Protección de sistemas y dispositivos conectados en Oracle® Solaris 11.2

Referencia: E53943-02
Septiembre de 2014

Contenido

Uso de esta documentación

Protección de sistemas y dispositivos conectados en Oracle® Solaris 11.2 explica cómo proteger y supervisar su sistema Oracle Solaris de acceso no autorizado.

- **Descripción general**: describe diferentes métodos de proteger los sistemas y los dispositivos de acceso no autorizado.
- **Destinatarios**: los administradores del sistema responsables de implementar la seguridad en la red corporativa.
- **Conocimiento necesario**: familiaridad con conceptos de seguridad y funciones que se admiten en Oracle Solaris.

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

Gestión de seguridad del equipo

Mantener la información de una máquina segura es una responsabilidad de administración del sistema importante. En este capítulo, se proporciona información general sobre la gestión de seguridad de equipos.

Novedades en protección de sistemas y dispositivos en Oracle Solaris 11.2

Esta sección resalta información importante para clientes existentes sobre nuevas funciones en esta versión que protegen los sistemas y dispositivos de acceso no autorizado.

- La asistencia de verificación de inicio protege los núcleos del sistema operativo. Para obtener más información, consulte "Uso de inicio verificado" [31].
- Asistencia para módulos de plataforma de confianza (TPM). Para obtener más información, consulte "Inicialización de TPM en sistemas Oracle Solaris" [39].

Control de acceso a un sistema informático

En el espacio de trabajo, todos los equipos conectados a un servidor pueden considerarse como un gran sistema multifacético. Usted es responsable de la seguridad de este sistema más grande. Debe proteger la red contra los desconocidos que intentan obtener acceso. También debe garantizar la integridad de los datos en los equipos de la red.

En el nivel de archivos, Oracle Solaris proporciona funciones de seguridad estándar que usted puede utilizar para proteger archivos, directorios y dispositivos. En los niveles de sistema y de

red, los problemas de seguridad son generalmente los mismos. La primera línea de defensa de seguridad es controlar el acceso a su sistema, tal como se describe en las siguientes secciones.

Mantenimiento de la seguridad física

Para controlar el acceso al sistema, debe mantener la seguridad física del entorno informático. Por ejemplo, un sistema cuya sesión está iniciada pero desatendida es vulnerable al acceso no autorizado. Un intruso puede obtener acceso al sistema operativo y a la red. El entorno y el hardware del equipo deben estar físicamente protegidos contra el acceso no autorizado.

Puede proteger un sistema SPARC de acceso no autorizado a la configuración de hardware. Utilice el comando `eeprom` para solicitar una contraseña para acceder a la PROM. Para obtener más información, consulte Cómo requerir una contraseña para el acceso al hardware de SPARC [57]. Para proteger el hardware x86, consulte la documentación del proveedor.

Mantenimiento del control de inicio de sesión

Debe prevenir los inicios de sesión no autorizados en la red mediante la asignación de contraseñas o el control de inicios de sesión. Una contraseña es un mecanismo de autenticación simple. Todas las cuentas de un sistema deben tener una contraseña. Si una cuenta no tiene una contraseña, un intruso que adivina el nombre de un usuario puede acceder a toda la red. Un algoritmo de contraseña complejo protege contra ataques por fuerza bruta.

Cuando un usuario inicia sesión en un sistema, el comando `login` verifica que el servicio de nombres o la base de datos de servicio de directorios sean apropiados según la información en el servicio de cambio de nombres, `svc:/system/name-service/switch`. Para cambiar los valores en una base de datos de servicio de nombres, utilice los comandos SMF. Los servicios de nombres indican la ubicación de las bases de datos que afectan el inicio de sesión:

- `files`: designa los archivos `/etc` en el sistema local
- `ldap`: designa el servicio de directorios LDAP en el servidor LDAP
- `nis`: designa la base de datos NIS en el servidor maestro NIS
- `dns`: designa el servicio de nombre de dominio en la red

Para obtener una descripción del servicio de nombres, consulte la página del comando man `nscd`(1M). Para obtener información sobre servicios de nombres y servicios de directorios, consulte “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: DNS y NIS ” y “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: LDAP ”.

El comando `login` verifica el nombre de usuario y la contraseña proporcionados por el usuario. Si el nombre de usuario no está en la base de datos de contraseñas, el comando `login` niega el acceso al sistema. Si la contraseña no es correcta para el nombre de usuario especificado,

el comando `login` niega el acceso al sistema. Cuando el usuario proporciona un nombre de usuario válido y la contraseña correspondiente, se le otorga acceso al sistema.

Los módulos PAM pueden optimizar el inicio de sesión a las aplicaciones después de iniciar sesión correctamente en el sistema. Para obtener más información, consulte Capítulo 1, “Uso de módulos de autenticación conectables” de “Gestión de Kerberos y otros servicios de autenticación en Oracle Solaris 11.2 ”.

Los sistemas Oracle Solaris disponen de mecanismos de autorización y autenticación sofisticados. Para ver una explicación de los mecanismos de autorización y autenticación en el nivel de red, consulte “Autenticación y autorización para acceso remoto” [26].

Gestión de información de contraseñas

Cuando los usuarios inician sesión en un sistema, deben proporcionar un nombre de usuario y una contraseña. Aunque los nombres de usuario son de conocimiento público, las contraseñas deben mantenerse en secreto. Únicamente cada usuario individual debe conocer su contraseña. Los usuarios deben seleccionar sus contraseñas con cuidado y cambiarlas con frecuencia.

Las contraseñas se crean inicialmente al configurar una cuenta de usuario. Para mantener la seguridad de las cuentas de usuario, puede configurar la caducidad de las contraseñas para forzar a los usuarios a que cambien las contraseñas regularmente. También puede desactivar una cuenta de usuario mediante el bloqueo de la contraseña. Para obtener información detallada sobre la administración de contraseñas, consulte el Capítulo 1, “Acerca de las cuentas de usuario y los entornos de usuario” de “Gestión de las cuentas de usuario y los entornos de usuario en Oracle Solaris 11.2 ” y la página del comando man `passwd`(1).

Contraseñas locales

Si la red utiliza archivos locales para autenticar usuarios, la información de contraseñas se conserva en los archivos `/etc/passwd` y `/etc/shadow` del sistema. Los nombres de usuarios y otra información se conservan en el archivo `/etc/passwd`. Las contraseñas cifradas se conserva en un archivo *shadow* separado, `/etc/shadow`. Esta medida de seguridad impide que un usuario obtenga acceso a las contraseñas cifradas. Mientras que el archivo `/etc/passwd` está disponible para cualquier persona que pueda iniciar sesión en un sistema, únicamente la cuenta `root` puede leer el archivo `/etc/shadow`. Puede utilizar el comando `passwd` para cambiar la contraseña de un usuario en un sistema local.

Contraseñas NIS

Si la red utiliza NIS para autenticar a los usuarios, la información de contraseñas se conserva en el mapa de contraseñas NIS. NIS no admite la caducidad de las contraseñas. Puede utilizar el

comando `passwd -r nis` para cambiar la contraseña de un usuario que está almacenada en un mapa de contraseñas NIS.

Contraseñas LDAP

El servicio de nombres LDAP de Oracle Solaris almacena información de contraseñas e información shadow en el contenedor `ou=people` del árbol de directorios LDAP. En el cliente del servicio de nombres LDAP de Oracle Solaris, puede utilizar el comando `passwd -r ldap` para cambiar la contraseña de un usuario. El servicio de nombres LDAP almacena la contraseña en el repositorio LDAP.

La política de contraseñas se aplica en Oracle Directory Server Enterprise Edition. En concreto, el módulo `pam_ldap` del cliente sigue los controles de políticas de contraseñas que se aplican en Oracle Directory Server Enterprise Edition. Para obtener más información, consulte "Modelo de seguridad de servicios de nombres LDAP" de "Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: LDAP ".

Cifrado de contraseña

El cifrado de contraseña seguro proporciona una barrera temprana contra un ataque. El software Oracle Solaris proporciona seis algoritmos de cifrado de contraseña. Los algoritmos Blowfish y SHA brindan un sólido cifrado de contraseñas.

Nota - Para obtener la aprobación de FIPS 140, use los algoritmos SHA. Para obtener información, consulte "passwd Command as a FIPS 140 Consumer" de "Using a FIPS 140 Enabled System in Oracle Solaris 11.2 ".

Identificadores de algoritmos de contraseña

Puede especificar la configuración de los algoritmos para su sitio en el archivo `/etc/security/policy.conf`. En el archivo `policy.conf` , los algoritmos se denominan según el identificador, como se muestra en la siguiente tabla. Para la asignación identificador-algoritmo, consulte el archivo `/etc/security/crypt.conf`.

Nota - Utilice algoritmos aprobados por FIPS siempre que sea posible. Para obtener una lista de los algoritmos aprobados por FIPS, consulte "FIPS 140 Algorithm Lists and Certificate References for Oracle Solaris Systems" de "Using a FIPS 140 Enabled System in Oracle Solaris 11.2 ".

TABLA 1-1 Algoritmos de cifrado de contraseña

Identificador	Descripción	Página del comando man de algoritmo
`1`	El algoritmo MD5 que es compatible con algoritmos MD5 en los sistemas BSD y Linux.	`crypt_bsdmd5`(5)
`2a`	El algoritmo Blowfish que es compatible con el algoritmo Blowfish en los sistemas BSD. **Nota -** Para promover la seguridad de FIPS 140, elimine el algoritmo Blowfish (2a) de la entrada `CRYPT_ALGORITHMS_ALLOW=2a,5,6` en el archivo `/etc/security/policy.conf`.	`crypt_bsdbf`(5)
`md5`	El algoritmo MD5 de Sun, que se considera más fuerte que la versión de MD5 de BSD y Linux.	`crypt_sunmd5`(5)
`5`	El algoritmo SHA256. SHA es la sigla en inglés correspondiente al algoritmo de hash seguro. Este algoritmo es un miembro de la familia SHA-2. SHA256 admite contraseñas de 255 caracteres. Este algoritmo es el predeterminado, `(CRYPT_DEFAULT)`.	`crypt_sha256`(5)
`6`	El algoritmo SHA512.	`crypt_sha512`(5)
`__unix__`	Obsoleto. El algoritmo de cifrado tradicional de UNIX. Este algoritmo puede ser útil cuando se conecte a sistemas antiguos.	`crypt_unix`(5)

Nota - El algoritmo que se utiliza para una contraseña inicial del usuario se sigue utilizando para la generación de la nueva contraseña para dicho usuario, aunque se haya seleccionado un algoritmo predeterminado diferente antes de generar una nueva contraseña para ese usuario. Este mecanismo se aplica en las siguientes condiciones:

- El algoritmo se incluye en la lista de algoritmos permitidos que se utilizará para el cifrado de contraseñas.
- El identificador no es `_unix_`.

Para conocer los procedimientos que describen cómo cambiar algoritmos para cifrado de contraseña, consulte “Cambio de algoritmo predeterminado para cifrado de contraseña” [51].

Configuración de algoritmos en el archivo `policy.conf`

La configuración predeterminada de los algoritmos en el archivo `policy.conf` es la siguiente:

```
#
…
# crypt(3c) Algorithms Configuration
#
```

```
# CRYPT_ALGORITHMS_ALLOW specifies the algorithms that are allowed
to
# be used for new passwords.  This is enforced only in crypt_gensalt(3c).
#
CRYPT_ALGORITHMS_ALLOW=1,2a,md5,5,6

# To deprecate use of the traditional unix algorithm, uncomment below
# and change CRYPT_DEFAULT= to another algorithm.  For example,
# CRYPT_DEFAULT=1 for BSD/Linux MD5.
#
#CRYPT_ALGORITHMS_DEPRECATE=__unix__

# The Oracle Solaris default is a SHA256 based algorithm.  To revert to
# the policy present in Solaris releases set CRYPT_DEFAULT=__unix__,
# which is not listed in crypt.conf(4) since it is internal to libc.
#
CRYPT_DEFAULT=5
…
```

Al cambiar el valor para `CRYPT_DEFAULT`, las contraseñas de los usuarios nuevos se cifran con el algoritmo que está asociado al valor nuevo.

Cuando los usuarios existentes cambian sus contraseñas, la manera en que se cifró la contraseña anterior afecta el algoritmo que se utiliza para cifrar la contraseña nueva. Por ejemplo, supongamos lo siguiente: `CRYPT_ALGORITHMS_ALLOW=1,2a,md5,5,6` y `CRYPT_DEFAULT=6`. La siguiente tabla muestra qué algoritmo se utilizaría para generar la contraseña cifrada. La contraseña consiste de identificador = algoritmo.

Contraseña inicial	Contraseña cambiada	Explicación
`1` = `crypt_bsdmd5`	Utiliza el mismo algoritmo	El identificador `1` está en la lista `CRYPT_ALGORITHMS_ALLOW`. La contraseña del usuario se seguirá cifrando con el algoritmo `crypt_bsdmd5`.
`2a` = `crypt_bsdbf`	Utiliza el mismo algoritmo	El identificador `2a` está en la lista `CRYPT_ALGORITHMS_ALLOW`. Por lo tanto, la contraseña nueva se cifra con el algoritmo `crypt_bsbdf`.
`md5` = `crypt_md5`	Utiliza el mismo algoritmo	El identificador `md5` está en la lista `CRYPT_ALGORITHMS_ALLOW`. Por lo tanto, la contraseña nueva se cifra con el algoritmo `crypt_md5`.
`5` = `crypt_sha256`	Utiliza el mismo algoritmo	El identificador `5` está en la lista `CRYPT_ALGORITHMS_ALLOW`. Por lo tanto, la contraseña nueva se seguirá cifrando con el algoritmo `crypt_sha256`.
`6` = `crypt_sha512`	Utiliza el mismo algoritmo	El identificador `6` es el valor de `CRYPT_DEFAULT`. Por lo tanto, la contraseña nueva se seguirá cifrando con el algoritmo `crypt_sha512`.
`__unix__` = `crypt_unix`	Utiliza el algoritmo `crypt_sha512`	El identificador `__unix__` no está en la lista `CRYPT_ALGORITHMS_ALLOW`. Por lo tanto, el algoritmo `crypt_unix` no se puede utilizar. La contraseña nueva se cifra con el algoritmo `CRYPT_DEFAULT`.

Para obtener más información sobre la configuración de opciones de algoritmos, consulte la página del comando man `policy.conf(4)`. Para especificar algoritmos de

cifrado de contraseña, consulte “Cambio de algoritmo predeterminado para cifrado de contraseña” [51].

Cuentas especiales del sistema

La cuenta `root` es una de las diversas cuentas del *sistema* especiales. De estas cuentas, sólo a la cuenta `root` se le asigna una contraseña y se la puede utilizar para iniciar sesión. Con la cuenta `nuucp`, se puede iniciar sesión para realizar transferencias de archivos. Las otras cuentas del sistema sirven para proteger archivos o ejecutar procesos administrativos sin utilizar el poder total de `root`.

Atención - Nunca cambie la configuración de contraseña de una cuenta del sistema. Las cuentas del sistema de Oracle Solaris se entregan en un estado seguro y protegido. No revise ni cree archivos del sistema con un UID que sea 101 o menor que ese valor.

En la siguiente tabla, se muestran algunas cuentas del sistema junto con sus usos. Las cuentas del sistema realizan funciones especiales. Cada cuenta de esta lista tiene un UID que es menor que 100. Para obtener una lista completa de los archivos del sistema, utilice el comando `logins -s`.

TABLA 1-2 Cuentas del sistema seleccionado y sus usos

Cuenta del sistema	UID	Uso
`root`	`0`	Prácticamente no tiene restricciones. Puede sustituir otros permisos y protecciones. La cuenta `root` tiene acceso a todo el sistema. La contraseña para la cuenta `root` debe estar protegida muy cuidadosamente. La cuenta `root` posee la mayoría de los comandos de Oracle Solaris.
`daemon`	`1`	Controla el procesamiento en segundo plano.
`bin`	`2`	Posee algunos de los comandos Oracle Solaris.
`sys`	`3`	Posee muchos archivos del sistema.
`adm`	`4`	Posee algunos archivos administrativos.
`lp`	`71`	Posee los archivos de datos del objeto y los archivos de datos de cola de impresión para la impresora.
`uucp`	`5`	Posee los archivos de datos del objeto y los archivos de datos de cola de impresión para UUCP, el programa de copia de UNIX a UNIX.
`nuucp`	`9`	Utilizada por los sistemas remotos para iniciar sesión en el sistema e iniciar transferencias de archivos.

Inicios de sesión remotos

Los inicios de sesión remotos ofrecen una vía tentadora para los intrusos. Oracle Solaris proporciona varios comandos para supervisar, limitar y desactivar los inicios de sesión remotos.

Para conocer los procedimientos, consulte la Tabla 3-1, “Protección de inicios de sesión y contraseñas (mapa de tareas)”.

De manera predeterminada, con los inicios de sesión remotos, no se pueden controlar ni leer determinados dispositivos del sistema, como el mouse, el teclado, el búfer de trama o el dispositivo de audio. Para obtener más información, consulte la página del comando man `logindevperm(4)`.

Control de acceso a dispositivos

Los dispositivos periféricos conectados a un sistema informático presentan un riesgo de seguridad. Los micrófonos pueden captar conversaciones y transmitirlas a sistemas remotos. Los CD-ROM pueden dejar evidencia de información que el siguiente usuario del dispositivo de CD-ROM podrá leer. Se puede acceder a las impresoras de forma remota. Dispositivos que son una parte integral del sistema, por ejemplo, las interfaces de red, como `bge0`, también pueden presentar problemas de seguridad.

El software Oracle Solaris proporciona varios métodos de control de acceso a los dispositivos.

- **Configurar política de dispositivos:** puede requerir que el proceso que accede a un dispositivo determinado se ejecute con un conjunto de privilegios. Los procesos sin estos privilegios no pueden utilizar el dispositivo. En el momento del inicio, el software Oracle Solaris configura la política de dispositivos. Los controladores de terceros se pueden configurar con la política de dispositivos durante la instalación. Después de la instalación, usted, como administrador, puede agregar la política de dispositivos a un dispositivo.
- **Permitir la asignación de dispositivos:** puede requerir que un usuario deba asignar un dispositivo antes del uso. La asignación restringe el uso de un dispositivo a un usuario a la vez. Además, puede exigir que el usuario esté autorizado para utilizar el dispositivo.
- **Impedir que se utilicen los dispositivos:** puede impedir que cualquier usuario de un sistema informático utilice un dispositivo, como un micrófono. Por ejemplo, un quiosco informático puede ser una buena opción para evitar que se utilicen determinados dispositivos.
- **Restringir un dispositivo a una zona determinada:** puede asignar el uso de un dispositivo a una zona no global. Para obtener más información, consulte “Uso de dispositivos en zonas no globales” de “Creación y uso de zonas de Oracle Solaris ”. Para obtener una explicación general de dispositivos y zonas, consulte “Sistema de archivos /dev en zonas no globales” de “Introducción a Zonas de Oracle Solaris ”.

Política de dispositivos

El mecanismo de política de dispositivos permite especificar que los procesos que abran un dispositivo requieren determinados privilegios. Únicamente los procesos que se ejecutan con los

privilegios especificados por la política de dispositivos pueden acceder a los dispositivos que están protegidos mediante la política de dispositivos. Oracle Solaris proporciona la política de dispositivos predeterminada. Por ejemplo, las interfaces de red, como `bge0`, requieren que los procesos que acceden a la interfaz se ejecuten con el privilegio `net_rawaccess`. El requisito se aplica en el núcleo. 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 ”.

En Oracle Solaris, los dispositivos están protegidos mediante permisos de archivo *y* la política de dispositivos. Por ejemplo, el archivo `/dev/ip` tiene `666`. Sin embargo, únicamente un proceso con los privilegios adecuados puede abrir el dispositivo.

La configuración de la política de dispositivos se puede auditar. El evento de auditoría `AUE_MODDEVPLCY` registra los cambios en la política de dispositivos.

Para obtener más información sobre la política de dispositivos, consulte lo siguiente:

- Tabla 4-1, “Configuración de política de dispositivos (mapa de tareas)”
- “Comandos de la política de dispositivos” [71]
- “Privilegios y dispositivos” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”

Asignación de dispositivos

El mecanismo de asignación de dispositivos permite restringir el acceso a un dispositivo periférico, como un CD-ROM. Si la asignación de dispositivos no está activada, los dispositivos periféricos se protegen únicamente mediante permisos de archivo. Por ejemplo, de manera predeterminada, los dispositivos periféricos están disponibles para los siguientes usos:

- Cualquier usuario puede leer y escribir en un disco o CD-ROM.
- Cualquier usuario puede conectar un micrófono.
- Cualquier usuario puede acceder a una impresora conectada.

La asignación de dispositivos puede restringir un dispositivo a usuarios autorizados. La asignación de dispositivos también puede impedir que se acceda a un dispositivo en todo momento. Un usuario que asigna un dispositivo tiene el uso exclusivo de ese dispositivo hasta que lo desasigne. Cuando se desasigna un dispositivo, las secuencias de comandos device-clean borran los datos restantes. Puede escribir una secuencia de comandos device-clean para depurar la información de los dispositivos que no tienen una secuencia de comandos. Para ver un ejemplo, consulte “Redacción de secuencias nuevas de comandos device-clean” [78].

Se pueden auditar los intentos de asignación de un dispositivo, desasignación de un dispositivo y enumeración de los dispositivos asignables. Los eventos de auditoría forman parte de la clase de auditoría `other`.

Para obtener más información sobre la asignación de dispositivos, consulte lo siguiente:

- Tabla 4-2, “Gestión de asignación de dispositivos (mapa de tareas)”
- “Asignación de dispositivos” [71]
- “Comandos de asignación de dispositivos” [73]

Control de acceso a recursos del equipo

Algunos recursos del sistema están protegidos de manera predeterminada. Además, como administrador del sistema, puede controlar y supervisar la actividad del sistema. Puede definir límites sobre quién puede utilizar determinados recursos. Puede registrar el uso de recursos y supervisar quién los está utilizando. También puede configurar los sistemas para minimizar el uso indebido de los recursos.

Ejecución aleatoria de la disposición del espacio de direcciones

Oracle Solaris etiqueta muchos de sus datos binarios de espacio de usuarios para activar la ejecución aleatoria de la disposición del espacio de direcciones (ASLR). ASLR ejecuta aleatoriamente la dirección de inicio de partes clave de un espacio de direcciones. Este mecanismo de defensa de seguridad puede hacer que los ataques de la programación orientada al retorno (ROP) fallen cuando traten de explotar las vulnerabilidades de software.

Las zonas heredan esta disposición de ejecución aleatoria para sus procesos. Como el uso de ASLR puede no ser óptimo para todos los datos binarios, el uso de ASLR se puede configurar en el nivel de zona y en el nivel binario.

Las tres configuraciones de ASLR son:

- **Desactivado:** ASLR está desactivado para todos los datos binarios.
- **Datos binarios etiquetados:** ASLR está controlado por la etiqueta codificada en los datos binarios.

  El valor de Oracle Solaris predeterminado para ASLR es `tagged-binaries`. Muchos datos binarios en la versión de Oracle Solaris están etiquetados para usar ASLR.
- **Activado:** ASLR está activado para todos los datos binarios, excepto aquellos explícitamente etiquetados para desactivarlos.

El comando `sxadm` se utiliza para configurar ASLR. Para ejecutar este comando, debe asumir el rol `root`. Para obtener más información y ejemplos, consulte la página del comando man `sxadm`(1M). Para obtener información adicional, consulte la “Developer’s Guide to Oracle Solaris 11 Security ”.

Limitación y supervisión del acceso del superusuario

El sistema requiere una contraseña `root` para el acceso del superusuario. En la configuración predeterminada, un usuario no puede iniciar sesión de manera remota en un sistema como `root`. Al iniciar sesión de manera remota, el usuario debe utilizar el nombre de usuario y, luego, el comando `su` para convertirse en `root`. Puede supervisar quién ha utilizado el comando `su`, en especial, aquellos usuarios que están intentando obtener acceso de superusuario. Para conocer los procedimientos para supervisar al superusuario y limitar el acceso al superusuario, consulte “Supervisión y restricción del acceso `root`” [54].

Configuración del control de acceso basado en roles para reemplazar al superusuario

El control de acceso basado en roles (RBAC), una función de Oracle Solaris, está diseñado para distribuir las capacidades de superusuario a roles administrativos. El superusuario (usuario `root`) tiene acceso a todos los recursos del sistema. Con RBAC, puede reemplazar muchas de las responsabilidades de `root` con un conjunto de roles con funciones discretas. Por ejemplo, puede configurar un rol para manejar la creación de cuentas de usuario y otro rol para manejar la modificación de archivos del sistema. Aunque puede que no modifique la cuenta `root`, puede dejar la cuenta como un rol y, entonces, no asignar el rol. Esta estrategia de forma eficaz elimina el acceso a la `root` del sistema.

Cada rol requiere que un usuario conocido inicie sesión con su nombre de usuario y contraseña. Después de iniciar sesión, el usuario asume el rol con una contraseña de rol específica.
Para obtener más información sobre RBAC, consulte “Gestión de derechos de usuario” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

Prevención del uso indebido involuntario de los recursos del sistema

Puede prevenir que los usuarios y que usted realicen errores involuntarios de las siguientes formas:

- Puede evitar ejecutar un caballo de Troya si configura correctamente la variable `PATH`.
- Puede asignar un shell restringido a los usuarios. Un shell restringido previene los errores del usuario al guiar a los usuarios a las partes del sistema que necesitan para su trabajo. De hecho, mediante una configuración cuidadosa, usted puede asegurarse de que los usuarios sólo accedan a las partes del sistema que los ayudan a trabajar de manera eficiente.

- Puede establecer permisos restrictivos para los archivos a los que los usuarios no necesitan acceder.

Configuración de la variable PATH

Debe asegurarse de configurar correctamente la variable PATH. De lo contrario, puede ejecutar accidentalmente un programa introducido por otra persona que crea un riesgo de seguridad. El programa intruso puede dañar los datos o el sistema. Este tipo de programa se conoce como *caballo de Troya*. Por ejemplo, es posible que se coloque un programa su sustituto en un directorio público y que usted, como administrador del sistema, ejecute el programa sustituto. Esa secuencia de comandos sería igual que el comando su habitual. Debido a que la secuencia de comandos se elimina sola después de la ejecución, habría pocas pruebas para mostrar que, en realidad, se ejecutó un caballo de Troya.

La variable PATH se configura automáticamente en el momento del inicio de sesión. La ruta se define mediante los archivos de inicialización, como .bashrc y /etc/profile. Si configura la ruta de búsqueda del usuario para que el directorio actual (.) esté en último lugar, estará protegido contra la ejecución de este tipo de caballo de Troya. La variable PATH para la cuenta root no debe incluir el directorio actual.

Asignación de un shell restringido a los usuarios

El shell estándar permite que un usuario abra archivos, ejecute comandos, etc. El shell restringido limita la capacidad de un usuario para cambiar directorios y para ejecutar comandos. El shell restringido se invoca con el comando /usr/lib/rsh. Tenga en cuenta que el shell restringido no es el shell remoto, que es /usr/sbin/rsh.

El shell restringido se diferencia de un shell estándar de las siguientes formas:

- El acceso de usuario está limitado al directorio principal del usuario, de modo que no puede utilizar el comando cd para cambiar de directorios. Por lo tanto, el usuario no puede examinar los archivos del sistema.
- El usuario no puede cambiar la variable PATH, de manera que puede utilizar comandos sólo en la ruta definida por el administrador del sistema. El usuario tampoco puede ejecutar comandos o secuencias de comandos mediante un nombre completo de ruta.
- El usuario no puede redirigir la salida con > o >>.

El shell restringido permite limitar la capacidad de un usuario para desviarse hacia los archivos del sistema. El shell crea un entorno limitado para un usuario que necesita realizar tareas específicas. Sin embargo, el shell restringido no es completamente seguro y sólo tiene el propósito de impedir que los usuarios sin experiencia causen daños involuntariamente.

Para obtener información acerca del shell restringido, use el comando man -s1m rsh para ver la página del comando man rsh(1M).

Restricción de acceso a datos de archivos

Dado que Oracle Solaris es un entorno multiusuario, la seguridad del sistema de archivos es el riesgo de seguridad más básico de un sistema. Puede utilizar las protecciones de archivos UNIX tradicionales para proteger los archivos. También puede utilizar las listas de control de acceso (ACL) más seguras.

Posiblemente desee permitir que algunos usuarios lean determinados archivos y conceder a otros usuarios permiso para cambiar o suprimir archivos. Es posible que existan datos que no desee que nadie más vea. En el Capítulo 1, “Control de acceso a archivos” de “Protección y verificación de la integridad de archivos en Oracle Solaris 11.2 ” se describe cómo establecer permisos de archivo.

Restricción de archivos ejecutables `setuid`

Los archivos ejecutables pueden constituir riesgos para la seguridad. Algunos programas ejecutables todavía deben ejecutarse como `root` para que funcionen correctamente. Estos programas `setuid` se ejecutan con el ID de usuario establecido en `0`. Cualquier persona que ejecuta estos programas lo hace con el ID `root`. Un programa que se ejecuta con el ID `root` crea un posible problema de seguridad si el programa no se escribió pensando en la seguridad.

Excepto para los ejecutables que Oracle Solaris envía con el bit `setuid` establecido en `root`, debe prohibir el uso de programas `setuid`. Si no puede prohibir el uso de programas `setuid`, debe restringir su uso. Una administración segura requiere pocos programas `setuid`.

Para obtener más información, consulte “Cómo evitar que los archivos ejecutables pongan en riesgo la seguridad” de “Protección y verificación de la integridad de archivos en Oracle Solaris 11.2 ”. Para conocer procedimientos, consulte “Protección contra programas con riesgo de seguridad” de “Protección y verificación de la integridad de archivos en Oracle Solaris 11.2 ”.

Uso de la configuración de seguridad predeterminada

De forma predeterminada, cuando Oracle Solaris está instalado, se desactiva un gran conjunto de servicios de red. Esta configuración se denomina "seguridad predeterminada" (SBD). Con SBD, el único servicio de red que acepta solicitudes de red es el daemon `sshd`. Todos los demás servicios de red están desactivados o solamente manejan solicitudes locales. Puede activar servicios de red individuales, como `ftp`, con la función de utilidad de gestión de servicios (SMF) de Oracle Solaris. Para obtener más información, consulte las páginas del comando man `netservices`(1M) y `smf`(5).

Uso de funciones de gestión de recursos

El software Oracle Solaris ofrece funciones de gestión de recursos. Con estas funciones, usted puede asignar, programar, supervisar y limitar el uso de recursos por parte de aplicaciones en un entorno de consolidación de servidores. La estructura de control de recursos permite establecer restricciones a los recursos del sistema consumidos por los procesos. Estas restricciones ayudan a prevenir ataques de denegación del servicio por parte de una secuencia de comandos que intenta colapsar los recursos del sistema.

Con estas funciones de gestión de recursos, puede designar recursos para proyectos determinados. También puede adaptar dinámicamente los recursos disponibles. Para obtener más información, consulte “Administración de la gestión de recursos en Oracle Solaris 11.2 ”.

Uso de zonas de Oracle Solaris

Las zonas de Oracle Solaris proporcionan un entorno de ejecución de aplicaciones en el que los procesos están aislados del resto del sistema dentro de una única instancia del Sistema operativo Oracle Solaris. Este aislamiento evita que los procesos que se están ejecutando en una zona sean controlados o se vean afectados por los procesos que se están ejecutando en otras zonas. Incluso un proceso que se está ejecutando con capacidades de superusuario no puede ver ni afectar la actividad de otras zonas.

Las zonas de Oracle Solaris son ideales para entornos que tienen varias aplicaciones en un único servidor. Para obtener más información, consulte “Introducción a Zonas de Oracle Solaris ”.

Supervisión del uso de los recursos del equipo

Como administrador del sistema, debe supervisar la actividad del sistema. Debe conocer todos los aspectos de los equipos, incluidos los siguientes:

- ¿Cuál es la carga normal?
- ¿Quién tiene acceso al sistema?
- ¿Cuándo acceden los usuarios al sistema?
- ¿Qué programas se ejecutan generalmente en el sistema?

Con este tipo de conocimiento, puede utilizar las herramientas disponibles para auditar el uso del sistema y supervisar las actividades de usuarios individuales. La supervisión es muy útil cuando se sospecha que existe una infracción de seguridad. Para obtener más información sobre el servicio de auditoría, consulte el Capítulo 1, “Acerca de la auditoría en Oracle Solaris” de “Gestión de auditoría en Oracle Solaris 11.2 ”.

Supervisión de la integridad de archivos

Como administrador del sistema, debe garantizar que los archivos instalados en los sistemas que administra no hayan cambiado de manera inesperada. En las instalaciones de gran tamaño, una herramienta de comparación y elaboración de informes sobre la pila de software en cada uno de los sistemas permite realizar un seguimiento de los sistemas. La herramienta básica de creación de informes de auditoría (BART) permite validar exhaustivamente los sistemas mediante comprobaciones en el nivel de archivos de uno o varios sistemas a lo largo del tiempo. Los cambios en un manifiesto BART en varios sistemas, o en un sistema a lo largo del tiempo, pueden validar la integridad de los sistemas. BART permite crear y comparar manifiestos, y proporciona reglas para los informes de secuencias de comandos. Para obtener más información, consulte el Capítulo 2, “Verificación de la integridad de archivos mediante el uso de BART” de “Protección y verificación de la integridad de archivos en Oracle Solaris 11.2 ”.

Control de acceso a archivos

Oracle Solaris es un entorno multiusuario donde todos los usuarios que iniciaron sesión en un sistema pueden leer los archivos que pertenecen a otros usuarios. Con los permisos de archivo adecuados, los usuarios también pueden utilizar archivos que pertenecen a otros usuarios. Para obtener más información, consulte el Capítulo 1, “Control de acceso a archivos” de “Protección y verificación de la integridad de archivos en Oracle Solaris 11.2 ”. Para obtener instrucciones paso a paso sobre cómo configurar permisos adecuados en los archivos, consulte “Protección de archivos” de “Protección y verificación de la integridad de archivos en Oracle Solaris 11.2 ”.

Cifrado de archivos en disco

Para mantener un archivo seguro, puede impedir que otros usuarios accedan a él. Por ejemplo, nadie puede leer un archivo con permisos de `600`, excepto el propietario y la cuenta `root`. De manera similar, un directorio con permisos de `700` es inaccesible. Sin embargo, alguien que adivine su contraseña o que descubra la contraseña `root` puede acceder a ese archivo. Además, el archivo inaccesible se conserva en una cinta de copia de seguridad cada vez que se realiza una copia de seguridad de los archivos del sistema en medios sin conexión. Para obtener protección adicional, puede utilizar cifrado en discos o utilizar comandos de la estructura criptográfica.

Para obtener más información sobre los sistemas de archivos ZFS, consulte “Cifrado de sistemas de archivos ZFS” de “Gestión de sistemas de archivos ZFS en Oracle Solaris 11.2 ”.

La estructura criptográfica proporciona los comandos `digest`, `mac` y `encrypt`. Los usuarios normales pueden utilizar estos comandos para proteger archivos y directorios. Para obtener

más información, consulte el Capítulo 1, “Estructura criptográfica” de “Gestión de cifrado y certificados en Oracle Solaris 11.2 ”.

Uso de listas de control de acceso

Las ACL pueden proporcionar un mayor control de los permisos de archivo. Puede agregar ACL cuando las protecciones de archivos UNIX tradicionales no son suficientes. Las protecciones de archivos UNIX tradicionales proporcionan permisos de lectura, escritura y ejecución para las tres clases de usuarios: propietario, grupo y otros usuarios. Una ACL proporciona un nivel de seguridad de archivos más específico.

Las ACL permiten definir permisos de archivos detallados, incluidos los siguientes:

- Permisos de propietario de archivo
- Permisos de archivo para el grupo del propietario
- Permisos de archivo para otros usuarios que están fuera del grupo del propietario
- Permisos de archivo para usuarios específicos
- Permisos de archivo para grupos específicos
- Permisos predeterminados para cada una de las categorías anteriores

Para proteger archivos ZFS con listas de control de acceso (ACL), consulte el Capítulo 7, “Uso de listas de control de acceso y atributos para proteger archivos Oracle Solaris ZFS” de “Gestión de sistemas de archivos ZFS en Oracle Solaris 11.2 ”. Para obtener información sobre el uso de las ACL en sistemas de archivos antiguos, consulte “Uso de listas de control de acceso para proteger archivos UFS” de “Protección y verificación de la integridad de archivos en Oracle Solaris 11.2 ”.

Uso compartido de archivos entre equipos

Un servidor de archivos de red puede controlar qué archivos están disponibles para uso compartido. Un servidor de archivos de red también puede controlar qué clientes tienen acceso a los archivos y qué tipo de acceso está permitido para esos clientes. El servidor de archivos puede otorgar acceso de lectura y escritura o acceso de sólo lectura a todos los clientes o a clientes específicos. El control de acceso se especifica cuando los recursos están disponibles con el comando `share`.

Al crear un recurso compartido NFS de un sistema de archivos ZFS, el sistema de archivos se comparte permanentemente hasta que se elimine el recurso compartido. SMF gestiona automáticamente el recurso compartido cuando el sistema se reinicia. Para obtener más información, consulte “Oracle Solaris ZFS y sistemas de archivos tradicionales” de “Gestión de sistemas de archivos ZFS en Oracle Solaris 11.2 ”.

Restricción de acceso `root` a archivos compartidos

En general, al superusuario no se le permite el acceso `root` a los sistemas de archivos que se comparten en la red. El sistema NFS impide el acceso `root` a los sistemas de archivos montados cambiando el usuario del solicitante al usuario `nobody` con el ID de usuario `60001`. Los derechos de acceso del usuario `nobody` son los mismos que se otorgan al público. El usuario `nobody` tiene los derechos de acceso de un usuario sin credenciales. Por ejemplo, si el público sólo tiene permiso de ejecución para un archivo, el usuario `nobody` sólo puede ejecutar ese archivo.

Un servidor NFS puede otorgar acceso `root` a un sistema de archivos compartidos por host. Para otorgar estos privilegios, utilice la opción `root=`*hostname* para el comando `share`. Debe utilizar esta opción con cuidado. Para obtener una explicación de opciones de seguridad con NFS, consulte el Capítulo 5, “Comandos para gestionar sistemas de archivos de red” de “Gestión de sistemas de archivos de red en Oracle Solaris 11.2 ”.

Control de acceso a la red

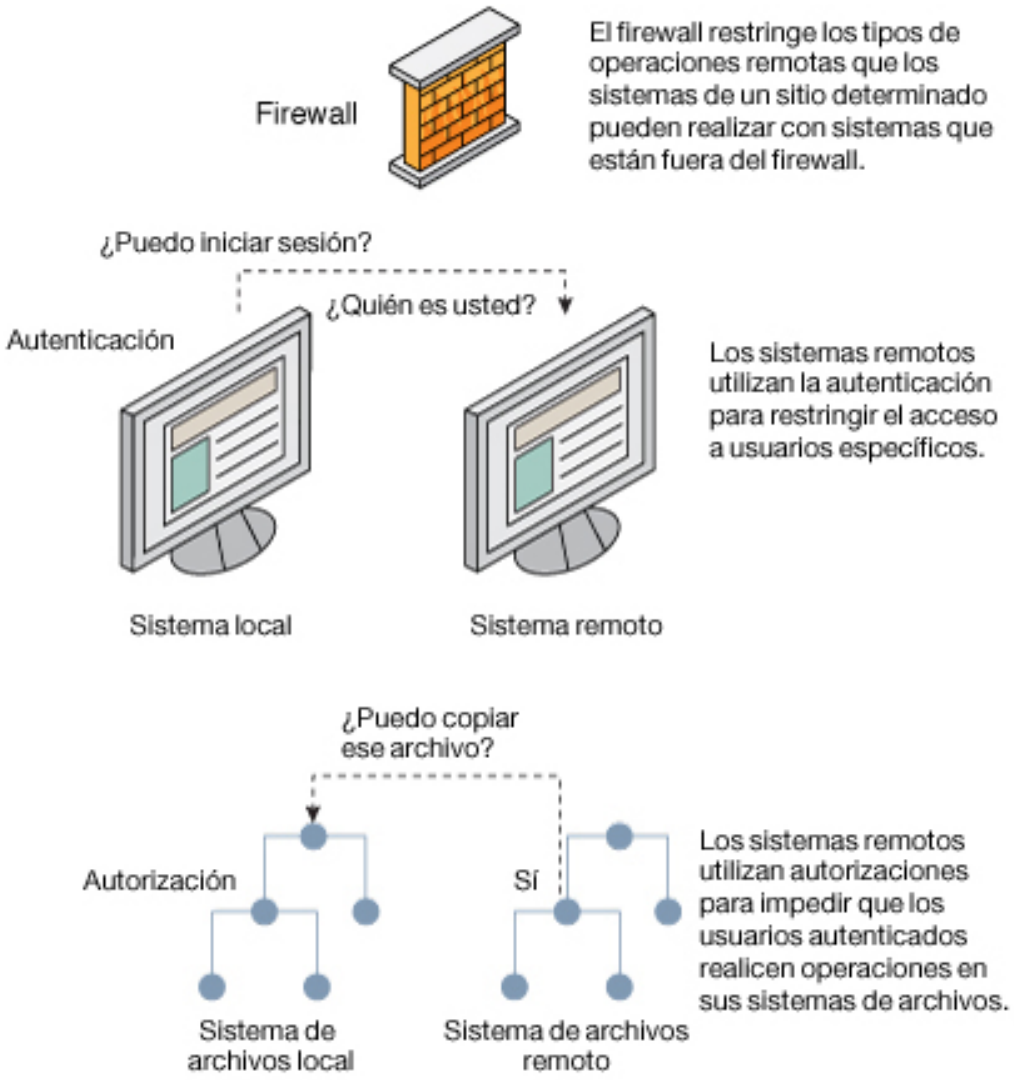
Los equipos suelen formar parte de una red de equipos que permite que los equipos conectados intercambien información. Los equipos conectados a la red pueden acceder a datos y demás recursos de otros equipos de la red. Aunque las redes de equipos crean un entorno informático potente y sofisticado, las redes también complican la seguridad de los equipos.

Por ejemplo, dentro de una red de equipos, los sistemas individuales permiten el uso compartido de información. El acceso no autorizado es un riesgo de seguridad. Debido a que muchas personas tienen acceso a una red, el acceso no autorizado es más probable, especialmente como consecuencia de errores del usuario. Un mal uso de contraseñas también puede originar el acceso no autorizado.

Mecanismos de seguridad de red

La seguridad de red, generalmente, se basa en la limitación o el bloqueo de operaciones de sistemas remotos. En la siguiente figura, se describen las restricciones de seguridad que se pueden imponer en las operaciones remotas.

FIGURA 1-1 Restricciones de seguridad para operaciones remotas



Autenticación y autorización para acceso remoto

La *autenticación* es una manera de controlar el acceso cuando los usuarios intentan acceder a un sistema remoto. La autenticación se puede configurar en el nivel del sistema y en el nivel

de red. Después de que un usuario haya obtenido acceso a un sistema remoto, la *autorización* es una manera de limitar las operaciones que el usuario puede realizar. En la siguiente tabla, se muestran los servicios que proporcionan autenticación y autorización.

TABLA 1-3 Servicios de autenticación para el acceso remoto

Servicio	Descripción	Más información
IPsec	IPsec proporciona autenticación basada en host y en certificado, y cifrado de tráfico de red.	Capítulo 6, “Acerca de la arquitectura de seguridad IP” de “Protección de la red en Oracle Solaris 11.2 ”
Kerberos	Kerberos utiliza el cifrado para autenticar y autorizar a un usuario que está iniciando sesión en el sistema.	Por ejemplo, consulte “Cómo funciona el servicio Kerberos” de “Gestión de Kerberos y otros servicios de autenticación en Oracle Solaris 11.2 ”.
LDAP	El servicio de directorios LDAP puede proporcionar autenticación y autorización a nivel de red.	“Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: DNS y NIS ”
Comandos de inicio de sesión remoto	Los comandos de inicio de sesión remoto permiten que los usuarios inicien sesión en un sistema remoto a través de la red y utilicen sus recursos. Algunos de los comandos de inicio de sesión remoto son `rlogin`, `rcp` y `ftp`. Si usted es un host de confianza, la autenticación es automática. De lo contrario, se le pedirá que se autentique.	Capítulo 3, “Acceso a sistemas remotos” de “Gestión de sistemas remotos en Oracle Solaris 11.2 ”
SASL	La autenticación sencilla y capa de seguridad (SASL) es una estructura que proporciona autenticación y servicios de seguridad opcionales a los protocolos de red. Los complementos permiten seleccionar el protocolo de autenticación adecuado.	“Acerca de SASL” de “Gestión de Kerberos y otros servicios de autenticación en Oracle Solaris 11.2 ”
RPC segura	Las RPC seguras mejoran la seguridad de los entornos de red al autenticar a los usuarios que realizan solicitudes en equipos remotos. Puede utilizar un mecanismo de autenticación UNIX, DES o Kerberos para las RPC seguras.	“Acerca de RPC seguras” de “Gestión de Kerberos y otros servicios de autenticación en Oracle Solaris 11.2 ”
	Las RPC seguras también se pueden utilizar para proporcionar seguridad adicional en un entorno NFS. Un entorno NFS con RPC seguras se denomina NFS seguro.	“Servicios NFS y RPC segura” de “Gestión de Kerberos y otros servicios de autenticación en Oracle Solaris 11.2 ”
Secure Shell	Secure Shell cifra el tráfico de red a través de una red no segura. Secure Shell proporciona autenticación mediante el uso de contraseñas, claves públicas, o ambos.	“Shell seguro (descripción general)” de “Gestión de acceso mediante shell seguro en Oracle Solaris 11.2 ”

Una posible alternativa a las RPC seguras es el mecanismo de *puerto con privilegios* de Oracle Solaris. A un puerto con privilegios se le asigna un número de puerto menor que `1024`. Después de que un sistema cliente haya autenticado la credencial del cliente, el cliente crea una conexión al servidor mediante el puerto con privilegios. A continuación, el servidor verifica la credencial del cliente examinando el número de puerto de la conexión.

Es posible que los clientes que no están ejecutando el software Oracle Solaris no puedan comunicarse mediante el puerto con privilegios. Si los clientes no se pueden comunicar a través del puerto, se mostrará un mensaje de error similar al siguiente:

```
“Weak Authentication
NFS request from unprivileged port”
```

Sistemas de firewall

Puede configurar un sistema de firewall para proteger los recursos de la red contra el acceso exterior. Un *sistema de firewall* es un host seguro que actúa como una barrera entre la red interna y las redes externas. La red interna trata las otras redes como si no fueran de confianza. Debe considerar esta configuración como obligatoria entre la red interna y cualquier red externa, como Internet, con la que se comunica.

Un firewall actúa como una puerta de enlace y como una barrera. Como puerta de enlace, transfiere datos entre las redes. Como barrera, bloquea la transferencia libre de datos desde y hacia la red. Un usuario de la red interna debe iniciar sesión en el sistema de firewall para acceder a hosts de redes remotas. De forma similar, un usuario de una red externa debe iniciar sesión en el sistema de firewall antes de que se le otorgue acceso a un host de la red interna.

Un firewall también puede ser útil entre algunas redes internas. Por ejemplo, puede configurar un firewall o un equipo de puerta de enlace segura para restringir la transferencia de paquetes por dirección o por protocolo. Puede permitir paquetes para transferir correo, pero no permitir paquetes para el comando `ftp`.

Además, todos los correos electrónicos que se envían desde la red interna primero se envían al sistema de firewall. A continuación, el firewall transfiere el correo a un host de una red externa. El sistema de firewall también recibe todos los correos electrónicos entrantes y los distribuye a los hosts de la red interna.

Atención - Incluso si mantiene una seguridad estricta y rigurosa en el firewall, si reduce el nivel de seguridad en otros hosts en la red, si un intruso logra entrar al sistema de firewall, puede acceder a todos las otros hosts de la red interna.

Un sistema de firewall no debe tener hosts de confianza. Un *host de confianza* es un host desde el cual un usuario puede iniciar sesión sin tener que proporcionar una contraseña. Un sistema de firewall no debe compartir ninguno de sus sistemas de archivos ni montar sistemas de archivos de otros servidores.

La función de filtro IP e IPsec de Oracle Solaris puede proporcionar protección de firewall. Para obtener más información sobre la protección de tráfico de red, consulte “Protección de la red en Oracle Solaris 11.2 ”.

Cifrado y sistemas de firewall

Los usuarios no autorizados desde fuera de una red pueden dañar o destruir los datos en paquetes capturando los paquetes antes de que alcancen su destino e insertando datos arbitrarios en el contenido antes enviar los paquetes de vuelta en su curso original. Este procedimiento es denominado *interceptación de paquetes*.

En una red de área local, la interceptación de paquetes es imposible porque los paquetes llegan a todos los sistemas, incluido el servidor, al mismo tiempo. La interceptación de paquetes puede producirse en una puerta de enlace; por lo tanto, asegúrese de que todas las puertas de enlace de la red estén protegidas.

Los ataques más peligrosos afectan la integridad de los datos. Estos ataques implican cambiar el contenido de los paquetes o suplantar a un usuario.

Otros ataques pueden implicar la intercepción de comunicaciones, pero no comprometen la integridad de los datos ni asumen la personalidad de un usuario. Una intrusión registra conversaciones para reproducirlas más adelante. Aunque los ataques de intrusión no afectan la integridad de los datos, afectan la privacidad. Puede proteger la privacidad de la información confidencial mediante el cifrado de los datos que se transmiten por la red.

- Para cifrar operaciones remotas a través de una red no segura, consulte el Capítulo 1, “Uso de shell seguro (tareas)” de “Gestión de acceso mediante shell seguro en Oracle Solaris 11.2 ”.
- Para cifrar y autenticar datos a través de una red, consulte el Capítulo 2, “Acerca del servicio Kerberos” de “Gestión de Kerberos y otros servicios de autenticación en Oracle Solaris 11.2 ”.
- Para cifrar datagramas de IP, consulte el Capítulo 6, “Acerca de la arquitectura de seguridad IP” de “Protección de la red en Oracle Solaris 11.2 ”.

Comunicación de problemas de seguridad

Si experimenta una presunta infracción de seguridad empresarial importante, puede ponerse en contacto con el Equipo de Respuesta ante Emergencias Informáticas/Centro de Coordinación (CERT/CC). El CERT/CC es una Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA) que se encuentra en el Instituto de Ingeniería de Software de Universidad Carnegie Mellon. Esta agencia puede ayudarlo con los problemas de seguridad que pueda tener. También puede derivarlo a otros equipos de respuesta ante emergencias informáticas que puedan ser más adecuados para sus necesidades específicas. Para conocer la información de contacto actual, consulte el sitio web de CERT/CC (http://www.cert.org/contact_cert/).

♦ ♦ ♦ CAPÍTULO 2

Protección de integridad de los sistemas Oracle Solaris

Los sistemas Oracle Solaris pueden protegerse de módulos de núcleo no autorizados, aplicaciones de caballo de Troya y otras amenazas que se cargan al sistema. En este capítulo se describen funciones de seguridad en Oracle Solaris que proporcionan protección frente a amenazas y mantienen la integridad del sistema en general. En este capítulo, se tratan los siguientes temas:

Uso de inicio verificado

El inicio verificado en Oracle Solaris asegura un proceso de inicio del sistema. La función protege el sistema de amenazas como las siguientes:

- Corrupción de módulos de núcleo
- La inserción o sustitución de programas maliciosos que enmascaran módulos de núcleo como legítimos, por ejemplo, virus de caballo de Troya, spyware y rootkits.
- Instalación de módulos de núcleo de terceros no autorizados

Los programas maliciosos pueden transferir información a terceros, así como modificar el comportamiento de Oracle Solaris. Aunque los módulos de terceros normalmente no son maliciosos, pueden infringir políticas que controlan los cambios del sitio. Por lo tanto, el sistema también necesita protección de instalación no autorizada de estos módulos.

Inicio verificado y firmas ELF

En Oracle Solaris, la verificación de inicio es realizada mediante claves o firmas `elfsign`. Según la configuración de fábrica, los módulos de núcleo de Oracle Solaris se firman con estas claves. Debido a su formato de archivo, estos módulos se denominan también objetos ELF. La firma se crea utilizando las sumas de comprobación SHA-1 o SHA-256 de los registros ELF seleccionados en un archivo de objeto. Las sumas de comprobación SHA-1 o SHA-256 se firman con un par de claves públicas y privadas SA-2048. La clave pública se distribuye en `/etc/certs` mientras que la clave privada no se distribuye.

Todas las claves se almacenan en el **entorno de inicio previo** del sistema, que es el software o firmware que se ejecuta previo al inicio de Oracle Solaris. El firmware carga e inicia `platform/.../unix`.

El entorno de inicio previo es diferente para cada categoría de sistemas. El entorno de inicio previo admitido para cada categoría es el siguiente:

- Sistemas SPARC y x86 antiguos: estos sistemas no tienen capacidades de almacenamiento fuera del sistema de archivos, por lo tanto los valores de configuración para verificación de inicio se almacenan en el sistema de archivos. Específicamente, la información de configuración se almacena en `/etc/system`. Las claves se almacenan en `/etc/certs/*SE` en el sistema de archivos root y el archivo de inicio.
- Sistemas SPARC con inicio verificado admitido en Oracle Integrated Lights Out Manager (ILOM): las claves y valores de configuración se almacenan en Oracle ILOM.

  Debido de que Oracle ILOM está fuera del sistema de archivos del sistema operativo, la configuración de inicio verificado está protegida de alteración por parte de los usuarios del sistema operativo, incluidos aquellos con privilegios (root) de administrador. Por lo tanto, el inicio verificado en esta categoría de sistemas es más seguro.

  Debe asegurarse de que el acceso a Oracle ILOM sea seguro para evitar cambios no autorizados a la configuración de inicio verificado. Para obtener más información sobre protección de Oracle ILOM, consulte la documentación en http://www.oracle.com/goto/ILOM/docs.
- Las series SPARC M5, SPARC M6 y SPARC T5: los valores de configuración se almacenan en Oracle ILOM del sistema. El firmware SPARC envía la información de configuración a Oracle Solaris.

Secuencia de verificación durante el inicio del sistema

El inicio verificado automatiza la verificación de las firmas `elfsign` de los módulos de núcleo de Oracle Solaris. Con inicio verificado, el administrador puede crear una cadena verificable de

confianza en el proceso de inicio empezando desde el reinicio del sistema hasta la finalización del proceso de inicio.

Durante el inicio del sistema, cada bloque de código que se inicia en el proceso de inicio verifica el siguiente bloque que se debe cargar. La secuencia de la verificación y carga continúa hasta que el último módulo de núcleo se carga.

Cuando se realiza un apagado y encendido del sistema, comienza una nueva secuencia de verificación. El administrador también puede configurar que el inicio verificado realice la acción adecuada en el caso de fallo de verificación.

Tenga en cuenta el flujo de inicio de Oracle Solaris en un sistema SPARC:

`Firmware -> Bootblock -> /platform/.../unix -> genunix ->` *other kernel modules*

El firmware SPARC viene instalado de fábrica. La firma digital del firmware también se puede actualizar mediante la utilidad `fwupdate`. El firmware verifica y, a continuación, carga el módulo `/platform/.../unix` de Oracle Solaris, que es el módulo de Oracle Solaris inicial. A su vez, el cargador de tiempo de ejecución de núcleo de Oracle Solaris `krtld`, que es parte del módulo, verifica y carga el módulo (`genunix`) de UNIX genérico y los módulos subsecuentes.

Políticas para inicio verificado

Dos políticas gestionan el inicio verificado:

- La política de inicio regula la verificación de los módulos `genunix` y UNIX. Estos módulos son los primeros que se van a cargar durante el proceso de inicio.
- La política del módulo regula la verificación de otros módulos de núcleo que necesitan cargarse después del módulo `genunix`.

En sistemas SPARC y x86 antiguos, las políticas están definidas en las variables `boot_policy` y `module_policy` del archivo `/etc/system`. En los sistemas SPARC con inicio verificado de Oracle ILOM admitido, `boot_policy` y `module_policy` son propiedades de Oracle ILOM en `/HOST`*x*`/verified_boot`, donde *x* es el número (PDomain) de dominio físico.

Ambas variables o propiedades se pueden configurar con uno de los siguientes valores:

- `none`: no se realiza verificación de inicio. De manera predeterminada, `boot_policy` y `module_policy` no están configuradas y, por lo tanto, el inicio verificado está desactivado.
- `warning`: la firma `elfsign` de cada módulo de núcleo se verifica antes de que se cargue el módulo. Si la verificación falla en un módulo, el módulo aún se carga. Las discrepancias se registran en la consola del sistema o, si está disponible, en el log del sistema. De manera predeterminada, el log es `/var/adm/messages`.
- `enforce`: la firma `elfsign` de cada módulo de núcleo se verifica antes de que se cargue el módulo. Si la verificación falla en un módulo, el módulo no se carga. Las discrepancias se

registran en la consola del sistema o, si está disponible, en el log del sistema. De manera predeterminada, el log es `/var/adm/messages`.

Además de configurar las políticas, también debe especificar los certificados de clave pública X.509 `elfsign` en el sistema. Similar a los módulos, especifique los certificados utilizando una variable o definiendo una propiedad de Oracle ILOM.

En sistemas con Oracle ILOM que admiten inicio verificado, un archivo de certificado de inicio verificado preinstalado, `/etc/certs/ORCLS11SE`, se proporciona como parte de Oracle ILOM. En sistemas SPARC y x86 antiguos, el certificado está disponible como el archivo de Oracle Solaris `/etc/certs/ORCLS11SE`.

El certificado contiene la clave pública RSA que se utiliza para verificar las firmas `elfsign` en los objetos ELF. Sin embargo, puede instalar un certificado proporcionado por la compañía para reemplazar `/etc/certs/ORCLS11SE`. Todos los certificados se cargan y gestionan en cada PDomain individual.

Activación de inicio verificado

De manera predeterminada, inicio verificado está desactivado en los sistemas. Los procedimientos para activar la función difieren en función de su sistema. Para activar la función, utilice uno de los procedimientos descritos en esta sección que se aplican a su sistema.

▼ SPARC: Cómo activar el inicio verificado en sistemas SPARC con compatibilidad de inicio verificado de Oracle ILOM

Para sistemas SPARC con compatibilidad de inicio verificado de Oracle ILOM, las propiedades de inicio verificado están en `/HOST`*x*`/verified_boot`, donde *x* es el número de PDomain, como `HOST0`, `HOST1`, etc.

Nota - Algunos sistemas SPARC sólo tienen un dominio físico, `/HOST`, mientras que otros tienen varios dominios físicos. Este procedimiento asume que está utilizando un sistema con varios dominios físicos y hace referencia a un dominio físico como `/HOST`*x*. Para las funciones de seguridad que son específicas de su sistema, consulte el manual de seguridad del sistema.

---

1. **(Opcional) Determine si el sistema admite inicio verificado.**

```
# show /HOSTx/verified_boot
```

```
show: Invalid target /HOST/verified_boot
```

Puede utilizar `fwupdate` para actualizar el firmware de Oracle ILOM del sistema.

2. **Como administrador, inicie sesión en la interfaz de usuario de Oracle ILOM.**

```
% ssh root@ilom
```

donde *ilom* puede ser la dirección IP de procesador de servicio de Oracle ILOM o la dirección IP del módulo de supervisión del chasis.

3. **Configure las propiedades del inicio verificado.**

```
--> set /HOSTx/verified_boot/boot_policy=warning
--> set /HOSTx/verified_boot/module_policy=warning
```

Nota - Especifique `warning` o `enforce` para cada propiedad. Las propiedades pueden tener diferentes configuraciones. Para obtener una explicación de estas configuraciones de políticas, consulte "Políticas para inicio verificado" [33].

Si la política de inicio está configurada con `enforce` y se detectan discrepancias en los módulos `genunix` o UNIX, el sistema no se inicia. En su lugar, el sistema vuelve a OpenBoot PROM (OBP).

---

4. **Especifique el certificado que desea utilizar en lugar del certificado que se proporciona con el sistema.**

```
--> load /HOSTx/verified_boot/cert -source ftp-location
```

donde *ftp-location* hace referencia al servidor FTP y el nombre de archivo que almacena el certificado. *ftp-location* debe estar en formato URL `ftp://server/filename`.

5. **(Opcional) Muestre la configuración de inicio verificado.**

```
--> show /HOSTx/verified_boot
/HOST0
Properties:
boot_policy = warning
module_policy = warning
cert = ftp://server/filename
```

▼ Cómo activar el inicio verificado en sistemas SPARC y x86 antiguos

Utilice este procedimiento si el sistema no tiene los medios para almacenar la configuración de verificación de inicio fuera del sistema de archivos local del sistema.

Al activar la verificación de inicio en este tipo de sistema, tenga en cuenta las siguientes consideraciones de seguridad:

- La información de configuración se almacena en el sistema de archivos local y, por lo tanto, es accesible.
- Cualquier usuario con privilegios puede modificar la configuración.
- La configuración de política se puede cambiar, y la verificación de inicio en sí se puede desactivar.
- Se pueden agregar claves extra que posiblemente permitan que cualquier firmante `elfsign` firme módulos de objeto.

1. **Edite el archivo `/etc/system`.**

   a. **Agregue y configure las variables `boot_policy` y `module_policy`.**

      Por ejemplo, en `/etc/system`, puede escribir lo siguiente (se muestra en negrita):

      ```
      * Verified Boot settings: 1=none (default), 2=warning, 3=enforce
      set boot_policy=2
      set module_policy=2
      ```

      Especifique el número que corresponde a la configuración que desea para cada variable. Las variables pueden tener diferentes configuraciones. Para obtener una explicación de estas configuraciones de políticas, consulte “Políticas para inicio verificado” [33].

      Si la política de inicio está configurada con `enforce` y se detectan discrepancias en los módulos `genunix` o UNIX, el sistema no se inicia. En su lugar, el sistema vuelve a OpenBoot PROM (OBP).

   b. **Especifique uno o más certificados clave X.509 `elfsign` para la variable `verified_boot_certs`.**

      ```
      set verified_boot_certs="/etc/certs/THIRDPARTYSE"
      ```

      donde *THIRDPARTY* es el nombre del archivo de certificado proporcionado por el usuario.

2. **Actualice el archivo `/etc/system` en el archivo de inicio.**

   ```
   # bootadm update-archive
   ```

3. **(Opcional) Visualice la configuración de inicio verificado.**

   a. **Monte el archivo.**

      - Para sistemas SPARC:

        ```
        # mount -r -F hsfs /platform/sun4v/boot_archive /mnt
        ```

      - Para sistemas x86:

```
# mount -r -F hsfs /platform/x86-type/boot_archive /mnt
```

donde *x86-type* es `i86pc` o `amd64`.

b. Muestre la configuración de inicio verificado y las claves `elfsign`.

```
# gzcat /mnt/etc/system | egrep 'verified|policy'
# ls -l /etc/certs
```

▼ Cómo administrar certificados en los sistemas con compatibilidad de inicio verificado de Oracle ILOM

Este procedimiento describe cómo gestionar los certificados de inicio verificado del sistema.

1. **Para reemplazar el certificado preinstalado con un certificado proporcionado por el usuario, escriba lo siguiente:**

```
--> load /HOSTx/verified_boot/cert -source ftp://server/filename
```

2. **Para guardar una copia del certificado actual para el origen proporcionado por el usuario, escriba lo siguiente:**

```
--> dump /HOSTx/verified_boot/cert -dest ftp://server/filename
```

3. **Para eliminar cualquier certificado instalado por el usuario y volver al certificado preinstalado del sistema, escriba lo siguiente:**

```
--> reset /HOSTx/verified_boot/cert
```

▼ Cómo verificar manualmente la firma `elfsign`

El inicio verificado es un mecanismo automático que proporciona una manera rápida y eficaz de garantizar la integridad del proceso de inicio. Sin embargo, aún puede verificar una firma del módulo de núcleo de manera manual.

- **Utilice la sintaxis de comando `elfsign` de la siguiente manera:**

```
$ elfsign verify -v kernel_module
```

Por ejemplo:

```
$ elfsign verify -v /kernel/misc/sparcv9/cardbus
elfsign: verification of /kernel/misc/sparcv9/cardbus passed.
format: rsa_sha1.
signer: O=Oracle Corporation, OU=Corporate Object Signing, \
               OU=Solaris Signed Execution, CN=Solaris 11
```

Acerca de Módulo de plataforma de confianza

Módulo de plataforma de confianza (TPM) hace referencia al dispositivo como también a la implementación mediante la cual se almacena información de configuración específica para el sistema. La información sirve como métricas contra las que los procesos se miden durante el inicio del sistema. Oracle Solaris utiliza TPM para almacenar de manera segura las claves de cifrado.

Los siguientes componentes implementan TPM en Oracle Solaris:

- El controlador de dispositivo de TPM se comunica con el dispositivo de TPM.
- Trusted Computing Group (TCG) Software Stack, o TSS, funciona como el canal de comunicación con el dispositivo de TPM mediante el daemon `tcsd`.
- Las bibliotecas PKCS #11 implementan un proveedor o token de hardware que utiliza TPM para generar claves y realizar operaciones delicadas. El proveedor protege todos los objetos de datos privados cifrándolos con claves que pueden utilizarse sólo dentro del dispositivo de TPM. Las bibliotecas PKCS #11 se adhieren al estándar siguiente: RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki).
- El comando `tpmadm` se utiliza para administrar los aspectos relacionados con TPM para verificación del proceso de inicio.

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

El propietario de la plataforma debe inicializar TPM definiendo una contraseña de propietario que se utiliza para autorizar las operaciones con privilegios. El propietario de la plataforma, también denominado propietario de TPM, difiere del superusuario tradicional de dos maneras:

- Para acceder a las funciones de TPM, el privilegio del proceso es irrelevante. Las operaciones con privilegios requieren el conocimiento de la contraseña del propietario independientemente del nivel de privilegios del proceso de llamada.
- El propietario de TPM no puede sobrescribir los controles de acceso para los datos protegidos por claves de TPM. El propietario puede destruir de manera eficaz los datos reinicializando el TPM. Sin embargo, el propietario no puede acceder a los datos que se han cifrado con claves de TPM que pertenecen a otros usuarios.

Módulo de plataforma de confianza, junto con las otras medidas descritas en esta guía, protege el sistema de acceso no autorizado de usuarios o aplicaciones.

Inicialización de TPM en sistemas Oracle Solaris

Esta sección contiene los procedimientos para inicializar TPM en sistemas Oracle Solaris. Los procedimientos difieren entre los sistemas SPARC y x86. Sin embargo, para inicializar TPM, determinados requisitos previos son comunes para ambas plataformas.

- El dispositivo de TPM `/dev/tpm` debe estar instalado en el sistema.
- TPM debe utilizar la especificación de módulo de plataforma de confianza TCG versión 1.2, también conocida como ISO/IEC 11889-1:2009. Consulte la especificación publicada en http://www.trustedcomputinggroup.org/resources/tpm_main_specification.
- Los siguientes paquetes de TPM de Oracle Solaris deben estar instalados:
  - Controlador de módulo de plataforma de confianza (`driver/crypto/TPM`)
  - Software TCG TrouSerS (`library/security/trousers`)

  Para instalar estos paquetes, utilice los comandos siguientes:

```
# pkg install driver/crypto/tpm
# pkg install library/security/trousers
```

▼ Cómo comprobar si el dispositivo de TPM es reconocido por el sistema operativo

Utilice este procedimiento para determinar si Oracle Solaris reconoce el dispositivo de TPM instalado. Este procedimiento se aplica al sistema SPARC y el sistema x86.

- **En la ventana de terminal, emita el siguiente comando:**

```
# prtconf -v |grep tpm
```

Si se reconoce el dispositivo de TPM, el comando genera una salida similar a la siguiente:

```
# prtconf -v |grep tpm
tpm, instance #0
dev_path=/pci@0,0/isa@lf/tpm@0,fed40000:tpm
dev_link=/dev/tpm
```

Si no se generó ninguna salida, el dispositivo podría estar desactivado. Para obtener información sobre cómo activar el dispositivo, consulte Cómo inicializar TPM mediante la interfaz de Oracle ILOM [40] o Cómo inicializar TPM mediante BIOS [41] en función de la plataforma del sistema.

Nota - Como alternativa, también puede utilizar el comando `ls` para obtener la misma información. Sin embargo, la salida debe contener menos información que la especificada por la sintaxis `prtconf`.

```
# ls -l /dev/tpm
lrwxrwxrwx  1 root root  44 May 22 2012 /dev/tpm ->
../devices/pci@0,0/isa@lf/tpm@0,fed40000:tpm
```

SPARC: Cómo inicializar TPM mediante la interfaz de Oracle ILOM

En sistemas SPARC, puede utilizar las interfaces Oracle Solaris y Oracle ILOM del sistema para inicializar TPM.

1. **En el indicador Oracle ILOM, corte la alimentación del sistema.**

   ```
   -> stop -f/SYS
   ```

2. **Active TPM.**

   Active TPM con uno de los siguientes conjuntos de comandos en función del sistema SPARC.

   - En los servidores serie SPARC M5 y SPARC T5, utilice el siguiente comando:

     ```
     -> set /HOST/tpm mode=activated
     ```

   - En los servidores serie SPARC M5-32, utilice el siguiente comando:

     ```
     -> set /HOST#/tpm mode=activated
     ```

     donde # es un número de instancia, por ejemplo, `HOST0/tpm`.

   - En los servidores SPARC T4, utilice los siguientes comandos:

     ```
     -> set /HOST/tpm enable=true activate=true
     -> show /HOST/tpm
     ```

3. **En el indicador Oracle Solaris, inicialice TPM.**

   La inicialización de TPM hace que se convierta en un propietario de TPM y requiere que asigne una contraseña de propietario, también conocida como PIN de propietario.

   ```
    # tpmadm init
   TPM Owner PIN:
   Confirm TPM Owner PIN
   ```

4. **Verifique el estado de TPM.**

```
 # tpmadm status
TPM Version: 1.2 (ATML Rev: 13.9, SpecLevel: 2, ErrataRev: 1)
TPM resources
Contexts: 16/16 available
Sessions: 2/3 available
Auth Sessions: 2/3 available
Loaded Keys: 18/21 available
Platform Configuration Registers (24)
PCR 0: E1 EE 40 D8 66 28 A9 08 B6 22 8E AF DC 3C BC 23 71 15 49 31
PCR 1: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
PCR 2: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
PCR 3: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
PCR 4: AF 98 77 B8 72 82 94 7D BE 09 25 10 2E 60 F9 60 80 1E E6 7C
PCR 5: E1 AA 8C DF 53 A4 23 BF DB 2F 4F 0F F2 90 A5 45 21 D8 BF 27
PCR 6: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
PCR 7: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
PCR 8: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 9: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 11: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 12: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 13: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 14: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 15: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 17: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
PCR 18: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
PCR 19: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
PCR 20: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
PCR 21: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
PCR 22: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
PCR 23: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

5. **(Opcional) Active el proveedor de cifrado de TPM.**

Nota - El proveedor de cifrado de TPM es más lento que Oracle Solaris. Realice este paso sólo si desea que TPM realice operaciones criptográficas.

```
# cryptoadm install provider='/usr/lib/security/$ISA/pkcs11_tpm.so'
# cryptoadm list -mv provider='/usr/lib/security/$ISA/pkcs11_tpm.so'
```

▼ x86: Cómo inicializar TPM mediante BIOS

En sistemas x86, realiza pasos en el BIOS del sistema antes de inicializar el servicio mediante Oracle Solaris.

1. **En el indicador Oracle Solaris, reinicie el sistema.**

```
# reboot -p
```

2. **Durante el inicio del sistema, presione F2 para acceder al menú del BIOS.**

3. **Mediante las opciones del menú del BIOS, configure TPM.**

   a. **Vaya a Advanced (Avanzado) → Trusted Computing (Computación de confianza).**

   b. **Defina TPM especificando valores para los siguientes elementos del menú.**

      ```
      TCG/TPM Support [Yes]
      Execute TPM Command [Enabled]
      ```

   c. **Presione la tecla ESC para salir del menú del BIOS.**

   d. **Elija guardar los cambios y salir.**

   e. **Para continuar con el proceso de inicio, seleccione OK (Aceptar).**

4. **Después de que el proceso de inicio finalice, active el daemon `tcsd`.**

   ```
   # svcadm enable -s svc:/application/security/tcsd
   ```

5. **Inicialice TPM.**

   La inicialización de TPM hace que se convierta en un propietario de TPM y requiere que asigne una contraseña de propietario.

   ```
   # tpmadm init
   TPM Owner PIN:
   Confirm TPM Owner PIN
   ```

6. **Verifique el estado de TPM.**

   ```
    # tpmadm status
   TPM Version: 1.2 (ATML Rev: 13.9, SpecLevel: 2, ErrataRev: 1)
   TPM resources
   Contexts: 16/16 available
   Sessions: 2/3 available
   Auth Sessions: 2/3 available
   Loaded Keys: 18/21 available
   Platform Configuration Registers (24)
   PCR 0: E1 EE 40 D8 66 28 A9 08 B6 22 8E AF DC 3C BC 23 71 15 49 31
   PCR 1: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
   PCR 2: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
   PCR 3: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
   PCR 4: AF 98 77 B8 72 82 94 7D BE 09 25 10 2E 60 F9 60 80 1E E6 7C
   PCR 5: E1 AA 8C DF 53 A4 23 BF DB 2F 4F 0F F2 90 A5 45 21 D8 BF 27
   PCR 6: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
   ```

```
PCR 7: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
PCR 8: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 9: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 11: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 12: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 13: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 14: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 15: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 17: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
PCR 18: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
PCR 19: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
PCR 20: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
PCR 21: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
PCR 22: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
PCR 23: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

7. (Opcional) Active el proveedor de cifrado de TPM.

Nota - El proveedor de cifrado de TPM es más lento que Oracle Solaris. Por lo tanto, realice este paso sólo si desea que TPM realice operaciones criptográficas.

```
# cryptoadm install provider='/usr/lib/security/$ISA/pkcs11_tpm.so'
# cryptoadm list -mv provider='/usr/lib/security/$ISA/pkcs11_tpm.so'
```

▼ Cómo permitir que los consumidores PKCS #11 utilicen TPM como almacén de claves seguro

Antes de empezar Para realizar este procedimiento, debe instalar y activar TPM en el sistema. Asegúrese de que el daemon `tcsd` también esté en ejecución.

1. Verifique que el dispositivo de TPM esté instalado.

```
# ls -alF /dev/tpm
lrwxrwxrwx 1 root 39 Dec 27 2011 /dev/tpm -> ../devices/pci@0,0/isa@1/tpm@1,1670:tpm
```

2. Active el daemon `tcsd`.

```
# svcadm enable tcsd
```

3. Inicialice el área de almacenamiento de token protegido por TPM personal.

```
$ pktool inittoken currlabel=TPM
```

Nota - Todos los usuarios individuales deben realizar este paso.

4. **Defina el PIN de token para el oficial de seguridad.**

```
$ pktool setpin token=tmp/TPM so
```

5. **Defina el PIN del usuario.**

```
$ pktool setpin token=tmp/TPM
```

6. **Genere claves y certificados que utilicen el dispositivo de TPM especificando el nombre de token que se utilizó cuando el token se inicializó.**

```
$ pktool gencert token=tpm/TPM -i
$ pktool list token=tpm/TPM
```

Las aplicaciones existentes que ya utilizan la estructura criptográfica en `libpkcs11` pueden utilizar el token de TPM para sus operaciones haciendo que las aplicaciones seleccionen el dispositivo de token de TPM para las sesiones.

ejemplo 2-1 Permiso de uso de TPM para consumidores PKCS #11

En este ejemplo, se asigna por primera vez un nuevo nombre al token de TPM. A partir de entonces, las siguientes acciones en el token hacen referencia al nuevo nombre.

```
$ pktool inittoken currlable=TPM newlabel=JohnDoeTPM
$ pktool setpin token=tmp/JohnDoeTPM so
$ pktool gencert token=tpm/JohnDoeTPM -i
$ pktool list token=tpm/JohnDoeTPM
```

Resolución de problemas de TPM

Utilice los comandos descritos en esta sección para supervisar los diferentes componentes operativos que le permiten utilizar correctamente TPM y solucionar problemas de TPM.

- Para verificar que el daemon `tcsd` esté en ejecución:

```
# svcs tcsd
STATE      STIME      FMRI
online     Nov_07     svc:/application/security/tcsd:default
```

- Para asegurarse de que el dispositivo de TPM esté instalado:

```
# ls -alF /dev/tpm
lrwxrwxrwx 1 root 39 Dec 27 2011 /dev/tpm -> ../devices/pci@0,0/isa@1/tpm@1,1670:tpm
```

- Para verificar que el paquete de software de TSS esté instalado:

```
# pkg info trousers
Name: library/security/trousers
```

```
Summary: TrouSerS TCG software to access a TPM device
Description: The TrouSerS library provides a software stack from the
Trusted Computer Group (TCG) that accesses a Trusted Platform Module
(TPM) hardware device.
Category: System/Security
State: Installed
Publisher: solaris
Version: 0.3.6
Build Release: 5.11
Branch: 0.175.1.0.0.24.0
Packaging Date: September 4, 2012 05:28:21 PM
Size: 3.65 MB
FMRI: pkg://solaris/library/security/
trousers@0.3.6,5.11-0.175.1.0.0.24.0:20120904T1728212
```

- Para borrar el TPM como un requisito después de que TPM se haya reinicializado previamente.
  - En el indicador de Oracle Solaris:

    ```
    # tpmadm clear owner
    ```

  - En el indicador de Oracle ILOM:

    ```
    -> stop /SYS
    -> set /HOST/tpm forceclear=true
    -> start /SYS
    ```

♦ ♦ ♦ CAPÍTULO 3

Control de acceso a sistemas

En este capítulo, se describen los procedimientos para controlar quién puede acceder a sistemas Oracle Solaris.

En este capítulo, se tratan los siguientes temas:

Para obtener una descripción general sobre la seguridad del sistema, consulte el Capítulo 1, Gestión de seguridad del equipo.

Protección de inicios de sesión y contraseñas

Para vigilar el acceso al sistema, puede limitar inicios de sesión remotos, solicitar que los usuarios tengan contraseñas y solicitar que la cuenta `root` tenga una contraseña compleja. Para gestionar accesos de usuarios, puede mostrar un mensaje de seguridad a los usuarios, supervisar los intentos de acceso incorrecto y desactivar los inicios de sesión temporalmente.

El siguiente mapa de tareas hace referencia a procedimientos que supervisan inicios de sesión de usuarios y que desactivan inicios de sesión de usuarios.

TABLA 3-1 Protección de inicios de sesión y contraseñas (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Informar a los usuarios de la seguridad de un sitio en el inicio de sesión.	Muestra un mensaje de texto en la pantalla de inicio de sesión con la información de seguridad del sitio.	"Cómo insertar un mensaje de seguridad en archivos de banner" de "Directrices de seguridad de Oracle Solaris 11 " "Cómo insertar un mensaje de seguridad en la pantalla de inicio de sesión del escritorio" de "Directrices de seguridad de Oracle Solaris 11 "

Tarea	Descripción	Para obtener instrucciones
Visualizar el estado de inicio de sesión del usuario.	Muestra amplia información sobre la cuenta de inicio de sesión de un usuario, por ejemplo, el nombre completo y la caducidad de la contraseña.	Cómo mostrar el estado de inicio de sesión de un usuario [48]
Buscar usuarios que no tienen contraseñas.	Busca sólo aquellos usuarios cuyas cuentas no necesitan una contraseña.	Cómo visualizar usuarios sin contraseñas [49]
Desactivar inicios de sesión temporalmente.	Deniega inicios de sesión de usuario a un equipo como parte del cierre o mantenimiento de rutina del sistema.	Cómo desactivar temporalmente inicios de sesión de usuarios [50]

▼ Cómo mostrar el estado de inicio de sesión de un usuario

Antes de empezar Para utilizar el comando `logins`, debe convertirse en un administrador que tiene asignado el perfil de derechos de seguridad de usuario o gestión de usuarios. De manera predeterminada, 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 ".

- **Visualice el estado de inicio de sesión de un usuario mediante el comando `logins`.**

  `# logins -x -l` *username*

  `-x` Muestra un conjunto ampliado de información de estado de inicio de sesión.

  `-l` *username* Muestra el estado de inicio de sesión para el usuario especificado. La variable *nombre_usuario* es el nombre de inicio de sesión de un usuario. Varios nombres de inicio se sesión se separan con comas.

  El comando `logins` utiliza la base de datos de contraseñas adecuada para obtener el estado de inicio de sesión de un usuario. La base de datos puede ser el archivo `/etc/passwd` local o una base de datos de contraseñas para el servicio de nombres. Para obtener más información, consulte la página del comando man `logins`(1M).

ejemplo 3-1 Visualización del estado de inicio de sesión de un usuario

En el ejemplo siguiente, se muestra el estado de inicio de sesión del usuario `jdoe`.

```
# logins -x -l jdoe
jdoe       500     staff          10   Jaylee Jaye Doe
```

```
/home/jdoe
/bin/bash
PS 010103 10 7 -1
```

`jdoe`	Identifica el nombre de inicio de sesión del usuario.
`500`	Identifica el ID de usuario (UID).
`staff`	Identifica el grupo principal del usuario.
`10`	Identifica el ID de grupo (GID).
Jaylee Jaye Doe	Identifica el comentario.
`/home/jdoe`	Identifica el directorio principal del usuario.
`/bin/bash`	Identifica el shell de inicio de sesión.
`PS 010170 10 7 -1`	Especifica la información de caducidad de las contraseñas: ■ Última fecha en la que se cambió la contraseña ■ Número de días que son necesarios entre los cambios ■ Número de días antes de que un cambio sea necesario ■ Período de advertencia

▼ Cómo visualizar usuarios sin contraseñas

Antes de empezar Para utilizar el comando `logins`, debe convertirse en un administrador que tiene asignado el perfil de derechos de seguridad de usuario o gestión de usuarios. De manera predeterminada, 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 ".

- **Visualice todos los usuarios que no tienen contraseñas con el comando `logins`.**

```
# logins -p
```

La opción `-p` muestra una lista de usuarios que no tienen contraseñas. El comando `logins` utiliza la base de datos `passwd` del sistema local a menos que se especifique un servicio de nombres distribuido en la propiedad `password` del servicio `system/name-service/switch`.

ejemplo 3-2 Visualización de cuentas sin contraseñas

En el siguiente ejemplo, el usuario `pmorph` y el rol `roletop` no tienen contraseñas.

```
# logins -p
pmorph          501     other           1       Polly Morph
```

```
roletop         211     admin           1       Role Top
#
```

▼ Cómo desactivar temporalmente inicios de sesión de usuarios

Desactive temporalmente inicios de sesión de usuarios durante el cierre o el mantenimiento de rutina del sistema.

Nota - Este procedimiento no afecta a todos los usuarios. Los siguientes pueden seguir iniciando sesión en el sistema a pesar de la presencia del archivo `/etc/nologin` creado por este procedimiento.

- Superusuario
- Los usuarios que tienen asignado el rol `root`
- Los usuarios que tienen asignada la autorización `solaris.system.maintenance`

Para obtener más información, consulte la página del comando man `nologin`(4).

Antes de empezar Debe convertirse en un administrador con la autorización `solaris.admin.edit/etc/nologin` asignada. De manera predeterminada, 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. **Cree el archivo `/etc/nologin` en un editor de texto.**

   ```
   # pfedit /etc/nologin
   ```

   Para ver un ejemplo del uso de la autorización `solaris.admin.edit/etc/nologin`, consulte Ejemplo 3-3, “Desactivación de inicios de sesión de usuarios”.

2. **Incluya un mensaje sobre la disponibilidad del sistema.**

3. **Cierre y guarde el archivo.**

ejemplo 3-3 Desactivación de inicios de sesión de usuarios

En este ejemplo, un usuario tiene autorización para escribir la notificación de que un sistema no está disponible.

```
% pfedit /etc/nologin
***No logins permitted.***

***The system will be unavailable until 12 noon.***
```

Cambio de algoritmo predeterminado para cifrado de contraseña

Para utilizar otro algoritmo para cifrado de contraseña, edite el archivo `/etc/security/policy.conf`. De manera predeterminada, las contraseñas de usuario se cifran con el algoritmo `crypt_sha256`. El algoritmo está representado por el identificador `5` asignado al parámetro `CRYPT_DEFAULT` en el archivo. Para cambiar a otro algoritmo, asigne un identificador diferente. Para obtener una lista de algoritmos de cifrado de contraseña y sus identificadores correspondientes, consulte la Tabla 1-1, “Algoritmos de cifrado de contraseña”.

Nota - Siempre que sea posible, utilice los algoritmos aprobados por FIPS. Consulte “FIPS 140 Algorithm Lists and Certificate References for Oracle Solaris Systems” de “Using a FIPS 140 Enabled System in Oracle Solaris 11.2 ” para obtener una lista de los algoritmos aprobados por FIPS y los algoritmos no aprobados.

Tenga en cuenta que el nuevo algoritmo se aplica sólo al cifrado de contraseña para los usuarios nuevos. Para los usuarios existentes, el algoritmo anterior permanece operativo si sigue definido en el parámetro `CRYPT_ALGORITHMS_ALLOW` y no es `unix`. Para ver cómo se implementa el cifrado en este caso, consulte “Configuración de algoritmos en el archivo `policy.conf`” [13]. Para incluir los usuarios existentes en el nuevo algoritmo de cifrado de contraseña, elimine también el algoritmo anterior del parámetro `CRYPT_ALGORITHMS_ALLOW`.

Para obtener más información sobre la configuración de opciones de algoritmos, consulte la página del comando man `policy.conf`(4).

▼ Cómo especificar un algoritmo para cifrado de contraseña

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. **En el archivo `/etc/security/polic.conf`, especifique el identificador para el algoritmo de cifrado seleccionado como el valor para la variable `CRYPT_DEFAULT`.**

2. **(Opcional) Comente el archivo para explicar su elección.**
   Por ejemplo:

```
# cat  /etc/security/policy.conf
…
# Sets the SHA256 (5) algorithm as default.
```

```
# SHA256 supports 255-character passwords.
# Passwords previously encrypted with MD5 (1) will be encrypted
# with SHA256 (5) when users change their passwords.
#CRYPT_DEFAULT=1
CRYPT_DEFAULT=5
```

En este ejemplo, el nuevo valor de `CRYPT_DEFAULT` es `5`, que es `SHA256`, el algoritmo SHA256. SHA es la sigla en inglés correspondiente al algoritmo de hash seguro. Este algoritmo es un miembro de la familia SHA-2. SHA256 admite contraseñas de 255 caracteres.

3. **(Opcional) Elimine el algoritmo anterior de `CRYPT_ALGORITHM_ALLOWED` para hacer que el nuevo algoritmo se aplique a usuarios existentes.**

   Por ejemplo, para asegurarse de que el algoritmo SHA256 también se aplica a los usuarios existentes, `CRYPT_ALGORITHM_ALLOWED` debe excluir el identificador `1` para MD5.

   Nota - Además, para promover la seguridad de FIPS 140, excluya el algoritmo Blowfish (2a) de la entrada.

   ```
   CRYPT_ALGORITHMS_ALLOW=5,6
   ```

ejemplo 3-4 Restricción de algoritmos de cifrado de contraseña en un entorno heterogéneo

En este ejemplo, el administrador en una red que incluye los sistemas BSD y Linux configura las contraseñas para que se puedan usar en todos los sistemas. Debido a que algunas aplicaciones de red no pueden manejar cifrado `SHA512`, el administrador no incluye su identificador en la lista de algoritmos permitidos. El administrador conserva el algoritmo `SHA256`, `5` como valor para la variable `CRYPT_DEFAULT`. La variable `CRYPT_ALGORITHMS_ALLOW` contiene el identificador `MD5`, que es compatible con sistemas BSD y Linux, y el identificador Blowfish, que es compatible con sistemas BSD. Debido a que `5` es el algoritmo `CRYPT_DEFAULT`, no es necesario incluirlo en la lista `CRYPT_ALGORITHMS_ALLOW`. Sin embargo, con fines de mantenimiento, el administrador coloca `5` en la lista `CRYPT_ALGORITHMS_ALLOW` y los identificadores no utilizados en la lista `CRYPT_ALGORITHMS_DEPRECATE`.

```
CRYPT_ALGORITHMS_ALLOW=1,2a,5
#CRYPT_ALGORITHMS_DEPRECATE=__unix__,md5,6
CRYPT_DEFAULT=5
```

▼ Cómo especificar un nuevo algoritmo de contraseña para un dominio NIS

Cuando los usuarios en un dominio NIS cambian sus contraseñas, el cliente NIS consulta su configuración local de algoritmos en el archivo `/etc/security/policy.conf`. El sistema cliente NIS cifra la contraseña.

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. **Especifique el algoritmo de cifrado de contraseña en el archivo `/etc/security/policy.conf` del cliente NIS.**
2. **Copie el archivo `/etc/security/policy.conf` modificado en cada sistema cliente del dominio NIS.**
3. **Para evitar confusiones, copie el archivo `/etc/security/policy.conf` modificado en el servidor root NIS y en los servidores esclavos.**

▼ Cómo especificar un nuevo algoritmo de contraseña para un dominio LDAP

Cuando el cliente LDAP se ha configurado correctamente, el cliente LDAP puede utilizar los nuevos algoritmos de contraseña. El cliente LDAP se comporta igual que el cliente NIS.

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. **Especifique un algoritmo de cifrado de contraseña en el archivo `/etc/security/policy.conf` del cliente LDAP.**
2. **Copie el archivo `policy.conf` modificado en cada sistema cliente del dominio LDAP.**
3. **Asegúrese de que el archivo `/etc/pam.conf` no utilice un módulo `pam_ldap`.**

   Asegúrese de que un signo de comentario (#) preceda las entradas que incluyen `pam_ldap.so.1`. Además, no utilice la opción `server_policy` con el módulo `pam_authtok_store.so.1`.

   Las entradas PAM en el archivo `pam.conf` del cliente permiten que la contraseña se cifre según la configuración local de algoritmos. Las entradas PAM también permiten que la contraseña se autentique.

   Cuando los usuarios en el dominio LDAP cambian sus contraseñas, el cliente LDAP consulta su configuración local de algoritmos en el archivo `/etc/security/policy.conf`. El sistema cliente LDAP cifra la contraseña. A continuación, el cliente envía la contraseña cifrada, con una etiqueta `{crypt}`, al servidor. La etiqueta indica al servidor que la contraseña ya se ha cifrado. La contraseña se almacena, tal como está, en el servidor. Para la autenticación, el

cliente recupera la contraseña almacenada desde el servidor. A continuación, el cliente compara la contraseña almacenada con la versión cifrada que el cliente acaba de generar a partir de la contraseña introducida del usuario.

Nota - Para aprovechar los controles de política de contraseña en el servidor LDAP, utilice la opción `server_policy` con las entradas `pam_authtok_store` en el archivo `pam.conf`. Las contraseñas se cifran en el servidor LDAP. Para conocer el procedimiento, consulte el Capítulo 4, “Configuración de Oracle Directory Server Enterprise Edition con clientes LDAP” de “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: LDAP ”.

Supervisión y restricción del acceso `root`

De manera predeterminada, el rol `root` se asigna el usuario inicial, y no puede iniciar sesión directamente en el sistema local ni de manera remota en cualquier sistema Oracle Solaris.

▼ Cómo supervisar quién está utilizando el comando `su`

El archivo `sulog` lista cada uso del comando (`su`) del usuario de cambio, no sólo los intentos de `su` que se utilizan para cambiar de usuario a `root`.

El registro de `su` en este archivo se activa de manera predeterminada mediante la siguiente entrada en el archivo `/etc/default/su`:

```
SULOG=/var/adm/sulog
```

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 ”.

- **Supervise el contenido del archivo `/var/adm/sulog` de manera regular.**

```
# more /var/adm/sulog
SU 12/20 16:26 + pts/0 stacey-root
SU 12/21 10:59 + pts/0 stacey-root
SU 01/12 11:11 + pts/0 root-rimmer
SU 01/12 14:56 + pts/0 jdoe-root
SU 01/12 14:57 + pts/0 jdoe-root
```

Las entradas muestran la información siguiente:

- La fecha y la hora en las que el comando se introdujo.
- Si el intento tuvo éxito. Un signo más (+) indica un intento con éxito. Un signo menos (-) indica un intento fallido.
- El puerto desde el que se ha ejecutado el comando.
- El nombre del usuario y el nombre de la identidad cambiada.

Errores más frecuentes

Las entradas que incluyen `???` indican que el terminal de control para el comando `su` no se pueden identificar. Normalmente, las invocaciones del sistema del comando `su` antes de que el escritorio aparezca incluyen `???`, como en `SU 10/10 08:08 + ??? root-root`. Después de que el usuario inicia una sesión de escritorio, el comando `ttynam` devuelve el valor del terminal de control a `sulog`: `SU 10/10 10:10 + pts/3 jdoe-root`.

Las entradas similares a las siguientes pueden indicar que el comando `su` no fue invocado en la línea de comandos: `SU 10/10 10:20 + ??? root-oracle`. Es posible que un usuario de Trusted Extensions haya cambiado al rol `oracle` utilizando una GUI.

▼ Cómo restringir y supervisar inicios de sesión de `root`

Este método permite detectar inmediatamente los intentos de acceso al sistema local por parte del usuario `root`.

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. **Consulte la entrada `CONSOLE` en el archivo `/etc/default/login`.**

   ```
   CONSOLE=/dev/console
   ```

   De manera predeterminada, el dispositivo de consola se establece en `/dev/console`. Con este valor, `root` puede iniciar sesión en la consola. `root` no puede iniciar sesión de manera remota.

2. **Verifique que `root` no pueda iniciar sesión de manera remota.**

   Desde un sistema remoto, intente iniciar sesión como `root`.

   ```
   mach2 % ssh -l root mach1
   Password:      <Type root password of mach1>
   Password:
   Password:
   Permission denied (gssapi-keyex,gssapi-with-mic,publickey,keyboard-interactive).
   ```

En la configuración predeterminada, root es un rol, y los roles no pueden iniciar sesión. Además, en la configuración predeterminada el protocolo ssh impide el inicio de sesión por parte del usuario root.

3. Supervise intentos de convertirse en usuario root.

De manera predeterminada, los intentos de convertirse en usuario root se imprimen en la consola mediante la utilidad SYSLOG.

a. Abra una consola del terminal en el escritorio.

b. En otra ventana, utilice el comando su para convertirse en root.

```
% su -
Password:       <Type root password>
#
```

Se imprime un mensaje en la consola del terminal.

```
Sep 7 13:22:57 mach1 su: 'su root' succeeded for jdoe on /dev/pts/6
```

ejemplo 3-5 Registro de intentos de acceso root

En este ejemplo, los intentos de root no están siendo registrados por SYSLOG. Por lo tanto, el administrador está registrando esos intentos eliminando el comentario de la entrada #CONSOLE=/dev/console en el archivo /etc/default/su.

```
# CONSOLE determines whether attempts to su to root should be logged
# to the named device
#
CONSOLE=/dev/console
```

Cuando un usuario intenta convertirse en root, el intento se imprime en la consola del terminal.

```
SU 09/07 16:38 + pts/8 jdoe-root
```

Errores más frecuentes

Para convertirse en root desde un sistema remoto cuando el archivo /etc/default/login contiene la entrada CONSOLE predeterminada, los usuarios primero deben iniciar sesión con su nombre de usuario. Después de iniciar sesión con su nombre de usuario, los usuarios pueden utilizar el comando su para convertirse en root.

Si la consola muestra una entrada similar a Last login: Wed Sep 7 15:13:11 2011 from mach2, el sistema se configura para permitir inicios de sesión root remotos. Para evitar el acceso remoto de root, cambie la entrada #CONSOLE=/dev/console a CONSOLE=/dev/console en el archivo /etc/default/login. Para saber cómo volver el protocolo ssh al valor predeterminado, consulte la página del comando man sshd_config(4).

Control de acceso a hardware del sistema

Puede proteger el sistema físico mediante la solicitud de una contraseña para obtener acceso a la configuración del hardware. También puede proteger el sistema impidiendo que un usuario use la secuencia de interrupción para salir del sistema de ventanas.

Para proteger el BIOS, consulte la documentación de ese proveedor.

▼ Cómo requerir una contraseña para el acceso al hardware de SPARC

Antes de empezar Se debe convertir en administrador con perfiles de derechos asignados de seguridad de dispositivos, mantenimiento y reparación, o administrador del sistema. 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 una ventana de terminal, active el modo de seguridad de PROM.**

```
# eeprom security-mode=command

Changing PROM password:
New password:      <Type password>
Retype new password:      <Retype password>
```

Seleccione el valor `command` o `full`. Para obtener más información, consulte la página del comando man `eeprom`(1M).

Si, cuando escribe el comando anterior, no se le solicita una contraseña para la PROM, el sistema ya tiene una.

2. **(Opcional) Cambie la contraseña PROM.**

Atención - No olvide la contraseña de la PROM. El hardware no se puede utilizar sin esta contraseña.

```
# eeprom security-password=      Press Return
Changing PROM password:
New password:      <Type password>
Retype new password:      <Retype password>
```

El modo de seguridad y la contraseña nuevos de la PROM entran en vigor inmediatamente. Sin embargo, es más probable que se puedan observar en el próximo inicio.

▼ Cómo desactivar una secuencia de interrupción del sistema

Nota - Algunos sistemas del servidor tienen un conmutador de claves. Cuando el conmutador de claves se establece en la posición segura, el conmutador sustituye la configuración de interrupción de teclado del software. Por lo tanto, los cambios que realice con el siguiente procedimiento podrían no ser implementados.

Antes de empezar Debe convertirse en un administrador con la autorización `solaris.admin.edit/etc/default/kbd` asignada. De manera predeterminada, 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. **Cambie el valor de `KEYBOARD_ABORT` a `disable`.**

   Elimine el comentario de la línea `enable` en el archivo `/etc/default/kbd`. Luego, agregue una línea `disable`:

   ```
   # cat /etc/default/kbd
   …
   # KEYBOARD_ABORT affects the default behavior of the keyboard abort
   # sequence, see kbd(1) for details.  The default value is "enable".
   # The optional value is "disable".  Any other value is ignored.
   …
   #KEYBOARD_ABORT=enable
   KEYBOARD_ABORT=disable
   ```

2. **Actualice los valores predeterminados del teclado.**

   ```
   # kbd -i
   ```

♦ ♦ ♦ CAPÍTULO 4

Control de acceso a dispositivos

Este capítulo proporciona instrucciones paso a paso para proteger dispositivos, además de una sección de referencia. En este capítulo, se tratan los siguientes temas:

- “Configuración de política de dispositivos” [59]
- “Gestión de asignación de dispositivos” [61]
- “Asignación de dispositivos” [67]
- “Protección de dispositivos (referencia)” [71]

Para obtener información general sobre la protección de dispositivos, consulte “Control de acceso a dispositivos” [16].

Configuración de política de dispositivos

La política de dispositivos restringe o impide el acceso a los dispositivos que son una parte integral del sistema. La política se aplica en el núcleo.

El siguiente mapa de tareas hace referencia a los procedimientos de configuración de dispositivos relativos a la política de dispositivos.

TABLA 4-1 Configuración de política de dispositivos (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Ver la política de dispositivos para los dispositivos del sistema.	Muestra los dispositivos y su política de dispositivos.	Cómo ver una política de dispositivos [60]
Auditar cambios en la política de dispositivos.	Registra los cambios en la política de dispositivos en la pista de auditoría.	Cómo auditar cambios en la política de dispositivos [60]
Acceder a `/dev/arp`.	Obtiene información MIB-II IP de Oracle Solaris.	Cómo recuperar información MIB-II IP de un dispositivo `/dev/*` [61]

▼ Cómo ver una política de dispositivos

- **Visualice la política de dispositivos para todos los dispositivos del sistema.**

```
% getdevpolicy | more
DEFAULT
read_priv_set=none
write_priv_set=none
ip:*
read_priv_set=net_rawaccess
write_priv_set=net_rawaccess
…
```

ejemplo 4-1 Visualización de la política de dispositivos para un dispositivo específico

En este ejemplo, se muestra la política de dispositivos para tres dispositivos.

```
% getdevpolicy /dev/allkmem /dev/ipsecesp /dev/bge
/dev/allkmem
read_priv_set=all
write_priv_set=all
/dev/ipsecesp
read_priv_set=sys_net_config
write_priv_set=sys_net_config
/dev/bge
read_priv_set=net_rawaccess
write_priv_set=net_rawaccess
```

▼ Cómo auditar cambios en la política de dispositivos

De manera predeterminada, la clase de auditoría `as` incluye el evento de auditoría `AUE_MODDEVPLCY`.

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 ”.

- **Preseleccione la clase de auditoría que incluye el evento de auditoría `AUE_MODDEVPLCY`.**

```
# auditconfig -getflags
current-flags
# auditconfig -setflags current-flags,as
```

Para obtener instrucciones detalladas, consulte “Cómo preseleccionar clases de auditoría” de “Gestión de auditoría en Oracle Solaris 11.2 ”.

▼ Cómo recuperar información MIB-II IP de un dispositivo /dev/*

Las aplicaciones que recuperan información MIB-II IP de Oracle Solaris deben abrir /dev/arp, no /dev/ip.

1. **Determine la política de dispositivos en /dev/ip y /dev/arp.**

```
% getdevpolicy /dev/ip /dev/arp
/dev/ip
read_priv_set=net_rawaccess
write_priv_set=net_rawaccess
/dev/arp
read_priv_set=none
write_priv_set=none
```

Tenga en cuenta que se requiere el privilegio net_rawaccess para la lectura y escritura en /dev/ip. No se requieren privilegios para /dev/arp.

2. **Abra /dev/arp y utilice los módulos tcp y udp.**

No se requieren privilegios. Este método es equivalente a abrir /dev/ip y utilizar los módulos arp, tcp y udp. Como la apertura de /dev/ip requiere ahora un privilegio, es preferible usar el método /dev/arp.

Gestión de asignación de dispositivos

La asignación de dispositivos se suele implementar en sitios que requieren un nivel adicional de seguridad de dispositivos. Generalmente, los usuarios deben tener autorización para acceder a dispositivos asignables.

El siguiente mapa de tareas hace referencia a los procedimientos para activar y configurar la asignación de dispositivos, y para la resolución de problemas de la asignación de dispositivos. La asignación de dispositivos está desactivada de manera predeterminada. Después de que la asignación de dispositivos esté activada, consulte “Asignación de dispositivos” [67] para obtener instrucciones sobre la asignación de dispositivos.

TABLA 4-2 Gestión de asignación de dispositivos (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Permitir que un dispositivo pueda asignarse.	Permite que un dispositivo se asigne a un usuario a la vez.	Cómo activar la asignación de dispositivos [62]

Tarea	Descripción	Para obtener instrucciones
Desactivar la asignación de dispositivos.	Elimina las restricciones de asignación de todos los dispositivos.	
Autorizar a los usuarios a asignar un dispositivo.	Asigna autorizaciones de asignación de dispositivos a los usuarios.	Cómo autorizar a usuarios para que asignen un dispositivo [63]
Ver los dispositivos asignables del sistema.	Muestra los dispositivos que se pueden asignar y el estado del dispositivo.	Cómo ver la información de asignación de un dispositivo [64]
Asignar de manera forzada un dispositivo.	Asigna un dispositivo a un usuario que tiene una necesidad inmediata.	Cómo asignar de manera forzada un dispositivo [64]
Desasignar de manera forzada un dispositivo.	Desasigna un dispositivo que está asignado actualmente a un usuario.	Cómo desasignar de manera forzada un dispositivo [65]
Cambiar las propiedades de asignación de un dispositivo.	Cambia los requisitos para asignar un dispositivo.	Cómo cambiar los dispositivos que se pueden asignar [65]
Auditar la asignación de dispositivos.	Registra la asignación de dispositivos en la pista de auditoría.	Cómo auditar la asignación de dispositivos [66]
Crear una secuencia de comandos device-clean.	Depura datos de un dispositivo físico.	"Redacción de secuencias nuevas de comandos device-clean" [78]

▼ Cómo activar la asignación de dispositivos

Antes de empezar Debe convertirse en un administrador con el perfil de derechos de seguridad de dispositivo 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. Active el servicio de asignación de dispositivos y verifique que el servicio esté activado.

```
# svcadm enable svc:/system/device/allocate
# svcs -x allocate
svc:/system/device/allocate:default (device allocation)
State: online since September 10, 2011 01:10:11 PM PDT
See: allocate(1)
See: deallocate(1)
See: list_devices(1)
See: device_allocate(1M)
See: mkdevalloc(1M)
See: mkdevmaps(1M)
See: dminfo(1M)
See: device_maps(4)
```

```
See: /var/svc/log/system-device-allocate:default.log
Impact: None.
```

2. **Para desactivar el servicio de asignación de dispositivos, utilice el subcomando `disable`.**

```
# svcadm disable device/allocate
```

▼ Cómo autorizar a usuarios para que asignen un dispositivo

Antes de empezar Debe convertirse en un administrador con el perfil de derechos de seguridad de usuario asignado. Los perfiles de derechos deben incluir la autorización `solaris.auth.delegate`. 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 perfil de derechos que incluya la autorización y los comandos adecuados.**

   Generalmente, debe crear un perfil de derechos que incluya la autorización `solaris.device.allocate`. Siga las instrucciones en “Cómo crear un perfil de derechos” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”. Otorgue al perfil de derechos las propiedades adecuadas, como las siguientes:

   - Nombre del perfil de derechos: `Device Allocation`
   - Autorizaciones otorgadas: `solaris.device.allocate`
   - Comandos con privilegios: `mount` con privilegio `sys_mount` y `umount` con privilegio `sys_mount`

2. **(Opcional) Cree un rol para el perfil de derechos.**

   Para ver el procedimiento paso a paso, consulte “Asignación de derechos a usuarios” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”. Utilice las siguientes propiedades del rol como guía:

   - Nombre del rol: `devicealloc`
   - Nombre completo del rol: `Device Allocator`
   - Descripción del rol: `Allocates and mounts allocated devices`
   - Perfil de derechos: `Device Allocation`

     Este perfil de derechos debe ser el primero de la lista de perfiles incluidos en el rol.

3. **Asigne el perfil de derechos a usuarios autorizados o roles autorizados.**

4. **Enseñe a los usuarios cómo utilizar la asignación de dispositivos.**

Para ver ejemplos de cómo asignar medios extraíbles, consulte Cómo asignar un dispositivo [67].

▼ Cómo ver la información de asignación de un dispositivo

Antes de empezar Complete Cómo activar la asignación de dispositivos [62].

Debe convertirse en un administrador con el perfil de derechos de seguridad de dispositivo 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 ".

- **Visualice información sobre los dispositivos asignables en el sistema.**

```
# list_devices device-name
```

Donde *device-name* es uno de los siguientes:

- `audio`[*n*]: micrófono y altavoz.
- `rmdisk`[*n*]: dispositivo de medios extraíbles, como una unidad flash USB.
- `sr`[*n*]: unidad de CD-ROM.
- `st`[*n*]: unidad de cinta.

Errores más frecuentes Si el comando `list_devices` devuelve un mensaje de error similar al siguiente, es posible que la asignación de dispositivos no esté activada o que usted no cuente con permisos suficientes para recuperar la información.

```
list_devices: No device maps file entry for specified device.
```

Para que el comando se ejecute correctamente, active la asignación de dispositivos y asuma un rol con la autorización `solaris.device.revoke`.

▼ Cómo asignar de manera forzada un dispositivo

La asignación forzada se utiliza cuando alguien ha olvidado desasignar un dispositivo. La asignación forzada también se puede utilizar cuando un usuario tiene una necesidad inmediata de un dispositivo.

Antes de empezar Debe convertirse en un administrador con la autorización `solaris.device.revoke` asignada. 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 si tiene las autorizaciones adecuadas en el rol.**

```
$ auths
solaris.device.allocate solaris.device.revoke
```

2. **Asigne de manera forzada el dispositivo al usuario que lo necesita.**

   En este ejemplo, la unidad flash USB se asigna de manera forzada al usuario `jdoe`.

```
$ allocate -U jdoe
```

▼ Cómo desasignar de manera forzada un dispositivo

Los dispositivos que un usuario ha asignado no se desasignan automáticamente cuando finaliza el proceso o cuando el usuario cierra la sesión. La desasignación forzada se utiliza cuando un usuario ha olvidado desasignar un dispositivo.

Antes de empezar Debe convertirse en un administrador con la autorización `solaris.device.revoke` asignada. 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 si tiene las autorizaciones adecuadas en el rol.**

```
$ auths
solaris.device.allocate solaris.device.revoke
```

2. **Desasigne el dispositivo de manera forzada.**

   En este ejemplo, una impresora se desasigna de manera forzada para que quede disponible para asignación por otro usuario.

```
$ deallocate -f /dev/lp/printer-1
```

▼ Cómo cambiar los dispositivos que se pueden asignar

Antes de empezar La asignación de dispositivos debe estar activada para que este procedimiento se realice correctamente. Para activar la asignación de dispositivos, consulte Cómo activar la asignación de dispositivos [62]. Debe asumir el rol `root`.

- **Cambie el quinto campo en la entrada del dispositivo del archivo `device_allocate` para especificar si se requiere autorización o especifique la autorización `solaris.device.allocate`.**

```
audio;audio;reserved;reserved;solaris.device.allocate;/etc/security/lib/audio_clean
fd0;fd;reserved;reserved;solaris.device.allocate;/etc/security/lib/fd_clean
sr0;sr;reserved;reserved;solaris.device.allocate;/etc/security/lib/sr_clean
```

Donde `solaris.device.allocate` indica que un usuario debe tener la autorización `solaris.device.allocate` para utilizar el dispositivo.

ejemplo 4-2 Permiso para que cualquier usuario asigne un dispositivo

En el ejemplo siguiente, cualquier usuario del sistema puede asignar cualquier dispositivo. El quinto campo en cada entrada de dispositivo del archivo `device_allocate` se cambió al símbolo arroba (`@`).

```
# pfedit /etc/security/device_allocate
audio;audio;reserved;reserved;@;/etc/security/lib/audio_clean
fd0;fd;reserved;reserved;@;/etc/security/lib/fd_clean
sr0;sr;reserved;reserved;@;/etc/security/lib/sr_clean
…
```

ejemplo 4-3 Prevención de uso de algunos dispositivos periféricos

En el ejemplo siguiente, el dispositivo de audio no se puede utilizar. El quinto campo en la entrada del dispositivo de audio del archivo `device_allocate` se cambió a un asterisco (*).

```
# pfedit /etc/security/device_allocate
audio;audio;reserved;reserved;*;/etc/security/lib/audio_clean
fd0;fd;reserved;reserved;solaris device.allocate;/etc/security/lib/fd_clean
sr0;sr;reserved;reserved;solaris device.allocate;/etc/security/lib/sr_clean
…
```

ejemplo 4-4 Prevención de uso de todos los dispositivos periféricos

En el ejemplo siguiente, no se puede utilizar ningún dispositivo periférico. El quinto campo en cada entrada de dispositivo del archivo `device_allocate` se cambió a un asterisco (*).

```
# pfedit /etc/security/device_allocate
audio;audio;reserved;reserved;*;/etc/security/lib/audio_clean
fd0;fd;reserved;reserved;*;/etc/security/lib/fd_clean
sr0;sr;reserved;reserved;*;/etc/security/lib/sr_clean
…
```

▼ Cómo auditar la asignación de dispositivos

De manera predeterminada, los comandos de asignación de dispositivos se encuentran en la clase de auditoría `other`.

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 ”.

- **Preseleccione la clase de auditoría `ot`.**

```
$ auditconfig -getflags
current-flags
$ auditconfig -setflags current-flags,ot
```

Para obtener instrucciones detalladas, consulte “Cómo preseleccionar clases de auditoría” de “Gestión de auditoría en Oracle Solaris 11.2 ”.

Asignación de dispositivos

La asignación de dispositivos reserva el uso de un dispositivo a un usuario a la vez. Los dispositivos que requieren un punto de montaje deben montarse. Los siguientes procedimientos muestran a los usuarios la manera de asignar dispositivos.

▼ Cómo asignar un dispositivo

Antes de empezar La asignación de dispositivos debe estar activada, como se describe en Cómo activar la asignación de dispositivos [62]. Si se requiere autorización, el usuario debe contar con la autorización.

1. **Asigne el dispositivo.**

   Especifique el nombre del dispositivo.

```
% allocate device-name
```

2. **Verifique que el dispositivo esté asignado repitiendo el comando.**

```
% allocate device-name
allocate. Device already allocated.
```

ejemplo 4-5 Asignación de un micrófono

En este ejemplo, el usuario `jdoe` asigna el micrófono: `audio0`.

```
% whoami
jdoe
% allocate audio0
```

ejemplo 4-6 Asignación de una impresora

En este ejemplo, un usuario asigna una impresora. Nadie más puede imprimir en `printer-1` hasta que el usuario la haya desasignado o hasta que la impresora se asigne de manera forzada a otro usuario.

```
% allocate /dev/lp/printer-1
```

Para ver un ejemplo de una desasignación forzada, consulte Cómo desasignar de manera forzada un dispositivo [65].

ejemplo 4-7 Asignación de una unidad flash USB

En este ejemplo, un usuario asigna una unidad flash USB, `rmdisk1`.

```
% allocate rmdisk1
```

Errores más frecuentes

Si el comando `allocate` no puede asignar el dispositivo, se muestra un mensaje de error en la ventana de consola. Para obtener una lista de los mensajes de error de asignación, consulte la página del comando man `allocate`(1).

▼ Cómo montar un dispositivo asignado

Los dispositivos se montan automáticamente si se le otorgan los privilegios adecuados. Siga este procedimiento si el dispositivo no logra montarse.

Antes de empezar

Ha asignado el dispositivo. Se le asignaron los privilegios requeridos para montar el dispositivo, como se describe en Cómo autorizar a usuarios para que asignen un dispositivo [63].

1. **Asuma un rol que permita asignar y montar un dispositivo.**

   ```
   % su - role-name
   Password:       <Type role-name password>
   $
   ```

2. **Cree y proteja un punto de montaje en el directorio principal del rol.**
   Únicamente debe realizar este paso la primera vez que necesita un punto de montaje.

   ```
   $ mkdir mount-point ; chmod 700 mount-point
   ```

3. **Enumere los dispositivos asignables.**

   ```
   $ list_devices -l
   List of allocatable devices
   ```

4. **Asigne el dispositivo.**
   Especifique el nombre del dispositivo.

```
$ allocate device-name
```

5. Monte el dispositivo.

```
$ mount -o ro -F filesystem-type device-path mount-point
```

`-o ro`	Indica que el dispositivo se montará en el modo de sólo lectura. Utilice `-o rw` para que el dispositivo pueda escribirse.
`-F` *filesystem-type*	Indica el formato del sistema de archivos del dispositivo. Generalmente, un CD-ROM se formatea con un sistema de archivos HSFS. Un disquete suele formatearse con un sistema de archivos PCFS.
device-path	Indica la ruta del dispositivo. La salida del comando `list_devices -l` incluye *ruta_dispositivo*.
mount-point	Indica el punto de montaje creado en el Paso 2.

ejemplo 4-8 Asignación de una unidad de CD-ROM

En este ejemplo, un usuario asume un rol que permite asignar y montar una unidad de CD-ROM: `sr0`. La unidad está formateada como un sistema de archivos HSFS.

```
% roles
devicealloc
% su - devicealloc
Password:       <Type devicealloc password>
$ mkdir /home/devicealloc/mymnt
$ chmod 700 /home/devicealloc/mymnt
$ list_devices -l
...
device: sr0 type: sr files: /dev/sr0 /dev/rsr0 /dev/dsk/c0t2d0s0 ...
...
$ allocate sr0
$ mount -o ro -F hsfs /dev/sr0 /home/devicealloc/mymnt
$ cd /home/devicealloc/mymnt ; ls
List of the contents of CD-ROM
```

Errores más frecuentes

Si el comando `mount` no puede montar el dispositivo, se muestra un mensaje de error: `mount: insufficient privileges`. Compruebe lo siguiente:

- Verifique que está ejecutando el comando `mount` en un shell de perfil. Si asumió un rol, el rol tiene un shell de perfil. Si es un usuario y se le asignó un perfil con el comando `mount`, debe crear un shell de perfil. Para obtener una lista de shells de perfiles disponibles, consulte la página del comando man `pfexec`(1).
- Verifique que es el propietario del punto de montaje especificado. Debe tener acceso de lectura, escritura y ejecución al punto de montaje.

Póngase en contacto con el administrador si todavía no puede montar el dispositivo asignado. Consultar "Cómo resolver problemas de las asignaciones de derechos" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 " es un punto de partida.

▼ Cómo desasignar un dispositivo

La desasignación permite que otros usuarios asignen y utilicen el dispositivo cuando usted haya terminado.

Antes de empezar Debe haber asignado el dispositivo. Para obtener más información, consulte Cómo asignar un dispositivo [67].

1. **Si el dispositivo está montado, desmóntelo.**

```
$ cd $HOME
$ umount mount-point
```

2. **Desasigne el dispositivo.**

```
$ deallocate device-name
```

ejemplo 4-9 Desasignación de un micrófono

En este ejemplo, el usuario `jdoe` desasigna el micrófono: `audio`.

```
% whoami
jdoe
% deallocate audio0
```

ejemplo 4-10 Desasignación de una unidad de CD-ROM

En este ejemplo, el rol de asignador de dispositivos desasigna una unidad de CD-ROM. Después de que se imprime el mensaje, se expulsa el CD-ROM.

```
$ whoami
devicealloc
$ cd /home/devicealloc
$ umount /home/devicealloc/mymnt
$ ls /home/devicealloc/mymnt
$
$ deallocate sr0
/dev/sr0:      326o
/dev/rsr0:     326o
…
sr_clean: Media in sr0 is ready.  Please, label and store safely.
```

Protección de dispositivos (referencia)

Los dispositivos en Oracle Solaris están protegidos por una política de dispositivos en núcleo. Los dispositivos periféricos se pueden proteger mediante la asignación de dispositivos. La asignación de dispositivos se activa de manera opcional y se aplica en el nivel de usuario.

Comandos de la política de dispositivos

Los comandos de gestión de dispositivos administran la política de dispositivos en archivos locales. La política de dispositivos puede incluir requisitos de privilegios. Los usuarios asignados a los perfiles de derechos de seguridad de dispositivos y de gestión de dispositivos pueden gestionar dispositivos.

En la siguiente tabla, se muestran los comandos de gestión de dispositivos.

TABLA 4-3 Comandos de gestión de dispositivos

Comando	Objetivo
`add_drv`(1M)	Agrega un nuevo controlador de dispositivos a un sistema en ejecución. Contiene opciones para agregar la política de dispositivos al nuevo dispositivo. Generalmente, este comando se invoca en una secuencia de comandos cuando se está instalando un controlador de dispositivos.
`devfsadm`(1M)	Administra los dispositivos y los controladores de dispositivos en un sistema en ejecución. También carga la política de dispositivos. El comando `devfsadm` permite la limpieza de enlaces `/dev` sin referencia a dispositivos de disco, cinta, puerto, audio y pseudodispositivos. Los dispositivos para un controlador con nombre también se pueden volver a configurar.
`getdevpolicy`(1M)	Muestra la política asociada con uno o varios dispositivos. Cualquier usuario puede ejecutar este comando.
`rem_drv`(1M)	Elimina un dispositivo o un controlador de dispositivos.
`update_drv`(1M)	Actualiza los atributos de un controlador de dispositivos existente. Contiene opciones para actualizar la política de dispositivos para el dispositivo. Generalmente, este comando se invoca en una secuencia de comandos cuando se está instalando un controlador de dispositivos.

Asignación de dispositivos

La asignación de dispositivos puede proteger su sitio contra pérdida de datos, virus informáticos y otras infracciones de seguridad. A diferencia de la política de dispositivos, la asignación de dispositivos es opcional. La asignación de dispositivos utiliza autorizaciones para limitar el acceso a los dispositivos asignables.

Componentes de la asignación de dispositivos

Los componentes del mecanismo de asignación de dispositivos son los siguientes:

- El servicio `svc:/system/device/allocate`. Para obtener más información, consulte la página del comando man `smf`(5) y las páginas del comando man para los comandos de asignación de dispositivos.
- Los comandos `allocate`, `deallocate`, `dminfo` y `list_devices`. Para obtener más información, consulte “Comandos de asignación de dispositivos” [73].
- Los perfiles de derechos de seguridad de dispositivos y de gestión de dispositivos. Para obtener más información, consulte “Perfiles de derechos de asignación de dispositivos” [72].
- Secuencias de comandos device-clean para cada dispositivo asignable.

Estos comandos y las secuencias de comandos utilizan los siguientes archivos locales para implementar la asignación de dispositivos:

- El archivo `/etc/security/device_allocate`. Para obtener más información, consulte la página del comando man `device_allocate`(4).
- El archivo `/etc/security/device_maps`. Para obtener más información, consulte la página del comando man `device_maps`(4).
- Un archivo de bloqueo, en el directorio `/etc/security/dev`, para cada dispositivo asignable.
- Los atributos modificados de los archivos de bloqueo que están asociados con cada dispositivo asignable.

Servicio de asignación de dispositivos

El servicio `svc:/system/device/allocate` controla la asignación de dispositivos. Este servicio está desactivado de manera predeterminada.

Perfiles de derechos de asignación de dispositivos

Los perfiles de derechos de seguridad de dispositivos y de gestión de dispositivos son necesarios para la gestión de dispositivos y la asignación de dispositivos.

Estos perfiles de derechos incluyen las siguientes las autorizaciones:

- `solaris.device.allocate`: necesaria para asignar un dispositivo
- `solaris.device.cdrw`: necesaria para leer y escribir un CD-ROM

- `solaris.device.config`: necesaria para configurar los atributos de un dispositivo
- `solaris.device.mount.alloptions.fixed`: necesaria para especificar opciones de montaje cuando se monta un dispositivo fijo
- `solaris.device.mount.alloptions.removable`: necesaria para especificar opciones de montaje cuando se monta un dispositivo extraíble
- `solaris.device.mount.fixed`: necesaria para montar un dispositivo fijo
- `solaris.device.mount.removable`: necesaria para montar un dispositivo extraíble
- `solaris.device.revoke`: necesaria para revocar o recuperar un dispositivo

Comandos de asignación de dispositivos

Con opciones de mayúsculas, los comandos `allocate`, `deallocate` y `list_devices` son comandos administrativos. De lo contrario, estos comandos son comandos de usuario. En la siguiente tabla, se muestran los comandos de asignación de dispositivos.

TABLA 4-4 Comandos de asignación de dispositivos

Página del comando man	Objetivo
`allocate`(1)	Reserva un dispositivo asignable para que lo utilice un usuario. De manera predeterminada, un usuario debe tener la autorización `solaris.device.allocate` para poder asignar un dispositivo. Puede modificar el archivo `device_allocate` para que no requiera autorización del usuario. De esa manera, cualquier usuario del sistema puede solicitar la asignación del dispositivo para su uso.
`deallocate`(1)	Elimina la reserva de asignación de un dispositivo.
`dminfo`(1M)	Busca un dispositivo asignable por tipo de dispositivo, nombre del dispositivo y nombre de ruta completa.
`list_devices`(1)	Muestra el estado de los dispositivos asignables. Muestra todos los archivos especiales del dispositivo que están asociados con los dispositivos enumerados en el archivo `device_maps`. Con la opción `-U`, se muestran los dispositivos que se pueden asignar o que están asignados al ID de usuario especificado. Esta opción permite comprobar cuáles dispositivos son asignables y cuáles están asignados a otro usuario. Debe tener la autorización `solaris.device.revoke`.

Autorizaciones para los comandos de asignación

De manera predeterminada, los usuarios deben tener la autorización `solaris.device.allocate` para reservar un dispositivo asignable. Para crear un perfil de derechos a fin de incluir la autorización `solaris.device.allocate`, consulte Cómo autorizar a usuarios para que asignen un dispositivo [63].

Los administradores deben tener la autorización `solaris.device.revoke` para cambiar el estado de asignación de cualquier dispositivo. Por ejemplo, la opción `-U` de los comandos `allocate` y `list_devices`, y la opción `-F` del comando `deallocate` requieren la autorización `solaris.device.revoke`.

Para obtener más información, consulte “Comandos seleccionados que requieren autorizaciones” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

Estado de error de asignación

Un dispositivo está en un *estado de error de asignación* cuando el comando `deallocate` no puede realizar la desasignación o cuando el comando `allocate` no puede realizar la asignación. Cuando un dispositivo asignable se encuentra en un estado de error de asignación, se debe desasignar de manera forzada. Sólo un usuario o un rol con el perfil de derechos de gestión de dispositivos o de seguridad de dispositivos puede manejar un estado de error de asignación.

El comando `deallocate` con la opción `-F` fuerza la desasignación. O bien, puede usar `allocate -U` para asignar el dispositivo a un usuario. Una vez que el dispositivo está asignado, puede investigar los mensajes de error que aparecen. Después de corregir los problemas con el dispositivo, puede desasignarlo de manera forzada.

Archivo `device_maps`

Los mapas de dispositivos se crean al configurar la asignación de dispositivos. El archivo `/etc/security/device_maps` incluye los nombres de los dispositivos, los tipos de dispositivos y los archivos especiales de los dispositivos que están asociados con cada dispositivo asignable.

El archivo `device_maps` define las asignaciones de archivos especiales para cada dispositivo, que en muchos casos no son intuitivas. Este archivo permite que los programas descubran qué archivos especiales de dispositivos se deben asignar a determinados dispositivos. Puede utilizar el comando `dminfo`, por ejemplo, para recuperar el nombre del dispositivo, el tipo de dispositivo y los archivos especiales del dispositivo que se deben especificar al configurar un dispositivo asignable. El comando `dminfo` utiliza el archivo `device_maps` para comunicar esta información.

Cada dispositivo se representa con una entrada de una línea con el siguiente formato:

device-name:*device-type*:*device-list*

EJEMPLO 4-11 Ejemplo de entrada `device_maps`

El siguiente ejemplo muestra una entrada en un archivo `device_maps`.

```
audio0:\
audio:\
/dev/audio /dev/audioctl /dev/dsp /dev/dsp0 /dev/mixer0 /dev/sound/0
/dev/sound/0ctl /dev/sound/audio810\:0mixer /dev/sound/audio810\:0dsp
/dev/sound/audio810\:0 /dev/sound/audio810\:0ctl
```

Las líneas en el archivo `device_maps` pueden finalizar con una barra diagonal inversa (\) para continuar una entrada en la línea siguiente. También se pueden incluir comentarios. Un signo de almohadilla (#) indica que hay comentarios en todo el texto subsiguiente hasta la siguiente línea nueva que no está inmediatamente precedida por una barra diagonal inversa. En todos los campos, se permiten espacios iniciales y finales. Los campos se definen del modo siguiente:

device-name — Especifica el nombre del dispositivo. Para obtener una lista de los nombres actuales de dispositivos, consulte Cómo ver la información de asignación de un dispositivo [64].

device-type — Especifica el tipo de dispositivo genérico. El nombre genérico es el nombre para la clase de dispositivos, como `st`, `fd`, `rmdisk` o `audio`. El campo *device-type* agrupa lógicamente dispositivos relacionados.

device-list — Muestra los archivos especiales del dispositivo que están asociados con el dispositivo físico. *device-list* debe contener todos los archivos especiales que permiten el acceso a un dispositivo determinado. Si la lista está incompleta, un usuario malintencionado podrá obtener o modificar información privada. Las entradas válidas para el campo *device-list* reflejan los archivos del dispositivo que están ubicados en el directorio `/dev`.

Archivo `device_allocate`

Puede modificar el archivo `/etc/security/device_allocate` para cambiar dispositivos de asignables a no asignables, o para agregar nuevos dispositivos.

Una entrada en el archivo `device_allocate` no significa que el dispositivo es asignable, a menos que la entrada indique específicamente que el dispositivo es asignable.

En el archivo `device_allocate`, cada dispositivo se representa con una entrada de una línea con el siguiente formato:

device-name`;`*device-type*`;reserved;reserved;`*auths*`;`*device-exec*

El siguiente ejemplo muestra un archivo `device_allocate` de ejemplo.

```
st0;st;;;;/etc/security/lib/st_clean
fd0;fd;;;;/etc/security/lib/fd_clean
```

```
sr0;sr;;;;/etc/security/lib/sr_clean
audio;audio;;;*;/etc/security/lib/audio_clean
```

Observe el asterisco (*) en el quinto campo de la entrada del dispositivo `audio`.

Las líneas en el archivo `device_allocate` pueden finalizar con una barra diagonal inversa (\) para continuar una entrada en la línea siguiente. También se pueden incluir comentarios. Un signo de almohadilla (#) indica que hay comentarios en todo el texto subsiguiente hasta la siguiente línea nueva que no está inmediatamente precedida por una barra diagonal inversa. En todos los campos, se permiten espacios iniciales y finales. Los campos se definen del modo siguiente:

device-name
: Especifica el nombre del dispositivo. Para obtener una lista de los nombres actuales de dispositivos, consulte Cómo ver la información de asignación de un dispositivo [64].

device-type
: Especifica el tipo de dispositivo genérico. El nombre genérico es el nombre para la clase de dispositivos, como `st`, `fd` y `sr`. El campo *device-type* agrupa lógicamente dispositivos relacionados. Cuando permita que un dispositivo pueda asignarse, recupere el nombre del dispositivo del campo *tipo_dispositivo* en el archivo `device_maps`.

`reserved`
: Oracle reserva para uso futuro los dos campos marcados como `reserved`.

auths
: Especifica si el dispositivo es asignable. Un asterisco (`*`) en este campo indica que el dispositivo no es asignable. Una cadena de autorización, o un campo vacío, indica que el dispositivo es asignable. Por ejemplo, la cadena `solaris.device.allocate` en el campo *auths* indica que se necesita la autorización `solaris.device.allocate` para poder asignar el dispositivo. Un símbolo arroba (`@`) en este archivo indica que cualquier usuario puede asignar el dispositivo.

device-exec
: Proporciona el nombre de ruta de una secuencia de comandos que se debe invocar para tratamiento especial, como limpieza y protección contra la reutilización del objeto durante el proceso de asignación. La secuencia de comandos *device-exec* se ejecuta cuando el comando `deallocate` se ejecuta en el dispositivo.

Por ejemplo, la entrada siguiente para el dispositivo `sr0` indica que un usuario que cuente con la autorización `solaris.device.allocate` puede asignar la unidad de CD-ROM:

```
sr0;sr;reserved;reserved;solaris.device.allocate;/etc/security/lib/sr_clean
```

Puede decidir aceptar los servicios predeterminados y sus características definidas. Después de instalar un dispositivo nuevo, puede modificar las entradas. Los dispositivos que requieren asignación antes de su uso deben definirse en los archivos `device_allocate` y `device_maps` del

sistema de ese dispositivo. En la actualidad, las unidades de cinta de cartucho, las unidades de disquete, las unidades de CD-ROM, los dispositivos de medios extraíbles y los chips de audio se consideran asignables. Estos tipos de dispositivos tienen secuencias de comandos device-clean.

Nota - Las unidades de cinta Xylogics o Archive también utilizan la secuencia de comandos `st_clean` proporcionada para los dispositivos SCSI. Debe crear sus propias secuencias de comandos device-clean para otros dispositivos, como terminales, tabletas gráficas y otros dispositivos asignables. La secuencia de comandos debe cumplir con los requisitos de reutilización de objetos para ese tipo de dispositivo.

Secuencias de comandos device-clean

La asignación de dispositivos cumple parte de lo que se conoce como requisito de *reutilización de objetos*. Las secuencias de comandos device-clean abordan el requisito de seguridad que establece que todos los datos utilizables deben depurarse de un dispositivo físico antes de volver a utilizarlo. Los datos se limpian antes de que otro usuario asigne el dispositivo. De manera predeterminada, las unidades de cinta de cartucho, las unidades de disquete, las unidades de CD-ROM y los dispositivos de audio requieren secuencias de comandos device-clean, las cuales Oracle Solaris proporciona. Esta sección describe qué acciones realizan las secuencias de comandos device-clean.

Secuencia de comandos device-clean para cintas

La secuencia de comandos `st_clean` admite tres dispositivos de cinta:

- Cinta SCSI de ¼ de pulgada
- Cinta Archive de ¼ de pulgada
- Cinta de carrete abierto de ½ pulgada

La secuencia de comandos `st_clean` usa la opción `rewoffl` para el comando `mt` para limpiar el dispositivo. Para obtener más información, consulte la página del comando man `mt(1)`. Si la secuencia de comandos se ejecuta durante el inicio del sistema, la secuencia de comandos consulta el dispositivo para determinar si está en línea. Si el dispositivo está en línea, la secuencia de comandos determina si el dispositivo tiene medios. Los dispositivos de cinta de ¼ de pulgada que tienen medios se colocan en el estado de error de asignación. El estado de error de asignación fuerza al administrador a limpiar manualmente el dispositivo.

Durante el funcionamiento normal del sistema, cuando el comando `deallocate` se ejecuta en modo interactivo, se le indica al usuario que extraiga los medios. La desasignación se retrasa hasta que los medios se hayan extraído del dispositivo.

Secuencias de comandos device-clean para disquetes y unidades de CD-ROM

Las siguientes secuencias de comandos device-clean se proporcionan para disquetes y unidades de CD-ROM:

- Secuencia de comandos **`fd_clean`**: secuencia de comandos device-clean para disquetes.
- Secuencia de comandos **`sr_clean`**: secuencia de comandos device-clean para unidades de CD-ROM.

Las secuencias de comandos utilizan el comando `eject` para extraer los medios de la unidad. Si el comando `eject` falla, el dispositivo se coloca en el estado de error de asignación. Para obtener más información, consulte la página del comando man `eject`(1).

Secuencia de comandos device-clean para audio

Los dispositivos de audio se limpian con una secuencia de comandos `audio_clean`. La secuencia de comandos realiza una llamada del sistema ioctl `AUDIO_GETINFO` para leer el dispositivo. A continuación, la secuencia de comandos realiza una llamada del sistema ioctl `AUDIO_SETINFO` para restablecer la configuración del dispositivo a los valores predeterminados.

Redacción de secuencias nuevas de comandos device-clean

Si agrega más dispositivos asignables al sistema, posiblemente deba crear sus propias secuencias de comandos device-clean. El comando `deallocate` pasa un parámetro a las secuencias de comandos device-clean. El parámetro, que se muestra aquí, es una cadena que contiene el nombre del dispositivo. Para obtener más información, consulte la página del comando man `device_allocate`(4).

clean-script `-[I|i|f|S]` *device-name*

Si las secuencias de comandos device-clean devuelven “`0`” son correctas; si devuelven valores mayores que “`0`”, fallaron. Las opciones `-I`, `-f` y `-S` determinan el modo de ejecución de la secuencia de comandos:

`-I` Se necesita durante el inicio del sistema únicamente. Todas las salidas deben ir a la consola del sistema. Si no se pueden expulsar de manera forzada los medios o si la expulsión falla, el dispositivo debe pasar al estado de error de asignación.

`-i` Similar a la opción `-I`, excepto que se suprime la salida.

`-f`	Se utiliza para la limpieza forzada. La opción es interactiva y asume que el usuario está disponible para responder a las peticiones de datos. Una secuencia de comandos con esta opción debe intentar completar la limpieza si se produce un error en una parte de ésta.
`-S`	Limpieza estándar. La opción es interactiva y asume que el usuario está disponible para responder a las peticiones de datos.

♦ ♦ ♦ CAPÍTULO 5

Servicio de análisis de virus

En este capítulo, se proporciona información sobre el uso del software antivirus y se tratan los siguientes temas:

Acerca del análisis de virus

Los datos están protegidos contra virus por un servicio de análisis, vscan, que utiliza varios *motores de análisis*. Un motor de exploración es una aplicación de terceros que reside en un host externo, que examina un archivo para ver si contiene virus conocidos. Un archivo es un candidato para el análisis de virus si el sistema de archivos admite el servicio vscan, el servicio se ha activado y el tipo de archivo no ha quedado exento. El análisis de virus se realiza en un archivo durante operaciones de apertura y cierre si el archivo no se ha analizado previamente con las definiciones de virus actuales o si el archivo se ha modificado desde el último análisis.

El servicio vscan se puede configurar para que utilice varios motores de análisis. La práctica recomendada es utilizar un mínimo de dos motores de análisis. Las solicitudes para análisis de virus se distribuyen entre todos los motores de análisis disponibles.

El comando vscanadm show enumera los motores de análisis configurados en el sistema.

```
# vscanadm show
max-size=1GB max-size-action=allow
types=+*
no scan engines configured
```

Acerca del servicio vscan

La ventaja del método de análisis en tiempo real es que un archivo se escanea con las últimas definiciones de virus *antes* de que se utilice. Con este enfoque, los virus pueden ser detectados antes de que pongan en peligro los datos.

Cuando un usuario abre un archivo desde el cliente, el proceso de análisis de virus funciona de la siguiente manera:

1. El servicio vscan determina si el archivo debe ser analizado según si el archivo se ha analizado previamente con las definiciones de virus actuales y si el archivo se ha modificado desde el último análisis.

   Si no es necesario un análisis, el proceso termina y se le permite al usuario acceder al archivo
2. Si el análisis es necesario, el archivo se transfiere al motor de análisis.

   Si la transferencia es correcta, el motor analiza el archivo utilizando las definiciones de virus actuales para determinar si el archivo está infectado.

   Si la transferencia falla, el proceso continúa del siguiente modo:

   - El archivo se transfiere al siguiente motor de análisis que pueda analizar el archivo.
   - Si no existe un motor alternativo o no está disponible, el análisis de virus se considera fallido y es posible que no se otorgue acceso al archivo.
3. Si no se detecta un virus, el archivo se etiqueta con un sello de análisis y se le permite al cliente acceder al archivo.

   Si se detecta un virus, el archivo se marca como en cuarentena. Un archivo en cuarentena no se puede leer, ejecutar ni cambiar de nombre pero se puede suprimir. El log del sistema registra el nombre del archivo en cuarentena y el nombre del virus, y, si la auditoría se ha activado, se crea el registro de auditoría con la misma información.

Uso del servicio vscan

El análisis de archivos en busca de virus está disponible cuando se cumplen los siguientes requisitos:

- Al menos un motor de análisis está instalado y configurado.
- Los archivos residen en un sistema de archivos que admite análisis de virus.
- El análisis de virus está activado en un sistema de archivos.
- El servicio vscan está activado.
- El servicio vscan está configurado para analizar archivos del tipo de archivo especificado.

En la siguiente tabla se señalan las tareas que puede realizar para configurar el servicio vscan.

Tarea	Descripción	Para obtener instrucciones
Instalar un motor de análisis.	Instala y configura uno o varios de los productos antivirus de terceros admitidos en Oracle Solaris.	Consulte la documentación del producto.
Activar el sistema de archivos para permitir el análisis de virus.	Permite el análisis de virus en un sistema de archivos ZFS. De manera predeterminada, los análisis están desactivados.	Cómo activar el análisis de virus en un sistema de archivos [83]
Activar el servicio `vscan`.	Inicia el servicio de análisis.	Cómo activar el servicio `vscan` [84]
Agregar un motor de análisis al servicio `vscan`.	Incluye motores de análisis específicos en el servicio `vscan`.	Cómo agregar un motor de análisis [84]
Configurar el servicio `vscan`.	Muestra y modifica las propiedades de `vscan`.	Cómo ver propiedades de Vscan [84] Cómo limitar el tamaño de los archivos analizados [85]
Configurar el servicio `vscan` para tipos de archivos específicos.	Especifica los tipos de archivo que se van a incluir y excluir en un análisis.	Cómo excluir archivos del análisis de virus [85]

▼ Cómo activar el análisis de virus en un sistema de archivos

Utilice el comando del sistema de archivos para permitir el análisis de virus de archivos. Por ejemplo, para incluir un sistema de archivos ZFS en un análisis de virus, utilice el comando `zfs`(1M).

El sistema de archivos ZFS permite que algunas tareas administrativas se deleguen a usuarios específicos. Para obtener más información acerca de la administración delegada, consulte el Capítulo 8, “Administración delegada de ZFS Oracle Solaris” de “Gestión de sistemas de archivos ZFS en Oracle Solaris 11.2 ”.

Antes de empezar Debe convertirse en un administrador con el perfil de derechos de gestión del sistema de archivos ZFS o el perfil de derechos de gestión de almacenamiento ZFS 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 ”.

- **Active el análisis de virus en un sistema de archivos ZFS.**

```
# zfs set vscan=on zfs-file-system
```

Por ejemplo, si el sistema de archivos ZFS es *path*`/pool/volumes/vol1`, escriba el siguiente comando:

```
# zfs set vscan=on path/pool/volumes/vol1
```

▼ Cómo activar el servicio vscan

Antes de empezar Debe convertirse en un administrador con el perfil de derechos de gestión VSCAN 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 ".

- **Active el servicio de detección de virus.**

```
# svcadm enable vscan
```

▼ Cómo agregar un motor de análisis

Antes de empezar Debe convertirse en un administrador con el perfil de derechos de gestión VSCAN 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 agregar un motor de análisis al servicio vscan con propiedades predeterminadas, escriba:**

```
# vscanadm add-engine engineID
```

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

▼ Cómo ver propiedades de Vscan

Antes de empezar Debe convertirse en un administrador con el perfil de derechos de gestión VSCAN 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 ".

- **Visualice las propiedades del servicio vscan, de todos los motores de análisis o de un motor de análisis específico.**
  - **Para ver las propiedades de un motor de análisis específico, escriba:**

```
# vscanadm get-engine engineID
```

  - **Para ver las propiedades de todos los motores de análisis, escriba:**

```
# vscanadm get-engine
```

  - **Para ver una de las propiedades del servicio vscan, escriba:**

```
# vscanadm get -p property
```

Donde *propiedad* es uno de los parámetros descriptos en la página del comando man para el comando `vscanadm`(1M).

Por ejemplo, si desea ver el tamaño máximo de un archivo que se puede analizar, escriba:

```
# vscanadm get max-size
```

▼ Cómo limitar el tamaño de los archivos analizados

Muchos motores de análisis limitan el tamaño de los archivos que analizan, por lo que la propiedad `max-size` del servicio `vscan` se debe establecer en un valor menor o igual que el tamaño máximo permitido del motor de análisis. Luego se define si los archivos que son más grandes que el tamaño máximo, y que por lo tanto no se analizan, son accesibles.

Antes de empezar Debe convertirse en un administrador con el perfil de derechos de gestión VSCAN 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 las propiedades actuales.**

   ```
   # vscanadm show
   ```

2. **Establezca el tamaño máximo para el análisis de virus.**

   Por ejemplo, para establecer un límite de 128 megabytes:

   ```
   # vscanadm set -p max-size=128M
   ```

3. **Especifique que se deniega el acceso a cualquier archivo no analizado debido a su tamaño.**

   ```
   # vscanadm set -p max-size-action=deny
   ```

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

▼ Cómo excluir archivos del análisis de virus

Cuando activa la protección antivirus, puede especificar que todos los archivos de tipos específicos se excluyan del análisis de virus. Debido a que el servicio `vscan` afecta el rendimiento del sistema, puede conservar los recursos del sistema especificando tipos de archivo específicos para el análisis de virus.

Antes de empezar Debe convertirse en un administrador con el perfil de derechos de gestión VSCAN 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 lista de todos los tipos de archivos que se incluyen en el análisis de virus.**

   ```
   # vscanadm get -p types
   ```

2. **Especifique los tipos de archivo que se van a analizar en busca de virus.**

   Por ejemplo:

   - **Para excluir un tipo de archivo específico, por ejemplo el tipo JPEG, del análisis de virus.**

     ```
     # vscanadm set -p types=-jpg,+*
     ```

   - **Para incluir un tipo de archivo específico, como archivos ejecutables, en el análisis de virus.**

     ```
     # vscanadm set -p types=+exe,-*
     ```

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

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 y no por 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 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 usuarios, un permiso que se puede asignar a un rol o a un usuario (o que está integrado en un perfil de derechos) para realizar un tipo de operaciones que, de lo contrario, está prohibido por la política de seguridad. Las autorizaciones se aplican en el nivel de aplicación del usuario, no en el núcleo.

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 procesos permiten a una organización dividir los privilegios del superusuario y asignarlos a usuarios o roles. Los derechos en Oracle Solaris se implementan como privilegios de núcleo, autorizaciones y la capacidad de ejecutar un proceso como UID o GID específicos. 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 sobrescriben los derechos 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 exploración 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 para 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 rol o usuario asignado escriba una contraseña antes de ejecutar una operación desde el perfil. Este comportamiento es similar al comportamiento `sudo`. Se puede configurar el período de tiempo que la contraseña es válida.

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 del Sistema operativo Oracle Solaris, consulte política de auditoría, política en la estructura criptográfica, política de dispositivos, política 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 la política de privilegios extendidos, 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 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 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 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, la facultad o capacidad de realizar una operación en un sistema informático que supera las facultades de un usuario común. Los privilegios de superusuario son todos los derechos que se otorgan a un superusuario. Un usuario con privilegios o una aplicación con privilegios es un usuario o aplicación a los que se les ha 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. Los privilegios también se denominan *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.

protección La modificación de la configuración predeterminada del sistema operativo para eliminar las vulnerabilidades de seguridad inherentes al host.

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, una función de gestión de derechos de usuarios 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 del producto para la versión inicial de Kerberos en sistemas Solaris. Este producto se basa en la tecnología Kerberos V5 que fue desarrollada en el Instituto Tecnológico de Massachusetts (Massachusetts Institute of Technology). SEAM ahora se denomina servicio Kerberos. Aún difiere levemente de la versión de 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 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 de 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 al que se asignan derechos más allá de los derechos de usuario común en un sistema informático. Consulte también usuarios de confianza.

usuarios de confianza Los usuarios que ha decidido que pueden realizar tareas administrativas en cualquier nivel de confianza. Normalmente, los administradores crean los inicios de sesión para usuarios de confianza primero y asignan derechos administrativos que coinciden con el nivel de confianza y habilidad de los usuarios. Estos usuarios, luego, ayudan a configurar y mantener el sistema. También denominados *usuarios con privilegios*.

índice

Números y símbolos

A

D

E

F

G

S

T

U

V

Z