para el procesamiento posterior.

También puede utilizar los comandos `auditreduce` y `praudit` juntos conduciendo la salida del comando `praudit` desde el comando `auditreduce`.

EJEMPLO 5-7 Visualización de los registros de auditoría en formato corto

En este ejemplo, los eventos de inicio y cierre de sesión que se extraen mediante el comando `auditreduce` se muestran en formato corto.

```
# auditreduce -c lo | praudit -s

header,69,2,AUE_screenlock,,mach1,2010-10-14 08:02:56.348 -07:00
subject,jdoe,root,staff,jdoe,staff,856,50036632,82 0 mach1
return,success,0
sequence,1298
```

EJEMPLO 5-8 Visualización de los registros de auditoría en formato básico

En este ejemplo, los eventos de inicio y cierre de sesión que se extraen mediante el comando `auditreduce` se muestran en formato básico.

```
# auditreduce -c lo | praudit -r

21,69,2,6222,0x0000,10.132.136.45,1287070091,698391050
36,26700,0,10,26700,10,856,50036632,82 0 10.132.136.45
39,0,0
47,1298
```

EJEMPLO 5-9 Paso de registros de auditoría a formato XML

En este ejemplo, los registros de auditoría se convierten a formato XML.

```
# praudit -x 20100827183214.20100827215318.logins > 20100827.logins.xml
```

De manera similar, puede mostrar los registros de auditoría filtrados mediante el comando `auditreduce` en formato XML.

```
# auditreduce -c lo | praudit -x
<record version="2" event="screenlock - unlock" host="mach1"
iso8601="2010-10-14 08:28:11.698 -07:00">
<subject audit-uid="jdoe" uid="root" gid="staff" ruid="jdoe
```

```
rgid="staff" pid="856" sid="50036632" tid="82 0 mach1"/>
<return errval="success" retval="0"/>
<sequence seq-num="1298"/>
</record>
```

El contenido del archivo sólo puede ser operado por una secuencia de comandos para extraer la información relevante.

EJEMPLO 5-10 Modificación de registros de auditoría en formato XML para que pueda leerlos un explorador

Puede cambiar el formato de los registros del archivo XML para que puedan leerse en cualquier explorador mediante la herramienta `xsltproc`. Esta herramienta aplica las definiciones de las hojas de estilo al contenido del archivo. Para colocar en un archivo diferente el contenido cuyo formato se cambió, debe escribir lo siguiente:

```
# auditreduce -c lo | praudit -x | xsltproc - > logins.html
```

En un explorador, el contenido de `logins.html` se mostrará en un formato similar al siguiente:

```
                    Audit Trail Data

File: time: 2013-11-04 12:54:28.000 -08:00

Event: login - local
time: 2013-11-04 12:54:28.418 -08:00 vers: 2 mod: host: host
SUBJECT audit-uid: jdoe uid: jdoe gid: staff ruid: jdoe rgid: staff
      pid: 1534 sid: 3583012893 tid: 0 0 host
RETURN errval: success retval: 0

Event: connect to RAD
time: 2013-11-04 12:54:52.029 -08:00 vers: 2 mod: host: host
SUBJECT audit-uid: jdoe uid: jdoe gid: staff ruid: jdoe rgid: staff
      pid: 1835 sid: 3583012893 tid: 0 0 host
RETURN errval: success retval: 0

Event: role login
time: 2013-11-08 08:42:52.286 -08:00 vers: 2 mod: host: host
SUBJECT audit-uid: jdoe uid: root gid: root ruid: root rgid: root
      pid: 4265 sid: 3583012893 tid: 0 0 host
RETURN errval: success retval: 0

Event: role logout
time: 2013-11-08 08:43:37.125 -08:00 vers: 2 mod: host: host
SUBJECT audit-uid: jdoe uid: root gid: root ruid: root rgid: root
      pid: 4265 sid: 3583012893 tid: 0 0 host
RETURN errval: success retval: 0

Event: login - ssh
time: 2013-12-23 12:24:37.292 -08:00 vers: 2 mod: host: host
SUBJECT audit-uid: jsmith uid: jsmith gid: staff ruid: jsmith rgid: staff
      pid: 2002 sid: 39351741 tid: 14632 202240 host.example.com
```

```
RETURN errval: success retval: 0

Event: role login
time: 2013-12-23 12:25:07.345 -08:00 vers: 2 mod: fe host: host
SUBJECT audit-uid: jsmith uid: root gid: root ruid: root rgid: root
      pid: 2023 sid: 39351741 tid: 14632 202240 host.example.com
RETURN errval: failure retval: Permission denied

Event: su
time: 2013-12-23 17:19:24.031 -08:00 vers: 2 mod: na host: host
RETURN errval: success retval: 0

Event: su logout
time: 2013-12-23 17:19:24.362 -08:00 vers: 2 mod: na host: host
RETURN errval: success retval: 0

Event: login - ssh
time: 2013-12-23 17:27:21.306 -08:00 vers: 2 mod: host: host
SUBJECT audit-uid: jsmith uid: jsmith gid: staff ruid: jsmith rgid: staff
      pid: 2583 sid: 3401970889 tid: 13861 5632 host.example.com
RETURN errval: success retval: 0

Event: role login
time: 2013-12-23 17:27:28.361 -08:00 vers: 2 mod: host: host
SUBJECT audit-uid: jsmith uid: root gid: root ruid: root rgid: root
      pid: 2593 sid: 3401970889 tid: 13861 5632 host.example.com
RETURN errval: success retval: 0

Event: role logout
time: 2013-12-23 17:30:39.029 -08:00 vers: 2 mod: host: host
SUBJECT audit-uid: jsmith uid: root gid: root ruid: root rgid: root
      pid: 2593 sid: 3401970889 tid: 13861 5632 host.example.com
RETURN errval: success retval: 0
```

Other events

EJEMPLO 5-11 Visualización de sólo registros `pfedit`

Puede utilizar filtros para extraer y ver sólo registros específicos de la pista de auditoría. En este ejemplo, se filtran los registros que capturan el uso del comando `pfedit`. Suponga que el archivo de resumen es `20130827183936.20130827232326.logins`. El uso del comando `pfedit` genera el evento `AUE_admin_edit`. Por lo tanto, para extraer los registros de `pfedit`, ejecute el siguiente comando:

```
auditreduce -m AUE_admin_edit 20130827183936.20130827232326.logins | praudit
```

EJEMPLO 5-12 Impresión de toda la pista de auditoría

Con una conducción al comando de impresión, la salida de toda la pista de auditoría pasa a la impresora. Por motivos de seguridad, la impresora tiene acceso limitado.

```
# auditreduce | praudit | lp -d example.protected.printer
```

EJEMPLO 5-13 Visualización de un archivo de auditoría específico

En este ejemplo, se examina un archivo de inicio de sesión de resumen en la ventana de terminal.

```
# cd /var/audit/audit_summary/logins

# praudit 20100827183936.20100827232326.logins | more
```

EJEMPLO 5-14 Procesamiento de la salida de `praudit` con una secuencia de comandos

Es posible que quiera procesar la salida del comando `praudit` como líneas de texto. Por ejemplo, es posible que quiera seleccionar registros que el comando `auditreduce` no pueda seleccionar. Puede utilizar una secuencia de comandos de shell sencilla para procesar la salida del comando `praudit`. La siguiente secuencia de comandos de ejemplo coloca un registro de auditoría en una línea, busca una cadena especificada por el usuario y devuelve el archivo de auditoría a su forma original.

```
#!/bin/sh
#
## This script takes an argument of a user-specified string.
#  The sed command prefixes the header tokens with Control-A
#  The first tr command puts the audit tokens for one record
#  onto one line while preserving the line breaks as Control-A
#
praudit | sed -e '1,2d' -e '$s/^file.*$//' -e 's/^header/^aheader/' \\
| tr '\\012\\001' '\\002\\012' \\
| grep "$1" \\
```
Finds the user-specified string

```
| tr '\\002' '\\012'
```
Restores the original newline breaks

Tenga en cuenta que `^a` en la secuencia de comandos equivale a Control-A, no los dos caracteres `^` y `a`. El prefijo distingue el token `header` de la cadena `header` que podría aparecer como texto.

Un mensaje similar al siguiente indica que no tiene privilegios suficientes para usar el comando `praudit`:

```
praudit: Can't assign 20090408164827.20090408171614.sys1.1 to stdin.
```

Ejecute el comando `praudit` un shell de perfil. Debe convertirse en un administrador con el perfil de derechos de revisión de auditoría asignado. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

Gestión de registros de auditoría en sistemas locales

El siguiente mapa de tareas hace referencia a los procedimientos para seleccionar, analizar y gestionar los registros de auditoría.

TABLA 5-1 Mapa de tareas de gestión de registros de auditoría en sistemas locales

Tarea	Descripción	Más instrucciones
Fusionar registros de auditoría.	Combina los archivos de auditoría de varias máquinas en una pista de auditoría.	Cómo fusionar archivos de auditoría de la pista de auditoría [102]
Depurar archivos de auditoría denominados incorrectamente.	Proporciona un registro de hora final para archivos de auditoría que quedaron abiertos accidentalmente en el servicio de auditoría.	Cómo depurar un archivo de auditoría `not_terminated` [104]
Evitar el desbordamiento de la pista de auditoría.	Impide que los sistemas de archivos de auditoría se llenen.	"Cómo evitar el desbordamiento de la pista de auditoría" [105]

▼ Cómo fusionar archivos de auditoría de la pista de auditoría

Mediante la fusión de los archivos de auditoría de todos los directorios de auditoría, puede analizar el contenido de toda la pista de auditoría.

Nota - Debido a que los registros de hora en la pista de auditoría están en la hora universal coordinada (UTC), la fecha y la hora se deben traducir a la zona horaria actual para que tengan sentido. Tenga en cuenta este punto siempre que manipule estos archivos con los comandos de archivo estándar en lugar de utilizar el comando `auditreduce`.

Antes de empezar Debe convertirse en un administrador con el perfil de derechos de revisión de auditoría asignado. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

1. **Cree un sistema de archivos para almacenar los archivos de auditoría fusionados.**

   Para reducir la posibilidad de que se alcance el límite de espacio en disco, este sistema de archivos debe estar en *otra zpool* de los sistemas de archivos que creó en Cómo crear sistemas de archivos ZFS para archivos de auditoría [76] para almacenar los archivos originales.

2. **Fusione los registros de auditoría en la pista de auditoría.**

   Vaya al directorio para almacenar archivos de auditoría fusionados. Desde este directorio, fusione los registros de auditoría en un archivo con un sufijo con nombre. Todos los directorios de la pista de auditoría en el sistema local se fusionan y se almacenan en este directorio.

```
# cd audit-storage-directory
# auditreduce -Uppercase-option -O suffix
```

Las opciones en mayúscula del comando `auditreduce` manipulan los archivos en la pista de auditoría. Las opciones en mayúscula incluyen las siguientes:

`-A`	Selecciona todos los archivos en la pista de auditoría.
`-C`	Selecciona únicamente archivos completos.
`-M`	Selecciona los archivos con un sufijo determinado. El sufijo puede ser un nombre de equipo o un sufijo que haya especificado para un archivo de resumen.
`-O`	Crea un archivo de auditoría con registros de hora de 14 caracteres para la hora de inicio y la hora de finalización, con el sufijo *suffix* en el directorio actual.
`-R` *pathname*	Especifica la lectura de archivos de auditoría en *pathname*, un directorio raíz de auditoría alternativo.
`-S` *server*	Especifica la lectura de archivos de auditoría del servidor especificado.

Para obtener una lista completa de las opciones, consulte la página del comando man `auditreduce`(1M).

ejemplo 5-15 Copia de archivos de auditoría a un archivo de resumen

En el ejemplo siguiente, un administrador que tiene asignado el perfil de derechos de administrador del sistema copia todos los archivos de la pista de auditoría en un archivo fusionado, en un sistema de archivos diferente. El sistema de archivos `/var/audit/storage` está en un disco separado del sistema de archivos `/var/audit`, el sistema de archivos raíz de auditoría.

```
$ cd /var/audit/storage
$ auditreduce -A -O All
$ ls /var/audit/storage/*All
20100827183214.20100827215318.All
```

En el siguiente ejemplo, únicamente se copian archivos completos de la pista de auditoría a un archivo fusionado. La ruta completa se especifica como el valor de la opción `-O`. El último elemento de la ruta, `Complete`, se utiliza como el sufijo.

```
$ auditreduce -C -O /var/audit/storage/Complete

$ ls /var/audit/storage/*Complete
20100827183214.20100827214217.Complete
```

En el siguiente ejemplo, si agrega la opción -D, se suprimen los archivos de auditoría originales.

```
$ auditreduce -C -O daily_sys1.1 -D sys1.1

$ ls *sys1.1
20100827183214.20100827214217.daily_sys1.1
```

▼ Cómo depurar un archivo de auditoría not_terminated

Cuando se producen interrupciones anómalas del sistema, el servicio de auditoría se cierra mientras su archivo de auditoría aún está abierto. O bien un sistema de archivos se vuelve inaccesible y hace que el sistema cambie a un nuevo sistema de archivos. En esos casos, un archivo de auditoría permanece con la cadena not_terminated como registro de hora final, aunque el archivo ya no se utilice para los registros de auditoría. Utilice el comando auditreduce -O para otorgar al archivo el registro de hora correcto.

Antes de empezar Debe convertirse en un administrador con el perfil de derechos de revisión de auditoría asignado. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

1. **Enumere los archivos con la cadena not_terminated en el sistema de archivos de auditoría según el orden de creación.**

   ```
   # ls -R1t audit-directory */* | grep not_terminated
   ```

-R	Muestra los archivos en los subdirectorios.
-t	Muestra la lista de archivos desde el más reciente hasta el más antiguo.
-1	Muestra los archivos en una columna.

2. **Depure el archivo not_terminated anterior.**

   Especifique el nombre del archivo anterior en el comando auditreduce -O.

   ```
   # auditreduce -O system-name old-not-terminated-file
   ```

3. **Elimine el archivo not_terminated anterior.**

   ```
   # rm system-name old-not-terminated-file
   ```

ejemplo 5-16 Depuración de archivos de auditoría not_terminated cerrados

En el siguiente ejemplo, se encontraron archivos not_terminated, se renombraron y se eliminaron los originales.

```
ls -R1t */* | grep not_terminated
…/egret.1/20100908162220.not_terminated.egret
…/egret.1/20100827215359.not_terminated.egret

# cd */egret.1
# auditreduce -O egret 20100908162220.not_terminated.egret
# ls -1t
20100908162220.not_terminated.egret      Current audit file

20100827230920.20100830000909.egret      Cleaned-up audit file

20100827215359.not_terminated.egret      Input (old) audit file

# rm 20100827215359.not_terminated.egret
# ls -1t
20100908162220.not_terminated.egret      Current audit file

20100827230920.20100830000909.egret      Cleaned-up audit file
```

El registro de hora de inicio en el nuevo archivo refleja la hora del primer evento de auditoría en el archivo `not_terminated`. El registro de hora final refleja la hora del último evento de auditoría en el archivo.

Cómo evitar el desbordamiento de la pista de auditoría

Si la política de seguridad requiere que todos los datos de auditoría se guarden, evite la pérdida de registros de auditoría cumpliendo con las siguientes prácticas.

Nota - Debe asumir el rol `root`. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

- Establezca un tamaño libre mínimo en el complemento `audit_binfile`.

  Utilice el atributo `p_minfree`.

  El alias de correo electrónico `audit_warn` envía una advertencia cuando el espacio en disco llega al tamaño libre mínimo. Consulte el Ejemplo 4-7, "Definición de un límite variable para advertencias".
- Configure un programa para archivar con regularidad los archivos de auditoría.

  Almacene los archivos de auditoría mediante una copia de los archivos en los medios sin conexión. También puede mover los archivos a un sistema de archivos de almacenamiento.

  Si recopila logs de auditoría de texto con la utilidad `syslog`, archive los logs de texto. Para obtener más información, consulte la página del comando man `logadm`(1M).

- Establezca un programa para suprimir los archivos de auditoría archivados del sistema de archivos de auditoría.
- Guarde y almacene información auxiliar.

  Archive la información que sea necesaria para interpretar los registros de auditoría junto con la pista de auditoría. Como mínimo, guarde los archivos `passwd`, `group` y `hosts`. También podría archivar los archivos `audit_event` y `audit_class`.
- Mantenga registros de qué archivos de auditoría se han archivado.
- Almacene los medios archivados adecuadamente.
- Reduzca la cantidad de capacidad del sistema de archivos que se necesita activando la compresión ZFS.

  En un sistema de archivos ZFS que está dedicado a archivos de auditoría, la compresión reduce los archivos considerablemente. Para ver un ejemplo, consulte Cómo comprimir archivos de auditoría en un sistema de archivos dedicado [66].

  Consulte también “Interacciones entre propiedades de compresión, eliminación de datos duplicados y cifrado de ZFS” de “Gestión de sistemas de archivos ZFS en Oracle Solaris 11.2 ”.
- Reduzca el volumen de los datos de auditoría que almacene mediante la creación de archivos de resumen.

  Puede extraer archivos de resumen de la pista de auditoría mediante las opciones en el comando `auditreduce`. Los archivos de resumen contienen únicamente registros para tipos especificados de eventos de auditoría. Para extraer archivos de resumen, consulte el Ejemplo 5-4, “Combinación y reducción de archivos de auditoría” y el Ejemplo 5-6, “Fusión de registros seleccionados en un archivo único”.

♦ ♦ ♦ CAPÍTULO 6

Análisis y resolución de problemas del servicio de auditoría

En este capítulo, se proporcionan procedimientos para ayudarle a solucionar problemas relacionados con la auditoría. Además, en los siguientes capítulos, se describen otras tareas de gestión de auditoría:

- Capítulo 3, Gestión del servicio de auditoría
- Capítulo 4, Supervisión de actividades del sistema
- Capítulo 5, Cómo trabajar con datos de auditoría

Para obtener una descripción general del servicio de auditoría, consulte el Capítulo 1, Acerca de la auditoría en Oracle Solaris. Para obtener sugerencias de planificación, consulte el Capítulo 2, Planificación de la auditoría. Para obtener información de referencia, consulte el Capítulo 7, Referencia sobre auditoría.

Resolución de problemas del servicio de auditoría

En esta sección, se tratan distintos mensajes de error de auditoría, las preferencias y la auditoría proporcionada por otras herramientas a fin de ayudarle a depurar problemas de auditoría.

Por lo general, se envían diferentes avisos para alertar al usuario acerca de errores en el servicio de auditoría. Revise su correo electrónico y los archivos log si cree que existen problemas con el servicio de auditoría.

- Lea el correo electrónico enviado al alias `audit_warn`.

  La secuencia de comandos `audit_warn` envía mensajes de alerta al alias de correo electrónico `audit_warn`. Ante la ausencia de un alias configurado correctamente, los mensajes se envían a la cuenta `root`.
- Revise los archivos log para el servicio de auditoría.

  La salida del comando `svcs -s auditd` muestra la ruta completa a los registros de auditoría que el servicio de auditoría produce.
- Revise los archivos log del sistema.

La secuencia de comandos `audit_warn` escribe mensajes `daemon.alert` en el archivo `/var/log/syslog`.

El archivo `/var/adm/messages` podría contener información.

Después de encontrar y corregir los problemas, active o reinicie el servicio de auditoría.

```
# audit -s
```

En las siguientes secciones, se describen casos de posibles problemas y los pasos para resolverlos.

Nota - Antes de realizar cualquier tarea de resolución de problemas, asegúrese de que tiene la autorización adecuada. Por ejemplo, para configurar la auditoría, debe convertirse en un administrador con el perfil de derechos de configuración de auditoría asignado. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

Los registros de auditoría no se registran

La auditoría está activada de manera predeterminada. Si cree que la auditoría no se ha desactivado, pero no se están enviando registros de auditoría al complemento activo, la causa puede ser uno o una combinación de los factores que se describen en esta sección. Tenga en cuenta que, para modificar un sistema de archivos, debe tener asignada la autorización `solaris.admin.edit/`*path-to-system-file*. De manera predeterminada, el rol root tiene esta autorización.

El servicio de auditoría no está en ejecución

Para comprobar si la auditoría se está ejecutando, utilice cualquiera de los siguientes métodos:

- Compruebe la condición actual de la auditoría.

  La siguiente salida indica que la auditoría no se está ejecutando:

  ```
  # auditconfig -getcond
  audit condition = noaudit
  ```

  La siguiente salida indica que la auditoría se está ejecutando:

  ```
  # auditconfig -getcond
  audit condition = auditing
  ```

- Compruebe que el servicio de auditoría se esté ejecutando.

La siguiente salida indica que la auditoría no se está ejecutando:

```
# svcs -x auditd

svc:/system/auditd:default (Solaris audit daemon)
State: disabled since Sun Oct 10 10:10:10 2010
Reason: Disabled by an administrator.
See: http://support.oracle.com/msg/SMF-8000-05
See: auditd(1M)
See: audit(1M)
See: auditconfig(1M)
See: audit_flags(5)
See: audit_binfile(5)
See: audit_syslog(5)
See: audit_remote(5)
See: /var/svc/log/system-auditd:default.log
Impact: This service is not running.
```

La siguiente salida indica que el servicio de auditoría se está ejecutando:

```
# svcs auditd
STATE          STIME    FMRI
online         10:10:10 svc:/system/auditd:default
```

Si el servicio de auditoría no se está ejecutando, actívelo. Para conocer el procedimiento, consulte “Activación y desactivación del servicio de auditoría” [44].

No hay un complemento de auditoría activo

Use el siguiente comando para comprobar si hay algún complemento activo. Al menos un complemento debe estar activo para que el servicio de auditoría funcione.

```
# audit -v
audit: no active plugin found
```

Si no hay ningún complemento activo, active uno.

```
# auditconfig -setplugin audit_binfile active
# audit -v
configuration ok
```

Clase de auditoría no definida

Es posible que esté intentando utilizar una clase de auditoría que no se ha definido. Para obtener una descripción de la creación de la clase `pf`, consulte Cómo agregar una clase de auditoría [56].

Por ejemplo, la siguiente lista de indicadores contiene la clase `pf`, que el software Oracle Solaris no entregó:

```
# auditconfig -getflags
active user default audit flags = pf,lo(0x0100000000000000,00x0100000000001000)
configured user default audit flags = pf,lo(0x0100000000000000,00x0100000000001000)
```

Si no desea definir la clase, ejecute el comando `auditconfig -setflags` con los valores válidos para restablecer los indicadores actuales. De lo contrario, asegúrese de lo siguiente al definir una clase:

- La clase de auditoría está definida en el archivo `audit_class`.

  ```
  # grep pf /etc/security/audit_class
      Verify class exists

  0x0100000000000000:pf:profile
  ```

- La máscara es única. Si no es única, reemplace la máscara.

  ```
  # grep 0x0100000000000000 /etc/security/audit_class
      Ensure mask is unique

  0x0100000000000000:pf:profile
  ```

No hay eventos asignados a la clase de auditoría

Es posible que la clase personalizada que está utilizando, aunque esté definida, no tenga ningún evento asignado.

Para verificar si hay eventos asignados a la clase personalizada, utilice uno de los siguientes métodos:

```
# auditconfig -lsevent | egrep " pf|,pf|pf,"
AUE_PFEXEC      116 pf execve(2) with pfexec enabled

# auditrecord -c pf
    List of audit events assigned to pf class
```

Si los eventos no están asignados a la clase, asigne los eventos adecuados a esta clase.

Volumen grande de registros de auditoría

Después de determinar qué eventos deben auditarse en su sitio, utilice las siguientes sugerencias para crear los archivos de auditoría sólo con la información necesaria. Tenga en cuenta que,

para asignar indicadores de auditoría a usuarios, roles y perfiles de derechos, debe asumir el rol `root`.

- En concreto, evite agregar eventos y tokens de auditoría a la pista de auditoría. Las siguientes políticas aumentan el tamaño de la pista de auditoría.

`arge`	Agrega variables de entorno a los eventos de auditoría `execv`. Si bien auditar eventos `execv` puede ser muy costoso, agregar variables al registro de auditoría no lo es.
argv	Agrega parámetros de comandos a los eventos de auditoría `execv`. Agregar parámetros de comandos para el registro de auditoría no es costoso.
group	Agrega un token de grupo a los eventos de auditoría que incluyen un token `newgroups` opcional.
path	Agrega un token `path` a los eventos de auditoría que incluyen un token `path` opcional.
public	Si va a auditar eventos de archivos, agregue un evento a la pista de auditoría cada vez que ocurra un evento auditable en un objeto público. Las clases de archivos incluyen `fa`, `fc` , `fd`, `fm`, `fr`, `fw` y `cl`. Para la definición de un archivo público, consulte “Conceptos y terminología de auditoría” [11].
seq	Agrega un token de secuencia a cada evento de auditoría.
trail	Agrega un token de ubicador a cada evento de auditoría.
windata_down	En un sistema configurado con Trusted Extensions, agrega eventos cuando se disminuye el nivel de la información en una ventana con etiqueta.
windata_up	En un sistema configurado con Trusted Extensions, agrega eventos cuando se eleva el nivel de la información en una ventana con etiqueta.
zonename	Agrega el nombre de zona a cada evento de auditoría. Si la zona global es la única zona configurada, agrega la cadena `zone, global` a cada evento de auditoría.

  El siguiente registro de auditoría muestra el uso del comando `ls`. La clase `ex` se está auditando y la política predeterminada está en uso:

```
header,129,2,AUE_EXECVE,,mach1,2010-10-14 11:39:22.480 -07:00
```

```
path,/usr/bin/ls
attribute,100555,root,bin,21,320271,18446744073709551615
subject,jdoe,root,root,root,root,2404,50036632,82 0 mach1
return,success,0
```

A continuación, se muestra el mismo registro cuando se activan todas las políticas:

```
header,1578,2,AUE_EXECVE,,mach1,2010-10-14 11:45:46.658 -07:00
path,/usr/bin/ls
attribute,100555,root,bin,21,320271,18446744073709551615
exec_args,2,ls,/etc/security
exec_env,49,MANPATH=/usr/share/man,USER=jdoe,GDM_KEYBOARD_LAYOUT=us,EDITOR=gedit,
LANG=en_US.UTF-8,GDM_LANG=en_US.UTF-8,PS1=#,GDMSESSION=gnome,SESSIONTYPE=1,SHLVL=2,
HOME=/home/jdoe,LOGNAME=jdoe,G_FILENAME_ENCODING=@locale,UTF-8, PRINTER=example-dbl,
...
path,/lib/ld.so.1
attribute,100755,root,bin,21,393073,18446744073709551615
subject,jdoe,root,root,root,root,2424,50036632,82 0 mach1
group,root,other,bin,sys,adm,uucp,mail,tty,lp,nuucp,daemon
return,success,0
zone,global
sequence,197
trailer,1578
```

- Utilice el complemento `audit_syslog` para enviar algunos eventos de auditoría a `syslog`.

  No envíe dichos eventos de auditoría al complemento `audit_binfile` o `audit_remote`. Esta estrategia funciona sólo si no es necesario mantener registros binarios de los eventos de auditoría que envía a los registros `syslog`.

- Defina menos indicadores de auditoría en todo el sistema y audite usuarios individuales.

  Reduzca la cantidad de auditoría para todos los usuarios mediante la reducción del número de clases de auditoría que se auditan en todo el sistema.

  Utilice la palabra clave `audit_flags` para los comandos `roleadd`, `rolemod`, `useradd` y `usermod` con el fin de auditar eventos de usuarios y roles específicos. Para ver ejemplos, consulte el Ejemplo 4-11, “Especificación de clases de auditoría para salida de `syslog`” y la página del comando man `usermod`(1M).

  Utilice las propiedades `always_audit` y `never_audit` del comando `profiles` para auditar eventos de perfiles de derechos específicos. Para obtener más información, consulte la página del comando man `profiles`(1).

Nota - Al igual que otros atributos de seguridad, los indicadores de auditoría son afectados por orden de búsqueda. Para obtener más información, consulte “Orden de búsqueda para derechos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

- Cree sus propias clases de auditoría personalizadas.

Puede crear clases de auditoría en el sitio. En estas clases, coloque sólo los eventos de auditoría que necesita supervisar. Para conocer el procedimiento, consulte Cómo agregar una clase de auditoría [56].

Nota - Para obtener información sobre los efectos de modificar un archivo de configuración de auditoría, consulte “Archivos de configuración de auditoría y empaquetado” [119].

Los archivos de auditoría binarios crecen sin límite

Como administrador que tiene asignado el perfil de derechos de revisión de auditoría, puede limitar el tamaño de los archivos binarios para facilitar el archivado y la búsqueda. También puede crear archivos binarios más pequeños a partir del archivo original mediante una de las opciones descritas en esta sección.

- Utilice el atributo `p_fsize` para limitar el tamaño de archivos de auditoría binarios individuales.

  Para obtener una descripción del atributo `p_fsize`, consulte la sección ATRIBUTOS DE OBJETO de la página del comando man `audit_binfile`(5).

  Si desea ver un ejemplo, consulte el Ejemplo 4-3, “Limitación de tamaño de archivo para el complemento `audit_binfile`”.
- Utilice el comando `auditreduce` para seleccionar registros y escribir esos registros en un archivo más pequeño para un mayor análisis.

  Las opciones `auditreduce` *-lowercase* buscan registros específicos.

  Las opciones `auditreduce` *-mayúscula* escriben las selecciones en un archivo. Para obtener más información, consulte la página del comando man `auditreduce`(1M). Consulte también “Visualización de datos de pista de auditoría” [93].

No se auditan los inicios de sesión desde otros sistemas operativos

El sistema operativo Oracle Solaris puede auditar todos los inicios de sesión, independientemente del origen. Si no se auditan los inicios de sesión, es probable que la clase `lo` para los eventos atribuibles y no atribuibles no esté definida. Esta clase audita los inicios de sesión, los cierres de sesión y los bloqueos de pantalla. Estas clases se auditan de manera predeterminada.

Nota - Para auditar inicios de sesión `ssh`, su sistema debe ejecutar el daemon `ssh` de Oracle Solaris. Este daemon se modifica para el servicio de auditoría en un sistema Oracle Solaris. Para obtener más información, consulte “Shell seguro y el proyecto OpenSSH” de “Gestión de acceso mediante shell seguro en Oracle Solaris 11.2 ”.

EJEMPLO 6-1 Cómo asegurarse de que los inicios de sesión se auditen

En este ejemplo, la salida de los dos primeros comandos muestra que la clase `lo` para eventos atribuibles y no atribuibles no está establecida. A continuación, los dos últimos comandos configuran la clase `lo` para activar la auditoría de eventos de inicio de sesión.

```
# auditconfig -getflags
active user default audit flags = as,st(0x20800,0x20800)
configured user default audit flags = as,st(0x20800,0x20800)

# auditconfig -getnaflags
active non-attributable audit flags = na(0x400,0x400)
configured non-attributable audit flags = na(0x400,0x400)

# auditconfig -setflags lo,as,st
user default audit flags = as,lo,st(0x21800,0x21800)

# auditconfig -setnaflags lo,na
non-attributable audit flags = lo,na(0x1400,0x1400)
```

♦ ♦ ♦ CAPÍTULO 7

Referencia sobre auditoría

En este capítulo, se describen los componentes importantes de la auditoría y se tratan los siguientes temas:

Para obtener una descripción general de la auditoría, consulte el Capítulo 1, Acerca de la auditoría en Oracle Solaris. Para obtener sugerencias de planificación, consulte el Capítulo 2, Planificación de la auditoría. Si desea conocer los procedimientos para configurar la auditoría en su sitio, consulte los capítulos siguientes:

- Capítulo 3, Gestión del servicio de auditoría
- Capítulo 4, Supervisión de actividades del sistema
- Capítulo 5, Cómo trabajar con datos de auditoría
- Capítulo 6, Análisis y resolución de problemas del servicio de auditoría

Servicio de auditoría

El servicio de auditoría, `auditd`, está activado de manera predeterminada. Para averiguar cómo activar, refrescar o desactivar el servicio, consulte “Activación y desactivación del servicio de auditoría” [44].

Sin configuración de cliente, los siguientes valores predeterminados están establecidos:

- Se auditan todos los eventos de inicio se sesión.

  Se auditan los intentos de inicio de sesión correctos y con errores.
- Todos los usuarios se auditan para eventos de inicio y cierre de sesión, incluidos la asunción de roles y el bloqueo de pantalla.
- El complemento `audit_binfile` está activo. El directorio `/var/audit` almacena los registros de auditoría, el tamaño de un archivo de auditoría no está limitado y el tamaño de la cola es de 100 registros.
- La política `cnt` está establecida.

  Cuando los registros de auditoría llenan el espacio en disco disponible, el sistema realiza un seguimiento de la cantidad de registros de auditoría descartados. Una advertencia se emite cuando resta un uno por ciento de espacio en disco disponible.
- Los siguientes controles de cola de auditoría están establecidos.
  - El número máximo de registros en la cola de auditoría antes de generar los bloqueos de registros es 100
  - El número mínimo de registros en la cola de auditoría antes de que los procesos de auditoría bloqueados se desbloqueen es 10
  - El tamaño de buffer para la cola de auditoría es de 8.192 bytes
  - El intervalo de escritura de registros de auditoría en la pista de auditoría es de 20 segundos

Para mostrar los valores predeterminados, consulte “Visualización de los valores predeterminados del servicio de auditoría” [42].

El servicio de auditoría permite definir valores temporales o activos. Estos valores pueden diferir de los valores configurados o de los valores de propiedades.

- Los valores temporales no se restauran al refrescar o reiniciar el servicio de auditoría.

  La política de auditoría y los controles de cola de auditoría aceptan valores temporales. Los indicadores de auditoría no tienen un valor temporal.
- Los valores configurados se almacenan como valores de propiedades del servicio, por lo tanto, se restablecen al refrescar o reiniciar el servicio de auditoría.

Los perfiles de derechos controlan quién puede administrar el servicio de auditoría. Para obtener más información, consulte “Perfiles de derechos para administración de auditoría” [118].

De manera predeterminada, todas las zonas se auditan de la misma manera. Consulte “Auditoría y Oracle Solaris Zones” [119].

Páginas del comando man del servicio de auditoría

En la siguiente tabla se resumen las principales páginas del comando man administrativas para el servicio de auditoría.

Página del comando man	Resumen
audit(1M)	Comandos que controlan las acciones del servicio de auditoría `audit -n` inicia un nuevo archivo de auditoría para el complemento `audit_binfile`. `audit -s` activa y refresca la auditoría. `audit -t` desactiva la auditoría. `audit -v` verifica que al menos un complemento esté activo.
audit_binfile(5)	Complemento de auditoría predeterminado que envía registros de auditoría a un archivo binario. Consulte también “Complementos de auditoría” [121].
audit_remote(5)	Complemento de auditoría que envía registros de auditoría a un receptor remoto.
audit_syslog(5)	Complemento de auditoría que envía resúmenes de texto a la utilidad `syslog`.
audit_class(4)	Archivo que contiene las definiciones de clases de auditoría. Los ocho bits de orden superior están disponibles para que los clientes creen nuevas clases de auditoría. Para obtener más información acerca del efecto de modificar este archivo en la actualización del sistema, consulte Cómo agregar una clase de auditoría [56].
audit_event(4)	Archivo que contiene las definiciones de eventos de auditoría y asigna los eventos a clases de auditoría. La asignación se puede modificar. Para obtener más información acerca del efecto de modificar este archivo en la actualización del sistema, consulte Cómo cambiar una pertenencia a clase de un evento de auditoría [58].
audit_flags(5)	Describe la sintaxis de la preselección de clases de auditoría, los prefijos para seleccionar sólo los eventos con fallos o sólo los eventos correctos, y los prefijos que modifican una preselección existente.
audit.log(4)	Describe los nombres de archivos de auditoría binarios, la estructura interna de un archivo y la estructura de cada token de auditoría.
audit_warn(1M)	Secuencia de comandos que notifica a un alias de correo electrónico cuando el servicio de auditoría encuentra una condición poco habitual al escribir los registros de auditoría. Puede personalizar esta secuencia de comandos para su sitio a fin de advertir acerca de condiciones que puedan requerir intervención manual o puede especificar cómo manejar dichas condiciones automáticamente.
auditconfig(1M)	Comando que recupera y establece parámetros de configuración de auditoría. Emita el comando `auditconfig` sin opciones para mostrar una lista de parámetros que se pueden recuperar y establecer.

Página del comando man	Resumen
auditrecord(1M)	Comando que muestra la definición de eventos de auditoría en el archivo /etc/security/audit_event. Para conocer un ejemplo de salida, consulte “Visualización de definiciones de registros de auditoría” [93].
auditreduce(1M)	Comando que selecciona posteriormente y fusiona registros de auditoría que se almacenan en formato binario. El comando puede fusionar los registros de auditoría de uno o más archivos de auditoría de entrada. Los registros permanecen en formato binario. Las opciones de mayúscula afectan la selección de archivos. Las opciones de minúscula afectan la selección de registros.
auditstat(1M)	Comando que muestra estadísticas de auditoría de núcleo. Por ejemplo, el comando puede mostrar el número de registros en la cola de auditoría de núcleo, el número de registros descartados y el número de registros de auditoría que los procesos de usuario generaron en el núcleo como resultado de llamadas del sistema.
praudit(1M)	Comando que lee los registros de auditoría en formato binario a partir de la entrada estándar y muestra los registros en un formato presentable. La entrada puede conducirse desde el comando auditreduce o desde un único archivo de auditoría o una lista de archivos de auditoría. La entrada también se puede generar con el comando tail -0f para un archivo de auditoría actual. Para conocer un ejemplo de salida, consulte “Visualización del contenido de los archivos de auditoría binarios” [97].
syslog.conf(4)	Archivo configurado para enviar resúmenes de texto de registros de auditoría para la utilidad syslog para el complemento audit_syslog.

Perfiles de derechos para administración de auditoría

Oracle Solaris proporciona perfiles de derechos para configurar el servicio de auditoría, para activar y desactivar el servicio, y para analizar la pista de auditoría. Debe tener los privilegios de root para editar un archivo de configuración de auditoría.

- **Configuración de auditoría:** permite que un administrador configure los parámetros del servicio de auditoría y ejecute el comando auditconfig.
- **Control de auditoría:** permite que un administrador inicie, refresque y desactive el servicio de auditoría y ejecute el comando audit para iniciar, refrescar o detener el servicio.
- **Revisión de auditoría:** permite que un administrador analice registros de auditoría. Este perfil de derechos concede autorización para leer registros de auditoría con los comandos praudit y auditreduce. Este administrador también puede ejecutar el comando auditstat.
- **Administrador del sistema**: incluye el perfil de derechos de revisión de auditoría. Un administrador con el perfil de derechos de administrador del sistema puede analizar los registros de auditoría.

Para configurar roles para manejar el servicio de auditoría, consulte “Creación de roles” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

Auditoría y Oracle Solaris Zones

Las zonas no globales se pueden auditar exactamente como se audita la zona global, o las zonas no globales pueden establecer sus propios indicadores, almacenamiento y políticas de auditoría.

Cuando todas las zonas se auditan de manera idéntica, los archivos `audit_class` y `audit_event` en la zona global proporcionan las asignaciones de clase-evento para auditoría en cada zona. La opción de política `+zonename` es útil para la selección posterior de registros por nombre de zona.

Las zonas se pueden auditar individualmente. Cuando la opción de política, `perzone`, se establece en la zona global, cada zona no global ejecuta su propio servicio de auditoría, gestiona su propia cola de auditoría y especifica el contenido y la ubicación de los registros de auditoría. Una zona no global también puede definir la mayoría de las opciones de la política de auditoría. No puede definir una política que afecte a todo el sistema, por lo que una zona no global no puede definir las políticas `ahlt` o `perzone`. Para obtener más información, consulte “Auditoría en un sistema con Oracle Solaris Zones” [25] y “Planificación de la auditoría en zonas” [28].

Para obtener más información sobre las zonas, consulte “Introducción a Zonas de Oracle Solaris ”.

Archivos de configuración de auditoría y empaquetado

Los archivos de configuración de auditoría en Oracle Solaris se marcan en el paquete con el atributo de paquete `preserve=renamenew`. Este atributo mantiene cualquier modificación que realice en los archivos entre las actualizaciones. Para obtener información sobre los efectos de los valores `preserve`, consulte la página del comando man `pkg` (5).

Estos archivos de configuración también se marcan con el atributo de paquete `overlay=allow`. Este atributo le permite crear su propio paquete que contiene estos archivos y reemplazar los archivos de Oracle Solaris con archivos de su paquete. Cuando se establece el atributo `overlay` en `true` en su paquete, los subcomandos `pkg`, como `verify`, `fix`, `revert`, etc., devolverán resultados en sus paquetes. Para obtener más información, consulte las páginas del comando man `pkg`(1) y `pkg`(5).

Clases de auditoría

Oracle Solaris define clases de auditoría como contenedores prácticos para un gran número de eventos de auditoría.

Puede reconfigurar clases de auditoría y realizar nuevas clases de auditoría. Los nombres de clase de auditoría puede tener un máximo de 8 caracteres de longitud. La descripción de clase está limitada a 72 caracteres. Se permite el uso de caracteres numéricos y no alfanuméricos.

Para obtener más información, consulte la página del comando man `audit_class`(4) y Cómo agregar una clase de auditoría [56].

Atención - La clase `all` puede generar grandes cantidades de datos y llenar rápidamente los discos. Utilice la clase `all` sólo si se tienen motivos extraordinarios para auditar todas las actividades.

Sintaxis de la clase de auditoría

Los eventos en una clase de auditoría se pueden auditar para determinar si la clase es correcta, si tiene fallos o ambas cosas.

- Sin un prefijo, una clase de eventos se audita para determinar si es correcta o si falló.
- Con un prefijo de signo más (+), se audita una clase de eventos únicamente para determinar si son correctos.
- Con un prefijo de signo menos (-), se audita una clase de los eventos únicamente para determinar si tienen fallos.
- Para modificar una preselección actual, agregue un signo de intercalación (^) antes de un prefijo o un indicador de auditoría. Por ejemplo:
  - Si `ot` está preseleccionado para el sistema, y la preselección de un usuario es `^ot`, dicho usuario no se audita para eventos en la clase `other`.
  - Si `+ot` está preseleccionado para el sistema, y la preselección de un usuario es `^+ot`, dicho usuario no se audita para eventos correctos en la clase `other`.
  - Si `-ot` está preseleccionado para el sistema, y la preselección de un usuario es `^-ot`, dicho usuario no se audita para eventos con fallos en la clase `other`.

Para revisar la sintaxis de la preselección de clases de auditoría, consulte la página del comando man `audit_flags`(5).

Las clases de auditoría y sus prefijos se pueden especificar en los siguientes comandos:

- Como argumentos para las opciones del comando `auditconfig -setflags` y `-setnaflags`.
- Como valores del atributo `p_flags` para el complemento `audit_syslog`. Especifica el atributo como una opción para el comando `auditconfig -setplugin audit_syslog active`.
- Como valores para la opción `-K audit_flags=`*always-audit-flags*`:`*never-audit-flags* para los comandos `useradd`, `usermod`, `roleadd` y `rolemod`.

- Como valores para las propiedades `-always_audit` y `-never_audit` del comando `profiles`.

Complementos de auditoría

Los complementos de auditoría especifican cómo manejar los registros de auditoría en la cola de auditoría. Los complementos de auditoría se especifican por nombre: `audit_binfile`, `audit_remote` y `audit_syslog` como argumentos para el comando `auditconfig -setplugin`. Los complementos se pueden especificar en detalle mediante los siguientes atributos:

- Complemento `audit_binfile`

  Atributo `p_dir`: dónde enviar datos binarios

  Atributo `p_minfree`: espacio mínimo restante en un disco antes de que se le envíe una advertencia al administrador.

  Atributo `p_fsize`: tamaño máximo de un archivo de auditoría.
- Complemento `audit_remote`

  Atributo `p_hosts`: servidor de auditoría autenticado remoto al que se envían los datos de auditoría binarios.

  Atributo `p_retries`: el número de intentos que se deben hacer para comunicarse con un servidor de auditoría autenticado remoto.

  Atributo `p_timeout`: el número de segundos entre los intentos que hacen para comunicarse con un servidor de auditoría autenticado remoto.
- Complemento `audit_syslog`

  Atributo `p_flags`: selección de resúmenes de texto de registros de auditoría que se envían a la utilidad `syslog`.
- Para todos los complementos, el número máximo de registros de auditoría que están en cola para el complemento (atributo `-qsize`)

Consulte las páginas del comando man `audit_binfile`(5), `audit_remote`(5), `audit_syslog`(5) y `auditconfig`(1M).

Servidor de auditoría remoto

El servidor de auditoría remoto (ARS) recibe los registros de auditoría por un enlace seguro desde los sistemas auditados y almacena los registros.

La recepción se basa en que se configure lo siguiente:

- Un dominio Kerberos con principios de auditoría específicos y un mecanismo GSS-API.
- El ARS con al menos un *grupo de conexión* configurado y activo.
- Al menos un sistema auditado en el grupo de conexión y un complemento `audit_remote` configurado y activo.

En la propiedad `group` del ARS, se especifica un grupo de conexión. Para la gestión de archivos, `group` puede limitar el tamaño del archivo de auditoría y especificar el espacio libre mínimo. El motivo principal para especificar diferentes grupos de conexiones es especificar diferentes ubicaciones de almacenamiento en el ARS, como se muestra en el Ejemplo 4-9, “Transmisión por secuencias de registros de auditoría a diferentes ubicaciones de archivos en el mismo ARS”.

Para obtener más información acerca del ARS, consulte la página del comando man `ars`(5). Para obtener información de configuración del ARS, consulte las opciones `-setremote` en la página del comando man `auditconfig`(1M).

Para configurar los sistemas auditados, consulte la página del comando man `audit_remote`(5) y la opción `-setplugin` en la página del comando man `auditconfig`(1M).

Política de auditoría

La política de auditoría determina si se agrega información adicional a la pista de auditoría.

Las siguientes políticas agregan tokens a los registros de auditoría: `arge`, `argv`, `group`, `path`, `seq`, `trail`, `windata_down`, `windata_up` y `zonename`. Las políticas `windata_down` y `windata_up` son utilizadas por la función Trusted Extensions de Oracle Solaris. Para obtener más información, consulte el Capítulo 22, “Trusted Extensions y la auditoría” de “Configuración y administración de Trusted Extensions ”.

Las políticas restantes no agregan tokens. La política `public` limita la auditoría de archivos públicos. La política `perzone` establece colas de auditoría independientes para zonas no globales. Las políticas `ahlt` y `cnt` determinan qué sucede cuando no se pueden enviar registros de auditoría. Para obtener más detalles, consulte “Políticas de auditoría para eventos síncronos y asíncronos” [123].

Los efectos de las diferentes opciones de políticas de auditoría se describen en “Comprensión de la política de auditoría” [35]. Para obtener una descripción de las opciones de política de auditoría, consulte la opción `-setpolicy` en la página del comando man `auditconfig`(1M). Para obtener una lista de las opciones de política disponibles, ejecute el comando `auditconfig -lspolicy`. Para la política actual, ejecute el comando `auditconfig -getpolicy`.

Políticas de auditoría para eventos síncronos y asíncronos

Juntas, la política `ahlt` y la política `cnt` rigen lo que ocurre cuando la cola de auditoría está completa y no puede aceptar más eventos.

Nota - Las políticas `cnt` o `ahlt` no se activan si la cola para al menos un complemento puede aceptar registros de auditoría.

Las políticas `cnt` y `ahlt` son independientes y están relacionadas. Las combinaciones de las políticas tienen los siguientes efectos:

- `-ahlt +cnt` es la política predeterminada que se envía. Este valor predeterminado permite el procesamiento de un evento auditado incluso si no se puede registrar el evento.

  La política `-ahlt` indica que si un registro de auditoría de un evento asíncrono no se puede ubicar en la cola de auditoría de núcleo, el sistema contará los eventos y continuará el procesamiento. En la zona global, el contador `as_dropped` registra el recuento.

  La política `+cnt` indica que si llega un evento síncrono y el evento no se puede ubicar en la cola de auditoría de núcleo, el sistema contará el evento y continuará el procesamiento. El contador `as_dropped` de la zona registra el recuento.

  La configuración `-ahlt +cnt` se usa generalmente en sitios donde el procesamiento debe continuar, incluso si continuar con el procesamiento puede producir una pérdida de registros de auditoría. El campo `auditstat drop` muestra el número de registros de auditoría que se descartan en una zona.
- La política `+ahlt -cnt` indica que el procesamiento se detiene cuando un evento asíncrono no se puede agregar a la cola de auditoría de núcleo.

  La política `+ahlt` indica que si un registro de auditoría de un evento asíncrono no se puede ubicar en la cola de auditoría de núcleo, todo el procesamiento se detiene. El sistema entrará en estado de alerta. El evento asíncrono no estará en la cola de auditoría y se debe recuperar de punteros en la pila de llamadas.

  La política `-cnt` indica que si un evento síncrono no se puede ubicar en la cola de auditoría de núcleo, el subproceso que intenta entregar el evento se bloqueará. El subproceso se coloca en una cola inactiva hasta que el espacio de auditoría pase a estar disponible. Ningún recuento se mantiene. Los programas podrían parecer bloquearse hasta que el espacio de auditoría pase a estar disponible.

  La configuración `+ahlt -cnt` se usa generalmente en sitios donde el registro de cada evento de auditoría tiene prioridad sobre la disponibilidad del sistema. El campo `auditstat wblk` muestra el número de veces que los subprocesos se bloquearon.

  Sin embargo, si un evento asíncrono se produce, el sistema entrará en estado de alerta, lo que lleva a una interrupción. La cola de núcleo de eventos de auditoría se puede recuperar

manualmente de un volcado de bloqueo guardado. El evento asíncrono no estará en la cola de auditoría y se debe recuperar de punteros en la pila de llamadas.

- La política `-ahlt -cnt` indica que si un evento asíncrono no se puede ubicar en la cola de auditoría de núcleo, el evento se contará y continuará el procesamiento. Cuando un evento síncrono no se puede ubicar en la cola de auditoría de núcleo, el subproceso que intenta entregar el evento se bloqueará. El subproceso se coloca en una cola inactiva hasta que el espacio de auditoría pase a estar disponible. Ningún recuento se mantiene. Los programas podrían parecer bloquearse hasta que el espacio de auditoría pase a estar disponible.

  La configuración `-ahlt -cnt` se usa generalmente en los sitios donde el registro de todos los eventos de auditoría síncronos tiene prioridad sobre alguna posible pérdida de registros de auditoría asíncronos. El campo `auditstat wblk` muestra el número de veces que los subprocesos se bloquearon.
- La política `+ahlt +cnt` indica que si un evento asíncrono no se puede ubicar en la cola de auditoría de núcleo, el sistema entrará en estado de alerta. Si un evento síncrono no se puede ubicar en la cola de auditoría de núcleo, el sistema contará el evento y continuará el procesamiento.

Características del proceso de auditoría

Las siguientes características de auditoría se definen en el primer inicio de sesión:

- **Máscara de preselección de procesos:** una combinación de la máscara de auditoría en todo el sistema y la máscara de auditoría específica de usuario, si una máscara de auditoría de usuario se ha especificado. Cuando un usuario inicia sesión, el proceso de inicio de sesión combina las clases preseleccionadas para establecer la *máscara de preselección de proceso* para los procesos del usuario. La máscara de preselección de proceso especifica los sucesos que generan registros de auditoría.

  El siguiente algoritmo describe el modo en que el sistema obtiene la máscara de preselección de proceso del usuario:

  `(system-wide default flags` + *always-audit-classes*`)` - *never-audit-classes*

  Agregue clases de auditoría en todo el sistema de los resultados del comando `auditconfig -getflags` a las clases del valor *always-audit-classes* para la palabra clave `always_audit` del usuario. Luego, reste del total las clases del campo *never-audit-classes* del usuario.

  Consulte también la página del comando man `audit_flags`(5).
- **ID de usuario de auditoría**: un proceso adquiere un ID de usuario de auditoría inmutable cuando el usuario inicia sesión. Este ID es heredado por todos los procesos secundarios comenzados por el proceso inicial del usuario. El ID de usuario de auditoría ayuda a aplicar responsabilidad. Incluso después de que un usuario asume un rol, el ID del usuario de auditoría sigue siendo el mismo. El ID del usuario de auditoría que se guarda en cada registro de auditoría le permite siempre rastrear las acciones hasta el usuario de inicio de sesión.

- **ID de sesión de auditoría**: el ID de sesión de auditoría se asigna cuando se inicia sesión. Este ID de sesión es heredado por todos los procesos secundarios.
- **ID de terminal**: para un inicio de sesión local, el ID de terminal está formado por la dirección IP del sistema local seguido por un número único que identifica el dispositivo físico en el que inició sesión el usuario. La mayoría de las veces, el inicio de sesión es a través de la consola. El número que corresponde al dispositivo de la consola es `0,0`. Para un inicio de sesión remoto, el ID de terminal consta de una dirección IP del host remoto seguido del número de puerto remoto y el número de puerto local.

Pista de auditoría

La *pista de auditoría* contiene archivos de auditoría binarios. La pista se crea mediante el complemento `audit_binfile`. El servicio de auditoría recopila los registros en la cola de auditoría y los envía al complemento, que los escribe en el disco.

Convenciones de nombres de archivos de auditoría binarios

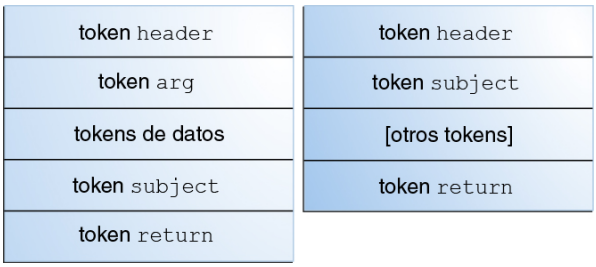
El complemento `audit_binfile` crea archivos de auditoría binarios. Cada archivo de auditoría binario es una recopilación de registros autocontenidos. El nombre del archivo identifica el período durante el cual los registros se generaron y el sistema que los generó. Las indicaciones de hora que indican el período de tiempo se especifican en formato de hora universal coordinada (UTC) para asegurarse de que se muestren en orden correcto, incluso entre zonas horarias.

Para obtener más información, consulte la página del comando man `audit.log`(4). Para obtener ejemplos de nombres de archivos de auditoría abiertos y cerrados, consulte Cómo depurar un archivo de auditoría `not_terminated` [104].

Estructura de registro de auditoría

Un registro de auditoría es una secuencia de tokens de auditoría. Cada token de auditoría contiene información del evento, como ID de usuario, hora y fecha. Un token `header` comienza un registro de auditoría, y un token opcional `trailer`, lo concluye. Otras tokens de auditoría contienen información relevante para el evento de auditoría. En la siguiente figura se muestra un registro de auditoría de núcleo típico y un registro de auditoría de nivel de usuario típico.

FIGURA 7-1 Estructuras de registros de auditoría típicas



Análisis de registro de auditoría

El análisis de registro de auditoría incluye la selección posterior de los registros de la pista de auditoría. Puede utilizar uno de estos dos métodos para analizar los datos binarios recopilados.

- Puede utilizar para ello el comando `praudit`. Las opciones para el comando proporcionan diferentes salidas de texto. Por ejemplo, el comando `praudit -x` proporciona XML para introducir en secuencias de comandos y exploradores. La salida de `praudit` no incluye campos cuyo único propósito es ayudar a analizar los datos binarios. Tenga en cuenta que el orden y el formato de la salida de `praudit` no están garantizados entre las versiones de Oracle Solaris.

  Para ver ejemplos de una salida de `praudit`, consulte “Visualización del contenido de los archivos de auditoría binarios” [97].

  Para obtener ejemplos de una salida `praudit` para cada token de auditoría, consulte los tokens individuales en “Formatos de token de auditoría” [127].
- Puede escribir un programa para analizar el flujo de datos binarios. El programa deben tener en cuenta las variantes de un registro de auditoría. Por ejemplo, la llamada del sistema `ioctl()` crea un registro de auditoría para "nombre de archivo incorrecto". Este registro contiene diferentes tokens del registro de auditoría `ioctl()` para "descriptor de archivo no válido".
  - Para obtener una descripción del orden de los datos binarios en cada token de auditoría, consulte la página del comando man `audit.log`(4).
  - Para valores del manifiesto, consulte el archivo `/usr/include/bsm/audit.h`.
  - Para ver el orden de los tokens en un registro de auditoría, use el comando `auditrecord`. La salida del comando `auditrecord` incluye los diferentes tokens para los diferentes valores de manifiesto. Los corchetes (`[]`) indican que un token de auditoría es

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

Formatos de token de auditoría

Cada token de auditoría tienen un identificador de tipo de token, que está seguido por los datos específicos para el token. La siguiente tabla muestra los nombres de token con una breve descripción de cada uno. Los tokens obsoletos se mantienen por motivos de compatibilidad con las versiones anteriores de Solaris.

TABLA 7-1 Tokens de auditoría para auditoría

Nombre de token	Descripción	Más información
acl	Información de entrada de control de acceso (ACE) y lista de control de acceso (ACL)	"Token acl" [128]
arbitrary	Datos con información de formato y de tipo	Página del comando man audit.log(4)
argument	Valor de argumento de llamada de sistema	"Token argument" [129]
attribute	Información del archivo vnode	"Token attribute" [129]
cmd	Argumentos de comandos y variables de entornos	"Token cmd" [129]
exec_args	Argumentos de llamada de sistema exec	"Token exec_args" [130]
exec_env	Variables de entorno de llamada de sistema exec	"Token exec_env" [130]
exit	Información de salida de programa	Página del comando man audit.log(4)
file	Información de archivo de auditoría	"Token file" [130]
fmri	Indicador de recursos de gestión de estructura	"Token fmri" [131]
group	Información de grupos de procesos	"Token group" [131]
header	Indica el comienzo del registro de auditoría	"Token header" [131]
ip	Información de encabezado IP	Página del comando man audit.log(4)
ip address	Dirección de Internet	"Token ip address" [132]
ip port	Dirección de puerto de Internet	"Token ip port" [132]
ipc	Información de System V IPC	"Token ipc" [132]
IPC_perm	Información de acceso de objetos de System V IPC	"Token IPC_perm" [133]
opaque	Datos no estructurados (sin especificar formato)	Página del comando man audit.log(4)
path	Información de ruta	"Token path" [133]
path_attr	Información de ruta de acceso	"Token path_attr" [133]
privilege	Información de conjunto de privilegios	"Token privilege" [134]
process	Información de proceso	"Token process" [134]

Nombre de token	Descripción	Más información
`return`	Estado de llamada de sistema	"Token `return`" [134]
`sequence`	Número de secuencia	"Token `sequence`" [135]
`socket`	Direcciones y tipo de socket	"Token `socket`" [135]
`sujeto`	Información de "subject" (tiene el mismo formato que `process`)	"Token `subject`" [135]
`text`	Cadena ASCII	"Token `text`" [136]
`trailer`	Indica el final del registro de auditoría	"Token `trailer`" [136]
`use of authorization`	Uso de autorización	"Token `use of authorization`" [136]
`use of privilege`	Uso de privilegio	"Token `use of privilege`" [137]
`user`	ID de usuario y nombre de usuario	"Token `user`" [137]
`xclient`	Identificación de los clientes X	"Token `xclient`" [137]
`zonename`	Nombre de la zona	"Token `zonename`" [137]
Tokens de Trusted Extensions	`label` e información de sistema de ventanas X	"Referencia de auditoría de Trusted Extensions" de "Configuración y administración de Trusted Extensions "

Los siguientes tokens son obsoletos:

- `liaison`
- `host`
- `tid`

Para obtener más información sobre tokens obsoletos, consulte el material de referencia para la versión que incluye el token.

Un registro de auditoría comienza siempre con un token `header`, que indica dónde comienza el registro de auditoría en la pista de auditoría. En el caso de eventos atribuibles, los tokens `subject` y `process` hacen referencia a los valores del proceso que causaron el evento. En el caso de eventos no atribuibles, el token `process` hace referencia al sistema.

Token `acl`

El token `acl` tiene dos formatos diferentes para registrar información sobre entradas de control de acceso (ACE) para un sistema de archivos ZFS y listas de control de acceso (ACL) para un sistema de archivos UFS antiguo.

Cuando el token `acl` está registrado para un sistema de archivos UFS, el comando `praudit -x` muestra los campos de la siguiente manera:

```
<acl type="1" value="root" mode="6"/>
```

Cuando el token `acl` está registrado para un conjunto de datos ZFS, el comando `praudit -x` muestra los campos de la siguiente manera:

```
<acl who="root" access_mask="default" flags="-i,-R" type="2"/>
```

Token `argument`

El token `argument` contiene información sobre los argumentos de una llamada del sistema: el número de argumentos de la llamada del sistema, el valor de los argumento y una descripción opcional. Este token permite un argumento de llamada de sistema de número entero de 32 bits en un registro de auditoría.

El comando `praudit -x` muestra los campos del token `argument` de la siguiente manera:

```
<argument arg-num="2" value="0x5401" desc="cmd"/>
```

Token `attribute`

El token `attribute` contiene información del `vnode` del archivo.

El token `attribute` por lo general acompaña un token `path`. El token `attribute` se produce durante búsquedas de ruta. Si ocurre un error de búsqueda de ruta, `vnode` no está disponible para obtener la información de archivo necesaria. Por lo tanto, el token `attribute` no se encuentra incluido como parte del registro de auditoría. El comando `praudit -x` muestra los campos del token `attribute` de la siguiente manera:

```
<attribute mode="20620" uid="root" gid="tty" fsid="0" nodeid="9267" device="108233"/>
```

Token `cmd`

El token `cmd` registra la lista de argumentos y la lista de variables del entorno asociadas con un comando.

El comando `praudit -x` muestra los campos del token `cmd`. El siguiente ejemplo es un token `cmd` truncado. La línea se ajusta con fines de visualización.

```
<cmd><arge>WINDOWID=6823679</arge>
<arge>COLORTERM=gnome-terminal</arge>
<arge>...LANG=C</arge>...<arge>HOST=machine1</arge>
<arge>LPDEST=printer1</arge>...</cmd>
```

Token exec_args

El token exec_args registra los argumentos en una llamada de sistema exec().

El comando praudit -x muestra los campos del token exec_args de la siguiente manera:

```
<exec_args><arg>/usr/bin/sh</arg><arg>/usr/bin/hostname</arg></exec_args>
```

Nota - El token exec_args sólo se muestra cuando está activada la opción de política de auditoría argv.

Token exec_env

El token exec_env registra las variables de entorno actuales en una llamada de sistema exec().

El comando praudit -x muestra los campos del token exec_env. La línea en el siguiente ejemplo se ajustó con fines de visualización.

```
<exec_env><env>_=/usr/bin/hostname</env>
<env>LANG=C</env><env>PATH=/usr/bin</env>
<env>LOGNAME=jdoe</env><env>USER=jdoe</env>
<env>DISPLAY=:0</env><env>SHELL=/bin/csh</env>
<env>HOME=/home/jdoe</env><env>PWD=/home/jdoe</env><env>TZ=US/Pacific</env>
</exec_env>
```

Nota - El token exec_env sólo se muestra cuando está activada la opción de política de auditoría arge.

Token file

El token file es un token especial que marca el inicio de un nuevo archivo de auditoría y el fin de un antiguo archivo de auditoría cuando se desactiva el archivo antiguo. El token file inicial identifica el archivo anterior en la pista de auditoría. El token file final identifica el archivo siguiente en la pista de auditoría. Estos tokens unen archivos de auditoría sucesivos en una pista de auditoría.

El comando praudit -x muestra los campos del token file. La línea en el siguiente ejemplo se ajustó con fines de visualización.

```
<file iso8601="2009-04-08 14:18:26.200 -07:00">
/var/audit/machine1/files/20090408211826.not_terminated.machine1</file>
```

Token `fmri`

El token `fmri` registra el uso de un indicador de recursos de gestión de fallos (FMRI). Para obtener más información, consulte la página del comando man `smf(5)`.

El comando `praudit -x` muestra el contenido del token `fmri` de la siguiente manera:

```
<fmri service_instance="svc:/system/cryptosvc"</fmri>
```

Token `group`

El token `group` registra las entradas del grupo de la credencial del proceso. El token `group` sólo se muestra cuando está activada la opción de política de auditoría `group`.

El comando `praudit -x` muestra los campos del token `group` de la siguiente manera:

```
<group><gid>staff</gid><gid>other</gid></group>
```

Token `header`

El token `header` es especial en cuanto marca el inicio de un registro de auditoría. El token `header` se combina con el token `trailer` para encerrar todos los tokens en el registro.

De manera poco frecuente, un token `header` puede incluir uno o más modificadores de eventos:

- `fe` indica un evento de auditoría con errores
- `fp` indica el uso con errores de privilegios
- `na` indica un evento no atribuible

  ```
  header,52,2,system booted,na,mach1,2011-10-10 10:10:20.564 -07:00
  ```

- `rd` indica que los datos se leen del objeto
- `sp` indica el uso correcto del privilegio

  ```
  header,120,2,exit(2),sp,mach1,2011-10-10 10:10:10.853 -07:00
  ```

- `wr` indica que los datos se escriben en el objeto

El comando `praudit` muestra el token `header` de la siguiente manera:

```
header,756,2,execve(2),,machine1,2010-10-10 12:11:10.209 -07:00
```

El comando `praudit -x` muestra los campos del token `header` al comienzo del registro de auditoría. La línea en el siguiente ejemplo se ajustó con fines de visualización.

```
<record version="2" event="execve(2)" host="machine1"
iso8601="2010-10-10 12:11:10.209 -07:00">
```

Token `ip address`

El token `ip address` contiene una dirección de protocolo de Internet (dirección IP). La dirección IP se pueden mostrar en formato IPv4 o IPv6. La dirección IPv4 utiliza 4 bytes. La dirección IPv6 utiliza 1 byte para describir el tipo de dirección y 16 bytes para describir la dirección.

El comando `praudit -x` muestra el contenido del token `ip address` de la siguiente manera:

```
<ip_address>machine1</ip_address>
```

Token `ip port`

El token `ip port` contiene las direcciones de los puertos TCP o UDP.

El comando `praudit` muestra el token `ip port` de la siguiente manera:

```
ip port,0xf6d6
```

Token `ipc`

El token `ipc` contiene el identificador de mensaje de System V IPCe, los indicadores de semáforo o el identificador de memoria compartida usado por el emisor de llamada para identificar un objeto IPC determinado.

Los identificadores del objeto IPC infringen la naturaleza sin contexto de los tokens de auditoría. Ningún “nombre” global identifica de forma exclusiva objetos IPC. En su lugar, los objetos IPC se identifican por sus identificadores. Los identificadores sólo son válidos durante el tiempo que los objetos IPC están activos. Sin embargo, la identificación de los objetos IPC no debería suponer ningún problema. Los mecanismos de System V IPC rara vez se utilizan, y todos los mecanismos comparten la misma clase de auditoría.

La siguiente tabla muestra los posibles valores del campo de tipo de objeto IPC. Los valores se definen en el archivo `/usr/include/bsm/audit.h`.

TABLA 7-2 Valores para el campo de tipo de objeto IPC

Nombre	Valor	Descripción
AU_IPC_MSG	1	Objeto de mensaje IPC
AU_IPC_SEM	2	Objeto de semáforo IPC
AU_IPC_SHM	3	Objeto de memoria compartida IPC

El comando `praudit -x` muestra los campos del token `ipc` de la siguiente manera:

```
<IPC ipc-type="shm" ipc-id="15"/>
```

Token `IPC_perm`

El token `IPC_perm` contiene una copia de los permisos de acceso de System V IPC. Este token se agrega a los registros de auditoría generados por los eventos de memoria compartida IPC, los eventos de semáforo IPC y los eventos de mensajes IPC.

El comando `praudit -x` muestra los campos del token `IPC_perm`. La línea en el siguiente ejemplo se ajustó con fines de visualización.

```
<IPC_perm uid="jdoe" gid="staff" creator-uid="jdoe"
creator-gid="staff" mode="100600" seq="0" key="0x0"/>
```

Los valores se toman de la estructura de `IPC_perm` asociada con el objeto IPC.

Token `path`

El token de auditoría `path` contiene información sobre la ruta de acceso para un objeto.

El comando `praudit -x` muestra el contenido del token `path` de la siguiente manera:

```
<path>/export/home/srv/.xsession-errors</path>
```

Token `path_attr`

El token de auditoría `path_attr` contiene información sobre la ruta de acceso para un objeto. La ruta de acceso especifica la secuencia de los objetos de archivo de atributos en el objeto de token `path`. Las llamadas de sistema, como `openat()`, permiten acceder a los archivos de atributos. Para obtener más información acerca de los objetos de archivos de atributos, consulte la página del comando man `fsattr`(5).

El comando `praudit` muestra el token `path_attr` de la siguiente manera:

```
path_attr,1,attr_file_name
```

Token `privilege`

El token `privilege` registra el uso de privilegios en un proceso. El token `privilege` no registra privilegios en la configuración básica. Si un privilegio se ha eliminado del conjunto básico por una acción administrativa, entonces la utilización de ese privilegio se registra. Para obtener más información sobre los privilegios, consulte “Gestión de derechos de procesos” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

El comando `praudit -x` muestra los campos del token `privilege`.

```
<privilege set-type="Inheritable">ALL</privilege>
```

Token `process`

El token `process` contiene información acerca del usuario asociado con un proceso, como el destinatario de una señal.

El comando `praudit -x` muestra los campos del token `process`. La línea en el siguiente ejemplo se ajustó con fines de visualización.

```
<process audit-uid="-2" uid="root" gid="root" ruid="root"
rgid="root" pid="567" sid="0" tid="0 0 0.0.0.0"/>
```

Token `return`

El token `return` contiene el estado de devolución de la llamada de sistema (`u_error`) y el valor de devolución de proceso (`u_rval1`).

El token `return` siempre se devuelve como parte de los registros de auditoría generadas por el núcleo para las llamadas de sistema. En la auditoría de la aplicación, este token indica el estado de salida y otros valores de devolución.

El comando `praudit` muestra el token `return` para una llamada de sistema de la siguiente manera:

```
return,failure: Operation now in progress,-1
```

El comando `praudit -x` muestra los campos del token `return` de la siguiente manera:

```
<return errval="failure: Operation now in progress" retval="-1/">
```

Token `sequence`

El token `sequence` contiene un número de secuencia. El número de secuencia se incrementa cada vez que un registro de auditoría se agregue a la pista de auditoría. El token `sequence` sólo se muestra cuando está activada la opción de política de auditoría `seq`. Este token es útil para la depuración.

El comando `praudit -x` muestra el contenido del token `sequence`:

```
<sequence seq-num="1292"/>
```

Token `socket`

El token `socket` contiene información que describe un socket de Internet. En algunos casos, el token incluye solamente el puerto remoto y la dirección IP remota.

El comando `praudit` muestra esta instancia del token `socket` de la siguiente manera:

```
socket,0x0002,0x83b1,localhost
```

El token ampliado agrega información, incluidos el tipo de socket e información sobre el puerto local.

El comando `praudit -x` muestra esta instancia del token `socket` de la siguiente manera. La línea en el siguiente ejemplo se ajustó con fines de visualización.

```
<socket sock_domain="0x0002" sock_type="0x0002" lport="0x83cf"
laddr="example1" fport="0x2383" faddr="server1.Subdomain.Domain.COM"/>
```

Token `subject`

El token `subject` describe un usuario que lleva a cabo o intenta llevar a cabo una operación. El formato es el mismo que el del token `process`.

El token `subject` siempre se devuelve como parte de los registros de auditoría generadas por el núcleo para las llamadas de sistema. El comando `praudit` muestra el token `subject` de la siguiente manera:

```
subject,jdoe,root,root,root,root,1631,1421584480,8243 65558 machine1
```

El comando `praudit -x` muestra los campos del token `subject`. La línea en el siguiente ejemplo se ajustó con fines de visualización.

```
<subject audit-uid="jdoe" uid="root" gid="root" ruid="root"
rgid="root" pid="1631" sid="1421584480" tid="8243 65558 machine1"/>
```

Token `text`

El token `text` contiene una cadena de texto.

El comando `praudit -x` muestra el contenido del token `text` de la siguiente manera:

```
<text>booting kernel</text>
```

Token `trailer`

Los dos tokens, `header` y `trailer`, son especiales en cuanto distinguen los puntos iniciales y finales de un registro de auditoría y encierran todos los demás tokens. Un token `header` comienza un registro de auditoría. Un token `trailer` finaliza un registro de auditoría. El token `trailer` es un token opcional y se agrega como el último token de cada registro sólo cuando la opción de política de auditoría `trail` está configurada.

Si un registro de auditoría se genera cuando los ubicadores están activados, el comando `auditreduce` puede verificar que el token `trailer` haga referencia correctamente al encabezado del registro. El token `trailer` admite búsquedas hacia atrás en la pista de auditoría.

El comando `praudit` muestra el token `trailer` de la siguiente manera:

```
trailer,136
```

Token `use of authorization`

El token `use of authorization` registra el uso de autorizaciones.

El comando `praudit` muestra el token `use of authorization` de la siguiente manera:

```
use of authorization,solaris.role.delegate
```

Token `use of privilege`

El token `use of privilege` registra el uso de privilegios.

El comando `praudit -x` muestra los campos del token `use of privilege` de la siguiente manera:

```
<use_of_privilege result="successful use of priv">proc_setid</use_of_privilege>
```

Token `user`

El token `user` registra el nombre de usuario y el ID de usuario. Este token está presente si el nombre de usuario es diferente del emisor de la llamada.

El comando `praudit -x` muestra los campos del token `user` de la siguiente manera:

```
<user uid="123456" username="tester1"/>
```

Token `xclient`

El token `xclient` contiene el número de conexiones de cliente al servidor X.

El comando `praudit -x` muestra el contenido del token `xlient` de la siguiente manera:

```
<X_client>15</X_client>
```

Token `zonename`

El token `zonename` registra la zona en la que ocurrió el evento de auditoría. La cadena “global” indica los eventos de auditoría que se producen en la zona global.

El comando `praudit -x` muestra el contenido del token `zonename` de la siguiente manera:

```
<zone name="graphzone"/>
```

Glosario de seguridad

AES Estándar de cifrado avanzado. Una técnica de cifrado de datos en bloques de 128 bits simétricos. En octubre de 2000, el gobierno de los Estados Unidos adoptó la variante Rijndael del algoritmo como estándar de cifrado. AES sustituye el cifrado principal de usuario como estándar gubernamental.

algoritmo Un algoritmo criptográfico. Se trata de un procedimiento informático establecido que realiza el cifrado o el hashing de una entrada.

algoritmo criptográfico Consulte algoritmo.

almacén de claves Un almacén de claves contiene contraseñas, frases de contraseña, certificados y otros objetos de autenticación para que recuperen las aplicaciones. Un almacén de claves puede ser específico para una tecnología o puede ser una ubicación que utilizan varias aplicaciones.

ámbito del servicio de nombres El ámbito en el que un rol puede operar, es decir, un host individual o todos los hosts gestionados por un servicio de nombres especificado, como NIS o LDAP.

aplicación con privilegios Una aplicación que puede sustituir los controles del sistema. La aplicación comprueba los atributos de seguridad, como UID, GID, autorizaciones o privilegios específicos.

archivo de ticket Consulte caché de credenciales.

archivo intermedio Un archivo intermedio contiene una copia cifrada de la clave maestra para el KDC. Esta clave maestra se utiliza cuando un servidor se reinicia para autenticar automáticamente el KDC antes de que inicie los procesos `kadmind` y `krb5kdc`. Dado que el archivo intermedio incluye la clave maestra, el archivo y sus copias de seguridad deben mantenerse en un lugar seguro. Si el cifrado está en peligro, la clave podría utilizarse para acceder o modificar la base de datos del KDC.

archivo keytab Un archivo de tabla de claves que contiene una o varias claves (principales). Un host o servicio utiliza un archivo keytab de la misma manera que un usuario utiliza una contraseña.

archivos de auditoría Logs de auditoría binarios. Los archivos de auditoría se almacenan de manera independiente en un sistema de archivos de auditoría.

asignación de dispositivos Protección de dispositivos en el nivel de usuario. La asignación de dispositivos restringe el uso exclusivo de un dispositivo a un usuario a la vez. Los datos del dispositivo se depuran antes de volver a utilizar el dispositivo. Las autorizaciones se pueden utilizar para limitar quién tiene permiso para asignar un dispositivo.

atributos de seguridad Sustituciones a la política de seguridad que permiten que un comando administrativo se ejecute correctamente al ser ejecutado por un usuario que no sea un superusuario. En el modelo de superusuario, los programas `setuid root` y `setgid` son atributos de seguridad. Cuando estos atributos se aplican a un comando, el comando se ejecuta correctamente sin importar quién lo ejecuta. En el modelo de privilegios, los privilegios de núcleo y otros derechos reemplazan a los programas `setuid root` como atributos de seguridad. El modelo de privilegios es compatible con el modelo de superusuario, ya que el modelo de privilegios reconoce también los programas `setuid` y `setgid` como atributos de seguridad.

autenticación Proceso de verificación de la identidad reclamada de un principal.

autenticador Los clientes trasfieren autenticadores al solicitar tickets (desde un KDC) y servicios (desde un servidor). Contienen información que se genera mediante una clave de sesión conocida sólo por el cliente y el servidor y que se puede verificar como de origen reciente, lo cual indica que la transacción es segura. Cuando se utiliza con un ticket, un autenticador sirve para autenticar un principal de usuario. Un autenticador incluye el nombre de principal del usuario, la dirección IP del host del usuario y una indicación de hora. A diferencia de un ticket, un autenticador se puede utilizar sólo una vez, generalmente, cuando se solicita acceso a un servicio. Un autenticador se cifra mediante la clave de sesión para ese cliente y ese servidor.

autorización 1. En Kerberos, el proceso para determinar si un principal puede utilizar un servicio, a qué objetos puede acceder el principal y el tipo de acceso permitido para cada objeto.

2. En la gestión de derechos de usuario, un derecho que se puede asignar a un rol o a un usuario (o que está incrustado en un perfil de derechos) para realizar una clase de operaciones que, de lo contrario, están prohibidas por la política de seguridad. Las autorizaciones se aplican en el nivel de aplicación del usuario, no en el núcleo.

blindaje La modificación de la configuración predeterminada del sistema operativo para eliminar las vulnerabilidades de seguridad inherentes al host.

Blowfish Algoritmo cifrado de bloques simétricos con una clave de tamaño variable que va de 32 a 448 bits. Bruce Schneier, su creador, afirma que Blowfish se optimiza en el caso de aplicaciones en que la clave se modifica con poca frecuencia.

caché de credenciales Un espacio de almacenamiento (generalmente, un archivo) que contiene credenciales recibidas del KDC.

cifrado de clave privada En el cifrado de clave privada, el remitente y el receptor utilizan la misma clave para el cifrado. Consulte también cifrado de clave pública.

cifrado de clave pública Un esquema de cifrado en el que cada usuario tiene dos claves, una clave pública y una clave privada. En el cifrado de clave pública, el remitente utiliza la clave pública del receptor para

cifrar el mensaje y el receptor utiliza una clave privada para descifrarlo. El servicio Kerberos es un sistema de clave privada. Consulte también cifrado de clave privada.

clave

1. Generalmente, uno de los dos tipos principales de claves:

- *Clave simétrica*: una clave de cifrado que es idéntica a la clave de descifrado. Las claves simétricas se utilizan para cifrar archivos.
- *Claves asimétrica* o *clave pública*: una clave que se utiliza en algoritmos de clave pública, como Diffie-Hellman o RSA. Las claves públicas incluyen una clave privada que sólo conoce un usuario, una clave pública utilizada por el servidor o recurso general y un par de claves privada-pública que combina ambas. La clave privada también se denomina clave *secreta*. La clave pública también se denomina clave *compartida* o clave *común*.

2. Una entrada (nombre de principal) en un archivo keytab. Consulte también archivo keytab.

3. En Kerberos, una clave de cifrado, que puede ser de tres tipos:

- *Clave privada*: una clave de cifrado que comparten un principal y el KDC, y que se distribuye fuera de los límites del sistema. Consulte también clave privada.
- *Clave de servicio*: esta clave tiene el mismo propósito que la clave privada, pero la utilizan servidores y servicios. Consulte también clave de servicio.
- *Clave de sesión*: una clave de cifrado temporal que se utiliza entre dos principales y cuya duración se limita a la duración de una única sesión de inicio. Consulte también clave de sesión.

clave de servicio

Una clave de cifrado que se comparte entre un principal de servicio y el KDC, y se distribuye fuera de los límites del sistema. Consulte también clave.

clave de sesión

Una clave generada por el servicio de autenticación o el servicio de otorgamiento de tickets. Una clave de sesión se genera para proporcionar transacciones seguras entre un cliente y un servicio. La duración de una clave de sesión está limitada a una única sesión de inicio. Consulte también clave.

clave privada

Una clave que se asigna a cada principal de usuario y que sólo conocen el usuario del principal y el KDC. Para los principales de usuario, la clave se basa en la contraseña del usuario. Consulte también clave.

clave secreta

Consulte clave privada.

cliente

De manera restringida, un proceso que utiliza un servicio de red en nombre de un usuario; por ejemplo, una aplicación que utiliza `rlogin`. En algunos casos, un servidor puede ser el cliente de algún otro servidor o servicio.

De manera más amplia, un host que: a) recibe una credencial de Kerberos y b) utiliza un servicio proporcionado por un servidor.

Informalmente, un principal que utiliza un servicio.

código de autenticación de mensajes (MAC) MAC proporciona seguridad en la integridad de los datos y autentica el origen de los datos. MAC no proporciona protección contra intromisiones externas.

confidencialidad Consulte privacidad.

conjunto básico El conjunto de privilegios asignados al proceso de un usuario en el momento de inicio de sesión. En un sistema sin modificaciones, cada conjunto heredable inicial del usuario es equivalente al conjunto básico en el inicio de sesión.

conjunto de privilegios Una recopilación de privilegios. Cada proceso tiene cuatro conjuntos de privilegios que determinan si un proceso puede utilizar un privilegio determinado. Consulte límite definido, conjunto vigente, conjunto permitido y conjunto heredable.

Además, el conjunto básico de privilegios es la recopilación de privilegios asignados al proceso de un usuario en el momento de inicio de sesión.

conjunto heredable El conjunto de privilegios que un proceso puede heredar a través de una llamada a `exec`.

conjunto permitido El conjunto de privilegios que están disponibles para que utilice un proceso.

conjunto vigente El conjunto de privilegios que actualmente están vigentes en un proceso.

consumidor En la función de estructura criptográfica de Oracle Solaris, un consumidor es un usuario de los servicios criptográficos prestados por los proveedores. Los consumidores pueden ser aplicaciones, usuarios finales u operaciones de núcleo. Kerberos, IKE e IPsec son ejemplos de consumidores. Para ver ejemplos de proveedores, consulte proveedor.

credencial Un paquete de información que incluye un ticket y una clave de sesión coincidente. Se utiliza para autenticar la identidad de un principal. Consulte también ticket, clave de sesión.

derechos Una alternativa al modelo de superusuario de todo o nada. La gestión de derechos de usuario y la gestión de derechos de proceso permiten a una organización dividir los privilegios de superusuario y asignarlos a usuarios o roles. Los derechos de Oracle Solaris se implementan como privilegios de núcleo, autorizaciones y la capacidad para ejecutar un proceso como un UID o GID determinado. Los derechos se pueden recopilar en un perfil de derechos y en un rol.

DES Estándar de cifrado de datos. Método de cifrado de clave simétrica que se desarrolló en 1975 y que ANSI estandarizó en 1981 como ANSI X.3.92. DES utiliza una clave de 56 bits.

dominio 1. La red lógica gestionada por una única base de datos de Kerberos y un juego de centros de distribución de claves (KDC).

2. La tercera parte de un nombre de principal. Para el nombre de principal `jdoe/admin@CORP.EXAMPLE.COM`, el dominio es `CORP.EXAMPLE.COM`. Consulte también nombre de principal.

DSA Algoritmo de firma digital. Algoritmo de clave pública con un tamaño de clave variable que va de 512 a 4096 bits. DSS, el estándar del gobierno de los Estados Unidos, llega hasta los 1024 bits. DSA se basa en el algoritmo SHA1 para las entradas.

ECDSA Algoritmo de firma digital de curva elíptica. Un algoritmo de clave pública que se basa en matemáticas de curva elíptica. El tamaño de una clave ECDSA es significativamente menor que el tamaño de una clave pública DSA necesaria para generar una firma de la misma longitud.

elemento inicial Un iniciador numérico para generar números aleatorios. Cuando el iniciador comienza desde un origen aleatorio, el elemento inicial se denomina *elemento inicial aleatorio*.

escalada de privilegios Obtención de acceso a recursos que se encuentran fuera del rango de recursos permitidos por los derechos asignados, incluidos los derechos que anulan los valores predeterminados. Como resultado, un proceso puede realizar operaciones no autorizadas.

evento asíncrono de auditoría Los eventos asíncronos constituyen la minoría de los eventos del sistema. Estos eventos no están asociados con ningún proceso; por lo tanto, no hay procesos disponibles para bloquear y reactivar más adelante. Los eventos de salida y entrada de la PROM, y de inicio del sistema inicial son ejemplos de eventos asíncronos.

evento de auditoría no atribuible Un evento de auditoría cuyo iniciador no se puede determinar, como el evento AUE_BOOT.

evento síncrono de auditoría La mayoría de los eventos de auditoría. Estos eventos están asociados con un proceso en el sistema. Un evento no atribuible que está asociado con un proceso es un evento síncrono, como un error de inicio de sesión.

FQDN Siglas en inglés de Fully Qualified Domain Name, nombre de dominio completo. Por ejemplo, `central.example.com` (en lugar de simplemente `denver`).

frase de contraseña Una frase que se utiliza para verificar que una clave privada haya sido creada por el usuario de la frase de contraseña. Una buena frase de contraseña tiene una longitud de 10 a 30 caracteres, combina caracteres alfabéticos y numéricos, y evita el texto y los nombres simples. Se le pedirá la frase de contraseña para autenticar el uso de la clave privada para cifrar y descifrar comunicaciones.

GSS-API Generic Security Service Application Programming Interface. Una capa de red que proporciona apoyo para diversos servicios de seguridad modulares, incluido el servicio Kerberos. GSS-API proporciona servicios de privacidad, integridad y autenticación de seguridad. Consulte también autenticación, integridad, privacidad.

host Un sistema al que se puede acceder a través de una red.

imagen de único sistema Una imagen de único sistema se utiliza en la auditoría Oracle Solaris para describir un grupo de sistemas auditados que utilizan el mismo servicio de nombres. Estos sistemas envían sus

registros de auditoría a un servidor de auditoría central, donde los registros se pueden comparar como si procedieran de un sistema.

instancia La segunda parte de un nombre de principal; una instancia cualifica la primera parte del nombre de principal. En el caso de un principal de servicio, la instancia es obligatoria. La instancia es el nombre de dominio completo del host, como en `host/central.example.com`. Para los principales de usuario, una instancia es opcional. Sin embargo, tenga en cuenta que `jdoe` y `jdoe/admin` son principales únicos. Consulte también nombre primario, nombre de principal, principal de servicio, principal de usuario.

integridad Un servicio de seguridad que, además de la autenticación del usuario, permite validar los datos transmitidos mediante una suma de comprobación criptográfica. Consulte también autenticación y privacidad.

KDC Centro de distribución de claves. Un equipo que tiene tres componentes Kerberos V5:

- Base de datos de claves y principal
- Servicio de autenticación
- Servicio de otorgamiento de tickets

Cada dominio tiene un KDC maestro y debe tener uno o varios KDC esclavos.

KDC esclavo Una copia de un KDC maestro, que es capaz de realizar la mayoría de las funciones del maestro. Cada dominio, generalmente, tiene varios KDC esclavos (y un solo KDC maestro). Consulte también KDC, KDC maestro.

KDC maestro El KDC maestro en cada dominio, que incluye un servidor de administración Kerberos, `kadmind`, y un daemon de otorgamiento de tickets y autenticación, `krb5kdc`. Cada dominio debe tener al menos un KDC maestro y puede tener varios KDC duplicados, o esclavos, que proporcionan servicios de autenticación a los clientes.

Kerberos Un servicio de autenticación, el protocolo utilizado por ese servicio o el código utilizado para implementar ese servicio.

La implementación de Kerberos en Oracle Solaris que está estrechamente basada en la implementación de Kerberos V5.

Aunque son técnicamente diferentes, "Kerberos" y "Kerberos V5" suelen utilizarse de forma indistinta en la documentación de Kerberos.

En la mitología griega, Kerberos (también escrito Cerberus) era un mastín feroz de tres cabezas que protegía las puertas de Hades.

kvno Siglas en inglés de Key Version Number, número de versión de clave. Un número de secuencia que realiza un seguimiento de una clave determinada en orden de generación. El kvno más alto corresponde a la clave más reciente y actual.

límite definido El límite exterior que indica qué privilegios están disponibles para un proceso y sus procesos secundarios.

Lista de control de acceso Una lista de control de acceso (ACL) proporciona un nivel de seguridad de archivos más específico que la protección de archivos UNIX tradicionales. Por ejemplo, una ACL permite autorizar el acceso de lectura de grupo a un archivo, pero permitir que un solo miembro de ese grupo escriba en el archivo.

MAC 1. Consulte código de autenticación de mensajes (MAC).

2. También se denomina etiquetado. En la terminología de seguridad gubernamental, MAC significa control de acceso obligatorio (del inglés Mandatory Access Control). Etiquetas como Top Secret y Confidential son ejemplos de MAC. MAC se diferencia de DAC, que significa control de acceso discrecional (del inglés Discretionary Access Control). Los permisos UNIX son un ejemplo de DAC.

3. En hardware, la dirección única del sistema en una LAN. Si el sistema está en una Ethernet, la dirección MAC es la dirección Ethernet.

MD5 Una función de hash criptográfica iterativa utilizada para autenticar mensajes, incluso las firmas digitales. Rivest desarrolló esta función en 1991. Su uso está descartado.

mecanismo 1. Un paquete de software que especifica técnicas criptográficas para lograr la autenticación o confidencialidad de los datos. Ejemplos: clave pública Diffie-Hellman, Kerberos V5.

2. En la función de estructura criptográfica de Oracle Solaris, la implementación de un algoritmo para un propósito determinado. Por ejemplo, un mecanismo DES que se aplica a la autenticación, como CKM_DES_MAC, es un mecanismo distinto de un mecanismo DES que se aplica al cifrado, CKM_DES_CBC_PAD.

mecanismo de seguridad Consulte mecanismo.

minimización La instalación del sistema operativo mínimo necesario para ejecutar el servidor. Cualquier software que no se relacione directamente con el funcionamiento del servidor no se instala o se suprime después de la instalación.

modelo de privilegios Un modelo de seguridad más estricto en un sistema informático que el modelo de superusuario. En el modelo de privilegios, los procesos requieren un privilegio para ejecutarse. La administración del sistema se puede dividir en partes discretas que se basan en los privilegios que los administradores tienen en sus procesos. Los privilegios se pueden asignar al proceso de inicio de sesión de un administrador. O bien, los privilegios se pueden asignar para que estén vigentes para determinados comandos solamente.

modelo de superusuario El modelo de seguridad UNIX típico en un sistema informático. En el modelo de superusuario, un administrador tiene todo el control del sistema o ningún control (todo o nada). Generalmente, para administrar el equipo, un usuario se convierte en superusuario (`root`) y puede llevar a cabo todas las actividades administrativas.

motor de análisis Una aplicación de terceros, que reside en un host externo, que examina un archivo para ver si contiene virus conocidos.

nombre de principal

1. El nombre de un principal, con el formato *nombre primario/instancia@DOMINIO*. Consulte también, instancia, nombre primario, dominio.

2. (RPCSEC_GSS API) Consulte principal de cliente, principal de servidor.

nombre primario

La primera parte de un nombre de principal. Consulte también instancia, nombre de principal, dominio.

NTP

Siglas en inglés de Network Time Protocol, protocolo de hora de red. Software de la Universidad de Delaware que permite gestionar la sincronización precisa del tiempo o del reloj de la red, o de ambos, en un entorno de red. Puede usar NTP para mantener el desfase de reloj en un entorno de Kerberos. Consulte también desfase de reloj.

nueva autenticación

El requisito de proporcionar una contraseña para realizar una operación informática. Normalmente, las operaciones `sudo` requieren una nueva autenticación. Los perfiles de derechos autenticados pueden contener comandos que requieren una nueva autenticación. Consulte perfil de derechos autenticado.

objeto público

Un archivo que es propiedad del usuario `root` y que todos pueden leer, como cualquier archivo en el directorio `/etc`.

PAM

Siglas en inglés de Pluggable Authentication Module, módulo de autenticación conectable. Una estructura que permite que se utilicen varios mecanismos de autenticación sin que sea necesario recompilar los servicios que los utilizan. PAM permite inicializar la sesión de Kerberos en el momento del inicio de sesión.

perfil de derechos

Se conoce también como perfil. Una recopilación de sustituciones de seguridad que se puede asignar a un rol o a un usuario. Un perfil de derechos puede incluir autorizaciones, privilegios, comandos con atributos de seguridad y otros perfiles de derechos que se denominan perfiles complementarios.

perfil de derechos autenticado

Un perfil de derechos que requiere que el usuario o rol asignado escriba una contraseña antes de ejecutar una operación en el perfil. Este comportamiento es similar al comportamiento de `sudo`. El período de tiempo durante el cual la contraseña es válida es configurable.

pista de auditoría

La recopilación de todos los archivos de auditoría de todos los hosts.

política

Generalmente, un plan o curso de acción que influye sobre decisiones y acciones, o las determina. Para los sistemas informáticos, la política suele hacer referencia a la política de seguridad. La política de seguridad de su sitio es el conjunto de reglas que definen la confidencialidad de la información que se está procesando y las medidas que se utilizan para proteger la información contra el acceso no autorizado. Por ejemplo, la política de seguridad puede requerir que se auditen los sistemas, que los dispositivos se asignen para su uso y que las contraseñas se cambien cada seis semanas.

Para la implementación de la política en áreas específicas de Sistema operativo Oracle Solaris, consulte política de auditoría, política en la estructura criptográfica, política de dispositivos, política de Kerberos, política de contraseñas y política de derechos.

política de auditoría La configuración global y por usuario que determina qué eventos de auditoría se registran. La configuración global que se aplica al servicio de auditoría, generalmente, afecta qué información opcional se incluye en la pista de auditoría. Dos valores, `cnt` y `ahlt`, afectan al funcionamiento del sistema cuando se completa la cola de auditoría. Por ejemplo, es posible que la política de auditoría requiera que un número de secuencia forme parte de cada registro de auditoría.

política de contraseñas Los algoritmos de cifrado que se pueden utilizar para generar contraseñas. También puede referirse a cuestiones más generales sobre las contraseñas, como la frecuencia con la que deben cambiarse las contraseñas, cuántos intentos de escribir la contraseña se permiten y otras consideraciones de seguridad. La política de seguridad requiere contraseñas. La política de contraseñas requiere que las contraseñas se cifren con el algoritmo AES y puede exigir requisitos adicionales relacionados con la seguridad de las contraseñas.

política de derechos La política de seguridad que está asociada a un comando. Actualmente,`solaris` es la política válida para Oracle Solaris. La política `solaris` reconoce privilegios y una política de privilegio extendida, autorizaciones y atributos de seguridad `setuid`.

política de dispositivos Protección de dispositivos en el nivel de núcleo. La política de dispositivos se implementa como dos conjuntos de privilegios en un dispositivo. Un conjunto de privilegios controla el acceso de lectura al dispositivo. El segundo conjunto de privilegios controla el acceso de escritura al dispositivo. Consulte también política.

política de Kerberos Un conjunto de reglas que rige el uso de contraseñas en el servicio Kerberos. Las políticas pueden regular los accesos de los principales, o los parámetros de tickets, como la duración.

política de seguridad Consulte política.

política en la estructura criptográfica En la función de estructura criptográfica de Oracle Solaris, la política es la desactivación de mecanismos criptográficos existentes. Después de esto, los mecanismos no se pueden utilizar. La política en la estructura criptográfica puede impedir el uso de un mecanismo determinado, como `CKM_DES_CBC`, de un proveedor, como DES.

política para tecnologías de clave pública En la estructura de gestión de claves (KMF), la política es la gestión del uso de certificados. La base de datos de políticas KMF puede limitar el uso de las claves y los certificados administrados por la biblioteca KMF.

política RBAC Consulte política de derechos.

políticas de red Los valores configurados por las utilidades de red para proteger el tráfico de red. Para obtener información sobre la seguridad de la red, consulte “Protección de la red en Oracle Solaris 11.2 ”.

principal 1. Un cliente o usuario con un nombre único o una instancia de servidor o servicio que participa en una comunicación de red. Las transacciones de Kerberos implican interacciones

entre principales (principales de servicio y principales de usuario) o entre principales y KDC. En otras palabras, un principal es una entidad única a la que Kerberos puede asignar tickets. Consulte también nombre de principal, principal de servicio, principal de usuario.

2. (RPCSEC_GSS API) Consulte principal de cliente, principal de servidor.

principal admin Un principal de usuario con un nombre del tipo *nombre de usuario*`/admin` (como en `jdoe/admin`). Un principal admin puede tener más privilegios (por ejemplo, para modificar las políticas) que un principal de usuario común. Consulte también nombre de principal, principal de usuario.

principal de cliente (RPCSEC_GSS API) Un cliente (un usuario o una aplicación) que utiliza los servicios de red RPCSEC_GSS seguros. Los nombres de principales de cliente se almacenan con el formato `rpc_gss_principal_t`.

principal de host Una instancia determinada de un principal de servicio en la que el principal (indicado por el nombre principal `host`) está configurado para proporcionar un rango de servicios de red, como `ftp`, `rcp` o `rlogin`. Un ejemplo de un principal de host principal es `host/central.example.com@EXAMPLE.COM`. Consulte también principal de servidor.

principal de servicio Un principal que proporciona autenticación Kerberos para un servicio o servicios. Para los principales de servicio, el nombre de principal es el nombre de un servicio, como `ftp` y su instancia es el nombre de host completo del sistema que proporciona el servicio. Consulte también principal de host, principal de usuario.

principal de servidor (RPCSEC_GSS API) Un principal que proporciona un servicio. El principal de servidor se almacena como una cadena ASCII con el formato *servicio*`@`*host*. Consulte también principal de cliente.

principal de usuario Un principal atribuido a un usuario determinado. El nombre primario de un principal de usuario es un nombre de usuario y su instancia opcional es un nombre que se utiliza para describir el uso que se pretende hacer de las credenciales correspondientes (por ejemplo, `jdoe` o `jdoe/admin`). También se conoce como instancia de usuario. Consulte también principal de servicio.

principio de privilegio mínimo Consulte privilegio mínimo.

privacidad Un servicio de seguridad en el que los datos transmitidos se cifran antes de enviarse. La privacidad también incluye la integridad de los datos y la autenticación de usuario. Consulte también autenticación, integridad y servicio.

privilegio 1. En general, un poder o una capacidad para realizar una operación en un sistema informático que supera el poder de un usuario común. Los privilegios de superusuario son todos los derechos que se otorgan al superusuario. Una aplicación con privilegios o un usuario con privilegios o es una aplicación o un usuario al que se han concedido derechos adicionales.

2. Un derecho discreto en un proceso de un sistema Oracle Solaris. Los privilegios ofrecen un control más específico de los procesos que `root`. Los privilegios se definen y se aplican en el núcleo. A los privilegios también se los denomina *privilegios de proceso* o *privilegios de núcleo*. Para obtener una descripción completa de los privilegios, consulte la página del comando man `privileges`(5).

privilegio mínimo Un modelo de seguridad que ofrece a un proceso especificado sólo un subconjunto de poderes de superusuario. El modelo de privilegios básico asigna suficientes privilegios a los usuarios comunes para que puedan realizar tareas administrativas personales, como montar sistemas de archivos o cambiar la propiedad de los archivos. Por otro lado, los procesos se ejecutan sólo con esos privilegios, que son necesarios para completar la tarea, en lugar de con toda la capacidad de superusuario, es decir, todos los privilegios. Los daños debidos a errores de programación como desbordamiento de la memoria intermedia se pueden contener para un usuario que no es root, que no tiene acceso a capacidades críticas como la lectura o escritura en archivos de sistema protegidos o la detención del equipo.

protocolo de Diffie-Hellman También se lo denomina "criptografía de claves públicas". Se trata de un protocolo de claves criptográficas asimétricas que desarrollaron Diffie y Hellman en 1976. Este protocolo permite a dos usuarios intercambiar una clave secreta mediante un medio no seguro, sin ningún otro secreto. Kerberos utiliza el protocolo Diffie-Hellman.

proveedor En la función de estructura criptográfica de Oracle Solaris, un servicio criptográfico proporcionado a los consumidores. Las bibliotecas PKCS #11, los módulos criptográficos y los aceleradores de hardware son ejemplos de proveedores. Los proveedores se conectan a la estructura criptográfica y también se conocen como *complementos*. Para ver ejemplos de consumidores, consulte consumidor.

proveedor de hardware En la función de estructura criptográfica de Oracle Solaris, un controlador del dispositivo y su acelerador de hardware. Los proveedores de hardware descargan operaciones criptográficas costosas del sistema informático y, de esa manera, liberan los recursos de la CPU para otros usos. Consulte también proveedor.

proveedor de software En la función de estructura criptográfica de Oracle Solaris, un módulo de software de núcleo o una biblioteca PKCS #11 que proporciona servicios criptográficos. Consulte también proveedor.

QOP Siglas en inglés de Quality of Protection, calidad de protección. Un parámetro que se utiliza para seleccionar los algoritmos criptográficos que se utilizan junto con el servicio de integridad o de privacidad.

RBAC Control de acceso basado en roles, la función de gestión de derechos de usuario de Oracle Solaris. Consulte derechos.

reconocimiento de privilegios Programas, secuencias de comandos y comandos que activan y desactivan el uso de privilegios en su código. En un entorno de producción, los privilegios que estén activados deben proporcionarse al proceso, por ejemplo, solicitando a los usuarios del programa que utilicen

un perfil de derechos que agrega los privilegios al programa. Para obtener una descripción completa de los privilegios, consulte la página del comando man `privileges`(5).

red privada virtual (VPN) Una red que proporciona comunicaciones seguras al utilizar el cifrado y el establecimiento de túneles para conectar usuarios a través de una red pública.

relación Una variable de configuración o un vínculo definidos en los archivos `kdc.conf` o `krb5.conf`.

resumen Consulte resumen de mensaje.

resumen de mensaje Un resumen de mensaje es un valor hash que se calcula a partir de un mensaje. El valor hash identifica el mensaje casi de manera exclusiva. Un resumen es útil para verificar la integridad de un archivo.

rol Una identidad especial para ejecutar aplicaciones con privilegios que sólo los usuarios asignados pueden asumir.

RSA Método para la obtención de firmas digitales y criptosistemas de claves públicas. Dicho método lo describieron sus creadores, Rivest, Shamir y Adleman, en 1978.

SEAM El nombre de producto para la primera versión de Kerberos en los sistemas Solaris. Este producto se basa en la tecnología Kerberos V5 desarrollada en Massachusetts Institute of Technology. SEAM ahora se denomina servicio Kerberos. Continúa siendo levemente diferente a la versión del MIT.

Secure Shell Un protocolo especial para el inicio de sesión remoto seguro y otros servicios de red seguros a través de una red no segura.

separación de tareas Parte de la noción de privilegio mínimo. La separación de tareas impide que un usuario realice o apruebe todas las operaciones que permiten completar una transacción. Por ejemplo, en RBAC, puede separar la creación de un usuario de inicio de sesión de la asignación de sustituciones de seguridad. Un rol crea el usuario. Un rol individual puede asignar atributos de seguridad, como perfiles de derechos, roles y privilegios a los usuarios existentes.

servicio 1. Un recurso proporcionado a clientes de la red, a menudo, por más de un servidor. Por ejemplo, si ejecuta `rlogin` en el equipo `central.example.com`, ese equipo es el servidor que proporciona el servicio `rlogin`.

2. Un servicio de seguridad (ya sea de integridad o privacidad) que proporciona un nivel de protección más allá de la autenticación. Consulte también integridad y privacidad.

servicio de seguridad Consulte servicio.

servidor Un principal que proporciona un recurso a los clientes de la red. Por ejemplo, si ejecuta `ssh` en el sistema `central.example.com`, ese sistema es el servidor que proporciona el servicio `ssh`. Consulte también principal de servicio.

servidor de aplicaciones Consulte servidor de aplicaciones de red.

servidor de aplicaciones de red Un servidor que proporciona aplicaciones de red, como `ftp`. Un dominio puede contener varios servidores de aplicaciones de red.

sesgo de reloj La cantidad máxima de tiempo que pueden diferir los relojes del sistema interno de todos los hosts que participan en el sistema de autenticación Kerberos. Si el sesgo de reloj se excede entre cualquiera de los hosts participantes, las solicitudes se rechazan. El desfase de reloj se puede especificar en el archivo `krb5.conf`.

SHA1 Algoritmo de hash seguro. El algoritmo funciona en cualquier tamaño de entrada que sea inferior a 2^{64} para generar una síntesis del mensaje. El algoritmo SHA-1 es la entrada de DSA.

shell de perfil En la gestión de derechos, un shell que permite que un rol (o un usuario) ejecute desde la línea de comandos cualquier aplicación con privilegios asignada a los perfiles de derechos del rol. Las versiones del shell de perfil corresponden a los shells disponibles en el sistema, como la versión `pfbash` de `bash`.

TGS Siglas en inglés de Ticket-Granting Service, servicio de otorgamiento de tickets. La parte del KDC que es responsable de emitir tickets.

TGT Siglas en inglés de Ticket-Granting Ticket, Ticket de otorgamiento de tickets. Un ticket emitido por el KDC que permite que un cliente solicite tickets para otros servicios.

ticket Un paquete de información que se utiliza para transmitir de manera segura la identidad de un usuario a un servidor o servicio. Un ticket es válido únicamente para un solo cliente y un servicio determinado en un servidor específico. Un ticket contiene el nombre de principal del servicio, el nombre de principal del usuario, la dirección IP del host del usuario, una indicación de hora y un valor que define la duración del ticket. Un ticket se crea con una clave de sesión aleatoria que utilizará el cliente y el servicio. Una vez que se ha creado un ticket, se puede volver a utilizar hasta que caduque. Un ticket sólo sirve para autenticar un cliente cuando se presenta junto con un autenticador nuevo. Consulte también autenticador, credencial, servicio y clave de sesión.

ticket de sustituto Un ticket que puede utilizar un servicio en nombre de un cliente para realizar una operación para el cliente. Por lo tanto, se dice que el servicio actúa como sustituto del cliente. Con el ticket, el servicio puede asumir la identidad del cliente. El servicio puede utilizar un ticket de sustituto para obtener un ticket de servicio para otro servicio, pero no puede obtener un ticket de otorgamiento de tickets. La diferencia entre un ticket de sustituto y un ticket reenviable es que un ticket de sustituto únicamente es válido para una sola operación. Consulte también ticket reenviable.

ticket inicial Un ticket que se emite directamente (es decir, que no se basa en un ticket de otorgamiento de tickets existente). Algunos servicios, como las aplicaciones que cambian las contraseñas, posiblemente requieran que los tickets se marquen como `iniciales` para garantizar que el cliente pueda demostrar que conoce su clave secreta. Esta garantía es importante porque un

ticket inicial indica que el cliente se ha autenticado recientemente (en lugar de basarse en un ticket de otorgamiento de tickets, que posiblemente haya existido durante mucho tiempo).

ticket no válido Un ticket posfechado que todavía no puede utilizarse. Un servidor de aplicaciones rechaza un ticket no válido hasta que se valide. Para validar un ticket no válido, el cliente debe presentarlo al KDC en una solicitud TGS, con el indicador `VALIDATE` definido, después de que haya pasado la hora de inicio. Consulte también ticket posfechado.

ticket posfechado Un ticket posfechado no es válido hasta que transcurra un tiempo especificado tras su creación. Un ticket de este tipo es útil, por ejemplo, para los trabajos por lotes que deben ejecutarse tarde por la noche, ya que si el ticket es robado, no se puede utilizar hasta que se ejecute el trabajo por lotes. Los tickets posfechados se emiten como `no válidos` y siguen teniendo ese estado hasta que: a) haya pasado su hora de inicio, y b) el cliente solicite la validación por parte del KDC. Generalmente, un ticket posfechado es válido hasta la hora de vencimiento del ticket de otorgamiento de tickets. Sin embargo, si el ticket posfechado se marca como `renovable`, su duración suele definirse para que coincida con la duración total del ticket de otorgamiento de tickets. Consulte también, ticket no válido, ticket renovable.

ticket reenviable Un ticket que un cliente puede utilizar para solicitar un ticket en un host remoto sin que sea necesario que el cliente complete todo el proceso de autenticación en ese host. Por ejemplo, si el usuario `david` obtiene un ticket reenviable mientras está en el equipo de `jennifer`, `david` puede iniciar sesión en su propio equipo sin tener que obtener un ticket nuevo (y, por lo tanto, autenticarse nuevamente). Consulte también ticket de sustituto.

ticket renovable Debido a que los tickets con duraciones muy largas constituyen un riesgo de seguridad, los tickets se pueden designar como `renovables`. Un ticket renovable tiene dos horas de vencimiento: a) la hora de vencimiento de la instancia actual del ticket, y b) la duración máxima de cualquier ticket. Si un cliente desea seguir utilizando un ticket, debe renovarlo antes del primer vencimiento. Por ejemplo, un ticket puede ser válido por una hora, pero todos los tickets tienen una duración máxima de 10 h. Si el cliente que tiene el ticket desea conservarlo durante más de una hora, debe renovarlo. Cuando un ticket alcanza la duración máxima, vence automáticamente y no se puede renovar.

tipo Históricamente, *tipo de seguridad* y *tipo de autenticación* tenían el mismo significado; ambos indicaban el tipo de autenticación (AUTH_UNIX, AUTH_DES, AUTH_KERB). RPCSEC_GSS también es un tipo de seguridad, aunque proporciona servicios de privacidad e integridad, además de autenticación.

tipo de seguridad Consulte tipo.

usuario con privilegios Un usuario a quien se le asignan derechos que se encuentran más allá de los derechos de un usuario común en un sistema informático. Consulte también usuarios de confianza.

usuarios de confianza Los usuarios que se ha decidido que pueden realizar tareas administrativas con cierto nivel de confianza. Normalmente, los administradores crean inicios de sesión para usuarios de confianza y asignan derechos administrativos que coinciden con el nivel de confianza y la capacidad de

los usuarios. Estos usuarios luego pueden ayudar a configurar y a mantener el sistema. También son denominados *usuarios con privilegios*.

Índice

B

C

D

E

F

G

H

I

L

M

N

O

R

S

T

U

V

Z