Directrices de seguridad de Oracle® Solaris 11

Referencia: E53925-02
Septiembre de 2014

ORACLE

Contenido

Lista de tablas

Uso de esta documentación

- **Descripción general**: proporciona una descripción general de las funciones de seguridad de Oracle Solaris y las directrices de uso de las funciones para reforzar y proteger un sistema instalado y sus aplicaciones.
- **Destinatarios**: administradores del sistema, administradores de seguridad, desarrolladores de aplicaciones y auditores que desarrollan, implementan o evalúan la seguridad en sistemas Oracle Solaris 11.
- **Conocimiento necesario**: requisitos de seguridad del sitio.

Biblioteca de documentación del producto

En la biblioteca de documentación, que se encuentra en 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 disponen de asistencia a través de Internet en el portal My Oracle Support. Para obtener más información, visite http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info o, si tiene alguna discapacidad auditiva, visite http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs.

Comentarios

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

♦ ♦ ♦ CAPÍTULO 1

Acerca de la seguridad de Oracle Solaris

Oracle Solaris es un sistema operativo para empresas sólido y de primera calidad que ofrece funciones de seguridad comprobadas. Con un sofisticado sistema de seguridad para toda la red que controla la forma en que los usuarios acceden a los archivos, protegen las bases de datos y usan los recursos del sistema, Oracle Solaris 11 se ocupa de los requisitos de seguridad en todas las capas. Mientras que los sistemas operativos tradicionales pueden tener debilidades de seguridad inherentes, la flexibilidad de Oracle Solaris 11 permite satisfacer una variedad de objetivos de seguridad, desde los servidores de la empresa hasta los clientes de escritorio. Oracle Solaris está completamente probado y se admite en una gran variedad de sistemas basados en SPARC y x86 de Oracle y en otras plataformas de hardware de otros proveedores.

Novedades de las funciones de seguridad en Oracle Solaris 11.2

En esta sección, se destaca información para clientes existentes sobre las nuevas funciones de seguridad importantes en esta versión.

- Puede evaluar la conformidad de los sistemas con los estándares de seguridad utilizando el nuevo comando `compliance`. Este comando permite evaluar e informar la conformidad del sistema con referencias de seguridad de estándares del sector, incluido PCI-DSS. Para obtener detalles, consulte la "Guía de cumplimiento de la seguridad de Oracle Solaris 11.2 " y la página del comando man `compliance`(1M).

- La función de estructura criptográfica de Oracle Solaris está validada en FIPS 140-2, Nivel 1 validada para funciones de espacio de usuario y núcleo en las versiones Oracle Solaris 11.1 SRU 5.5 y Oracle Solaris 11.1 SRU 3.
  - Para obtener una lista de los productos validados por Oracle FIPS 140, consulte Oracle FIPS 140 Software Validations (http://www.oracle.com/technetwork/topics/security/fips140-software-validations-1703049.html).
  - Para obtener información acerca de la activación de Modo FIPS 140 en su sistema, consulte "Using a FIPS 140 Enabled System in Oracle Solaris 11.2 ".
- Oracle Solaris 11.1 está certificado según el esquema de criterios comunes de Canadá. Consulte "Certificación EAL4+ de criterios comunes de Oracle Solaris 11" [29].
- El servicio de auditoría puede utilizar Oracle Audit Vault para almacenar, revisar y analizar los registros de auditoría. Consulte "Uso de Oracle Audit Vault and Database Firewall para el almacenamiento y el análisis de registros de auditoría" de "Gestión de auditoría en Oracle Solaris 11.2 ".
- El inicio verificado protege el proceso de inicio contra amenazas en servidores SPARC T5 de Oracle y en servidores SPARC T7 de Oracle. Para obtener más información, consulte "Uso de inicio verificado" de "Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 ".
- Puede proteger las instalaciones de Automatic Installation (AI) con certificados y claves para el servidor de instalación, para sistemas cliente especificados, para todos los clientes de un servicio de instalación especificado y para cualquier otro cliente AI. El AI seguro protege la transmisión de paquetes de Oracle Solaris a los sistemas. Consulte "Aumento de la seguridad para las instalaciones automatizadas" de "Instalación de sistemas Oracle Solaris 11.2 ".
- Hay un nuevo paquete de instalación de grupo disponible, `pkg:/group/system/solaris-minimal-server`. Para obtener una descripción y una comparación de los contenidos del paquete de grupo, consulte "Oracle Solaris 11.2 Package Group Lists ".
- Puede instalar clientes Kerberos mediante el AI para que el cliente sea un sistema Kerberizado en el primer inicio. Consulte "Cómo configurar clientes Kerberos mediante AI" de "Instalación de sistemas Oracle Solaris 11.2 ".
- En esta versión, las zonas globales físicas, denominadas zonas globales inmutables, y las zonas globales virtuales, denominadas zonas de núcleo de Oracle Solaris, pueden ser de sólo lectura. Las zonas globales inmutables son levemente más potentes que las zonas de núcleo, pero tampoco pueden cambiar de manera permanente el hardware ni la configuración del sistema. Las zonas de sólo lectura se inician más rápido y son más seguras que las zonas que permiten escritura.

  Para el mantenimiento, las zonas globales inmutables definen un conjunto especial de procesos denominado base de computación de confianza (TCB), que se puede configurar mediante un inicio de sesión protegido denominado ruta de acceso de confianza. Para obtener más información, consulte el Capítulo 12, "Configuración y administración de zonas inmutables" de "Creación y uso de zonas de Oracle Solaris ". Para obtener información sobre los recursos de configuración de zonas, consulte "Introducción a Zonas de Oracle Solaris ". También consulte las páginas del comando man `mwac`(5) y `tpd`(5).

Las zonas de núcleo de Oracle Solaris son útiles para implementar un sistema compatible. Por ejemplo, puede configurar un sistema compatible, crear un archivo unificado y luego implementar la imagen como una zona de núcleo. Para obtener más información, consulte la página del comando man `solaris-kz`(5), "Creación y uso de zonas del núcleo de Oracle Solaris ", "Descripción general de Oracle Solaris Zones" de "Introducción a los entornos de virtualización de Oracle Solaris 11.2 " y "Uso de Unified Archives para la clonación y la recuperación del sistema en Oracle Solaris 11.2 ".

- Las nuevas funciones en derechos de procesos y usuarios incluyen lo siguiente:
  - control de acceso basado en ubicación y basado en tiempo para servicios PAM,
  - roles predefinidos de roles de autorización gestionados en RBAC (ARMOR),
  - perfiles de derechos que fuerzan a los usuarios a proporcionar una contraseña antes de ejecutar una acción con privilegios.
  - Los perfiles de derechos de observabilidad de red u observabilidad de sistema para ejecutar los comandos de diagnóstico `ipstat`, `tcpstat`, `snoop` y `intrstat` con privilegio y sin ser `root`

  Para obtener detalles, consulte "Novedades de los derechos en Oracle Solaris 11.2" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".
- La versión 2 del intercambio de claves de Internet (IKEv2) proporciona el protocolo IKE más reciente para la gestión automática de claves de paquetes de red protegidos por IPsec. Para obtener detalles, consulte "Novedades de seguridad de red en Oracle Solaris 11.2" de "Protección de la red en Oracle Solaris 11.2 ".
- Oracle Hardware Management Pack (HMP) proporciona herramientas de línea de comandos para configurar y actualizar el firmware. Para obtener información sobre cómo usar HMP de manera segura con otros productos de hardware de Oracle, como conmutadores de red y tarjetas de interfaz de red, consulte "Guía de seguridad de Oracle Hardware Management Pack para Oracle Solaris ".

Seguridad de Oracle Solaris 11 después de la instalación

Oracle Solaris se instala con seguridad predeterminada (SBD). Esta postura de seguridad protege el sistema contra la intrusión y supervisa los intentos de inicio de sesión, entre otras funciones de seguridad.

El sistema de acceso está limitado y supervisado

Cuentas de usuario inicial y de rol `root`: la cuenta de usuario inicial puede iniciar sesión desde la consola. A esta cuenta se le asigna el rol `root`. La contraseña para el usuario inicial y las cuentas `root` es idéntica en la instalación.

- Después del inicio de sesión, el usuario inicial puede asumir el rol `root` para configurar más el sistema. Cuando el usuario asume el rol, se le solicita que cambie la contraseña `root`. Ningún rol puede iniciar sesión de manera directa, ni siquiera el rol `root`.
- Al usuario inicial se le asignan valores predeterminados del archivo `/etc/security/policy.conf`. Entre los valores predeterminados se incluyen el perfil de derechos del usuario de Solaris básico y el perfil de derechos del usuario de la consola. Estos perfiles de derechos permiten a los usuarios leer y escribir en un CD o DVD, ejecutar cualquier otro comando en el sistema sin privilegios, y detener y reiniciar el sistema cuando están en la consola.
- También se asigna a la cuenta de usuario inicial el perfil de derechos del administrador del sistema. Por lo tanto, sin asumir el rol `root`, el usuario inicial tiene algunos derechos administrativos, como el derecho de instalación de software y el de gestión del servicio de nombres.

Requisitos de contraseña: las contraseñas de los usuarios deben tener seis caracteres como mínimo y deben tener al menos dos caracteres alfabéticos y un carácter no alfabético. En las contraseñas, se aplica el algoritmo hash `SHA256`. Cuando cambian la contraseña, todos los usuarios, incluso el rol `root`, deben cumplir con estos requisitos de contraseña.

Acceso a la red limitado: después de la instalación, el sistema queda protegido de la intrusión por medio de la red. El usuario inicial tiene permitido efectuar un inicio de sesión remoto mediante una conexión cifrada y autenticada con el protocolo `ssh`. Este es el único protocolo de red que acepta los paquetes entrantes. La clave `ssh` está envuelta por el algoritmo `AES128`. Con la autenticación y el cifrado establecidos, el usuario puede acceder al sistema remoto sin intercepción, modificación ni falsificación.

Intentos de inicio de sesión registrados: el servicios de auditoría se activa para todos los eventos de `login/logout` (inicio de sesión, cierre de sesión, cambio de usuario, inicio y cierre de una sesión `ssh` y bloqueo de pantalla) y para todos los inicios de sesión que no se pueden atribuir (con errores). Dado que el rol `root` no puede iniciar sesión, se registra el nombre del usuario que está actuando como `root` en la pista de auditoría. El usuario inicial puede revisar los registros de auditoría con un derecho concedido mediante el perfil de derechos del administrador del sistema.

Las protecciones del núcleo, los archivos y el escritorio están en su lugar

Una vez que el usuario inicial inicia sesión, el núcleo, los sistemas de archivos, los archivos del sistema y las aplicaciones de escritorio están protegidos con permisos de archivo, privilegios y derechos de usuario. Los derechos de usuario también se conocen como *control de acceso basado en roles* (RBAC).

Protecciones del núcleo: muchos daemons y comandos administrativos tienen asignados únicamente los privilegios que les permiten ejecutarse correctamente. Muchos daemons se

ejecutan desde cuentas administrativas especiales que no tienen privilegios `root` (`UID=0`) a fin de impedir que se usurpen para realizar otras tareas. Estas cuentas administrativas especiales no pueden iniciar sesión. Los dispositivos están protegidos por privilegios.

Sistemas de archivos: de manera predeterminada, todos los sistemas de archivos son sistemas de archivos ZFS. El valor `umask` del usuario es `022`, por lo que cuando el usuario cree un nuevo archivo o directorio, solamente él tendrá permiso para modificarlo. Los miembros del grupo del usuario tienen permitido leer y buscar en el directorio, y leer el archivo. Los inicios de sesión que se realizan fuera del grupo del usuario pueden enumerar el directorio y leer el archivo. Los permisos de directorio predeterminados son `drwxr-xr-x` (`755`). Los permisos de archivo son `-rw-r--r--` (`644`).

Archivos del sistema: los archivos de configuración del sistema están protegidos con permisos de archivo. Solamente el rol `root` o un usuario que tiene asignado el derecho para editar un archivo específico del sistema pueden modificar un archivo del sistema.

Applets de escritorio: los applets de escritorio están protegidos con gestión de derechos. Por lo tanto, las acciones administrativas, como la agregación de impresoras remotas en el gestor de impresión, están limitadas a los usuarios y los roles que tienen derechos administrativos para imprimir.

Oracle Hardware Management Package

Oracle Hardware Management Package proporciona un conjunto de utilidades para configurar, gestionar y supervisar servidores Oracle. Este conjunto de herramientas de valor agregado para el hardware de Oracle siempre está disponible. Puede entregar automáticamente a ILOM cierta información relacionada con el hardware para completar la vista que tiene del hardware del sistema. Para obtener información sobre las utilidades y la seguridad, consulte Systems Management and Diagnostics Documentation"> (http://www.oracle.com/goto/ohmp/docs).

Seguridad configurable de Oracle Solaris

Además de la base sólida que proporcionan los valores predeterminados de seguridad de Oracle Solaris, la postura de seguridad de un sistema Oracle Solaris es altamente configurable para cumplir con diversos requisitos de seguridad.

En las siguientes secciones se proporciona una breve introducción a las funciones de seguridad de Oracle Solaris. Las descripciones incluyen referencias a explicaciones más detalladas y a procedimientos de esta guía y de otras guías de administración del sistema de Oracle Solaris que explican estas funciones.

Protección de datos

Oracle Solaris protege los datos desde el inicio hasta la instalación, el uso y el archivo.

Permisos de archivo y entradas de control de acceso

La primera línea de defensa para proteger los objetos de un sistema de archivos son los permisos UNIX predeterminados que se asignan a cada objeto del sistema de archivos. Los permisos UNIX admiten la asignación de derechos de acceso únicos al propietario del objeto, a un grupo asignado al objeto o a cualquier otra persona. Además, el sistema de archivos predeterminado, ZFS, admite listas de control de acceso (ACL), que controlan más detalladamente el acceso a objetos del sistema de archivos individuales o en grupos.

Para obtener más información, consulte lo siguiente:

- Para obtener una descripción general de los permisos de archivo, consulte "Uso de permisos UNIX para proteger archivos" de "Protección y verificación de la integridad de archivos en Oracle Solaris 11.2 ".
- Para obtener una descripción general y ejemplos sobre cómo proteger archivos ZFS, 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 " y las páginas del comando man.
- Para obtener instrucciones sobre cómo configurar ACL en archivos ZFS, consulte la página del comando man `chmod(1)`.

Servicios criptográficos

Las funciones de estructura criptográfica de Oracle Solaris y de estructura de gestión de claves (KMF) de Oracle Solaris proporcionan repositorios centrales para los servicios criptográficos y la gestión de claves. El hardware, el software y los usuarios finales disponen de un acceso ininterrumpido a algoritmos optimizados. KMF proporciona una interfaz unificada para mecanismos de almacenamiento, utilidades administrativas e interfaces de programación diferentes para varias infraestructuras de clave pública (PKI).

La estructura criptográfica proporciona un almacén común de algoritmos y bibliotecas PKCS #11 para manejar los requisitos criptográficos. Las bibliotecas PKCS #11 se implementan según el estándar RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki). Los servicios criptográficos, como el cifrado y el descifrado de archivos, están disponibles para los usuarios comunes.

KMF proporciona herramientas e interfaces de programación para gestionar de manera centralizada los objetos de clave pública, como certificados X.509 y pares de claves públicas o

privadas. Los formatos para almacenar estos objetos pueden variar. KMF también proporciona una herramienta para administrar políticas que definan el uso de certificados X. 509 por parte de las aplicaciones. KMF admite complementos de terceros.

Para obtener más información, consulte lo siguiente:

- Las páginas del comando man seleccionadas son `cryptoadm`(1M), `encrypt`(1), `mac`(1), `pktool`(1) y `kmfcfg`(1).
- Para obtener una descripción general de los servicios criptográficos, consulte el Capítulo 1, “Estructura criptográfica” de “Gestión de cifrado y certificados en Oracle Solaris 11.2 ” y el Capítulo 4, “Estructura de gestión de claves” de “Gestión de cifrado y certificados en Oracle Solaris 11.2 ”.
- Para obtener ejemplos sobre cómo usar la estructura criptográfica, consulte el Capítulo 3, “Estructura criptográfica” de “Gestión de cifrado y certificados en Oracle Solaris 11.2 ” y las páginas del comando man.
- Para activar el proveedor FIPS 140 de estructura criptográfica, consulte, “Cómo crear un entorno de inicio con FIPS 140 activado” de “Gestión de cifrado y certificados en Oracle Solaris 11.2 ” .

Sistema de archivos ZFS de Oracle Solaris

ZFS es el sistema de archivos predeterminado de Oracle Solaris 11. El sistema de archivos ZFS cambia radicalmente el modo de administración de los sistemas de archivos de Oracle Solaris. ZFS es sólido, escalable y fácil de administrar. Dado que la creación de sistemas de archivos en ZFS es ligera, fácilmente se pueden establecer cuotas y espacios reservados. Las ACL y los permisos UNIX protegen los archivos, y usted puede cifrar todo el conjunto de datos en la creación. La gestión de derechos de Oracle Solaris admite la administración delegada de conjuntos de datos ZFS; es decir, los usuarios que tienen asignado un conjunto limitado de privilegios pueden administrar conjuntos de datos ZFS.

Para obtener más información, consulte lo siguiente:

- “Gestión de derechos de usuario” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”
- Capítulo 1, “Sistema de archivos ZFS de Oracle Solaris (introducción)” de “Gestión de sistemas de archivos ZFS en Oracle Solaris 11.2 ”
- “Oracle Solaris ZFS y sistemas de archivos tradicionales” de “Gestión de sistemas de archivos ZFS en Oracle Solaris 11.2 ”
- Capítulo 5, “Administración de sistemas de archivos ZFS de Oracle Solaris” de “Gestión de sistemas de archivos ZFS en Oracle Solaris 11.2 ”
- “Cómo administrar ZFS con shell seguro de forma remota” de “Gestión de acceso mediante shell seguro en Oracle Solaris 11.2 ”
- Las páginas del comando man seleccionadas son `zfs`(1M) y `zfs`(7FS).

Java Cryptography Extension

Java ofrece Java Cryptography Extension (JCE) para los desarrolladores de aplicaciones Java. Para obtener más información, consulte Java SE Security (http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136007.html).

Protección y aislamiento de aplicaciones

Las aplicaciones pueden ser puntos de entrada de malware y usuarios malintencionados. En Oracle Solaris, estas amenazas se mitigan con el uso de privilegios y la contención de aplicaciones dentro de zonas. Las aplicaciones pueden ejecutarse simplemente con los privilegios que necesitan para que un usuario malintencionado no tenga privilegios de usuario root para acceder al resto del sistema. Las zonas pueden limitar el alcance de un ataque. Los ataques en las aplicaciones de una zona no global pueden afectar los procesos de esa zona solamente, no el sistema host de la zona.

La ejecución aleatoria de la disposición del espacio de direcciones (ASLR) y la utilidad de gestión de servicios (SMF) son funciones adicionales que protegen las aplicaciones. La ASLR dificulta la tarea de los intrusos para usurpar un ejecutable, y las funciones de SMF permiten a los administradores restringir el inicio, la detención y el uso de una aplicación.

Privilegios en Oracle Solaris

Los privilegios son derechos discretos específicos de procesos que se aplican en el núcleo. Oracle Solaris define más de 80 privilegios, desde los básicos, como `file_read`, hasta los más especializados, como `proc_clock_highres`. Se pueden otorgar privilegios a un proceso, un usuario o un rol. Muchos comandos y daemons de Oracle Solaris se ejecutan solamente con los privilegios requeridos para realizar su tarea. Los programas que reconocen privilegios pueden impedir que los intrusos obtengan más privilegios que los que utiliza el propio programa.

El uso de privilegios también se denomina *gestión de derechos de procesos*. Los privilegios permiten a las organizaciones especificar, y por lo tanto limitar, los privilegios que se otorgan a los servicios y los procesos que se ejecutan en sus sistemas.

Para obtener más información, consulte lo siguiente:

- "Gestión de derechos de procesos" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 "
- Capítulo 2, "Developing Privileged Applications" de "Developer's Guide to Oracle Solaris 11 Security "
- Las páginas del comando man seleccionadas son `ppriv`(1) y `privileges`(5).

Zonas de Oracle Solaris

La tecnología de partición de software de las zonas de Oracle Solaris permite mantener el modelo de implementación de una aplicación por servidor y, a la vez, compartir recursos de hardware.

Las zonas son entornos operativos virtuales que permiten que distintas aplicaciones se ejecuten de manera aislada en un mismo hardware físico. El aislamiento impide que los procesos que se ejecutan dentro de una zona controlen o afecten los procesos que se ejecutan en otras zonas, ya sea viendo los datos de los demás o manipulando el hardware subyacente. Además, las zonas proporcionan un capa de abstracción que separa las aplicaciones de los atributos físicos del sistema en donde están implementadas, como las rutas de dispositivos físicos y los nombres de interfaz de red.

En Oracle Solaris 11.2, puede configurar sistemas de archivos raíz inmutables.

Para obtener más información, consulte lo siguiente:

- "Configuración de zonas de sólo lectura" de "Creación y uso de zonas de Oracle Solaris "
- "Introducción a Zonas de Oracle Solaris "
- Las páginas del comando man seleccionadas son `brands`(5), `zoneadm`(1M) y `zonecfg`(1M).

Ejecución aleatoria de la disposición del espacio de direcciones

La ejecución aleatoria de la disposición del espacio de direcciones (ASLR) ejecuta aleatoriamente las direcciones que utiliza un determinado programa. La ASLR puede impedir determinados tipos de ataques que están basados en el conocimiento de la ubicación exacta de ciertos intervalos de memoria y puede detectar el intento cuando es probable que detenga el programa. Para obtener más información, consulte "Ejecución aleatoria de la disposición del espacio de direcciones" de "Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 " y Cómo verificar que la ASLR esté activada [33].

Utilidad de gestión de servicios

Los *servicios* ejecutan continuamente aplicaciones. Un servicio puede representar una aplicación en ejecución, el estado del software de un dispositivo o un conjunto de otros servicios. La utilidad de gestión de servicios (SMF, Service Management Facility) de Oracle Solaris se utiliza para agregar, eliminar, configurar y gestionar servicios. SMF utiliza la gestión de derechos para controlar el acceso a las funciones de gestión de servicios en el sistema. En

particular, SMF utiliza autorizaciones para determinar quién puede gestionar un servicio y qué funciones puede realizar.

SMF permite a las organizaciones controlar el acceso a los servicios y también el modo de inicio, detención y refrescamiento de los servicios.

Para obtener más información, consulte lo siguiente:

- "Gestión de los servicios del sistema en Oracle Solaris 11.2 "
- "Cómo asignar los privilegios específicos al servidor web Apache" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 "
- Las páginas del comando man seleccionadas son `svcadm`(1M), `svcs`(1) y `smf`(5).

Protección de usuarios y asignación de derechos adicionales

A los usuarios se les asigna un conjunto básico de privilegios, perfiles de derechos y autorizaciones del archivo `/etc/security/policy.conf`, al igual que al usuario inicial, como se describe en "El sistema de acceso está limitado y supervisado" [13]. Estos derechos se pueden configurar. Puede denegar los derechos básicos y aumentar los derechos para un usuario.

Oracle Solaris protege a los usuarios con requisitos de complejidad flexibles para contraseñas, autenticación que se puede configurar para diferentes requisitos de sitios y gestión de derechos de usuario que utiliza perfiles de derechos, autorizaciones y privilegios para limitar y distribuir derechos administrativos a usuarios de confianza. Además, las cuentas compartidas especiales denominadas *roles* asignan al usuario solamente los derechos administrativos cuando el usuario asume el rol. El paquete de Authorization Rules Managed On RBAC (ARMOR) proporciona roles predefinidos.

Las contraseñas y sus restricciones

Las contraseñas de usuario seguras son una defensa contra ataques de adivinación por fuerza bruta.

Oracle Solaris tiene diversas funciones que se pueden utilizar con el fin de configurar contraseñas de usuario para cumplir con los requisitos del sitio. Puede especificar la longitud de la contraseña, el contenido, la frecuencia de cambio y los requisitos de modificación, y mantener un historial de contraseñas. Se proporciona un diccionario que contiene las contraseñas que deben evitarse. Hay varios algoritmos hash de contraseña posibles. El predeterminado es SHA256.

Para obtener más información, consulte lo siguiente:

- “Mantenimiento del control de inicio de sesión” de “Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 ”
- “Protección de inicios de sesión y contraseñas” de “Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 ”
- Las páginas del comando man seleccionadas son `passwd`(1) y `crypt.conf`(4).

Módulos de autenticación conectables

La estructura del módulo de autenticación conectable (PAM) permite a los administradores coordinar y configurar requisitos de autenticación de usuarios para cuentas, credenciales, sesiones y contraseñas sin modificar los servicios que requieren autenticación.

La estructura PAM permite a las organizaciones personalizar la experiencia de autenticación del usuario y la función de administración de contraseñas, sesiones y cuentas. Los servicios de entrada del sistema, como `login` y `ssh`, utilizan la estructura PAM para proteger todos los puntos de entrada del sistema recién instalado. PAM permite la sustitución o modificación de los módulos de autenticación en el campo para proteger el sistema contra cualquier debilidad recién detectada sin la necesidad de realizar cambios a ningún servicio del sistema que use la estructura PAM.

Oracle Solaris ofrece un amplio conjunto de configuraciones y módulos PAM para cumplir con la mayoría de las políticas del sitio. Para obtener más información, consulte lo siguiente:

- Capítulo 1, “Uso de módulos de autenticación conectables” de “Gestión de Kerberos y otros servicios de autenticación en Oracle Solaris 11.2 ”
- “Writing Applications That Use PAM Services” de “Developer’s Guide to Oracle Solaris 11 Security ”
- Página del comando man `pam.conf`(4)

Gestión de derechos de usuario

En Oracle Solaris, los derechos de usuario son determinados por el principio de seguridad de privilegio mínimo. Las organizaciones pueden otorgar derechos administrativos de manera selectiva a usuarios o roles según las necesidades y los requisitos particulares que tengan. También pueden denegar derechos a los usuarios cuando sea necesario. Los derechos se implementan como privilegios en procesos y como autorizaciones en usuarios o métodos SMF. Los perfiles de derechos proporcionan una forma cómoda para recopilar privilegios y autorizaciones en un grupo de derechos relacionados.

Para obtener más información, consulte lo siguiente:

- “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”
- Las páginas del comando man seleccionadas son `auths`(1), `privileges`(5). `profiles`(1), `rbac`(5), `roleadd`(1M), `roles`(1) y `user_attr`(4).

Protección de las comunicaciones de red

Las comunicaciones de red se pueden proteger mediante diversas funciones, como firewalls, envoltorios TCP en aplicaciones de red y conexiones remotas autenticadas y cifradas.

Filtros de paquetes

Los filtros de paquetes ofrecen protección básica contra ataques de la red. Oracle Solaris incluye la función de filtro IP y los envoltorios TCP.

Firewall

La función de filtro IP de Oracle Solaris crea un cortafuegos para impedir ataques basados en la red.

En concreto, el filtro IP proporciona capacidades de filtrado de paquetes con estado y puede filtrar paquetes por red o dirección IP, por puerto, por protocolo, por interfaz de red y por dirección de tráfico. También realiza el filtrado de paquetes sin estado y tiene la capacidad de crear y administrar agrupaciones de direcciones. Además, el filtro IP también tiene la capacidad para realizar la traducción de direcciones de red (NAT) y la traducción de direcciones de puerto (PAT).

Para obtener más información, consulte lo siguiente:

- Para obtener una descripción general del filtro IP, consulte el Capítulo 4, “Acerca del filtro IP en Oracle Solaris” de “Protección de la red en Oracle Solaris 11.2 ”.
- Para obtener ejemplos sobre cómo usar el filtro IP, consulte el Capítulo 5, “Configuración del filtro IP” de “Protección de la red en Oracle Solaris 11.2 ” y las páginas del comando man.
- Para obtener información y ejemplos sobre la sintaxis del lenguaje de la política del filtro de IP, consulte la página del comando man `ipnat`(4).
- Las páginas del comando man seleccionadas son `ipfilter`(5), `ipf`(1M), `ipnat`(1M), `svc.ipfd`(1M) y `ipf`(4).

Envoltorios TCP

Los envoltorios TCP proporcionan control de acceso para los servicios de Internet. Cuando hay varios servicios (`inetd`) de Internet activados, el daemon `tcpd` comprueba la dirección de un host solicitando un servicio de red determinado en una ACL. Las solicitudes se otorgan o se rechazan según corresponda. Los envoltorios TCP también registran solicitudes de servicios de red por parte de los hosts en `syslog` porque son una función de supervisión muy útil.

Las funciones Shell seguro (`ssh`) y `sendmail` de Oracle Solaris están configuradas para utilizar los envoltorios TCP. Los servicios de red que tienen una asignación uno a uno para los archivos ejecutables, como `proftpd` y `rpcbind`, son candidatos para los envoltorios TCP.

Los envoltorios TCP admiten un lenguaje de política de configuración muy rico, que permite a las organizaciones especificar una política de seguridad no sólo de manera global sino también por servicio. Se puede admitir o restringir un acceso más amplio a los servicios en función del nombre de host, la dirección IPv4 o IPv6, el nombre del grupo de red, la red, e, incluso, el dominio de DNS.

Para obtener información sobre los envoltorios TCP, consulte lo siguiente:

- Cómo utilizar los envoltorios TCP [48]
- Para obtener información y ejemplos de la sintaxis del lenguaje de control de acceso para los envoltorios TCP, consulte la página del comando man `hosts_access`(4).
- Las páginas del comando man seleccionadas son `tcpd`(1M) y `inetd`(1M).

Acceso remoto

Los ataques de acceso remoto pueden dañar un sistema y una red. Oracle Solaris proporciona una protección profunda para las transmisiones de red. Las funciones de protección incluyen comprobaciones de autenticación y cifrado para transmisión de datos, autenticación de inicio de sesión y desactivación de servicios remotos innecesarios.

IPsec e IKE

La seguridad IP (IPsec) protege las transmisiones de red mediante la autenticación o el cifrado de paquetes IP, o mediante ambos métodos. Dado que IPsec se implementa muy por debajo de la capa de aplicación, las aplicaciones de Internet pueden beneficiarse de IPsec sin necesidad de modificar su código.

IPsec y su protocolo de intercambio de claves (IKE) automático utilizan algoritmos de la estructura criptográfica. Además, la estructura criptográfica proporciona un almacén de claves central. Si IKE está configurado para usar la metarranura, las organizaciones pueden optar por guardar las claves en el disco, en un almacén de claves de hardware conectado o en el almacén de claves de software *softtoken*.

IPsec e IKE requieren configuración, por lo que están instalados, pero no están activados de manera predeterminada. Cuando se administra correctamente, la directiva IPsec es una herramienta eficaz para proteger el tráfico de la red.

Para obtener más información, consulte lo siguiente:

- Capítulo 6, “Acerca de la arquitectura de seguridad IP” de “Protección de la red en Oracle Solaris 11.2 ”

- Capítulo 7, “Configuración de IPsec” de “Protección de la red en Oracle Solaris 11.2 ”
- “IPsec y FIPS 140” de “Protección de la red en Oracle Solaris 11.2 ”
- Capítulo 8, “Acerca del intercambio de claves de Internet” de “Protección de la red en Oracle Solaris 11.2 ”
- Capítulo 9, “Configuración de IKEv2” de “Protección de la red en Oracle Solaris 11.2 ”
- Las páginas del comando man seleccionadas son `ipsecconf`(1M) e `in.iked`(1M).

Shell seguro

De manera predeterminada, la función de Shell seguro de Oracle Solaris es el único mecanismo de acceso remoto activo en un sistema recién instalado. Todos los demás servicios de red están desactivados o en modo de sólo escucha.

El Shell seguro crea un canal de comunicaciones cifradas entre los sistemas. El Shell seguro también puede utilizarse como una red privada virtual (VPN) a petición que envíe tráfico del sistema X Window o conecte números de puerto individuales entre un sistema local y sistemas remotos mediante un enlace de red autenticado y cifrado.

Por lo tanto, el Shell seguro impide que los posibles intrusos lean una comunicación interceptada o que los adversarios falsifiquen el sistema.

Para obtener más información, consulte lo siguiente:

- Capítulo 1, “Uso de shell seguro (tareas)” de “Gestión de acceso mediante shell seguro en Oracle Solaris 11.2 ”
- “Shell seguro y FIPS 140” de “Gestión de acceso mediante shell seguro en Oracle Solaris 11.2 ”
- Las páginas del comando man seleccionadas son `ssh`(1), `sshd`(1M), `sshd_config`(4) y `ssh_config`(4).

Servicio Kerberos

La función Kerberos de Oracle Solaris permite el inicio de sesión único y transacciones seguras, incluso en redes heterogéneas donde los sistemas ejecutan diferentes sistemas operativos y el servicio Kerberos.

Kerberos se basa en el protocolo de autenticación de red Kerberos V5, que fue desarrollado en el Instituto Tecnológico de Massachusetts (MIT, Massachusetts Institute of Technology). El servicio Kerberos ofrece una sólida autenticación de usuario y también integridad y privacidad. Con el servicio Kerberos, puede iniciar sesión una vez y acceder a otros sistemas, ejecutar comandos, intercambiar datos, y transferir archivos de manera segura. Además, el servicio permite a los administradores restringir el acceso a los servicios y a los sistemas.

Para obtener más información, consulte lo siguiente:

- “Gestión de Kerberos y otros servicios de autenticación en Oracle Solaris 11.2 ”
- “Tipos de cifrado de Kerberos y algoritmos de FIPS 140” de “Gestión de Kerberos y otros servicios de autenticación en Oracle Solaris 11.2 ”
- Las páginas del comando man seleccionadas son `kadmin`(1M), `kdcmgr`(1M), `kerberos`(5), `kinit`(1) y `krb5.conf`(4).

Mantenimiento de la seguridad del sistema

Oracle Solaris proporciona las siguientes funciones para mantener la seguridad de un sistema:

- Inicio verificado: protege el proceso de inicio. El inicio verificado está desactivado de manera predeterminada.
- Verificación de paquetes: verifica que los paquetes instalados sean idénticos a los paquetes en el repositorio de origen.
- Servicio de auditoría: audita el acceso al sistema y su uso. La auditoría está activada de manera predeterminada.
- Verificación de integridad de archivos: los manifiestos BART pueden mostrar una lista de todos los archivos del sistema, y se utilizan comparaciones de manifiestos para verificar que se mantenga la integridad de los archivos.
- Archivos log: la SMF proporciona archivos log para cada servicio. La utilidad `syslog` proporciona un archivo central para nombrar y configurar logs de servicios del sistema, y, opcionalmente, puede notificar a los administradores sobre los eventos críticos. Otras funciones, como la auditoría, también crean sus propios logs.
- Informes de conformidad: Oracle Solaris proporciona varias referencias de seguridad para evaluar el sistema. Estas evaluaciones generan informes que ayudan a evaluar la postura de seguridad del sistema.

Inicio verificado

El inicio verificado es una función de Oracle Solaris que protege el proceso de inicio del sistema. Esta función protege el sistema de amenazas, como la instalación de módulos de núcleo no autorizados y aplicaciones de caballo de Troya. De manera predeterminada, el inicio verificado está desactivado.

Para obtener más información, consulte el Capítulo 2, “Protección de integridad de los sistemas Oracle Solaris” de “Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 ”.

Verificación de integridad de paquetes

Después de instalar o actualizar paquetes, puede ejecutar el comando `pkg verify` para asegurarse de que los paquetes del sistema sean idénticos a los paquetes del repositorio de origen.

Para obtener más información, consulte la página del comando man `pkg`(1) y Cómo comprobar los paquetes [33].

Servicio de auditoría

Oracle Solaris proporciona un servicio de auditoría que recopila datos sobre el acceso al sistema y su uso. Los datos de auditoría proporcionan un log confiable con registro de hora de los eventos del sistema relacionados con la seguridad. Estos datos se pueden utilizar para asignar responsabilidad para acciones que ocurren en un sistema.

La auditoría es un requisito básico para la evaluación de la seguridad, la validación, la conformidad y los organismos de certificación. La auditoría también puede servir para disuadir a posibles intrusos.

Para obtener más información, consulte lo siguiente:

- Para obtener una lista de las páginas del comando man relacionadas con la auditoría, consulte el Capítulo 7, “Referencia sobre auditoría” de “Gestión de auditoría en Oracle Solaris 11.2 ”.
- Para obtener directrices, consulte Cómo auditar eventos importantes además del inicio y el cierre de sesión [44] and the man pages.
- Para obtener una descripción general de la auditoría, consulte el Capítulo 1, “Acerca de la auditoría en Oracle Solaris” de “Gestión de auditoría en Oracle Solaris 11.2 ”.
- Para conocer las tareas de auditoría, consulte el Capítulo 3, “Gestión del servicio de auditoría” de “Gestión de auditoría en Oracle Solaris 11.2 ”.

Verificación de integridad de archivos

La herramienta básica de creación de informes de auditoría (BART, Basic Audit Reporting Tool), de Oracle Solaris, permite validar exhaustivamente los sistemas mediante comprobaciones en el nivel de archivo de un sistema a lo largo del tiempo. Después de la instalación, el comando `pkg verify` confirma que el contenido del paquete de origen y del paquete de destino son idénticos. Después de la verificación de paquetes, los manifiestos BART pueden recopilar de manera fácil y confiable información sobre los archivos de un sistema.

BART es una herramienta útil para la gestión de la integridad en un sistema o en una red de sistemas. Los archivos de un sistema se pueden comparar con los archivos originales del

sistema y con los archivos de otro sistema. Los informes pueden indicar que no se aplicó un parche a un sistema, que un intruso instaló archivos no aprobados o que un intruso cambió los permisos o el contenido de archivos confidenciales, como los archivos que son propiedad de `root`.

Para obtener más información, consulte lo siguiente:

- Para obtener directrices, consulte “Verificación de la integridad de archivos mediante el uso de BART” [58], “Verificación de la integridad de archivos mediante el uso de BART” [58] y las páginas del comando man.
- Para obtener una descripción general de BART, 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 ”.
- Para obtener ejemplos sobre cómo usar BART, consulte “Acerca del uso de BART” de “Protección y verificación de la integridad de archivos en Oracle Solaris 11.2 ” y las páginas del comando man.
- Las páginas del comando man seleccionadas son `bart`(1M), `bart_rules`(4) y `bart_manifest`(4).

Archivos log

La función de utilidad de gestión de servicios (SMF) de Oracle Solaris registra el estado de sus servicios por servicio. Muchos servicios, como la auditoría y Shell seguro, escriben sus propios logs. El daemon `syslog` o `rsyslog` escribe un log centralizado que puede informar y advertir a los administradores sobre condiciones críticas en muchos servicios. Por ejemplo, la auditoría se puede configurar para escribir registros de auditoría resumidos en `syslog`. Consulte las páginas del comando man `syslogd`(1M) y `syslog.conf`(4).

Conformidad con estándares de seguridad

El comando `compliance assess` proporciona una instantánea de la postura de seguridad del sistema. Los informes de las evaluaciones sugieren cambios específicos al sistema para cumplir con las referencias de seguridad del sector. Para obtener más información, consulte “Guía de cumplimiento de la seguridad de Oracle Solaris 11.2 ” y la página del comando man `compliance`(1M).

Seguridad con etiquetas

La seguridad con etiquetas en Oracle Solaris es proporcionada por la función Trusted Extensions.

Función Trusted Extensions en Oracle Solaris

La función Trusted Extensions de Oracle Solaris es una capa con tecnología de etiquetado seguro que se activa de manera opcional y permite separar las políticas de seguridad de los datos de la propiedad de los datos. Trusted Extensions admite tanto las políticas tradicionales de control de acceso discrecional (DAC) basadas en la propiedad como las políticas de control de acceso obligatorio (MAC) basadas en etiquetas. A menos que la capa de Trusted Extensions esté activada, todas las etiquetas son iguales para que el núcleo no se configure para forzar las políticas de MAC. Cuando se activan las políticas de MAC basadas en etiquetas, se limitan todos los flujos de datos en función de una comparación de etiquetas asociadas con los procesos (sujetos) que solicitan acceso y los objetos que contienen los datos.

La implementación de Trusted Extensions tiene una capacidad única para proporcionar una gran garantía y, a la vez, maximizar la compatibilidad y minimizar los costos generales. Trusted Extensions es parte de la “Certificación EAL4+ de criterios comunes de Oracle Solaris 11” [29].

Trusted Extensions cumple con los requisitos del paquete de seguridad con etiquetas (LSP) de criterios comunes. Consulte “Certificación EAL4+ de criterios comunes de Oracle Solaris 11” [29].

Para obtener más información, consulte lo siguiente:

- Para obtener información sobre la configuración y el mantenimiento de Trusted Extensions, consulte “Configuración y administración de Trusted Extensions ”.
- Las páginas del comando man seleccionadas son `trusted_extensions`(5), `labeladm`(1M) y `labeld`(1M).

Sistema de archivos con etiquetas

De manera predeterminada, los sistemas de archivos tienen asignada una sola etiqueta en una zona en esa misma etiqueta. Puede crear un conjunto de datos ZFS de varios niveles, montarlo en un sistema Trusted Extensions y, con los permisos adecuados, subir o bajar el nivel de los archivos de ese conjunto de datos. Para obtener más información, consulte “Conjuntos de datos de varios niveles para volver a etiquetar archivos” de “Configuración y administración de Trusted Extensions ”.

Comunicaciones de red con etiquetas

Trusted Extensions etiqueta las comunicaciones de red. Los flujos de datos se restringen según una comparación de las etiquetas asociadas con el punto final de red de origen y el punto final de red de recepción. Las puertas de enlace y los saltos intermedios también deben estar

etiquetados para permitir la transferencia de información en la etiqueta de la comunicación. Los conjuntos de datos ZFS de varios niveles y NFS ofrecen funciones adicionales en una red.

Para obtener más información, consulte lo siguiente:

- "Configuración de las interfaces de red en Trusted Extensions" de "Configuración y administración de Trusted Extensions "
- Capítulo 15, "Redes de confianza" de "Configuración y administración de Trusted Extensions "
- Capítulo 16, "Gestión de redes en Trusted Extensions" de "Configuración y administración de Trusted Extensions "

Escritorio de varios niveles de Trusted Extensions

A diferencia de la mayoría del resto de los sistemas operativos de varios niveles, Trusted Extensions incluye un escritorio de varios niveles. Los usuarios se pueden configurar para que vean solamente sus etiquetas permitidas. Cada etiqueta puede estar configurada para solicitar una contraseña diferente.

Para obtener más información, consulte la "Guía del usuario de Trusted Extensions ". Para configurar usuarios, consulte el Capítulo 11, "Gestión de usuarios, derechos y roles en Trusted Extensions" de "Configuración y administración de Trusted Extensions ".

Certificación EAL4+ de criterios comunes de Oracle Solaris 11

Oracle Solaris 11 está certificado según el esquema de criterios comunes de Canadá con el nivel de confianza en la evaluación 4 (EAL4) y ampliado con corrección de errores (EAL4+). EAL4 es el nivel más alto de evaluación mutuamente reconocido por 26 países según el acuerdo de reconocimiento de criterios comunes (CCRA).

La certificación es para el perfil de protección de sistema operativo (OSPP) e incluye los siguientes paquetes extendidos:

- gestión avanzada
- identificación y autenticación extendidas
- seguridad con etiquetas
- virtualización

Para obtener información sobre la certificación, consulte:

- Oracle Security Evaluations Matrix (http://www.oracle.com/technetwork/topics/security/security-evaluations-099357.html)

- The Common Criteria Recognition Arrangement (http://www.commoncriteriaportal.org/ccra/)
- Operating System Protection Profile (http://www.commoncriteriaportal.org/files/ppfiles/pp0067b_pdf.pdf)

Práctica y política de seguridad del sitio

Para que un sistema o una red de sistemas sean seguros, el sitio debe tener una política de seguridad con prácticas de seguridad que apoyen la política. Si está desarrollando programas o instalando programas de terceros, debe desarrollar e instalar estos programas de manera segura.

Para obtener más información, consulte lo siguiente:

- Importance of Software Security Assurance (http://www.oracle.com/us/support/assurance/overview/index.html)
- Apéndice A, “Secure Coding Guidelines for Developers” de “Developer’s Guide to Oracle Solaris 11 Security ”
- Apéndice A, “Política de seguridad del sitio” de “Configuración y administración de Trusted Extensions ”
- “Aplicación de los requisitos de seguridad” de “Configuración y administración de Trusted Extensions ”
- Keeping Your Code Secure (http://blogs.oracle.com/maryanndavidson/entry/those_who_can_t_do)

♦ ♦ ♦ CAPÍTULO 2

Configuración de la seguridad de Oracle Solaris

En este capítulo, se describen las acciones que se deben realizar para configurar la seguridad en el sistema. El capítulo abarca la instalación de paquetes y la configuración del propio sistema y de varios subsistemas y aplicaciones adicionales que puedan ser necesarias, como IPsec.

Instalación del SO Oracle Solaris

El SO Oracle Solaris se instala seleccionando un conjunto de paquetes denominado *grupo* desde un repositorio de paquetes. Distintos grupos proporcionan paquetes para usos diferentes, como servidores multipropósito, sistemas instalados mínimamente y sistemas de escritorio. Los paquetes se firman, y su transferencia segura se puede verificar.

Cuando instale el SO Oracle Solaris, seleccione los medios que instalan el paquete de *grupo* adecuado, de la siguiente manera:

- **Servidor grande de Oracle Solaris**: tanto el manifiesto predeterminado en una instalación de Automated Installer (AI) como el instalador de texto instalan el grupo `group/system/solaris-large-server`, que proporciona un entorno de servidor grande de Oracle Solaris.
- Servidor pequeño de **Oracle Solaris:** la instalación del instalador automático (AI) y el instalador de texto opcionalmente instalan el grupo `group/system/solaris-small-server`, que proporciona un entorno útil de línea de comandos al que le puede agregar paquetes.
- Servidor mínimo de **Oracle Solaris:** la instalación del instalador automático (AI) y el instalador de texto opcionalmente instalan el grupo `group/system/solaris-minimal-server`, que proporciona un entorno mínimo de línea de comandos al que le puede agregar los paquetes que desee.

- **Escritorio de Oracle Solaris**: Live Media instala el grupo `group/system/solaris-desktop`, que proporciona un entorno de escritorio de Oracle Solaris 11.

  Para crear un sistema de escritorio para uso centralizado, agregue el grupo `group/feature/multi-user-desktop` al servidor de escritorio. Para obtener más información, consulte el artículo "Optimizing the Oracle Solaris 11 Desktop for a Multiuser Environment ".

Para la instalación automática con Automated Installer (AI), consulte la Parte III, "Instalación con un servidor de instalación" de "Instalación de sistemas Oracle Solaris 11.2 ".

Para informarse antes de elegir el medio de instalación y el contenido de los paquetes, consulte las siguientes guías:

- "Instalación de sistemas Oracle Solaris 11.2 "
- "Creación de una imagen de instalación personalizada de Oracle Solaris 11.2 "
- "Agregación y actualización de software en Oracle Solaris 11.2 "
- "Oracle Solaris 11.2 Package Group Lists "

Protección inicial del sistema

La mejor manera de realizar las siguientes tareas es siguiendo el orden. En este punto, se instala Oracle Solaris, y solamente el usuario inicial que puede asumir el rol `root` tiene acceso al sistema.

TABLA 2-1 Mapa de tareas de protección del sistema

Tarea	Descripción	Para obtener instrucciones
1. Revisar los paquetes en el sistema.	Comprobar que los paquetes del origen de instalación sean idénticos a los paquetes instalados.	Cómo comprobar los paquetes [33]
2. Garantizar que los archivos ejecutables estén protegidos.	Comprobar que la ASLR esté activada.	Cómo verificar que la ASLR esté activada [33]
3. Proteger la configuración del hardware en el sistema.	Se protege el hardware mediante la solicitud de una contraseña para cambiar la configuración del hardware. En x86, el acceso al menú de GRUB está controlado. En SPARC, el comando `eeprom` protege el hardware.	"Control de acceso a hardware del sistema" de "Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 "
3. Desactivar servicios innecesarios.	Evitar la ejecución de los procesos que no forman parte de las funciones requeridas del sistema.	Cómo desactivar los servicios innecesarios [34]
5. Evitar que el propietario de la estación de trabajo apague el sistema.	Impedir que el usuario de la consola cierre o suspenda el sistema.	Cómo eliminar la capacidad de gestión de energía de los usuarios [35]
6. Crear un mensaje de advertencia de inicio de sesión que refleje la política de seguridad del sitio.	Notificar a los usuarios que el sistema está supervisado antes y después de la autenticación.	Cómo insertar un mensaje de seguridad en archivos de banner [36]

Tarea	Descripción	Para obtener instrucciones
		Cómo insertar un mensaje de seguridad en la pantalla de inicio de sesión del escritorio [37]

▼ Cómo comprobar los paquetes

Inmediatamente después de la instalación, verifique los paquetes a fin de validar la instalación.

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. **Revise el log de instalación.**
2. **Ejecute el comando `pkg verify`.**

   Para llevar un registro, envíe la salida del comando en un archivo.

   ```
   # pkg verify > /var/pkgverifylog
   ```

3. **Fíjese si hay errores en el registro.**
4. **Si encuentra errores, vuelva a realizar la instalación desde los medios o corrija los errores.**

Véase también Para obtener más información, consulte las páginas del comando man pkg(1) y pkg(5). Las páginas del comando man incluyen ejemplos de uso del comando `pkg verify`.

▼ Cómo verificar que la ASLR esté activada

De manera predeterminada, las instrucciones ejecutables que están etiquetadas se escriben en espacios de direcciones sin conexión para reducir la capacidad de los intrusos de insertar instrucciones en la pila ejecutable.

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. **Verifique que la ASLR esté activada.**

   ```
   # sxadm info
   EXTENSION       STATUS                  CONFIGURATION
   aslr            enabled (all)           enabled (all)
   ```

El valor `all` es más potente que el predeterminado y puede provocar errores en aplicaciones que dependen de una pila consecutiva en la memoria. Por ejemplo, las bases de datos pueden depender de una pila consecutiva en la memoria.

2. **Si la ASLR está desactivada, active el valor predeterminado y verifique que esté vigente.**

```
# sxadm delcust aslr
# sxadm info
EXTENSION       STATUS                  CONFIGURATION
aslr            enabled (tagged-files)  system default (default)
```

Véase también Para fines de depuración, puede desactivar la ASLR llamando al comando `sxadm` en un binario particular. Para obtener ejemplos, consulte la página del comando man `sxadm`(1M).

▼ Cómo desactivar los servicios innecesarios

Utilice este procedimiento para desactivar servicios que no sean necesarios en este sistema.

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. **Indique los servicios de red en línea.**

```
# svcs | grep network
online         Sep_07   svc:/network/loopback:default
online         Sep_07   svc:/network/http:apache22
online         Sep_07   svc:/network/nfs/server:default
...
online         Sep_07   svc:/network/ssh:default
```

2. **Desactive los servicios que no sean necesarios en este sistema.**

   Por ejemplo, si el sistema no es un servidor NFS ni un servidor web, y los servicios están en línea, desactívelos.

```
# svcadm disable svc:/network/nfs/server:default
# svcadm disable svc:/network/http:apache22
```

Véase también Para obtener más información, consulte el Capítulo 1, "Introducción a la Utilidad de gestión de servicios" de "Gestión de los servicios del sistema en Oracle Solaris 11.2 " y la página del comando man `svcs`(1).

▼ Cómo eliminar la capacidad de gestión de energía de los usuarios

Utilice este procedimiento para evitar que los usuarios en la consola de un sistema suspendan o apaguen el sistema. Esta solución de software no es eficaz si el hardware del sistema puede ser desconectado por el usuario de la consola.

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. **Revise los contenidos del perfil de derechos del usuario de la consola.**

```
% profiles -p "Console User" info
 name=Console User
 desc=Manage System as the Console User
 auths=solaris.system.shutdown,solaris.device.cdrw,
             solaris.smf.manage.vbiosd,solaris.smf.value.vbiosd
 profiles=Suspend To RAM,Suspend To Disk,Brightness,CPU Power Management,
                Network Autoconf User
 help=RtConsUser.html
```

2. **Cree un perfil de derechos que incluya todos los derechos del perfil del usuario de la consola que quiera que los usuarios retengan.**

   Para obtener instrucciones, consulte "Cómo crear un perfil de derechos" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

3. **Comente el perfil de derechos de usuario de consola en el archivo `/etc/security/policy.conf`.**

```
#CONSOLE_USER=Console User
```

4. **Asigne el perfil de derechos que creó en el Paso 2.**

   - Si tiene muchos usuarios que comparten un perfil de derechos, definir este valor en un perfil de derechos puede ser una solución escalable.

     ```
     # usermod -P shared-profile username
     ```

   - También puede asignar el perfil por sistema en el archivo `policy.conf`.

     ```
     # pfedit /etc/security/policy.conf...
     #PROFS_GRANTED=Basic Solaris User
     PROFS_GRANTED=shared-profile,Basic Solaris User
     ```

Véase también Para obtener más información, consulte "Archivo policy.conf" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 " y las páginas del comando man `policy.conf`(4) y `usermod`(1M).

▼ Cómo insertar un mensaje de seguridad en archivos de banner

Utilice este procedimiento para crear mensajes de seguridad en dos archivos de banner que reflejen la política de seguridad del sitio. El archivo `/etc/issue` aparece antes de la autenticación, mientras que el archivo `/etc/motd` aparece después de la autenticación.

Nota - Los mensajes de ejemplo que se incluyen en este procedimiento no cumplen con los requisitos del Gobierno de los Estados Unidos y es probable que tampoco cumplan con su política de seguridad. Consulte con el abogado de su empresa acerca de los contenidos del mensaje de seguridad.

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

1. **Cree el archivo `/etc/issue` y agregue un mensaje de seguridad.**

```
# pfedit /etc/issue
ALERT   ALERT   ALERT   ALERT   ALERT

This machine is available to authorized users only.

If you are an authorized user, continue.

Your actions are monitored, and can be recorded.
```

El comando `login` muestra los contenidos de `/etc/issue` antes de la autenticación, al igual que `ssh`, `telnet` y los servicios FTP. Para mostrar los contenidos de `/etc/issue` en el inicio de sesión del escritorio, consulte Cómo insertar un mensaje de seguridad en la pantalla de inicio de sesión del escritorio [37].

Para obtener más información, consulte las páginas del comando man `issue`(4) y `pfedit`(1M).

2. **Agregue un mensaje de seguridad para el archivo `/etc/motd`.**

```
# pfedit /etc/motd
This system serves authorized users only. Activity is monitored and reported.
```

En Oracle Solaris, el shell inicial del usuario muestra los contenidos del archivo `/etc/motd`.

▼ Cómo insertar un mensaje de seguridad en la pantalla de inicio de sesión del escritorio

Elija entre varios métodos a fin de crear un mensaje de seguridad para que revisen los usuarios antes de la autenticación, después de la autenticación o en ambos casos. El archivo `/etc/issue` aparece antes de la autenticación, mientras que el archivo `/etc/motd` aparece después de la autenticación.

Para obtener más información, haga clic en Sistema -> Ayuda en el escritorio a fin de abrir el explorador de ayuda de GNOME. También puede usar el comando `yelp`. Las secuencias de comandos de inicio de sesión de escritorio se describen en la sección `GDM Login Scripts and Session Files` de la página del comando man `gdm`(1M).

Nota - El mensaje de ejemplo que se incluye en este procedimiento no cumple con los requisitos del Gobierno de los Estados Unidos y es probable que tampoco cumpla con su política de seguridad. Consulte con el abogado de su empresa acerca de los contenidos del mensaje de seguridad.

Antes de empezar Para crear un archivo, debe asumir el rol `root`. Para modificar un archivo existente, debe convertirse en administrador con la autorización `solaris.admin.edit/`*path-to-existing-file* asignada.

1. **Para insertar un mensaje de seguridad en la pantalla de inicio de sesión del escritorio antes de la autenticación, utilice una de las opciones que se indican a continuación.**

   Las opciones que crean un cuadro de diálogo antes de la autenticación usan el mensaje de seguridad en el archivo `/etc/issue` del Paso 1 en Cómo insertar un mensaje de seguridad en archivos de banner [36].

   - **OPCIÓN 1: modifique una secuencia de comandos de inicialización GDM para mostrar el mensaje de seguridad en un cuadro de diálogo.**

     El directorio `/etc/gdm` contiene tres secuencias de comandos de inicialización que muestran el mensaje de seguridad antes y después de la autenticación.

     ```
     # pfedit /etc/gdm/Init/Default
     /usr/bin/zenity --text-info --width=800 --height=300 \
     --title="Security Message"  --filename=/etc/issue
     ```

     Para obtener información sobre cómo editar archivos del sistema como usuario no `root`, consulte la página del comando man `pfedit`(1M).

   - **OPCIÓN 2: modifique la ventana de inicio de sesión para mostrar el mensaje de seguridad sobre el campo de entrada.**

La ventana de inicio de sesión se expande para ajustarse al mensaje. Este método no hace referencia al archivo `/etc/issue`. Debe escribir el texto en la interfaz gráfica de usuario.

Nota - La ventana de inicio de sesión `gdm-greeter-login-window.ui` se sobreescribe con los comandos `pkg fix` y `pkg update`. Para conservar los cambios, copie el archivo en un directorio de archivos de configuración y combine sus cambios con el nuevo archivo después de actualizar el sistema. Para obtener más información, consulte la página del comando man `pkg`(5).

---

a. Cambie el directorio a la interfaz de usuario de la ventana de inicio de sesión.

```
# cd /usr/share/gdm
```

b. (Opcional) Guarde una copia de la interfaz de usuario de la ventana de inicio de sesión original.

```
# cp gdm-greeter-login-window.ui /etc/gdm/gdm-greeter-login-window.ui.orig
```

c. Agregue una etiqueta a la ventana de inicio de sesión mediante el diseñador de interfaces GNOME Toolkit.

El programa `glade-3` abre el diseñador de interfaces GTK+. Debe escribir el mensaje de seguridad en una etiqueta que se muestra sobre el campo de entrada de usuario.

```
# /usr/bin/glade-3 /usr/share/gdm/gdm-greeter-login-window.ui
```

Para revisar la guía para el diseñador de interfaces, haga clic en Desarrollo, en el explorador de la ayuda de GNOME. La página del comando man `glade-3`(1) aparece en la sección Aplicaciones de las páginas manuales.

d. (Opcional) Guarde una copia de la interfaz de usuario de la ventana de inicio de sesión modificada.

```
# cp gdm-greeter-login-window.ui /etc/gdm/gdm-greeter-login-window.ui.site
```

2. Para insertar un mensaje de seguridad en la pantalla de inicio de sesión del escritorio después de la autenticación, utilice una de las opciones que se indican a continuación.

El archivo que crea un cuadro de diálogo después de la autenticación usa el mensaje de seguridad en el archivo `/etc/motd` del Paso 2 en Cómo insertar un mensaje de seguridad en archivos de banner [36].

- **OPCIÓN 1: inserte un mensaje de seguridad en el escritorio después de la autenticación.**

```
# pfedit /etc/gdm/PreSession/Default
```

```
/usr/bin/zenity --text-info --width=800 --height=300 \
--title="Security Message"  --filename=/etc/motd
```

Nota - El cuadro de diálogo se puede cubrir con ventanas en el espacio de trabajo del usuario.

- **OPCIÓN 2: cree un archivo de escritorio que muestre el mensaje de seguridad en una ventana adicional después de la autenticación.**

```
# pfedit /usr/share/gdm/autostart/LoginWindow/banner.desktop
[Desktop Entry]
Type=Application
Name=Banner Dialog
Exec=/usr/bin/zenity --text-info --width=800 --height=300 \
--title="Security Message" \
--filename=/etc/motd
OnlyShowIn=GNOME;
X-GNOME-Autostart-Phase=Application
```

Para acceder al espacio de trabajo después de la autenticación en la ventana de inicio de sesión, el usuario debe cerrar la ventana del mensaje de seguridad. Para las opciones que permiten el comando `zenity`, consulte la página del comando man `zenity`(1).

ejemplo 2-1 Creación de un breve mensaje de advertencia en el inicio de sesión del escritorio

En este ejemplo, el administrador escribe un mensaje breve como un argumento para el comando `zenity` en el archivo del escritorio. El administrador también utiliza la opción `--warning`, que muestra un icono de advertencia con el mensaje.

```
# pfedit /usr/share/gdm/autostart/LoginWindow/bannershort.desktop
[Desktop Entry]
Type=Application
Name=Banner Dialog
Exec=/usr/bin/zenity --warning --width=800  --height=150 --title="Security Message" \
--text="This system serves authorized users only. Activity is monitored and reported."
OnlyShowIn=GNOME;
X-GNOME-Autostart-Phase=Application
```

Protección de usuarios

En este momento, sólo el usuario inicial que pueda asumir el rol `root` tiene acceso al sistema. La mejor manera de realizar las siguientes tareas es siguiendo el orden, antes de que los usuarios comunes puedan iniciar sesión.

TABLA 2-2 Mapa de tareas de protección de usuarios

Tarea	Descripción	Para obtener instrucciones
Requerir contraseñas seguras y cambios de contraseña regulares.	Aumentar las limitaciones de la contraseña predeterminada en cada sistema.	Cómo establecer restricciones de contraseñas más seguras [40]
Configurar permisos de archivo restrictivos para los usuarios comunes.	Fijar un valor más restrictivo que `022` para los permisos de archivo de los usuarios comunes.	Cómo definir un valor `umask` más restrictivo para usuarios comunes [43]
Establecer el bloqueo de cuenta para los usuarios comunes.	En sistemas que no se usan para la administración, establecer el bloqueo de cuenta en todo el sistema y reducir la cantidad de inicios de sesión que activan el bloqueo.	Cómo establecer el bloqueo de cuenta para usuarios normales [41]
Preseleccionar la clase de auditoría `cusa` para todos los usuarios.	Proporcionar mejores supervisión y registro de las amenazas potenciales para el sistema.	Cómo auditar eventos importantes además del inicio y el cierre de sesión [44]
Crear roles.	Distribuir tareas administrativas discretas a varios usuarios de confianza para que ningún usuario pueda dañar el sistema. Puede utilizar roles predefinidos ARMOR, crear sus propios roles o ampliar ARMOR con sus propios roles.	"Gestión de cuentas de usuario mediante la interfaz de línea de comandos" de "Gestión de las cuentas de usuario y los entornos de usuario en Oracle Solaris 11.2 " "Asignación de derechos a usuarios" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 "
Reducir el número de aplicaciones de escritorio GNOME visibles.	Impedir que los usuarios utilicen las aplicaciones de escritorio que pueden afectar la seguridad.	Consulte el Capítulo 11, "Desactivación de funciones en el sistema Oracle Solaris Desktop" de "Guía del administrador de Oracle Solaris 11.2 Desktop ".
Limitar los privilegios del usuario.	Eliminar privilegios básicos que los usuarios no necesiten.	Cómo eliminar privilegios básicos innecesarios de los usuarios [45]

▼ Cómo establecer restricciones de contraseñas más seguras

Utilice este procedimiento si los valores predeterminados no cumplen con los requisitos de seguridad del sitio. Los pasos están en el orden de las entradas de variables en el archivo `/etc/default/passwd`.

Antes de empezar Debe convertirse en un administrador con la autorización `solaris.admin.edit/etc/default/passwd` 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 ".

- **Utilice el comando `pfedit` para realizar los siguientes cambios en el archivo `/etc/default/passwd`.**

  a. **Solicite a los usuarios que cambien sus contraseñas cada cuatro meses, pero nunca cada menos de tres semanas.**

```
## /etc/default/passwd
##
#MAXWEEKS=
#MINWEEKS=
MAXWEEKS=13
MINWEEKS=3
```

b. Solicite una contraseña de al menos ocho caracteres.

```
#PASSLENGTH=6
PASSLENGTH=8
```

c. Mantenga un historial de contraseñas.

```
#HISTORY=0
HISTORY=10
```

d. Requiera que haya alguna diferencia mínima con la última contraseña.

```
#MINDIFF=3
MINDIFF=4
```

e. Solicite que haya al menos una letra en mayúscula.

```
#MINUPPER=0
MINUPPER=1
```

f. Solicite que haya al menos un dígito.

```
#MINDIGIT=0
MINDIGIT=1
```

Véase también

- Para obtener la lista de variables que restringen la creación de contraseñas, consulte la página del comando man `passwd`(1).
- Para obtener información sobre las limitaciones de contraseña que se aplican después de la instalación, consulte “El sistema de acceso está limitado y supervisado” [13].

▼ Cómo establecer el bloqueo de cuenta para usuarios normales

Utilice este procedimiento para bloquear cuentas de usuarios comunes después de un determinado número de intentos de inicio de sesión fallidos.

Nota - Los roles son cuentas compartidas. No establezca el bloqueo de cuenta para los usuarios que pueden asumir roles, ya que un usuario bloqueado puede bloquear el rol.

Antes de empezar No establezca esta protección en la totalidad de un sistema que utilice para las actividades administrativas. En su lugar, supervise que no haya uso inusual en el sistema administrativo y manténgalo disponible para los administradores.

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. **Establezca el atributo de seguridad `LOCK_AFTER_RETRIES` en `YES` (sí).**

   Seleccione el ámbito del valor de atributo.

   - **Para todo el sistema.**

     Esta protección se aplica a cualquier usuario que intenta utilizar el sistema.

     ```
     # pfedit /etc/security/policy.conf
     ...
     #LOCK_AFTER_RETRIES=NO
     LOCK_AFTER_RETRIES=YES
     ...
     ```

   - **Para un usuario.**

     Esta protección se aplica únicamente al usuario para el que se ejecuta este comando. Si tiene muchos usuarios, no es una solución escalable.

     ```
     # usermod -K lock_after_retries=yes username
     ```

   - **Cree y asigne un perfil de derechos.**

     Esta protección se aplica a cualquier usuario o sistema al que se asigna este perfil de derechos.

     a. **Cree el perfil de derechos.**

        ```
        # profiles -p shared-profile -S ldap
        shared-profile: set lock_after_retries=yes
        ...
        ```

        Para obtener más información sobre cómo crear perfiles de derechos, consulte “Creación de perfiles de derechos y autorizaciones” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

     b. **Asigne el perfil de derechos a usuarios o a todo el sistema.**

Si tiene muchos usuarios que comparten un perfil de derechos, definir este valor en un perfil de derechos puede ser una solución escalable.

```
# usermod -P shared-profile username
```

También puede asignar el perfil por sistema en el archivo `policy.conf`.

```
# pfedit /etc/security/policy.conf
...
#PROFS_GRANTED=Basic Solaris User
PROFS_GRANTED=shared-profile,Basic Solaris User
```

2. **Establezca el atributo de seguridad `RETRIES` en `3`.**

   Seleccione el ámbito del valor de atributo.

   - **Para todo el sistema.**

     ```
     # pfedit /etc/default/login
     ...
     #RETRIES=5
     RETRIES=3
     ...
     ```

   - **Para un usuario.**

     ```
     # usermod -K lock_after_retries=3 username
     ```

   - **Cree y asigne un perfil de derechos.**

     Siga los pasos en el Paso 1.3 y cree un perfil de derechos que incluya `lock_after_retries=3`.

Véase también

- Para obtener una explicación de los atributos de seguridad de usuarios y roles, consulte el Capítulo 8, “Referencia para derechos Oracle Solaris” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.
- Las páginas del comando man seleccionadas son `policy.conf`(4), `profiles`(1), `user_attr`(4) y `usermod`(1M).

▼ Cómo definir un valor `umask` más restrictivo para usuarios comunes

La utilidad `umask` define los bits de permisos de archivos de los archivos creados por el usuario. Si el valor `umask` predeterminado (`022`) no es lo suficientemente restrictivo, defina una máscara más restrictiva mediante el siguiente procedimiento.

Antes de empezar Debe convertirse en un administrador que está autorizado para editar los archivos de estructura básica. Al rol `root` se le asignan estas autorizaciones. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

1. **Visualice los archivos de ejemplo que Oracle Solaris proporciona para los valores predeterminados de shell de usuario.**

```
# ls -1a /etc/skel
.bashrc
.profile
local.cshrc
local.login
local.profile
```

2. **Defina el valor `umask` en los archivos `/etc/skel` que asignará a los usuarios.**

   Elija uno de los siguientes valores:

   - `umask 026`: proporciona una protección de archivos moderada (`751`): `r` para el grupo, `x` para otros
   - `umask 027`: proporciona una protección de archivos estricta (`750`): `r` para el grupo, sin acceso para otros
   - `umask 077`: proporciona una protección de archivos completa (`700`): sin acceso ni para el grupo ni para otros

Véase también Para obtener más información, consulte lo siguiente:

- "Gestión de cuentas de usuario mediante la interfaz de línea de comandos" de "Gestión de las cuentas de usuario y los entornos de usuario en Oracle Solaris 11.2 "
- "Valor umask predeterminado" de "Protección y verificación de la integridad de archivos en Oracle Solaris 11.2 "
- Las páginas del comando man seleccionadas son `useradd`(1M) y `umask`(1).

▼ Cómo auditar eventos importantes además del inicio y el cierre de sesión

Utilice este procedimiento para auditar los comandos administrativos, el acceso al sistema y otros eventos importantes según lo especificado por la política de seguridad del sitio.

Nota - Puede que los ejemplos de este procedimiento no sean suficientes para su política de seguridad.

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. **Audite todos los usos de los comandos con privilegios por los usuarios que tienen asignados los roles y los perfiles de derechos administrativos.**

   Agregue la clase de auditoría `cusa` a su máscara de preselección.

   ```
   # usermod -K audit_flags=cusa:no username
   ```

   ```
   # rolemod -K audit_flags=cusa:no rolename
   ```

   Las clases de auditoría que incluye la metaclase `cusa` se muestran en el archivo `/etc/security/audit_class`.

2. **Registre los argumentos de los comandos auditados.**

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

3. **(Opcional) Registre el entorno en el que se ejecutan los comandos auditados.**

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

   Nota - Esta opción de política puede ser útil al solucionar problemas.

Véase también

- Para obtener información sobre la política de auditoría, consulte “Política de auditoría” de “Gestión de auditoría en Oracle Solaris 11.2 ”.
- Para obtener ejemplos sobre cómo establecer indicadores de auditoría, consulte “Configuración del servicio de auditoría” de “Gestión de auditoría en Oracle Solaris 11.2 ” y “Resolución de problemas del servicio de auditoría” de “Gestión de auditoría en Oracle Solaris 11.2 ”.
- Página del comando man `auditconfig`(1M)

▼ Cómo eliminar privilegios básicos innecesarios de los usuarios

En determinadas circunstancias, se pueden eliminar algunos privilegios básicos de un conjunto básico de usuario invitado o regular. Por ejemplo, podría evitarse que los usuarios Sun Ray examinen el estado de los procesos que no les pertenecen.

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. **Indique una definición completa del conjunto de privilegios básicos.**

   Los siguientes tres privilegios básicos son posibles candidatos para eliminación.

   ```
   % ppriv -lv basic
   file_link_any
    Allows a process to create hardlinks to files owned by a uid
    different from the process' effective uid.
   ...
   proc_info
    Allows a process to examine the status of processes other
    than those it can send signals to.  Processes which cannot
    be examined cannot be seen in /proc and appear not to exist.
   proc_session
    Allows a process to send signals or trace processes outside its
    session.
   ...
   ```

2. **Seleccione el ámbito de la eliminación de privilegios.**

   - **Para todo el sistema.**

     A cualquier usuario que intenta usar el sistema se le niega estos privilegios. Este método de eliminación de privilegios puede ser adecuado para un equipo disponible públicamente.

     ```
     # pfedit /etc/security/policy.conf
     ...
     #PRIV_DEFAULT=basic
     PRIV_DEFAULT=basic,!file_link_any,!proc_info,!proc_session
     ```

   - **Elimine privilegios de usuarios individuales.**

     - **Impida que el usuario cree un enlace con un archivo que no sea de su propiedad.**

       ```
       # usermod -K 'defaultpriv=basic,!file_link_any' user
       ```

     - **Impida que el usuario examine procesos que no sean de su propiedad.**

       ```
       # usermod -K 'defaultpriv=basic,!proc_info' user
       ```

     - **Impida que un usuario inicie una segunda sesión, como el inicio de una sesión `ssh` desde la sesión actual del usuario.**

       ```
       # usermod -K 'defaultpriv=basic,!proc_session' user
       ```

     - **Quite los tres privilegios del conjunto básico de un usuario.**

       ```
       # usermod -K 'defaultpriv=basic,!file_link_any,!proc_info,!proc_session' user
       ```

   - **Cree y asigne un perfil de derechos.**

Esta protección se aplica a cualquier usuario o sistema al que se asigna este perfil de derechos.

a. Cree el perfil de derechos.

```
# profiles -p shared-profile -S ldap
shared-profile: set defaultpriv=basic,!file_link_any,!proc_info,!proc_session
...
```

Para obtener más información sobre cómo crear perfiles de derechos, consulte "Creación de perfiles de derechos y autorizaciones" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

b. Asigne el perfil de derechos a usuarios o a todo el sistema.

Si tiene muchos usuarios que comparten un perfil de derechos, como usuarios Sun Ray o remotos, definir este valor en un perfil de derechos puede ser una solución escalable.

```
# usermod -P shared-profile username
```

También puede asignar el perfil por sistema en el archivo `policy.conf`.

```
# pfedit /etc/security/policy.conf
...
#PROFS_GRANTED=Basic Solaris User
PROFS_GRANTED=shared-profile,Basic Solaris User
```

Véase también Para obtener más información, consulte el Capítulo 1, "Sobre el uso de los derechos para controlar los usuarios y los procesos" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 " y la página del comando man `privileges`(5).

Protección de la red

En este momento, puede que haya creado roles y también usuarios que puedan asumir dichos roles.

De las siguientes tareas de red, realice las que proporcionan seguridad adicional según los requisitos del sitio. Estas tareas de red refuerzan los protocolos IP, ARP y TCP.

TABLA 2-3 Mapa de tareas de protección de la red

Tarea	Descripción	Para obtener instrucciones
Desactivar el daemon de enrutamiento de red.	Limita el acceso a sistemas por parte de intrusos de una red.	"Cómo desactivar el daemon de enrutamiento de red" de "Protección de la red en Oracle Solaris 11.2 "

Tarea	Descripción	Para obtener instrucciones
Impedir la difusión de información sobre la topología de la red.	Impedir la difusión de paquetes.	“Cómo desactivar el reenvío de paquetes de difusión” de “Protección de la red en Oracle Solaris 11.2 ”
	Impedir que se envíen respuestas ante la difusión y la multidifusión de solicitudes de eco.	“Cómo desactivar las respuestas a las solicitudes de eco” de “Protección de la red en Oracle Solaris 11.2 ”
Para los sistemas que son puertas de enlace con otros dominios, como un cortafuegos o un nodo de VPN, activar los hosts múltiples de origen y destino estricto.	Impedir que los paquetes que no tienen la dirección de la puerta de enlace en su encabezado se muevan más allá de la puerta de enlace.	“Cómo establecer la función estricta de hosts múltiples” de “Protección de la red en Oracle Solaris 11.2 ”
Impedir ataques de denegación de servicio (DoS) mediante el control del número de conexiones del sistema incompletas.	Limitar el número permitido de conexiones TCP incompletas para una escucha TCP.	“Cómo definir el número máximo de conexiones TCP incompletas” de “Protección de la red en Oracle Solaris 11.2 ”
Impedir ataques de DoS mediante el control del número de conexiones entrantes permitidas.	Especificar el número máximo predeterminado de conexiones TCP pendientes para una escucha TCP.	“Cómo definir el número máximo de conexiones TCP pendientes” de “Protección de la red en Oracle Solaris 11.2 ”
Restablecer los valores seguros predeterminados de los parámetros de red.	Aumentar la seguridad que se redujo por acciones administrativas.	“Cómo restablecer los parámetros de red para proteger valores” de “Protección de la red en Oracle Solaris 11.2 ”
Agregar envoltorios TCP a los servicios de red para limitar las aplicaciones sólo a usuarios legítimos.	Especificar los sistemas que tienen permitido el acceso a los servicios de red, como el FTP.	Cómo utilizar los envoltorios TCP
Configurar un firewall.	Utilizar la función de filtro IP para proporcionar un firewall.	Capítulo 4, “Acerca del filtro IP en Oracle Solaris” de “Protección de la red en Oracle Solaris 11.2 ” Capítulo 5, “Configuración del filtro IP” de “Protección de la red en Oracle Solaris 11.2 ”
Configurar conexiones de red autenticadas y cifradas.	Utilizar IPsec e IKE para proteger las transmisiones de red entre los nodos y las redes que se configuran junto con IPsec e IKE.	Capítulo 7, “Configuración de IPsec” de “Protección de la red en Oracle Solaris 11.2 ” Capítulo 9, “Configuración de IKEv2” de “Protección de la red en Oracle Solaris 11.2 ”

▼ Cómo utilizar los envoltorios TCP

Los siguientes pasos muestran tres formas en que se utilizan los envoltorios TCP o que se pueden utilizar en Oracle Solaris.

Antes de empezar Debe asumir el rol `root` para modificar un programa para utilizar los envoltorios TCP.

1. **No necesita proteger la aplicación `sendmail` con envoltorios TCP.**

   De manera predeterminada, está protegida con envoltorios TCP, como se describe en “Compatibilidad con envoltorios TCP de la versión 8.12 de sendmail” de “Gestión de servicios de sendmail en Oracle Solaris 11.2 ”.

2. **Para activar los envoltorios TCP para todos los servicios `inetd`, consulte “Cómo utilizar los envoltorios TCP para controlar el acceso a los servicios TCP” de “Administración de redes TCP/IP, IPMP y túneles IP en Oracle Solaris 11.2 ”.**

3. **Proteja el servicio de red FTP con envoltorios TCP.**

   a. **Siga las instrucciones del módulo `/usr/share/doc/proftpd/modules/mod_wrap.html`.**

      Debido a que este módulo es dinámico, debe cargarlo para utilizar los envoltorios TCP con FTP.

   b. **Cargue el módulo agregando las siguientes instrucciones al archivo `proftpd.conf`:**

```
# pfedit /etc/proftpd.conf
<IfModule mod_dso.c>
    LoadModule mod_wrap.c
</IfModule>
```

   c. **Reinicie el servicio FTP.**

```
# svcadm restart svc:/network/ftp
```

Protección de sistemas de archivos

Los sistemas de archivos ZFS son ligeros y se pueden cifrar, comprimir y configurar con cuotas de espacio en disco y espacio reservado.

El sistema de archivos `tmpfs` puede aumentar de tamaño sin límites. Para impedir un ataque de denegación de servicio (DoS), complete Cómo limitar el tamaño del sistema de archivos `tmpfs` [50].

Las siguientes tareas configuran un límite de tamaño para `tmpfs` y ofrecen información sobre las protecciones que están disponibles en ZFS, el sistema de archivos predeterminado en Oracle Solaris. Para obtener más información, consulte “Configuración de cuotas y reservas de ZFS” de “Gestión de sistemas de archivos ZFS en Oracle Solaris 11.2 ” y la página del comando man `zfs`(1M).

TABLA 2-4 Mapa de tareas de protección de sistemas de archivos

Tarea	Descripción	Para obtener instrucciones
Impedir ataques de DoS mediante la gestión y la reserva de espacio en disco.	Especificar el uso del espacio en disco por sistema de archivos, por usuario o grupo, y por proyecto.	“Configuración de cuotas y reservas de ZFS” de “Gestión de sistemas de archivos ZFS en Oracle Solaris 11.2 ”

Tarea	Descripción	Para obtener instrucciones
Garantizar una cantidad mínima de espacio en disco para un conjunto de datos y sus descendientes.	Garantizar el espacio en disco por sistema de archivos, por usuario o grupo, y por proyecto.	"Establecimiento de reservas en sistemas de archivos ZFS" de "Gestión de sistemas de archivos ZFS en Oracle Solaris 11.2 "
Cifrar datos en un sistema de archivos.	Proteger un conjunto de datos con el cifrado y una contraseña para acceder al conjunto de datos en la creación del conjunto.	"Cifrado de sistemas de archivos ZFS" de "Gestión de sistemas de archivos ZFS en Oracle Solaris 11.2 " "Ejemplos de cifrado de sistemas de archivos ZFS" de "Gestión de sistemas de archivos ZFS en Oracle Solaris 11.2 "
Limitar el tamaño del sistema de archivos `tmpfs`.	Impedir que los usuarios malintencionados creen archivos de gran tamaño en `/tmp` para ralentizar el sistema.	Cómo limitar el tamaño del sistema de archivos `tmpfs` [50]

▼ Cómo limitar el tamaño del sistema de archivos `tmpfs`

El tamaño del sistema de archivos `tmpfs` no está limitado de manera predeterminada. Por lo tanto, `tmpfs` puede crecer y llenar la memoria disponible del sistema y los volúmenes de intercambio. Como el directorio `/tmp` es usado por todas las aplicaciones y todos los usuarios, una aplicación puede ocupar toda la memoria disponible del sistema. Del mismo modo, un usuario sin privilegios con malas intenciones podría provocar una ralentización del sistema al crear archivos de gran tamaño en el directorio `/tmp`. A fin de evitar un impacto en el rendimiento, puede limitar el tamaño de cada montaje de `tmpfs`.

Puede probar varios valores para conseguir el mejor rendimiento del sistema.

Antes de empezar Para editar el archivo `vfstab`, debe convertirse en un administrador que tiene asignada la autorización `solaris.admin.edit/etc/vfstab`. Para reiniciar el sistema, se le debe asignar el perfil de derechos de mantenimiento y reparación. El rol `root` tiene todos estos derechos. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

1. Determine la cantidad de memoria del sistema.

Nota - El sistema SPARC T3 que se usa para el siguiente ejemplo tiene un disco de estado sólido (ssd) para una E/S más rápida y tiene ocho discos de 279,40 MB. El sistema tiene aproximadamente 500 GB de memoria.

```
% prtconf | head
System Configuration:  Oracle Corporation  sun4v
Memory size: 523776 Megabytes
System Peripherals (Software Nodes):
```

```
ORCL,SPARC-T3-4
scsi_vhci, instance #0
disk, instance #4
disk, instance #5
disk, instance #6
disk, instance #8
```

2. Compute un límite de memoria para `tmpfs`.

Según el tamaño de la memoria del sistema, quizás quiera computar un límite de memoria de aproximadamente el 20% para sistemas de gran tamaño y alrededor del 30% para sistemas de menor tamaño.

Por lo tanto, para un sistema de menor capacidad, utilice `.30` como multiplicador.

```
10240M x .30 ≈ 340M
```

Para un sistema más grande, utilice `.20` como multiplicador.

```
523776M x .20 ≈ 10475M
```

3. Modifique la entrada `swap` en el archivo `/etc/vfstab` con el límite de tamaño.

```
# pfedit /etc/vfstab
#device     device       mount       FS      fsck    mount mount
#to mount   to fsck      point       type    pass    at boot options
#
...
#swap       -            /tmp        tmpfs   -       yes     -
swap        -            /tmp        tmpfs   -       yes     size=10400m
/dev/zvol/dsk/rpool/swap   -      -  swap    -       no      -
```

4. Reinicie el sistema.

```
# reboot
```

5. Compruebe que el límite de tamaño se haya aplicado.

```
% mount -v
swap on /system/volatile type tmpfs
read/write/setuid/devices/rstchown/xattr/dev=89c0006 on Tues Feb 4 14:07:27 2014
swap on /tmp type tmpfs
read/write/setuid/devices/rstchown/xattr/size=10400m/dev=89c0006 on Tues ...
```

6. Supervise el uso de memoria y ajústelo según los requisitos de su sitio.

El comando `df` puede llegar a ser útil. El comando `swap` proporciona las estadísticas más útiles.

```
% df -h /tmp
Filesystem Size Used Available Capacity Mounted on
swap          7.  4G     44M    7.4G 1%       /tmp

% swap -s
total: 190248k bytes allocated + 30348k reserved = 220596k used,
```

```
7743780k available
```

Para obtener más información, consulte las páginas del comando man `tmpfs`(7FS), `mount_tmpfs`(1M), `df`(1M) y `swap`(1M).

Protección y modificación de archivos

De manera predeterminada, solamente el rol `root` puede modificar permisos de archivos del sistema. Los roles y los usuarios que tienen asignada la autorización `solaris.admin.edit/`*path-to-system-file* pueden modificar *system-file*. Solamente el rol `root` puede buscar todos los archivos.

TABLA 2-5 Mapa de tareas de protección y modificación de archivos

Tarea	Descripción	Para obtener instrucciones
Configurar permisos de archivo restrictivos para los usuarios comunes.	Fijar un valor más restrictivo que `022` para los permisos de archivo de los usuarios comunes.	Cómo definir un valor `umask` más restrictivo para usuarios comunes [43]
Especificar las ACL para proteger archivos con una granularidad más específica que los permisos de archivo UNIX comunes.	Los atributos de seguridad ampliados pueden ser útiles para proteger archivos. Para ver una advertencia sobre el uso de las ACL, consulte Hiding Within the Trees (Ocultos entre los árboles) (http://www.usenix.org/publications/login/2004-02/pdfs/brunette.pdf).	ZFS End-to-End Data Integrity (Integridad de los datos de extremo a extremo de ZFS) (http://blogs.oracle.com/bonwick/entry/zfs_end_to_end_data)
Mantener la integridad de los archivos del sistema.	Encontrar archivos peligrosos mediante una secuencia de comandos o mediante BART.	"Cómo buscar archivos con permisos de archivo especiales" de "Protección y verificación de la integridad de archivos en Oracle Solaris 11.2 "

Protección del acceso al sistema y su uso

Puede configurar las funciones de seguridad de Oracle Solaris para proteger el uso del sistema, incluidas las aplicaciones y los servicios en el sistema y en la red.

TABLA 2-6 Mapa de tareas de protección del acceso al sistema y su uso

Tarea	Descripción	Para obtener instrucciones
Impedir que los programas se aprovechen de una pila ejecutable.	Definir una variable del sistema que evita que el desbordamiento del aprovechamiento de la memoria intermedia se aproveche de la pila ejecutable.	"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 "
Garantizar que los binarios que están etiquetados para la ejecución aleatoria	Permitir la ASLR para binarios etiquetados.	Cómo verificar que la ASLR esté activada [33]

Tarea	Descripción	Para obtener instrucciones
de la disposición del espacio de direcciones (ASLR) puedan utilizarla.		
Configurar las opciones de auditoría.	Personalizar la configuración de auditoría para la cobertura y la integridad de archivos.	“Uso del servicio de auditoría” [58]
Proteger los archivos del núcleo central que puedan contener información confidencial.	Crear un directorio con acceso limitado que está dedicado a archivos del núcleo central.	“Activación de rutas de archivos” de “Resolución de problemas de administración del sistema en Oracle Solaris 11.2 ” “Administración de las especificaciones del archivo del núcleo central” de “Resolución de problemas de administración del sistema en Oracle Solaris 11.2 ”
Proteger un servidor web con proxy SSL en el nivel del núcleo.	El protocolo de capa de conexión segura (SSL) se puede utilizar para cifrar y acelerar las comunicaciones del servidor web.	Capítulo 3, “Servidores web y el protocolo de capa de sockets seguros” de “Protección de la red en Oracle Solaris 11.2 ”
Crear zonas para contener aplicaciones.	Las zonas son contenedores que aíslan los procesos. Pueden aislar las aplicaciones y sus partes. Por ejemplo, las zonas pueden utilizarse para separar la base de datos de un sitio web del servidor web del sitio.	“Introducción a Zonas de Oracle Solaris ”
Gestionar los recursos en las zonas.	Las zonas proporcionan una cantidad de herramientas para gestionar los recursos de las zonas.	“Administración de la gestión de recursos en Oracle Solaris 11.2 ”

Protección de un servicio heredado con SMF

Puede limitar la configuración de aplicaciones a roles o usuarios de confianza agregando la aplicación a la función de utilidad de gestión de servicios (SMF) de Oracle Solaris y solicitando derechos para iniciar, refrescar y detener el servicio.

Para obtener información y conocer los procedimientos consulte lo siguiente:

- “Bloqueo de recursos utilizando privilegios ampliados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”
- Securing MySQL using SMF - the Ultimate Manifest (Cómo asegurar MySQL con SMF: el manifiesto clave) (http://blogs.oracle.com/bobn/entry/securing_mysql_using_smf_the)
- Las páginas del comando man seleccionadas son `smf`(5), `smf_security`(5), `svcadm`(1M), `svcbundle`(1M) y `svccfg`(1M).

Configuración de una red de Kerberos

Puede proteger su red con el servicio Kerberos. Esta arquitectura cliente-servidor proporciona transacciones seguras a través de redes. El servicio ofrece una sólida autenticación de usuario y también integridad y privacidad. Con el servicio Kerberos, puede iniciar sesión en otros sistemas, ejecutar comandos, intercambiar datos y transferir archivos de manera segura.

Además, el servicio permite a los administradores restringir el acceso a los servicios y a los sistemas. Como usuario de Kerberos, puede regular el acceso de otras personas a su cuenta.

Para obtener información y conocer los procedimientos consulte lo siguiente:

- Capítulo 3, “Planificación del servicio Kerberos” de “Gestión de Kerberos y otros servicios de autenticación en Oracle Solaris 11.2 ”
- Capítulo 4, “Configuración del servicio Kerberos” de “Gestión de Kerberos y otros servicios de autenticación en Oracle Solaris 11.2 ”
- Las páginas del comando man seleccionadas son `kadmin`(1M), `pam_krb5`(5) y `kclient`(1M).

Agregación de seguridad de varios niveles con etiquetas

Trusted Extensions amplía la seguridad de Oracle Solaris mediante la aplicación de una política de control de acceso obligatorio (MAC) basada en etiquetas. Las etiquetas de confidencialidad se aplican automáticamente a todas las fuentes de datos (redes, sistemas de archivos y ventanas) y también a los consumidores de datos (usuarios y procesos). El acceso a todos los datos se restringe según la relación entre la etiqueta de los datos (objeto) y el consumidor (sujeto). La funcionalidad en capas consta de un conjunto de servicios que reconocen etiquetas.

En una lista parcial de servicios de Trusted Extensions, se incluyen:

- redes con etiquetas
- uso compartido y montaje de sistema de archivos con reconocimiento de etiquetas
- escritorio con etiquetas
- traducción y configuración de etiquetas
- herramientas de gestión de sistemas con reconocimiento de etiquetas
- asignación de dispositivos con reconocimiento de etiquetas

Los paquetes `system/trusted` y `system/trusted/trusted-global-zone` son suficientes para un sistema sin periféricos o un servidor que no requiera un escritorio de varios niveles. El paquete `system/trusted/trusted-extensions` proporciona el entorno de escritorio de confianza de varios niveles de Oracle Solaris.

Configuración de Trusted Extensions

Debe instalar los paquetes de Trusted Extensions antes de configurar el sistema. Cuando instale el paquete `trusted-extensions`, el sistema puede ejecutar un escritorio con un dispositivo de visualización con mapa de bits conectado directamente, como un equipo portátil o una estación de trabajo. Se requiere una configuración de red para la comunicación con otros sistemas.

Para obtener información y conocer los procedimientos consulte lo siguiente:

- Parte I, “Configuración inicial de Trusted Extensions” de “Configuración y administración de Trusted Extensions ”
- Parte II, “Administración de Trusted Extensions” de “Configuración y administración de Trusted Extensions ”

Configuración de IPsec con etiquetas

Con IPsec puede proteger los paquetes con etiquetas.

Para obtener información y conocer los procedimientos consulte lo siguiente:

- Capítulo 6, “Acerca de la arquitectura de seguridad IP” de “Protección de la red en Oracle Solaris 11.2 ”
- “Administración de IPsec con etiquetas” de “Configuración y administración de Trusted Extensions ”
- “Configuración de IPsec con etiquetas” de “Configuración y administración de Trusted Extensions ”

♦ ♦ ♦ CAPÍTULO 3

Mantenimiento y supervisión de la seguridad de Oracle Solaris

Después de la instalación y la configuración iniciales, puede mantener y supervisar la postura de seguridad del sistema siguiendo los procedimientos para lo siguiente:

- revisar registros de auditoría con regularidad,
- ejecutar comprobaciones de integridad de paquetes y archivos,
- supervisar la actividad de la red,
- ejecutar comprobaciones de conformidad.

Mantenimiento y supervisión de la seguridad del sistema

Las siguientes tareas mantienen y supervisan el acceso al sistema y su uso, los datos y el cumplimiento de los requisitos de seguridad del sitio.

TABLA 3-1 Mapa de tareas de mantenimiento y supervisión del sistema

Tarea	Descripción	Para obtener instrucciones
Verificar los paquetes en el sistema.	Comprobar que los paquetes sean idénticos a los paquetes de origen tras una actualización.	Cómo comprobar los paquetes [33]
Verificar la integridad de archivos.	Comparar los manifiestos BART a intervalos regulares para garantizar que solamente se cambien los archivos que se deben cambiar tras la configuración.	"Verificación de la integridad de archivos mediante el uso de BART" [58]
Buscar archivos peligrosos.	Detectar el posible uso no autorizado de los permisos `setuid` y `setgid` en los programas.	"Cómo buscar archivos con permisos de archivo especiales" de "Protección y verificación de la integridad de archivos en Oracle Solaris 11.2 "
Revisar logs de auditoría con regularidad.	Buscar accesos al sistema y usos de él inusuales.	"Uso del servicio de auditoría" [58]
Revisar logs de auditoría para eventos de inicio y cierre de sesión en tiempo real.	Identificar intentos de infracción cerca del momento en que se producen.	"Supervisión de registros de auditoría en tiempo real" [59]
Ejecutar pruebas de conformidad.	Evaluar la conformidad del sistema con referencias de seguridad.	"Guía de cumplimiento de la seguridad de Oracle Solaris 11.2 " y la página del comando man `compliance`(1M)

Verificación de la integridad de archivos mediante el uso de BART

BART es una herramienta basada en reglas de generación de informes y análisis de la integridad de los archivos que utiliza hashes con potencia de cifrado y metadatos de sistema de archivos para informar cambios.

Para obtener información y conocer los procedimientos consulte lo siguiente:

- "Acerca de BART" de "Protección y verificación de la integridad de archivos en Oracle Solaris 11.2 "
- "Acerca del uso de BART" de "Protección y verificación de la integridad de archivos en Oracle Solaris 11.2 "
- "Manifiestos, archivos de reglas e informes de BART" de "Protección y verificación de la integridad de archivos en Oracle Solaris 11.2 "

Para obtener instrucciones específicas sobre cómo registrar cambios efectuados en sistemas instalados, consulte "Cómo comparar manifiestos para el mismo sistema a lo largo del tiempo" de "Protección y verificación de la integridad de archivos en Oracle Solaris 11.2 ".

Uso del servicio de auditoría

La auditoría permite llevar un registro del uso del sistema. El servicio de auditoría incluye herramientas para ayudar con el análisis de los datos de auditoría.

El servicio de auditoría se describe en "Gestión de auditoría en Oracle Solaris 11.2 ". Para obtener una lista con enlaces de las páginas del comando man, consulte "Páginas del comando man del servicio de auditoría" de "Gestión de auditoría en Oracle Solaris 11.2 ".

Los siguientes procedimientos del servicio de auditoría son útiles en muchos entornos seguros:

- Cree roles diferentes para configurar y para revisar la auditoría, y también para iniciar o detener el servicio de auditoría. Asigne los roles a usuarios de confianza.

  Utilice los perfiles de derechos de configuración de auditoría, de revisión de auditoría y de control de auditoría como base para los roles.

  Para crear roles o usar los roles predefinidos ARMOR, consulte "Asignación de derechos a usuarios" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".
- Audite a todos los administradores con la clase de auditoría `cusa`.

  Los eventos en la clase de auditoría `cusa` cubren las acciones administrativas que afectan la postura de seguridad del sistema. Para obtener una descripción, consulte el archivo `/etc/security/audit_class`. Para conocer el procedimiento, consulte Cómo auditar eventos importantes además del inicio y el cierre de sesión [44].
- Envíe registros de auditoría a un servidor central.

    - Configure la auditoría para trabajar con el servidor de auditoría remoto (ARS).

      Consulte “Cómo enviar archivos de auditoría a un repositorio remoto” de “Gestión de auditoría en Oracle Solaris 11.2 ”.
    - Programe la transferencia segura de los archivos de auditoría completos a un sistema de archivos de revisión de auditoría en una agrupación ZFS independiente.
- Supervise los resúmenes de texto de los eventos auditados seleccionados en la utilidad `syslog`.

  Active el complemento `audit_syslog` y, luego, supervise los eventos informados.

  Consulte “Cómo configurar registros de auditoría syslog” de “Gestión de auditoría en Oracle Solaris 11.2 ”.
- Limite el tamaño de los archivos de auditoría.

  Fije el atributo `p_fsize` para el complemento `audit_binfile` en un tamaño útil. Tenga en cuenta, entre otros factores, el programa de revisión, el espacio en disco y la frecuencia de trabajo de `cron`.

  Para obtener ejemplos, consulte “Cómo asignar espacio de auditoría para la pista de auditoría” de “Gestión de auditoría en Oracle Solaris 11.2 ”.
- Programe la transferencia segura de los archivos de auditoría completos a un sistema de archivos de revisión de auditoría en una agrupación ZFS independiente.
- Revise los archivos de auditoría completos en el sistema de archivos de revisión de auditoría.

Supervisión de registros de auditoría en tiempo real

El complemento `audit_syslog` permite registrar resúmenes de eventos de auditoría preseleccionados. Para mostrar los resúmenes de auditoría en una ventana de terminal a medida que se generan, ejecute un comando similar al siguiente:

```
# tail -0f  /var/adm/auditlog
```

Para configurar el log de auditoría, consulte “Cómo configurar registros de auditoría syslog” de “Gestión de auditoría en Oracle Solaris 11.2 ”.

Revisión y archivado de registros de auditoría

Los registros de auditoría se pueden visualizar en formato de texto o en un explorador con formato XML.

Para obtener información y conocer los procedimientos consulte lo siguiente:

- “Logs de auditoría” de “Gestión de auditoría en Oracle Solaris 11.2 ”

- “Cómo evitar el desbordamiento de la pista de auditoría” de “Gestión de auditoría en Oracle Solaris 11.2 ”
- “Visualización de datos de pista de auditoría” de “Gestión de auditoría en Oracle Solaris 11.2 ”

♦ ♦ ♦ APÉNDICE A

Bibliografía para la seguridad de Oracle Solaris

Las siguientes referencias contienen información de seguridad útil para los sistemas Oracle Solaris. La información de seguridad de las versiones anteriores de Oracle Solaris contiene algunos datos útiles y algunos datos obsoletos.

Referencias de seguridad en Oracle Technology Network

Los siguientes manuales y artículos en el sitio web Oracle Technology Network contienen descripciones sobre la seguridad de los sistemas Oracle Solaris 11:

- "Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 "
- "Protección y verificación de la integridad de archivos en Oracle Solaris 11.2 "
- "Protección de la red en Oracle Solaris 11.2 "
- "Protección de los usuarios y los procesos en Oracle Solaris 11.2 "
- "Gestión de cifrado y certificados en Oracle Solaris 11.2 "
- "Gestión de auditoría en Oracle Solaris 11.2 "
- "Gestión de Kerberos y otros servicios de autenticación en Oracle Solaris 11.2 "
- "Gestión de acceso mediante shell seguro en Oracle Solaris 11.2 "
- "Guía de cumplimiento de la seguridad de Oracle Solaris 11.2 "
- "Using a FIPS 140 Enabled System in Oracle Solaris 11.2 "

Referencias de seguridad de Oracle Solaris en publicaciones de terceros

Los siguientes manuales contienen descripciones sobre la seguridad de los sistemas Oracle Solaris 11:

- *Referencia de configuración de seguridad para Solaris 11 11/11 versión 1.0.0, 11 de junio de 2012*

  Esta referencia de seguridad es publicada por Center for Internet Security (CIS) http://cisecurity.org/ para la comunidad de seguridad. Este documento recomienda la

configuración de seguridad para el Sistema operativo Oracle Solaris. Entre los destinatarios, se incluyen los administradores de sistemas y aplicaciones, los especialistas en seguridad, los auditores, los ingenieros de soporte, y los instaladores y desarrolladores que desarrollan, instalan, evalúan y propocionan soluciones de seguridad para Oracle Solaris. Para obtener una copia, visite CIS Security Benchmarks (http://benchmarks.cisecurity.org/).

- *Oracle Solaris 11 System Administration: The Complete Reference* (Administración del sistema Oracle Solaris 11: La referencia completa). Michael Jang, Harry Foxwell, Christine Tran y Alan Formy-Duval. 2012. McGraw-Hill. ISBN 978007179042.

  Este manual incluye una cobertura sobre la seguridad de Oracle Solaris.
- *Oracle Solaris 11: First Look* (Oracle Solaris 11: La primera impresión). Philip P. Brown. 2013. Packt Publishing. ISBN 9781849688307.

  Este manual presenta a los administradores Oracle Solaris y su seguridad.
- *Oracle Solaris 11 System Administration* (Administración del sistema Oracle Solaris 11). BiIl Calkins. 2013. Prentice Hall. ISBN 9780133007114.

  Este manual cubre las nuevas funciones de Oracle Solaris, incluidas las funciones de seguridad.