Directrices de seguridad de Oracle® Solaris 11

Referencia: E25815
Marzo de 2012

ORACLE

120424@25097

Contenido

Prefacio

Esta guía presenta directrices de seguridad para el Sistema operativo Oracle Solaris (SO Oracle Solaris). En primer lugar, la guía describe problemas de seguridad que se deben atender en un SO para empresas. A continuación, describe las funciones de seguridad predeterminadas de SO Oracle Solaris. Por último, la guía proporciona pasos específicos que se deben seguir para reforzar el sistema y para utilizar las funciones de seguridad de Oracle Solaris para proteger los datos y las aplicaciones. Puede personalizar las recomendaciones de esta guía según la política de seguridad de su sitio.

Destinatarios

Directrices de seguridad de Oracle Solaris 11 está destinada a los administradores de la seguridad y otros administradores que realizan las siguientes tareas:

- Analizar los requisitos de seguridad
- Implementar la política de seguridad del sitio en el software
- Instalar y configurar el SO Oracle Solaris
- Mantener la seguridad de los sistemas y las redes

Para utilizar esta guía debe tener conocimientos generales de administración de UNIX, una buena base de seguridad de software y conocimientos acerca de la política de seguridad de su sitio.

Acceso a Oracle Support

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

Convenciones tipográficas

La siguiente tabla describe las convenciones tipográficas utilizadas en este manual.

TABLA P–1 Convenciones tipográficas

Tipos de letra	Descripción	Ejemplo
`AaBbCc123`	Los nombres de los comandos, los archivos, los directorios y los resultados que el equipo muestra en pantalla	Edite el archivo `.login`. Utilice el comando `ls -a` para mostrar todos los archivos. `nombre_sistema% tiene correo.`
`AaBbCc123`	Lo que se escribe, en contraposición con la salida del equipo en pantalla	`nombre_sistema%` **`su`** `Contraseña:`
aabbcc123	Marcador de posición: sustituir por un valor o nombre real	El comando necesario para eliminar un archivo es `rm` *nombre_archivo*.
AaBbCc123	Títulos de los manuales, términos nuevos y palabras destacables	Consulte el capítulo 6 de la *Guía del usuario*. Una *copia en antememoria* es aquella que se almacena localmente. *No* guarde el archivo. **Nota:** algunos elementos destacados aparecen en negrita en línea.

Indicadores de los shells en los ejemplos de comandos

La tabla siguiente muestra los indicadores de sistema UNIX predeterminados y el indicador de superusuario de shells que se incluyen en los sistemas operativos Oracle Solaris. Tenga en cuenta que el indicador predeterminado del sistema que se muestra en los ejemplos de comandos varía según la versión de Oracle Solaris.

TABLA P–2 Indicadores de shell

Shell	Indicador
Shell Bash, shell Korn y shell Bourne	`$`
Shell Bash, shell Korn y shell Bourne para superusuario	`#`
Shell C	`nombre_sistema%`
Shell C para superusuario	`nombre_sistema#`

◆ ◆ ◆ CAPÍTULO 1

1 Descripción general de la seguridad de Oracle Solaris 11

Oracle Solaris 11 es un sistema operativo para empresas sólido y de primera calidad que ofrece funciones de seguridad comprobadas. Con un sistema de seguridad en toda la red sofisticado 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 requerimientos 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 11 está completamente probado y admitido en una gran variedad de sistemas basados en SPARC y x86 de Oracle y en otras plataformas de hardware de otros proveedores.

Protecciones de seguridad de Oracle Solaris 11

Oracle Solaris proporciona una base sólida para las aplicaciones y los datos de la empresa mediante la protección de los datos que se encuentran en el disco o en tránsito. El administrador de recursos de Oracle Solaris (*gestión de recursos*) y las zonas de Oracle Solaris proporcionan funciones que alejan y protegen a las aplicaciones del mal uso. Esta contención, junto con el privilegio mínimo implementado mediante privilegios y la función de control de acceso basado en roles (RBAC) de Oracle Solaris, reduce el riesgo de seguridad que puedan causar los intrusos o los usuarios comunes. Los protocolos encriptados y autenticados, como la seguridad IP (IPsec), proporcionan redes privadas virtuales (VPN) a través de Internet y también túneles dentro de una LAN o una WAN para que la entrega de datos sea más segura. Además, la función de auditoría de Oracle Solaris garantiza que se guarden los registros de cualquier actividad de interés.

Los servicios de seguridad de Oracle Solaris 11 brindan una protección profunda, ya que ofrecen capas de protección para el sistema y para la red. Oracle Solaris protege el núcleo

limitando, dentro de las utilidades del núcleo, las acciones que la utilidad puede realizar. La configuración de red predeterminada protege los datos en el sistema y en toda la red. IPsec, la función de filtro IP de Oracle Solaris, y Kerberos pueden brindar protecciones adicionales.

Los servicios de seguridad de Oracle Solaris incluyen:

- Protección del núcleo: privilegios y permisos de archivos protegen los daemons y los dispositivos del núcleo.
- Protección de los inicios de sesión: se requiere una contraseña para iniciar sesión. Las contraseñas tienen un cifrado fuerte. De manera inicial, los inicios de sesión remotos están limitados a un canal autenticado y cifrado mediante la función Secure Shell de Oracle Solaris. La cuenta `root` no puede iniciar sesión directamente.
- Protección de datos: permisos de archivos protegen los datos en el disco. Se pueden configurar capas adicionales de protección. Por ejemplo, puede utilizar las listas de control de acceso (ACL), situar los datos en una zona, cifrar un archivo, cifrar un conjunto de datos ZFS de Oracle Solaris, crear un conjunto de datos ZFS de sólo lectura y montar sistemas de archivos para que no se puedan ejecutar ni los programas de `setuid` ni los archivos ejecutables.

Tecnologías de seguridad de Oracle Solaris 11

Las funciones de seguridad de Oracle Solaris se pueden configurar para implementar la política de seguridad del sitio.

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.

Servicio de auditoría

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

La auditoría es un requisito básico para la evaluación de la seguridad, la validación 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 páginas del comando man relacionadas con la auditoría, consulte el Capítulo 29, "Auditoría (referencia)" de *Administración de Oracle Solaris: servicios de seguridad*.
- Para obtener directrices, consulte "Auditar eventos importantes además del inicio y el cierre de sesión" en la página 35 y las páginas del comando man.
- Para obtener una descripción general de la auditoría, consulte el Capítulo 26, "Auditoría (descripción general)" de *Administración de Oracle Solaris: servicios de seguridad*.
- Para obtener información sobre las tareas de auditoría, consulte el Capítulo 28, "Gestión de auditoría (tareas)" de *Administración de Oracle Solaris: servicios de seguridad*.

Herramienta básica de creación de informes de auditoría

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. Mediante la creación de manifiestos de BART, de manera fácil y segura, podrá recopilar información sobre los componentes de la pila de software que esté instalado en los sistemas implementados.

BART es una herramienta útil para la gestión de la integridad en un sistema o en una red de sistemas.

Para obtener más información, consulte lo siguiente:

- Las páginas del comando man seleccionadas son: `bart(1M)`, `bart_rules(4)` y `bart_manifest(4)`.
- Para obtener directrices, consulte "Creación de una instantánea de BART del sistema" en la página 50, "Uso de la herramienta básica de creación de informes de auditoría" en la página 53 y las páginas del comando man.
- Para obtener una descripción general de BART, consulte el Capítulo 6, "Uso de la herramienta básica de creación de informes de auditoría (tareas)" de *Administración de Oracle Solaris: servicios de seguridad*.
- Para obtener ejemplos sobre cómo usar BART, consulte "Uso de BART (tareas)" de *Administración de Oracle Solaris: servicios de seguridad* y las páginas del comando man.

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. Los distintos mecanismos de almacenamiento, utilidades administrativas e interfaces de programación para varias infraestructuras de clave pública (PKI) pueden utilizar una interfaz unificada cuando incorporan interfaces KMF.

La estructura criptográfica proporciona servicios criptográficos a los usuarios y las aplicaciones por medio de comandos individuales, una interfaz de programación en el nivel de usuario y otra en el núcleo, y marcos en el nivel de usuario y en el núcleo. La estructura criptográfica proporciona estos servicios criptográficos a todas las aplicaciones y los módulos del núcleo de manera ininterrumpida para el usuario final. También brinda servicios criptográficos directos, como el cifrado y el descifrado de archivos, para el usuario final.

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 11, "Estructura criptográfica (descripción general)" de *Administración de Oracle Solaris: servicios de seguridad* y el Capítulo 13, "Estructura de gestión de claves" de *Administración de Oracle Solaris: servicios de seguridad*.
- Para obtener ejemplos sobre cómo usar la estructura criptográfica, consulte el Capítulo 12, "Estructura criptográfica (tareas)" de *Administración de Oracle Solaris: servicios de seguridad* y las páginas del comando man.

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, ZFS es compatible con las listas de control de acceso (ACL), también llamadas entradas de control de acceso (ACE), 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 instrucciones sobre la configuración de ACL en archivos ZFS, consulte la página del comando man `chmod(1)`.
- Para obtener una descripción general de los permisos de archivo, consulte "Uso de permisos UNIX para proteger archivos" de *Administración de Oracle Solaris: servicios de seguridad*.

- Para obtener una descripción general y ejemplos de la protección de archivos ZFS, consulte el Capítulo 8, "Uso de listas de control de acceso y atributos para proteger archivos Oracle Solaris ZFS" de *Administración de Oracle Solaris: sistemas de archivos ZFS* y las páginas del comando man.

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.

Filtro IP

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:

- Las páginas del comando man seleccionadas son: `ipfilter`(5), `ipf`(1M), `ipnat`(1M), `svc.ipfd`(1M) y `ipf`(4).
- Para obtener una descripción general del filtro IP, consulte el Capítulo 20, "Filtro IP en Oracle Solaris (descripción general)" de *Administración de Oracle Solaris: servicios IP*.
- Para obtener ejemplos sobre el uso del filtro IP, consulte el Capítulo 21, "Filtro IP (tareas)" de *Administración de Oracle Solaris: servicios IP* 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).

Envoltorios TCP

Los envoltorios TCP proporcionan un modo de implementar controles de acceso mediante la comprobación de que la dirección del host que solicita un servicio de red concreto aparezca 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 porque son una función de supervisión muy útil. Las funciones Secure Shell y `sendmail` de Oracle Solaris están configuradas para utilizar los envoltorios TCP. Entre los servicios de red que se podrían colocar en control de acceso se incluyen `ftpd` y `rpcbind`.

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 más información, consulte lo siguiente:

- Para obtener información sobre los envoltorios TCP, consulte "Cómo utilizar los envoltorios TCP para controlar el acceso a los servicios TCP" de *Administración de Oracle Solaris: servicios IP*.
- 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 contraseñas y sus restricciones

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

Oracle Solaris tiene una cantidad de funciones que se pueden usar para promover las contraseñas de usuario seguras. Se puede establecer la longitud, el contenido, la frecuencia de cambio y los requisitos de modificación de las contraseñas, y también se puede llevar un historial de las contraseñas. Se proporciona un diccionario que contiene las contraseñas que deben evitarse. Hay varios algoritmos de contraseña posibles.

Para obtener más información, consulte lo siguiente:

- "Mantenimiento del control de inicio de sesión" de *Administración de Oracle Solaris: servicios de seguridad*
- "Protección de inicios de sesión y contraseñas (tareas)" de *Administración de Oracle Solaris: servicios de seguridad*
- Las páginas del comando man seleccionadas son: `passwd`(1) y `crypt.conf`(4).

Módulo de autenticación conectable

El módulo de autenticación conectable (PAM, Pluggable Authentication Module) es una estructura que permite coordinar y configurar los requisitos de autenticación de usuario para las cuentas, las credenciales, las sesiones y las contraseñas.

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 `ftp` utilizan la estructura PAM a fin de garantizar que todos los puntos de entrada del sistema estén protegidos. Esta arquitectura permite la sustitución o

modificación de los módulos de autenticación en el campo para proteger el sistema contra cualquier fallo recién detectado sin la necesidad de realizar cambios a ningún servicio del sistema que use la estructura PAM.

Para obtener más información, consulte lo siguiente:

- El Capítulo 15, "Uso de PAM" de *Administración de Oracle Solaris: servicios de seguridad*
- La página del comando man `pam.conf(4)`

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`. Los privilegios se pueden otorgar a un comando, un usuario, un rol o un sistema. Muchos comandos y daemons de Oracle Solaris se ejecutan solamente con los privilegios requeridos para realizar su tarea. El uso de privilegios también se denomina *gestión de derechos de procesos*.

Los programas que reconocen privilegios pueden impedir que los intrusos obtengan más privilegios que los que utiliza el propio programa. Además, los privilegios permiten a las organizaciones 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:

- "Privilegios (descripción general)" de *Administración de Oracle Solaris: servicios de seguridad*
- "Uso de privilegios (tareas)" de *Administración de Oracle Solaris: servicios de seguridad*
- El 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)`.

Acceso remoto

Los ataques de acceso remoto pueden causar daños en el sistema y en la red. En el entorno de Internet actual, es necesario proteger el acceso a la red, incluso en entornos WAN y LAN.

IPsec e IKE

La seguridad IP (IPsec) protege paquetes IP mediante la autenticación y/o el cifrado de los paquetes. Oracle Solaris admite IPsec para IPv4 y para IPv6. 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) utilizan algoritmos de la estructura criptográfica. Además, la estructura criptográfica proporciona un almacén de claves softtoken para las aplicaciones que utilizan la metarranura. 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 softtoken.

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:

- El Capítulo 14, "Arquitectura de seguridad IP (descripción general)" de *Administración de Oracle Solaris: servicios IP*
- El Capítulo 15, "Configuración de IPsec (tareas)" de *Administración de Oracle Solaris: servicios IP*
- El Capítulo 17, "Intercambio de claves de Internet (descripción general)" de *Administración de Oracle Solaris: servicios IP*
- El Capítulo 18, "Configuración de IKE (tareas)" de *Administración de Oracle Solaris: servicios IP*
- Las páginas del comando man seleccionadas son: `ipsecconf`(1M) y `in.iked`(1M).

Secure Shell

La función Secure Shell de Oracle Solaris permite a los usuarios o los servicios acceder a archivos entre sistemas remotos, o transferirlos, mediante una canal de comunicaciones cifradas. En Secure Shell, todo el tráfico de red está cifrado. Secure Shell 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, Secure Shell impide que los posibles intrusos lean una comunicación interceptada o que los adversarios falsifiquen el sistema. De manera predeterminada, Secure Shell es el único mecanismo de acceso remoto activo en un sistema recién instalado.

Para obtener más información, consulte lo siguiente:

- Capítulo 17, "Uso de Secure Shell (tareas)" de *Administración de Oracle Solaris: servicios de seguridad*
- Las páginas del comando man seleccionadas son: `ssh`(1), `sshd`(1M), `sshd_config`(4) y `ssh_config`(4).

Servicio Kerberos

El función Kerberos de Oracle Solaris permite el inicio de sesión único y las transacciones seguras, incluso en redes heterogéneas que ejecutan 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 es una arquitectura de cliente-servidor que 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 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:

- La Parte VI, "Servicio Kerberos" de *Administración de Oracle Solaris: servicios de seguridad*
- Las páginas del comando man seleccionadas son: `kerberos(5)` y `kinit(1)`.

Control de acceso basado en roles

El control de acceso basado en roles (RBAC, Role-Based Access Control) aplica el principio de seguridad de privilegio mínimo, que permite a las organizaciones otorgar derechos administrativos de manera selectiva a usuarios o roles según sus necesidades y requisitos particulares.

La función RBAC de Oracle Solaris controla el acceso de usuario a las tareas que normalmente se limitan al rol `root`. Mediante la aplicación de atributos de seguridad a procesos y usuarios, RBAC puede distribuir los derechos administrativos entre varios administradores. RBAC también se denomina *gestión de derechos de usuarios*.

Para obtener más información, consulte lo siguiente:

- Parte III, "Roles, perfiles de derechos y privilegios" de *Administración de Oracle Solaris: servicios de seguridad*
- Las páginas del comando man seleccionadas son: `rbac(5)`, `roleadd(1M)`, `profiles(1)` y `user_attr(4)`.

Utilidad de gestión de 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 RBAC 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:

- Capítulo 6, "Gestión de servicios (descripción general)" de *Administración de Oracle Solaris: tareas comunes*
- El Capítulo 7, "Gestión de servicios (tareas)" de *Administración de Oracle Solaris: tareas comunes*
- La páginas del comando man seleccionadas son: `svcadm`(1M), `svcs`(1) y `smf`(5).

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. ACE y los permisos UNIX protegen los archivos, y RBAC admite la administración delegada de conjuntos de datos ZFS.

Para obtener más información, consulte lo siguiente:

- Capítulo 1, "Sistema de archivos ZFS de Oracle Solaris (introducción)" de *Administración de Oracle Solaris: sistemas de archivos ZFS*
- El Capítulo 3, "Oracle Solaris ZFS y sistemas de archivos tradicionales" de *Administración de Oracle Solaris: sistemas de archivos ZFS*
- El Capítulo 6, "Administración de sistemas de archivos ZFS de Oracle Solaris" de *Administración de Oracle Solaris: sistemas de archivos ZFS*
- Las páginas del comando man seleccionadas son: `zfs`(1M) y `zfs`(7FS).

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.

Para obtener más información, consulte lo siguiente:

- Parte II, "Zonas de Oracle Solaris" de *Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*
- Las páginas del comando man seleccionadas son: `brands(5)`, `zoneadm(1M)` y `zonecfg(1M)`.

Trusted Extensions

La función Trusted Extensions de Oracle Solaris es una capa con tecnología de etiquetado seguro que se habilita 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 habilitada, todas las etiquetas son iguales para que el núcleo no se configure para forzar las políticas de MAC. Cuando se habilitan 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. A diferencia de la mayoría del resto de los sistemas operativos de varios niveles, Trusted Extensions incluye un escritorio de varios niveles.

Trusted Extensions cumple con los requisitos del perfil de protección de acceso basado el roles (RBACPP, Role-Based Access Protection Profile), el perfil de protección de acceso controlado (CAPP, Controlled Access Protection Profile) y el perfil de protección de seguridad con etiquetas (LSPP, Labeled Security Protection Profile) de Common Criteria. Sin embargo, 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.

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*.
- Para obtener información sobre el uso del escritorio de varios niveles, consulte *Guía del usuario de Oracle Solaris Trusted Extensions*.
- Las páginas del comando man seleccionadas son: `trusted_extensions(5)` y `labeld(1M)`.

Valores predeterminados de seguridad de Oracle Solaris 11

Después de la instalación, Oracle Solaris protege el sistema de 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`. Al inicio, las contraseñas de las dos cuentas son idénticas.

- 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`.
- Se asignan al usuario inicial 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 usuario deben tener al menos seis caracteres de longitud e incluir, al menos, un carácter alfabético y un carácter numérico. 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 en su lugar, el usuario puede alcanzar el sistema sin intercepción, modificación ni falsificación.

Intentos de inicio de sesión registrados: el servicios de auditoría se habilita 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 puede buscar 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 y las aplicaciones de escritorio quedan protegidas por el privilegio mínimo, los permisos y el 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 son `drwxr-xr-x` (`755`). Los permisos de archivo son `-rw-r--r--` (`644`).

Applets de escritorio: los applets de escritorio están protegidos por RBAC. Por ejemplo, sólo el usuario inicial o el rol `root` pueden utilizar el applet Package Manager para instalar paquetes nuevos. Package Manager no se muestra a los usuarios comunes que no tengan asignados los derechos para utilizarlo.

Funciones de seguridad adicionales en su lugar

Oracle Solaris 11 proporciona funciones de seguridad que se pueden usar para configurar los sistemas y los usuarios a fin de satisfacer los requisitos de seguridad del sitio.

- **Control de acceso basado en roles (RBAC):** Oracle Solaris proporciona una cantidad de autorizaciones, privilegios y perfiles de derechos. El rol `root` es el único que está definido. Los perfiles de derechos proporcionan una buena base para los roles que se crean. Además, algunos comandos administrativos requieren autorizaciones RBAC para ejecutarse correctamente. Los usuarios sin autorizaciones no pueden ejecutar los comandos, ni siquiera aunque los usuarios tengan los privilegios requeridos.
- **Derechos de usuario:** a los usuarios se les asigna una 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" en la página 22. Los intentos de inicio de sesión del usuario no se encuentran limitados, pero el servicio de auditoría registra todos los inicios de sesión que fallan.
- **Protección de los archivos del sistema:** los archivos del sistema están protegidos con permisos de archivo. Sólo el rol `root` puede modificar los archivos de configuración del sistema.

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.

Para obtener más información, consulte lo siguiente:

- 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 11

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

Cuando instale el SO Oracle Solaris, elija los medios que instalen el paquete de *grupo* adecuado:

- **Servidor grande de Oracle Solaris**: el manifiesto predeterminado en una instalación de Automated Installer (AI) y el instalador de texto instalan el grupo `group/system/solaris-large-server`, que proporciona un entorno de servidor grande de Oracle Solaris.
- **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` a un servidor de Oracle Solaris. 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 Parte III, "Instalación con un servidor de instalación" de *Instalación de sistemas Oracle Solaris 11*.

Para informarse antes de elegir el medio, consulte las siguientes guías de instalación:

- *Instalación de sistemas Oracle Solaris 11*
- *Creación de una imagen de instalación personalizada de Oracle Solaris 11*
- *Adición y actualización de paquetes de software de Oracle Solaris 11*

Protección del sistema

La mejor manera de realizar las siguientes tareas es siguiendo el orden. En este momento, se instala el SO Oracle Solaris 11, y sólo el usuario inicial que puede asumir el rol `root` tiene acceso al sistema.

Tarea	Descripción	Para obtener instrucciones
1. Revisar los paquetes en el sistema.	Comprobar que los paquetes del medio de instalación sean idénticos a los paquetes instalados.	"Verificar los paquetes" en la página 27
2. Proteger la configuración del hardware en el sistema.	Se protege el hardware mediante la solicitud de una contraseña para cambiar la configuración del hardware.	"Control de acceso a hardware del sistema (tareas)" de *Administración de Oracle Solaris: servicios de seguridad*
3. Deshabilitar servicios innecesarios.	Evitar la ejecución de los procesos que no forman parte de las funciones requeridas del sistema.	"Deshabilitar servicios innecesarios" en la página 27
4. Requerir asignación de dispositivo.	Evitar el uso de medios extraíbles sin autorización explícita. Entre los dispositivos se incluyen los micrófonos, las unidades USB y los CD.	"Cómo habilitar la asignación de dispositivos" de *Administración de Oracle Solaris: servicios de seguridad*
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.	"Quitar a los usuarios la capacidad de gestión de energía" en la página 28
6. Crear un mensaje de advertencia de inicio de sesión que refleje la política de seguridad del sitio.	Notificar a los usuarios y a los posibles atacantes de que el sistema está supervisado.	"Inserción de un mensaje de seguridad en los archivos de carátula" en la página 28 "Inserción de un mensaje de seguridad en la pantalla de inicio de sesión del escritorio" en la página 29

▼ Verificar los paquetes

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

Antes de empezar Debe tener el rol `root`.

1. **Ejecute el comando `pkg verify`.**

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

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

2. **Fíjese si hay errores en el registro.**

3. **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`.

▼ Deshabilitar servicios innecesarios

Utilice este procedimiento para deshabilitar servicios que no sean necesarios por el propósito de su sistema.

Antes de empezar Debe tener el rol `root`.

1. **Enumere los servicios en línea.**

   ```
   # svcs | grep network
   online         Sep_07   svc:/network/loopback:default
   ...
   online         Sep_07   svc:/network/ssh:default
   ```

2. **Deshabilite 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, deshabilítelos.

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

Véase también Para obtener más información, consulte el Capítulo 6, "Gestión de servicios (descripción general)" de *Administración de Oracle Solaris: tareas comunes* and the `svcs`(1) man page.

▼ Quitar a los usuarios la capacidad de gestión de energía

Utilice este procedimiento para evitar que los usuarios de este sistema lo suspendan o lo apaguen.

Antes de empezar Debe tener el rol `root`.

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

```
% getent prof_attr | grep Console
Console User:RO::Manage System as the Console User:
profiles=Desktop Removable Media User,Suspend To RAM,Suspend To Disk,
Brightness,CPU Power Management,Network Autoconf User;
auths=solaris.system.shutdown;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 o cambiar un perfil de derechos" de *Administración de Oracle Solaris: servicios de seguridad*.

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

```
#CONSOLE_USER=Console User
```

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

```
# usermod -P +new-profile username
```

Véase también Para obtener más información, consulte "Archivo policy.conf" de *Administración de Oracle Solaris: servicios de seguridad* y las páginas del comando man `policy.conf`(4) y `usermod`(1M).

▼ Inserción de un mensaje de seguridad en los archivos de carátula

Utilice este procedimiento para crear mensajes de advertencia que reflejen la política de seguridad del sitio. El contenido de estos archivos se muestra en el inicio de sesión local y remoto.

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.

Antes de empezar Debe tener el rol `root`. Lo más recomendable es que consulte con el abogado de su empresa acerca de los contenidos del mensaje de seguridad.

1 **Escriba un mensaje de seguridad en el archivo `/etc/issue`.**

```
# vi /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.
```

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

El programa `telnet` muestra el contenido del archivo `/etc/issue` como mensaje de inicio de sesión. Para que otras aplicaciones usen este archivo, consulte "Visualización de mensajes de seguridad para usuarios `ssh` y `ftp`" en la página 39 and "Inserción de un mensaje de seguridad en la pantalla de inicio de sesión del escritorio" en la página 29.

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

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

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

Escoja entre varios métodos para crear un mensaje de seguridad para que los usuarios puedan revisar al iniciar sesión.

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 comando 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.

Antes de empezar Debe tener el rol `root`. Lo más recomendable es que consulte con el abogado de su empresa acerca de los contenidos del mensaje de seguridad.

- **Coloque un mensaje de seguridad en la pantalla de inicio de sesión del escritorio.**

  Dispone de varias opciones. Las opciones que crean un cuadro de diálogo pueden usar el archivo `/etc/issue` de Paso 1 of "Inserción de un mensaje de seguridad en los archivos de carátula" en la página 28.

  - **OPCIÓN 1: Cree un archivo de escritorio que muestra el mensaje de seguridad en un cuadro de diálogo en el momento del inicio de sesión.**

    ```
    # vi /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/issue
    OnlyShowIn=GNOME;
    X-GNOME-Autostart-Phase=Application
    ```

    Después de que se haya autenticado en la ventana de inicio de sesión, el usuario deberá cerrar el cuadro de diálogo para llegar al espacio de trabajo. Para las opciones que permiten el comando `zenity`, consulte la página del comando man `zenity`(1).

  - **OPCIÓN 2: Modifique una secuencia de comando de inicialización GDM para mostrar el mensaje de seguridad en un cuadro de diálogo.**

    El directorio `/etc/gdm` contiene tres secuencias de comando de inicialización que muestran el mensaje de seguridad antes, durante e inmediatamente después del inicio de sesión. Estas secuencias de comando también están disponibles en la versión Oracle Solaris 10.

    - **Muestre los mensaje de seguridad antes de que aparezca la pantalla de inicio de sesión.**

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

    - **Muestre los mensaje de seguridad en la pantalla de inicio de sesión después de la autenticación.**

      Esta secuencia de comandos se ejecuta antes de que aparezca el espacio de trabajo del usuario. Para crear esta secuencia de comandos, debe modificar la secuencia de comandos `Default.sample`.

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

    - **Muestre el mensaje de seguridad en el espacio de trabajo inicial del usuario después de la autenticación.**

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

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

- **OPCIÓN 3: 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 en 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) Después de modificar la interfaz gráfica de usuario de la ventana de inicio de sesión, guarde una copia.**

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

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.

```
# vi /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 los 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.

Tarea	Descripción	Para obtener instrucciones
Requerir contraseñas seguras y cambios de contraseña frecuentes.	Aumentar las limitaciones de la contraseña predeterminada en cada sistema.	"Establecer limitaciones de contraseña más seguras" en la página 33
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.	"Definir un valor `umask` más restrictivo para los usuarios comunes" en la página 35.
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.	"Establecer el bloqueo de cuenta para los usuarios comunes" en la página 34
Preseleccionar clases de auditoría adicionales.	Proporcionar mejores supervisión y registro de las amenazas potenciales para el sistema.	"Auditar eventos importantes además del inicio y el cierre de sesión" en la página 35
Enviar resúmenes de texto de eventos de auditoría a la utilidad `syslog`.	Proporcionar cobertura en tiempo real de eventos de auditoría importantes, como los inicios de sesión y los intentos de inicio de sesión.	"Supervisar eventos `lo` en tiempo real" en la página 36
Crear roles.	Distribuir tareas administrativas discretas a varios usuarios de confianza para que ningún usuario pueda dañar el sistema.	"Configuración de cuentas de usuario" de *Administración de Oracle Solaris: tareas comunes* "Cómo crear un rol" de *Administración de Oracle Solaris: servicios de seguridad* "Cómo asignar un rol" de *Administración de Oracle Solaris: servicios de seguridad*.
Mostrar aplicaciones permitidas solamente en el escritorio del usuario.	Impedir que los usuarios vean o usen aplicaciones para las que no tienen autorización de uso.	Consulte "Cómo limitar el acceso de un usuario a las aplicaciones de escritorio" de *Configuración y administración de Trusted Extensions*.

Tarea	Descripción	Para obtener instrucciones
Limitar los privilegios del usuario.	Eliminar privilegios básicos que los usuarios no necesiten.	"Eliminar privilegios básicos innecesarios de los usuarios" en la página 37

▼ Establecer limitaciones de contraseña más seguras

Utilice este procedimiento si los valores predeterminados no cumplen con los requisitos de seguridad del sitio. Los pasos siguen la lista de entradas en el archivo `/etc/default/passwd`.

Antes de empezar

Antes de cambiar los valores predeterminados, asegúrese de que los cambios permitan a todos los usuarios realizar la autenticación en sus aplicaciones y en otros sistemas de la red.

Debe tener el rol `root`.

- **Edite el archivo `/etc/default/passwd`.**

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

  ```
  ## /etc/default/passwd
  ##
  MAXWEEKS=
  MINWEEKS=
  MAXWEEKS=4
  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 ver la lista de variables que limitan la creación de contraseñas, consulte el archivo `/etc/default/passwd`. Los valores predeterminados se indican en el archivo.
- Para obtener información sobre las limitaciones de contraseña que se aplican después de la instalación, consulte "El sistema de acceso está limitado y supervisado" en la página 22.
- Página del comando man `passwd(1)`

▼ Establecer el bloqueo de cuenta para los usuarios comunes

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

Nota – No establezca el bloqueo de cuenta para los usuarios que pueden asumir roles, ya que esto puede bloquear el rol.

Antes de empezar Debe tener el rol `root`. No establezca esta protección en la totalidad de un sistema que utilice para las actividades administrativas.

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

- **Para todo el sistema.**

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

- **Para un usuario.**

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

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

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

Véase también

- Para leer una explicación de los atributos de seguridad de los usuarios y los roles, consulte el Capítulo 10, "Atributos de seguridad en Oracle Solaris (referencia)" de *Administración de Oracle Solaris: servicios de seguridad*.
- Las páginas del comando man seleccionadas son: `policy.conf(4)` y `user_attr(4)`.

▼ Definir un valor umask más restrictivo para los usuarios comunes

Si el valor `umask` predeterminado (`022`) no es lo suficientemente restrictivo, defina una máscara más restrictiva mediante el siguiente procedimiento.

Antes de empezar Debe tener el rol `root`.

- **Modifique el valor de umask en los perfiles de inicio de sesión de la estructura básica de directorios para los distintos shells.**

  Oracle Solaris proporciona directorios para que los administradores personalicen los valores predeterminados de shell de usuario. Estas estructuras de directorios incluyen archivos como `.profile` , `.bashrc` y `.kshrc`.

  Elija uno de los siguientes valores:

  - `umask 027`: proporciona una protección de archivos moderada

    (`740`) – `w` para el grupo, `rwx` para otros
  - `umask 026`: proporciona una protección de archivos un poco más estricta

    (`741`) – `w` para el grupo, `rw` 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:

- "Configuración de cuentas de usuario" de *Administración de Oracle Solaris: tareas comunes*
- "Valor umask predeterminado" de *Administración de Oracle Solaris: servicios de seguridad*
- Las páginas del comando man seleccionadas son: `usermod`(1M) y `umask`(1).

▼ Auditar eventos importantes además del inicio y el cierre de sesión

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

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

Antes de empezar Debe tener el rol `root`. Implementará la política de seguridad de su sitio respecto de la auditoría.

1. **Audite todos los usos de los comandos con privilegios por parte de los usuarios y los roles.**

   Para todos los usuarios y los roles, agregue el evento de auditoría `AUE_PFEXEC` a su máscara de preselección.

   ```
   # usermod -K audit_flags=lo,ps:no username

   # rolemod -K audit_flags=lo,ps:no rolename
   ```

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

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

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

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

Véase también

- Para obtener información sobre la política de auditoría, consulte "Política de auditoría" de *Administración de Oracle Solaris: servicios de seguridad*.
- Para obtener ejemplos sobre cómo establecer indicadores de auditoría, consulte "Configuración del servicio de auditoría (tareas)" de *Administración de Oracle Solaris: servicios de seguridad* y "Solución de problemas del servicio de auditoría (tareas)" de *Administración de Oracle Solaris: servicios de seguridad*.
- Para ver cómo configurar la auditoría, consulte la página del comando man `auditconfig(1M)`.

▼ Supervisar eventos lo en tiempo real

Utilice este procedimiento para activar el complemento `audit_syslog` para los eventos que desea supervisar en el momento en que se producen.

Antes de empezar

Debe estar en el rol `root` para modificar el archivo `syslog.conf`. Para realizar otros pasos debe tener asignado el perfil de derechos de configuración de auditoría.

1. **Envíe la clase `lo` al complemento `audit_syslog` para activarlo.**

   ```
   # auditconfig -setplugin audit_syslog active p_flags=lo
   ```

2. **Agregue una entrada `audit.notice` al archivo `syslog.conf`.**

   La entrada predeterminada incluye la ubicación del archivo de registro.

   ```
   # cat /etc/syslog.conf
   ...
   audit.notice       /var/adm/auditlog
   ```

3. **Cree el archivo de registro.**

   ```
   # touch /var/adm/auditlog
   ```

4. **Refresque la información de configuración para el servicio `syslog`.**

   ```
   # svcadm refresh system/system-log
   ```

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

   El servicio de auditoría lee los cambios en el complemento de auditoría tras el refrescamiento.

   ```
   # audit -s
   ```

Véase también

- Para ver cómo enviar resúmenes de auditoría a otro sistema, consulte el ejemplo de "Cómo configurar registros de auditoría syslog" de *Administración de Oracle Solaris: servicios de seguridad*.
- El servicio de auditoría puede generar muchas salidas. Para gestionar los registros, consulte la página del comando man `logadm`(1M).
- Para ver cómo supervisar la salida, consulte "Supervisión de los resúmenes de auditoría de `audit_syslog`" en la página 55.

▼ Eliminar privilegios básicos innecesarios de los usuarios

En determinadas circunstancias, uno o más de los tres privilegios básicos se pueden quitar del conjunto básico de un usuario común.

- `file_link_any`: permite a un proceso crear enlaces físicos con archivos que sean propiedad de un UID distinto del UID efectivo del proceso.
- `proc_info`: permite a un proceso examinar el estado de los procesos que no sean aquellos a los que puede enviar señales. Los procesos que no se pueden examinar no se pueden ver en `/proc` y aparecen como no existentes.
- `proc_session`: permite a un proceso enviar señales o rastrear procesos fuera de su sesión.

Antes de empezar

Debe tener el rol `root`.

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

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

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

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

3. **Impida que el 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
   ```

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

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

Véase también Para obtener más información, consulte el Capítulo 8, "Uso de roles y privilegios (descripción general)" de *Administración de Oracle Solaris: servicios de seguridad* y la página del comando man `privileges(5)`.

Protección del núcleo

En este momento, puede que haya creado roles y también usuarios que puedan asumir dichos roles. Sólo el rol `root` puede modificar archivos de sistema.

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 *Administración de Oracle Solaris: servicios de seguridad*
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.	"Cómo habilitar una ruta del archivo del núcleo central global" de *Administración de Oracle Solaris: tareas comunes* "Gestión de archivos del núcleo central (mapa de tareas)" de *Administración de Oracle Solaris: tareas comunes*

Configuración de la red

En este momento, puede que haya creado roles y también usuarios que puedan asumir dichos roles. Sólo el rol `root` puede modificar archivos de sistema.

De las siguientes tareas de red, realice las que proporcionan seguridad adicional según los requisitos del sitio. Estas tareas de red notifican a los usuarios que inician sesión de manera remota que el sistema está protegido y refuerzan los protocolos de IP, ARP y TCP.

Tarea	Descripción	Para obtener instrucciones
Mostrar mensajes de advertencia que reflejan la política de seguridad del sitio.	Notificar a los usuarios y a los posibles atacantes de que el sistema está supervisado.	"Visualización de mensajes de seguridad para usuarios `ssh` y `ftp`" en la página 39
Deshabilitar el daemon de enrutamiento de red.	Limita el acceso a sistemas por parte de intrusos de una red.	"Deshabilitar el daemon de enrutamiento de red." en la página 40

Tarea	Descripción	Para obtener instrucciones
Impedir la difusión de información sobre la topología de la red.	Impedir la difusión de paquetes.	"Deshabilitar el reenvío de paquetes de difusión" en la página 41
	Impedir que se envíen respuestas ante la difusión y la multidifusión de solicitudes de eco.	"Deshabilitar las respuestas a las solicitudes de eco" en la página 42
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.	"Establecer hosts múltiples estrictos" en la página 42
Impedir ataques de DOS mediante el control del número de conexiones del sistema incompletas.	Limitar el número permitido de conexiones TCP incompletas para una escucha TCP.	"Definir el número máximo de conexiones TCP incompletas" en la página 43
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.	"Definir el número máximo de conexiones TCP pendientes" en la página 43
Generar números aleatorios fuertes para las conexiones TCP iniciales.	Cumple con el valor de generación de número de secuencia especificado por RFC 1948.	"Especificación de un número aleatorio fuerte para la conexión TCP inicial" en la página 44
Restablecer los valores seguros predeterminados de los parámetros de red.	Aumentar la seguridad que se redujo por acciones administrativas.	"Restablecer los valores seguros de los parámetros de red" en la página 44
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. De manera predeterminada, la aplicación `sendmail` se protege con envoltorios TCP, como se describe en "Compatibilidad con envoltorios TCP de la versión 8.12 de sendmail" de *Oracle Administración Solaris: Servicios de red*.	Para habilitar los envoltorios TCP para todos los servicios `inetd`, consultar "Cómo utilizar los envoltorios TCP para controlar el acceso a los servicios TCP" de *Administración de Oracle Solaris: servicios IP*. Para ver un ejemplo de los envoltorios TCP que protegen el servicio de red de FTP, consultar "Cómo iniciar un servidor FTP mediante SMF" de *Oracle Administración Solaris: Servicios de red*.

▼ Visualización de mensajes de seguridad para usuarios ssh y ftp

Utilice este procedimiento para mostrar advertencias en el inicio de sesión remoto y la transferencia de archivos.

Antes de empezar

Debe tener el rol `root`. Creó el archivo `/etc/issue` en Paso 1 of "Inserción de un mensaje de seguridad en los archivos de carátula" en la página 28.

1. **Para mostrar un mensaje de seguridad a los usuarios que están conectados mediante `ssh`, haga lo siguiente:**

   a. **Elimine el comentario de la directiva Banner en el archivo `/etc/sshd_config`.**

   ```
   # vi /etc/ssh/sshd_config
   # Banner to be printed before authentication starts.
   Banner /etc/issue
   ```

   b. **Refresque el servicio `ssh`.**

   ```
   # svcadm refresh ssh
   ```

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

2. **Para mostrar un mensaje de seguridad a los usuarios que están conectados mediante `ftp`, haga lo siguiente:**

   a. **Agregue la directiva `DisplayConnect` al archivo `proftpd.conf`.**

   ```
   # vi /etc/proftpd.conf
   # Banner to be printed before authentication starts.
   DisplayConnect /etc/issue
   ```

   b. **Reinicie el servicio `ftp`.**

   ```
   # svcadm restart ftp
   ```

   Para obtener más información, consulte el sitio web ProFTPD (`http://www.proftpd.org/`).

▼ Deshabilitar el daemon de enrutamiento de red.

Utilice este procedimiento para impedir el enrutamiento de red después de la instalación mediante la especificación de un enrutador predeterminado. De lo contrario, lleve a cabo este procedimiento después de configurar manualmente la ruta.

Nota – Muchos de los procedimientos de configuración de red requieren que el daemon de enrutamiento se desactive. Por lo tanto, puede que haya desactivado este daemon durante la ejecución de un procedimiento de configuración mayor.

Antes de empezar Debe tener asignado el perfil de derechos de gestión de la red.

1. **Verifique que el daemon de enrutamiento se esté ejecutando.**

```
# svcs -x svc:/network/routing/route:default
svc:/network/routing/route:default (in.routed network routing daemon)
 State: online since April 10, 2011 05:15:35 AM PDT
```

```
   See: in.routed(1M)
   See: /var/svc/log/network-routing-route:default.log
Impact: None.
```

Si el servicio no se está ejecutando, puede detenerse aquí.

2 Deshabilite el daemon de enrutamiento.

```
# routeadm -d ipv4-forwarding -d ipv6-forwarding
# routeadm -d ipv4-routing -d ipv6-routing
# routeadm -u
```

3 Verifique que el daemon de enrutamiento esté deshabilitado.

```
# svcs -x routing/route:default
svc:/network/routing/route:default (in.routed network routing daemon)
 State: disabled since April 11, 2011 10:10:10 AM PDT
Reason: Disabled by an administrator.
   See: http://sun.com/msg/SMF-8000-05
   See: in.routed(1M)
Impact: This service is not running.
```

Véase también Página del comando man `routeadm(1M)`

▼ Deshabilitar el reenvío de paquetes de difusión

De manera predeterminada, Oracle Solaris reenvía los paquetes de difusión. Si la política de seguridad de su sitio requiere que se reduzca la posibilidad de desborde de difusión, cambie el valor predeterminado mediante este procedimiento.

Nota – Cuando deshabilita la propiedad de red `_forward_directed_broadcasts`, se deshabilitan los pings de difusión.

Antes de empezar Debe tener asignado el perfil de derechos de gestión de la red.

1 Establezca la propiedad de reenvío de paquetes de difusión en 0 para los paquetes IP.

```
# ipadm set-prop -p _forward_directed_broadcasts=0 ip
```

2 Verifique el valor actual.

```
# ipadm show-prop -p _forward_directed_broadcasts ip
PROTO  PROPERTY                    PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _forward_directed_broadcasts rw   0         --           0         0,1
```

Véase también Página del comando man `ipadm(1M)`

▼ Deshabilitar las respuestas a las solicitudes de eco

Utilice este procedimiento para impedir la difusión de información sobre la topología de la red.

Antes de empezar Debe tener asignado el perfil de derechos de gestión de la red.

1 Establezca en 0 la propiedad de respuesta de difusión de solicitudes de eco para los paquetes IP y, a continuación, verifique el valor actual.

```
# ipadm set-prop -p _respond_to_echo_broadcast=0 ip

# ipadm show-prop -p _respond_to_echo_broadcast ip
PROTO  PROPERTY                  PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_echo_broadcast rw   0         --           1         0,1
```

2 Establezca en 0 la propiedad de respuesta de multidifusión de solicitudes de eco para los paquetes IP y, a continuación, verifique el valor actual.

```
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv4
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv6

# ipadm show-prop -p _respond_to_echo_multicast ipv4
PROTO  PROPERTY                  PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _respond_to_echo_multicast rw   0         --           1         0,1
# ipadm show-prop -p _respond_to_echo_multicast ipv6
PROTO  PROPERTY                  PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _respond_to_echo_multicast rw   0         --           1         0,1
```

Véase también Para obtener más información, consulte "_respond_to_echo_broadcast y _respond_to_echo_multicast (ipv4 o ipv6)" de *Manual de referencia de parámetros ajustables de Oracle Solaris* y la página del comando man `ipadm`(1M).

▼ Establecer hosts múltiples estrictos

Para los sistemas que son puertas de enlace con otros dominios, como un cortafuegos o un nodo de VPN, utilice este procedimiento para activar la función de hosts múltiples estrictos.

La versión Oracle Solaris 11 presenta una nueva propiedad (`hostmodel`), para IPv4 e IPv6. Esta propiedad controla el funcionamiento del envío y la recepción de paquetes IP en un sistema que tiene hosts múltiples.

Antes de empezar Debe tener asignado el perfil de derechos de gestión de la red.

1 Establezca la propiedad `hostmodel` en `strong` para paquetes IP.

```
# ipadm set-prop -p hostmodel=strong ipv4
# ipadm set-prop -p hostmodel=strong ipv6
```

2. **Verifique el valor actual y tome nota de los valores posibles.**

```
# ipadm show-prop -p hostmodel ip
PROTO  PROPERTY    PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   hostmodel   rw   strong    strong       weak      strong,src-priority,weak
ipv4   hostmodel   rw   strong    strong       weak      strong,src-priority,weak
```

Véase también Para obtener más información, consulte "hostmodel (ipv4 or ipv6)" de *Manual de referencia de parámetros ajustables de Oracle Solaris* y la página del comando man `ipadm`(1M).

Para obtener más información sobre el uso de los hosts múltiples estrictos, consulte "Cómo proteger una VPN con IPsec en modo de túnel" de *Administración de Oracle Solaris: servicios IP*.

▼ Definir el número máximo de conexiones TCP incompletas

Utilice este procedimiento para impedir ataques de denegación de servicio (DOS) mediante el control del número de conexiones pendientes que están incompletas.

Antes de empezar Debe tener asignado el perfil de derechos de gestión de la red.

1. **Defina el número máximo de conexiones entrantes.**

```
# ipadm set-prop -p _conn_req_max_q0=4096 tcp
```

2. **Verifique el valor actual.**

```
# ipadm show-prop -p _conn_req_max_q0 tcp
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _conn_req_max_q0 rw   4096      --           128       1-4294967295
```

Véase también Para obtener más información, consulte "_conn_req_max_q0" de *Manual de referencia de parámetros ajustables de Oracle Solaris* y la página del comando man `ipadm`(1M).

▼ Definir el número máximo de conexiones TCP pendientes

Utilice este procedimiento para impedir ataques de DOS mediante el control del número de conexiones entrantes permitidas.

Antes de empezar Debe tener asignado el perfil de derechos de gestión de la red.

1. **Defina el número máximo de conexiones entrantes.**

```
# ipadm set-prop -p _conn_req_max_q=1024 tcp
```

2 **Verifique el valor actual.**

```
# ipadm show-prop -p _conn_req_max_q tcp
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _conn_req_max_q  rw   1024      --           128       1-4294967295
```

Véase también Para obtener más información, consulte "_conn_req_max_q" de *Manual de referencia de parámetros ajustables de Oracle Solaris* y la página del comando man `ipadm`(1M).

▼ Especificación de un número aleatorio fuerte para la conexión TCP inicial

Este procedimiento define el parámetro de generación de número de secuencia inicial TCP para cumplir con RFC 1948 (`http://www.ietf.org/rfc/rfc1948.txt`).

Antes de empezar Debe estar en el rol `root` para modificar un archivo de sistema.

- **Cambie el valor predeterminado para la variable `TCP_STRONG_ISS`.**

```
# vi /etc/default/inetinit
# TCP_STRONG_ISS=1
TCP_STRONG_ISS=2
```

▼ Restablecer los valores seguros de los parámetros de red

Muchos parámetros de red que son seguros de manera predeterminada son ajustables. Esto significa que pueden modificarse. Si las condiciones del sitio lo permiten, reestablezca los valores predeterminados de los siguientes parámetros ajustables.

Antes de empezar Debe tener asignado el perfil de derechos de gestión de la red. El valor actual del parámetro es menos seguro que el valor predeterminado.

1 **Establezca en 0 la propiedad de reenvío de paquetes de origen para paquetes IP y, a continuación, verifique el valor actual.**

El valor predeterminado impide los ataques de DOS de paquetes suplantados.

```
# ipadm set-prop -p _forward_src_routed=0 ipv4
# ipadm set-prop -p _forward_src_routed=0 ipv6
# ipadm show-prop -p _forward_src_routed ipv4
PROTO  PROPERTY             PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _forward_src_routed   rw   0         --           0         0,1
# ipadm show-prop -p _forward_src_routed ipv6
PROTO  PROPERTY             PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _forward_src_routed   rw   0         --           0         0,1
```

Para obtener más información, consulte "forwarding (ipv4 or ipv6)" de *Manual de referencia de parámetros ajustables de Oracle Solaris*.

2 Establezca en 0 la propiedad de respuesta de máscara de red para paquetes IP y, a continuación, verifique el valor actual.

El valor predeterminado impide la difusión de información sobre la topología de red.

```
# ipadm set-prop -p _respond_to_address_mask_broadcast=0 ip
# ipadm show-prop -p _respond_to_address_mask_broadcast ip
PROTO PROPERTY                       PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip    _respond_to_address_mask_broadcast rw   0         --           0         0,1
```

3 Establezca en 0 la propiedad de respuesta de indicación de hora para paquetes IP y, a continuación, verifique el valor actual.

El valor predeterminado elimina las demandas adicionales de CPU en los sistemas e impide la difusión de información sobre la red.

```
# ipadm set-prop -p _respond_to_timestamp=0 ip
# ipadm show-prop -p _respond_to_timestamp ip
PROTO  PROPERTY                     PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_timestamp        rw   0         --           0         0,1
```

4 Establezca en 0 la propiedad de respuesta de indicación de hora de difusión para paquetes IP y, a continuación, verifique el valor actual.

El valor predeterminado elimina las demandas adicionales de CPU en los sistemas e impide la difusión de información sobre la red.

```
# ipadm set-prop -p _respond_to_timestamp_broadcast=0 ip
# ipadm show-prop -p _respond_to_timestamp_broadcast ip
PROTO  PROPERTY                     PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_timestamp_broadcast  rw   0         --           0         0,1
```

5 Establezca en 0 la propiedad de ignorar redireccionamientos para paquetes IP y, a continuación, verifique el valor actual.

El valor predeterminado impide las demandas adicionales de CPU en los sistemas.

```
# ipadm set-prop -p _ignore_redirect=0 ipv4
# ipadm set-prop -p _ignore_redirect=0 ipv6
# ipadm show-prop -p _ignore_redirect ipv4
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _ignore_redirect  rw   0         --           0         0,1
# ipadm show-prop -p _ignore_redirect ipv6
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _ignore_redirect  rw   0         --           0         0,1
```

6 Impida el enrutamiento de origen de IP.

Si necesita el enrutamiento de origen de IP para realizar diagnósticos, no deshabilite este parámetro de red.

```
# ipadm set-prop -p _rev_src_routes=0 tcp
# ipadm show-prop -p _rev_src_routes tcp
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _rev_src_routes   rw   0         --           0         0,1
```

Para obtener más información, consulte "_rev_src_routes" de *Manual de referencia de parámetros ajustables de Oracle Solaris*.

7 Establezca en 0 la propiedad de ignorar redireccionamientos para paquetes IP y, a continuación, verifique el valor actual.

El valor predeterminado impide las demandas adicionales de CPU en los sistemas. Por lo general, los redireccionamientos no son necesarios en las redes que están bien diseñadas.

```
# ipadm set-prop -p _ignore_redirect=0 ipv4
# ipadm set-prop -p _ignore_redirect=0 ipv6
# ipadm show-prop -p _ignore_redirect ipv4
PROTO  PROPERTY           PERM  CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _ignore_redirect   rw    0         --           0         0,1
# ipadm show-prop -p _ignore_redirect ipv6
PROTO  PROPERTY           PERM  CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _ignore_redirect   rw    0         --           0         0,1
```

Véase también Página del comando man `ipadm`(1M)

Protección de los archivos y los sistemas de archivos

Los sistemas de archivos ZFS son ligeros y se pueden cifrar, comprimir y configurar en casos de espacio reservado o espacio de disco limitado.

Las siguientes tareas proporcionan una breve explicación de las protecciones que están disponibles en ZFS, el sistema de archivos predeterminado de Oracle Solaris. Para obtener más información, consulte "Configuración de cuotas y reservas de ZFS" de *Administración de Oracle Solaris: sistemas de archivos ZFS* y la página del comando man `zfs`(1M).

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 *Administración de Oracle Solaris: sistemas de archivos ZFS*
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 *Administración de Oracle Solaris: sistemas de archivos ZFS*
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 *Administración de Oracle Solaris: sistemas de archivos ZFS* "Ejemplos de cifrado de sistemas de archivos ZFS" de *Administración de Oracle Solaris: sistemas de archivos ZFS*

Tarea	Descripción	Para obtener instrucciones
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`)

Protección y modificación de archivos

Sólo el rol `root` puede modificar archivos de sistema.

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.	"Definir un valor `umask` más restrictivo para los usuarios comunes" en la página 35
Impedir la sustitución de los archivos del sistema con archivos peligrosos.	Encontrar archivos peligrosos mediante una secuencia de comandos o mediante BART.	"Cómo buscar archivos con permisos de archivo especiales" de *Administración de Oracle Solaris: servicios de seguridad*

Protección de aplicaciones y servicios

Puede configurar las funciones de seguridad de Oracle Solaris para proteger sus aplicaciones.

Creación de zonas para contener aplicaciones críticas

Las zonas son contenedores que aíslan los procesos. Estos contenedores son útiles para 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.

Para obtener información y conocer los procedimientos consulte lo siguiente:

- El Capítulo 15, "Introducción a Zonas de Oracle Solaris" de *Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*
- "Resumen de zonas por función" de *Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*
- "Capacidades proporcionadas por las zonas no globales" de *Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*

- "Configuración de zonas en el sistema (mapa de tareas)" de *Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*
- El Capítulo 16, "Configuración de zonas no globales (descripción general)" de *Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*
- *Hardening Oracle Database with Oracle Solaris Security Technologies (Fortalecimiento de la base de datos de Oracle mediante las tecnologías de seguridad de Oracle Solaris)* (`http://www.oracle.com/technetwork/server-storage/solaris/solaris-security-hardening-db-167784.pdf`)

Gestión de los recursos en las zonas

Las zonas proporcionan una cantidad de herramientas para gestionar los recursos de las zonas.

Para obtener información y conocer los procedimientos consulte lo siguiente:

- El Capítulo 14, "Ejemplo de configuración de administración de recursos" de *Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*
- Parte I, "Gestión de recursos de Oracle Solaris" de *Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*

Configuración de IPsec e IKE

IPsec e IKE protegen las transmisiones por red entre los nodos y las redes que se configuran junto con IPsec e IKE.

Para obtener información y conocer los procedimientos consulte lo siguiente:

- El Capítulo 14, "Arquitectura de seguridad IP (descripción general)" de *Administración de Oracle Solaris: servicios IP*
- El Capítulo 17, "Intercambio de claves de Internet (descripción general)" de *Administración de Oracle Solaris: servicios IP*
- El Capítulo 15, "Configuración de IPsec (tareas)" de *Administración de Oracle Solaris: servicios IP*
- El Capítulo 18, "Configuración de IKE (tareas)" de *Administración de Oracle Solaris: servicios IP*

Configuración de filtro IP

La función de filtro IP proporciona un cortafuegos.

Para obtener información y conocer los procedimientos consulte lo siguiente:

- El Capítulo 20, "Filtro IP en Oracle Solaris (descripción general)" de *Administración de Oracle Solaris: servicios IP*
- El Capítulo 21, "Filtro IP (tareas)" de *Administración de Oracle Solaris: servicios IP*

Configuración 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:

- El Capítulo 20, "Planificación del servicio Kerberos" de *Administración de Oracle Solaris: servicios de seguridad*
- El Capítulo 21, "Configuración del servicio Kerberos (tareas)" de *Administración de Oracle Solaris: servicios de seguridad*
- Las páginas del comando man seleccionadas incluyen: `kadmin`(1M), `pam_krb5`(5) y `kclient`(1M).

Adición de SMF a un servicio antiguo

Puede limitar la configuración de aplicaciones a los roles o usuarios de confianza mediante la adición de las aplicaciones a la utilidad de gestión de servicios (SMF, Service Management Facility) de Oracle Solaris.

Para obtener información y conocer los procedimientos consulte lo siguiente:

- "Cómo agregar propiedades RBAC a las aplicaciones antiguas" de *Administración de Oracle Solaris: servicios de seguridad*
- 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) y `svccfg`(1M).

Creación de una instantánea de BART del sistema

Después de configurar el sistema, puede crear uno o varios manifiestos de BART. Estos manifiestos proporcionan instantáneas del sistema. Luego puede programar instantáneas comunes y también comparaciones. Para obtener más información, consulte "Uso de la herramienta básica de creación de informes de auditoría" en la página 53.

Adición 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). 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 `group/feature/trusted-desktop` proporcionan 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. Después de la instalación de los paquetes, 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:

- El Capítulo 14, "Arquitectura de seguridad IP (descripción general)" de *Administración de Oracle Solaris: servicios IP*
- "Administración de IPsec con etiquetas" de *Configuración y administración de Trusted Extensions*
- "Configuración de IPsec con etiquetas (mapa de tareas)" de *Configuración y administración de Trusted Extensions*

◆ ◆ ◆ CAPÍTULO 3

Supervisión y mantenimiento de la seguridad de Oracle Solaris 11

Oracle Solaris proporciona dos herramientas de sistema para supervisar la seguridad: la herramienta básica de creación de informes de auditoría (BART) y el servicio de auditoría. Las aplicaciones y los programas individuales también pueden crear registros de uso y acceso.

Uso de la herramienta básica de creación de informes de auditoría

Los manifiestos de BART proporcionan un registro estático de lo que está instalado en el sistema. Los manifiestos de BART se pueden comparar, a lo largo del tiempo y en todos los sistemas, a fin de registrar los cambios realizados en los sistemas instalados y las diferencias entre los sistemas.

Para obtener información y conocer los procedimientos consulte lo siguiente:

- "Herramienta básica de creación de informes de auditoría (descripción general)" de *Administración de Oracle Solaris: servicios de seguridad*
- "Uso de BART (tareas)" de *Administración de Oracle Solaris: servicios de seguridad*
- "Manifiestos, archivos de reglas e informes de BART (referencia)" de *Administración de Oracle Solaris: servicios de seguridad*

Para obtener instrucciones específicas sobre el registro de cambios efectuados en sistemas instalados, consulte "Cómo comparar manifiestos para el mismo sistema a lo largo del tiempo" de *Administración de Oracle Solaris: servicios de seguridad*.

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 Parte VII, "Auditoría en Oracle Solaris" de *Administración de Oracle Solaris: servicios de seguridad*.

- Capítulo 26, "Auditoría (descripción general)" de *Administración de Oracle Solaris: servicios de seguridad*
- Capítulo 27, "Planificación de la auditoría" de *Administración de Oracle Solaris: servicios de seguridad*
- Capítulo 28, "Gestión de auditoría (tareas)" de *Administración de Oracle Solaris: servicios de seguridad*
- Capítulo 29, "Auditoría (referencia)" de *Administración de Oracle Solaris: servicios de seguridad*

  Para obtener una lista con enlaces de las páginas del comando man, consulte "Páginas del comando man del servicio de auditoría" de *Administración de Oracle Solaris: servicios de seguridad*.

Los siguientes procedimientos del servicio de auditoría pueden resultar útiles para cumplir con los requisitos del sitio:

- Cree roles diferentes para configurar y para revisar la auditoría, y también para iniciar o detener el servicio de auditoría.

  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 un rol, consulte "Cómo crear un rol" de *Administración de Oracle Solaris: servicios de seguridad*.
- Supervise los resúmenes de texto de los eventos auditados en la utilidad `syslog`

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

  Consulte "Cómo configurar registros de auditoría syslog" de *Administración de Oracle Solaris: servicios de seguridad*.
- 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 *Administración de Oracle Solaris: servicios de seguridad*.
- 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 los resúmenes de auditoría de audit_syslog

El complemento `audit_syslog` permite registrar resúmenes de eventos de auditoría preseleccionados.

Puede mostrar los resúmenes de auditoría en una ventana de terminal a medida que se generan mediante la ejecución de un comando similar al siguiente:

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

Revisión y archivado de registros de auditoría

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

Para obtener información y conocer los procedimientos consulte lo siguiente:

- "Registros de auditoría" de *Administración de Oracle Solaris: servicios de seguridad*
- "Cómo evitar el desbordamiento de la pista de auditoría" de *Administración de Oracle Solaris: servicios de seguridad*
- "Gestión de registros de auditoría en sistemas locales (tareas)" de *Administración de Oracle Solaris: servicios de seguridad*

Búsqueda de archivos peligrosos

Puede detectar el posible uso no autorizado de los permisos `setuid` y `setgid` en los programas. Un archivo ejecutable sospechoso concede propiedad a un usuario en lugar de a una cuenta del sistema, como `root` o `bin`.

Para conocer el procedimiento y ver un ejemplo, consulte "Cómo buscar archivos con permisos de archivo especiales" de *Administración de Oracle Solaris: servicios de seguridad*.

◆ ◆ ◆ 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 del SO Oracle Solaris contiene algo de información útil y algo de información caducada.

Referencias de Oracle Solaris 11

El manual y los artículos siguientes contienen descripciones sobre la seguridad de los sistemas Oracle Solaris 11:

- *Administración de Oracle Solaris: servicios de seguridad*

  Esta guía de seguridad fue publicada por Oracle para los administradores de Oracle Solaris 11. Esta guía describe las funciones de seguridad de Oracle Solaris y cómo usarlas al configurar sus sistemas. El prefacio contiene enlaces con otras guías de administración del sistema de Oracle Solaris que pueden contener información de seguridad.

- *Seguridad de Oracle Solaris: Oracle Solaris Express* (`http://www.oracle.com/technetwork/articles/servers-storage-admin/os11esecurity-186797.pdf`)

  Este artículo proporciona una instantánea de las funciones de seguridad de la versión de Oracle Solaris de noviembre de 2010.

- ORACLE SOLARIS 11 EXPRESS 2010.11 (`http://www.oracle.com/technetwork/server-storage/solaris11/documentation/solaris-express-whatsnew-201011-175308.pdf`)

  Este artículo proporciona una instantánea de las funciones de la versión de Oracle Solaris de noviembre de 2010.

Para obtener referencias de Oracle Solaris 10 que puedan resultar útiles, consulte *Oracle Solaris 10 Security Guidelines* .