Configuración y administración de Trusted Extensions

Referencia: E25901
Diciembre de 2011

ORACLE

120424@25097

Contenido

Lista de figuras

Lista de tablas

Prefacio

Configuración y administración de Trusted Extensions proporciona procedimientos para la habilitación y la configuración inicial de la función Trusted Extensions en el sistema operativo Oracle Solaris (SO Oracle Solaris). Esta guía también proporciona procedimientos para gestionar usuarios, zonas, dispositivos y hosts en un sistema Trusted Extensions.

Nota – Esta versión de Oracle Solaris es compatible con sistemas que usen arquitecturas de las familias de procesadores SPARC y x86. Los sistemas compatibles aparecen en las *Listas de compatibilidad del sistema operativo Oracle Solaris*. Este documento indica las diferencias de implementación entre los tipos de plataforma.

Usuarios a los que está destinada esta guía

Esta guía está destinada a administradores de sistemas y administradores de seguridad expertos que deben configurar y administrar el software Trusted Extensions. El nivel de confianza que requiere la política de seguridad del sitio y el grado de experiencia necesario determinan quién puede realizar las tareas de configuración.

Los administradores deben estar familiarizados con la administración de Oracle Solaris. Asimismo, los administradores deben comprender lo siguiente:

- Las funciones de seguridad de Trusted Extensions y la política de seguridad del sitio
- Los procedimientos y conceptos básicos para usar un host configurado con Trusted Extensions, según lo descrito en la *Guía del usuario de Oracle Solaris Trusted Extensions*
- La manera en que se dividen las tareas administrativas entre los roles en el sitio

Trusted Extensions y el sistema operativo Oracle Solaris

Trusted Extensions se ejecuta en el SO Oracle Solaris. Como el software Trusted Extensions puede modificar el SO Solaris, es posible que Trusted Extensions necesite una configuración específica para las opciones de instalación de Oracle Solaris. En la Parte I de esta guía, se describe cómo preparar el SO Oracle Solaris para Trusted Extensions, cómo habilitar Trusted Extensions y cómo configurar inicialmente el software. En la Parte II de esta guía, se describe cómo administrar las funciones Trusted Extensions exclusivas del sistema.

Cómo se organizan las guías de Trusted Extensions

En la siguiente tabla se muestran los temas que se tratan en las guías de Trusted Extensions y los destinatarios de cada guía.

Título de la guía	Temas	Destinatarios
Guía del usuario de Oracle Solaris Trusted Extensions	Describe las funciones básicas de Trusted Extensions. Esta guía contiene un glosario.	Usuarios finales, administradores y desarrolladores
Configuración y administración de Trusted Extensions	En la Parte I, se describe cómo preparar, habilitar y configurar inicialmente Trusted Extensions. En la Parte II, se describe cómo administrar un sistema Trusted Extensions. Esta guía contiene un glosario.	Administradores y desarrolladores
Trusted Extensions Developer's Guide	Describe cómo desarrollar aplicaciones con Trusted Extensions.	Desarrolladores y administradores
Trusted Extensions Label Administration	Proporciona información sobre cómo especificar componentes de etiquetas en el archivo de codificaciones de etiqueta.	Administradores
Compartmented Mode Workstation Labeling: Encodings Format	Describe la sintaxis utilizada en el archivo de codificaciones de etiqueta. La sintaxis aplica distintas reglas para dar un formato correcto a las etiquetas de un sistema.	Administradores

Guías de administración del sistema relacionadas

Las siguientes guías contienen información útil para la preparación y la ejecución del software Trusted Extensions.

Título de la guía	Temas
Inicio y cierre de Oracle Solaris en plataformas SPARC	Inicio y cierre de un sistema, gestión de servicios de inicio, modificación del comportamiento de inicio, inicio desde ZFS, gestión del archivo de inicio y resolución de problemas de inicio en plataformas SPARC.
Inicio y cierre de Oracle Solaris en plataformas x86	Inicio y cierre de un sistema, gestión de servicios de inicio, modificación del comportamiento de inicio, inicio desde ZFS, gestión del archivo de inicio y resolución de problemas de inicio en plataformas x86.

Título de la guía	Temas
Administración de Oracle Solaris: tareas comunes	Uso de comandos de Oracle Solaris, inicio y cierre de un sistema, gestión de grupos y cuentas de usuario, gestión de servicios, fallas de hardware, información del sistema, recursos del sistema y rendimiento del sistema, gestión del software, impresión, consola y terminales, y resolución de problemas del sistema y del software.
Administración de Oracle Solaris: dispositivos y sistemas de archivos	Medios extraíbles, discos y dispositivos, sistemas de archivos, y copia de seguridad y restauración de datos.
Administración de Oracle Solaris: servicios IP	Administración de redes TCP/IP, administración de direcciones IPv4 e IPv6, DHCP, IPsec, IKE, filtro IP e IPQoS.
Oracle Solaris Administration: Naming and Directory Services	Servicios de directorios y nombres DNS, NIS y LDAP, incluida la transición de NIS a LDAP.
Administración de Oracle Solaris: interfaces y virtualización de redes	Configuración automática y manual de interfaces IP, incluidas las redes WiFi inalámbricas; administración de puentes, VLAN, agregaciones, LLDP e IPMP; gestión de recursos y NIC virtuales.
Oracle Administración Solaris: Servicios de red	Servidores de caché web, servicios relacionados con el tiempo, sistemas de archivos de red (NFS y autofs), correo, SLP y PPP.
Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos	Funciones de gestión de recursos, que permiten controlar cómo las aplicaciones utilizan los recursos disponibles del sistema; tecnología de partición del software Oracle Solaris Zones, que virtualiza los servicios del sistema operativo para crear un entorno aislado para la ejecución de aplicaciones; y Oracle Solaris 10 Zones, que aloja entornos de Oracle Solaris 10 en el núcleo de Oracle Solaris 11.
Administración de Oracle Solaris: servicios de seguridad	Auditoría, gestión de dispositivos, seguridad de archivos, BART, servicios Kerberos, PAM, estructura criptográfica, gestión de claves, privilegios, RBAC, SASL, Secure Shell y análisis de virus.
Oracle Solaris Administration: SMB and Windows Interoperability	Servicio SMB, que permite configurar un sistema Oracle Solaris para que los recursos compartidos SMB estén disponibles para los clientes SMB; cliente SMB, que permite acceder a los recursos compartidos SMB; y servicios de asignación de identidades nativos, que permiten asignar identidades de usuarios y grupos entre los sistemas Oracle Solaris y los sistemas Windows.
Administración de Oracle Solaris: sistemas de archivos ZFS	Creación y gestión de sistemas de archivos y agrupaciones de almacenamiento ZFS, instantáneas, clones, copias de seguridad, uso de listas de control de acceso (ACL) para proteger archivos ZFS y uso de ZFS en un sistema Oracle Solaris con zonas instaladas.
Configuración y administración de Trusted Extensions	Instalación, configuración y administración del sistema específicas de Trusted Extensions.

Título de la guía	Temas
Directrices de seguridad de Oracle Solaris 11	Protección de un sistema Oracle Solaris, además de escenarios de uso para sus funciones de seguridad, como zonas, ZFS y Trusted Extensions.
Transición de Oracle Solaris 10 a Oracle Solaris 11	Información de administración del sistema y ejemplos de la transición de Oracle Solaris 10 a Oracle Solaris 11 en las áreas de instalación, gestión de sistemas de archivos, dispositivos y discos, gestión del software, redes, gestión del sistema, seguridad, virtualización, funciones de escritorio, gestión de cuentas de usuarios, volúmenes emulados de entornos de usuario, resolución de problemas y recuperación de datos.

Referencias relacionadas

Documento de la política de seguridad del sitio: describe la política y los procedimientos de seguridad de seguridad del sitio.

Guía del administrador para el sistema operativo instalado actualmente: describe cómo realizar una copia de seguridad de los archivos del sistema.

Referencias relacionadas con el sitio web de otras empresas

En este documento se proporcionan direcciones de Internet de terceros e información adicional relacionada.

Nota – Oracle no se hace responsable de la disponibilidad de los sitios web de terceros que se mencionen en este documento. Oracle no garantiza ni se hace responsable de los contenidos, la publicidad, los productos u otros materiales que puedan estar disponibles a través de dichos sitios o recursos. Oracle no se responsabiliza de ningún daño, real o supuesto, ni de posibles pérdidas que se pudieran derivar del uso de los contenidos, bienes o servicios que estén disponibles en dichos sitios o recursos.

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#`

PARTE I

Configuración inicial de Trusted Extensions

En los capítulos incluidos en esta parte, se describe cómo preparar los sistemas Oracle Solaris para ejecutar Trusted Extensions. Los capítulos tratan la habilitación de Trusted Extensions y las tareas de configuración inicial.

Capítulo 1, "Planificación de la seguridad para Trusted Extensions": describe los temas de seguridad que debe tener en cuenta al configurar el software Trusted Extensions en uno o varios sistemas Oracle Solaris.

Capítulo 2, "Guía básica de configuración de Trusted Extensions": proporciona mapas de tareas para configurar el software Trusted Extensions en los sistemas Oracle Solaris.

Capítulo 3, "Adición de la función Trusted Extensions a Oracle Solaris (tareas)": proporciona instrucciones sobre la preparación de un sistema Oracle Solaris para el software Trusted Extensions. Describe cómo habilitar Trusted Extensions y cómo iniciar sesión.

Capítulo 4, "Configuración de Trusted Extensions (tareas)": proporciona instrucciones sobre la configuración del software Trusted Extensions en un sistema con un monitor.

Capítulo 5, "Configuración de LDAP para Trusted Extensions (tareas)": proporciona instrucciones sobre la configuración del servicio de nombres LDAP en los sistemas Trusted Extensions.

◆ ◆ ◆ CAPÍTULO 1

Planificación de la seguridad para Trusted Extensions

La función Trusted Extensions de Oracle Solaris implementa una parte de la política de seguridad del sitio en el software. En este capítulo se proporciona una descripción general de la seguridad y los aspectos administrativos de la configuración del software.

Planificación de la seguridad en Trusted Extensions

En esta sección se detalla la planificación que se necesita antes de habilitar y configurar el software Trusted Extensions.

Para obtener una lista de comprobación de las tareas de configuración de Trusted Extensions, consulte el Apéndice B, "Lista de comprobación de configuración de Trusted Extensions". Si está interesado en la localización de su sitio, consulte "Para clientes internacionales de Trusted Extensions" en la página 30. Si está interesado en la ejecución de una configuración evaluada, consulte "Comprensión de la política de seguridad del sitio" en la página 28.

Comprensión de Trusted Extensions

La habilitación y configuración de Trusted Extensions implica más que cargar archivos ejecutables, especificar los datos del sitio y definir variables de configuración. Es preciso tener un nivel considerable de conocimientos previos. El software Trusted Extensions proporciona un entorno con etiquetas que se basa en dos funciones de Oracle Solaris:

- Las capacidades que en la mayoría de los entornos UNIX se asignan a superusuarios aquí son manejadas por roles administrativos discretos.
- La capacidad de ignorar la política de seguridad se puede asignar a usuarios y aplicaciones específicos.

En Trusted Extensions, el acceso a los datos se controla mediante marcas de seguridad especiales. Estas marcas se denominan etiquetas. Las etiquetas se asignan a usuarios, procesos y objetos, como archivos de datos y directorios. Estas etiquetas proporcionan control de acceso obligatorio (MAC, Mandatory Access Control), además permisos UNIX, o control de acceso discrecional (DAC, Discretionary Access Control).

Comprensión de la política de seguridad del sitio

Trusted Extensions le permite integrar eficazmente la política de seguridad del sitio con SO Oracle Solaris. Por lo tanto, debe comprender muy bien el alcance de su política y la manera en que el software Trusted Extensions puede implementar dicha política. Una configuración bien planificada debe proporcionar un equilibrio entre la coherencia con la política de seguridad del sitio y la comodidad para los usuarios que trabajan en el sistema.

Trusted Extensions está configurado de manera predeterminada según los criterios comunes para la evaluación de la seguridad informática (ISO/IEC 15408) con un nivel de seguridad EAL4 en los siguientes perfiles de protección:

- Perfil de protección de seguridad mediante etiquetas
- Perfil de protección de acceso controlado
- Perfil de protección de control de acceso basado en roles

Para alcanzar estos niveles de evaluación, debe configurar LDAP como el servicio de nombres. Tenga en cuenta que la configuración podría dejar de cumplir con los criterios de la evaluación si realiza cualquiera de las siguientes acciones:

- Cambiar la configuración de la conmutación de núcleo en el archivo `/etc/system`.
- Desactivar la auditoría o la asignación de dispositivos.
- Cambiar las entradas predeterminadas de archivos públicos en el directorio `/usr`.

Para obtener más información, consulte el sitio web de Common Criteria (`http://www.commoncriteriaportal.org/`).

Diseño de una estrategia de administración para Trusted Extensions

El rol `root` o el rol de administrador del sistema es el responsable de habilitar Trusted Extensions. Puede crear roles para dividir las responsabilidades administrativas entre varias áreas funcionales:

- El administrador de la seguridad es el responsable de las tareas relacionadas con la seguridad, como la creación y asignación de etiquetas de sensibilidad, la configuración de auditorías y el establecimiento de directivas de contraseña.
- El administrador del sistema es el responsable de los aspectos no relacionados con la seguridad de la configuración, el mantenimiento, y la administración general.
- Se pueden configurar roles más limitados. Por ejemplo, un operador podría ser el responsable de la copia de seguridad de los archivos.

Como parte de la estrategia de administración, tendrá que decidir lo siguiente:

- Qué usuario manejará cada responsabilidad administrativa
- Qué usuarios no administrativos podrán ejecutar aplicaciones de confianza, es decir, qué usuarios tendrán permiso para ignorar la política de seguridad, cuando sea necesario
- Qué usuarios tendrán acceso a determinados grupos de datos

Diseño de una estrategia de etiqueta

Para la planificación de etiquetas es necesario establecer una jerarquía de niveles de sensibilidad y categorizar la información del sistema. El archivo `label_encodings` contiene este tipo de información para el sitio. Puede utilizar uno de los archivos `label_encodings` que se suministran con el software Trusted Extensions. También podría modificar uno de los archivos suministrados o crear un nuevo archivo `label_encodings` específico para su sitio. El archivo debe incluir las extensiones locales específicas de Oracle, al menos la sección `COLOR NAMES`.

Precaución – Si proporciona un archivo `label_encodings`, se recomienda tener la versión final del archivo instalada antes de que el sistema verifique las etiquetas. Las etiquetas se verifican durante el primer inicio, una vez que el servicio de Trusted Extensions está habilitado. Después de crear su primera zona o plantilla de red, todos los cambios realizados en el archivo `label_encodings` deben ajustarse a las zonas y las plantillas existentes.

La planificación de etiquetas también implica la planificación de la configuración de etiquetas. Después de habilitar el servicio Trusted Extensions, tendrá que decidir si el sistema debe permitir inicios de sesión en varias etiquetas o si el sistema se puede configurar con una etiqueta de usuario solamente. Por ejemplo, un servidor LDAP es un buen candidato para tener una zona con etiquetas. Para la administración local del servidor, se crearía una zona en la etiqueta mínima. Para administrar el sistema, el administrador inicia sesión y, desde el espacio de trabajo de usuario, asume el rol adecuado.

Para obtener más información, consulte *Trusted Extensions Label Administration*. También puede consultar *Compartmented Mode Workstation Labeling: Encodings Format*.

Para clientes internacionales de Trusted Extensions

Al localizar un archivo `label_encodings`, los clientes internacionales deben localizar *sólo* los nombres de las etiquetas. Los nombres de las etiquetas administrativas, `ADMIN_HIGH` y `ADMIN_LOW`, no se deben localizar. Todos los hosts con etiquetas que contacte, de cualquier proveedor, deberán tener nombres de etiqueta que coincidan con los nombres de etiqueta incluidos en el archivo `label_encodings`.

Planificación del hardware y la capacidad del sistema para Trusted Extensions

El hardware del sistema incluye el sistema en sí y los dispositivos conectados. Estos dispositivos incluyen unidades de cinta, micrófonos, unidades de CD-ROM y paquetes de discos. La capacidad del hardware incluye la memoria del sistema, las interfaces de red y el espacio en el disco.

- Siga las recomendaciones para instalar una versión de Oracle Solaris, como se describe en *Instalación de sistemas Oracle Solaris 11* y la sección de instalación de las *Notas de la versión*.
- Las funciones de Trusted Extensions se pueden agregar a esas recomendaciones:
  - En los siguientes sistemas se requiere una memoria mayor al mínimo sugerido:
    - Sistemas en los que se ejecuta en más de una etiqueta de sensibilidad
    - Sistemas utilizados por usuarios que pueden asumir un rol administrativo
  - En los siguientes sistemas se necesitará más espacio en el disco:
    - Sistemas donde se almacenan archivos en más de una etiqueta

- Sistemas cuyos usuarios pueden asumir un rol administrativo

Planificación de la red de confianza

Para obtener ayuda con la planificación del hardware de red, consulte el Capítulo 1, "Planificación de la implementación de red" de *Administración de Oracle Solaris: servicios IP*.

El software Trusted Extensions reconoce dos tipos de host, "unlabeled" y "cipso". Cada tipo de host tiene una plantilla de seguridad predeterminada, como se muestra en la Tabla 1–1.

TABLA 1–1 Plantillas de host predeterminadas en Trusted Extensions

Tipo de host	Nombre de la plantilla	Finalidad
`unlabeled`	`admin_low`	Se utiliza para identificar hosts que no son de confianza que se pueden comunicar con la zona global. Estos hosts envían paquetes que no incluyen etiquetas. Para obtener más información, consulte sistema sin etiquetas.
`cipso`	`cipso`	Se utiliza para identificar los hosts o las redes que envían paquetes CIPSO. Los paquetes CIPSO tienen etiquetas.

Si otras redes pueden acceder a su red, debe especificar hosts y dominios disponibles. También debe identificar qué hosts de Trusted Extensions actuarán como puertas de enlace. Debe identificar la etiqueta rango de acreditación para estas puertas de enlace y la etiqueta de sensibilidad en la que se podrán ver los datos de otros hosts.

El etiquetado de hosts, puertas de enlace y redes se explica en el Capítulo 16, "Gestión de redes en Trusted Extensions (tareas)". La asignación de etiquetas a sistemas remotos se realiza después de la configuración inicial.

Planificación de zonas en Trusted Extensions

El software Trusted Extensions se agrega a Oracle Solaris en la zona global. A continuación, debe configurar las zonas no globales con etiquetas. Puede crear una zona con etiquetas para cada etiqueta única, aunque no es necesario crear una zona para cada la etiqueta en el archivo `label_encodings`. Una secuencia de comandos proporcionada permite crear dos zonas con etiquetas fácilmente para la etiqueta de usuario predeterminada y la acreditación de usuario predeterminada en el archivo `label_encodings`.

Después de crear las zonas con etiquetas, los usuarios comunes pueden utilizar el sistema configurado, pero no están conectados con otros sistemas.

- En Trusted Extensions, el transporte local para conectar con el servidor X es los sockets de dominio UNIX. De manera predeterminada, el servidor X no recibe conexiones TCP.
- De manera predeterminada, las zonas no globales no se pueden comunicar con hosts que no son de confianza. Debe especificar las máscaras de red o las direcciones IP explícitas del host remoto a las que puede acceder cada zona.

Zonas de Trusted Extensions y Oracle Solaris Zones

Las zonas de Trusted Extensions, es decir, las zonas con etiquetas, son una *marca* de Oracle Solaris Zones. Las zonas con etiquetas se usan principalmente para separar datos. En Trusted Extensions, los usuarios comunes no pueden iniciar sesión de manera remota en una zona con etiquetas, excepto una zona con etiquetas iguales en otro sistemas de confianza. Los administradores autorizados pueden acceder a una zona con etiquetas desde la zona global. Para obtener más información sobre las marcas de zona, consulte la página del comando man `brands(5)`.

Creación de zonas en Trusted Extensions

La creación de zonas en Trusted Extensions es similar a la creación de zonas en Oracle Solaris. Trusted Extensions proporciona la secuencia de comandos `txzonemgr` para guiarlo a través del proceso. La secuencia de comandos tiene varias opciones de línea de comandos para automatizar la creación de zonas con etiquetas.

Acceso a zonas con etiquetas

En un sistema configurado correctamente, cada zona debe poder utilizar una dirección de red para comunicarse con otras zonas que comparten la misma etiqueta. Las siguientes configuraciones proporcionan a las zonas con etiquetas acceso a otras zonas con etiquetas:

- **Interfaz all-zones**: se asigna una dirección `all-zones`. En esta configuración predeterminada, sólo se necesita una dirección IP. Cada zona, global y con etiquetas, se puede comunicar con zonas con etiquetas idénticas de sistemas remotos mediante esta dirección compartida.

  Un refinamiento de esta configuración consiste en crear una segunda instancia de IP para que la zona global utilice de manera exclusiva. Esta segunda instancia no será una dirección `all-zones`. La instancia de IP no se podrá utilizar para alojar un servicio de varios niveles ni para proporcionar una ruta a un subred privada.
- **Instancias de IP**: como en el SO Oracle Solaris, se asigna una dirección IP a cada zona, incluida la zona global. Las zonas comparten la pila de IP. En el caso más simple, todas las zonas comparten la misma interfaz física.

Un refinamiento de esta configuración consiste en asignar una tarjeta de información de red (NIC) por separado a cada zona. Una configuración de ese tipo se utiliza para separar físicamente las redes de una sola etiqueta que están asociadas a cada NIC.

Un refinamiento adicional consiste en usar una o más interfaces `all-zones` además de un instancia de IP por zona. Esta configuración permite utilizar interfaces internas, como `vni0`, para acceder a la zona global, lo que protege a la zona global contra ataques remotos. Por ejemplo, un servicio con privilegios que enlaza un puerto de varios niveles en una instancia de `vni0` en la zona global sólo se puede contactar internamente mediante las zonas que utilizan la pila compartida.

- **Pila de IP exclusiva**: como en Oracle Solaris, se asigna una dirección IP a cada zona, incluida la zona global. Se crea una tarjeta de interfaz de red virtual (VNIC) para cada zona con etiquetas.

  Un refinamiento de esta configuración consiste en crear cada VNIC mediante una interfaz red independiente. Una configuración de ese tipo se utiliza para separar físicamente las redes de una sola etiqueta que están asociadas a cada NIC. Las zonas que están configuradas con una pila de IP exclusiva no pueden utilizar la interfaz `all-zones`.

Planificación de los servicios de varios niveles

De manera predeterminada, Trusted Extensions no proporciona servicios de varios niveles. La mayoría de los servicios se configuran fácilmente como servicios de zona a zona, es decir, servicios de una sola etiqueta. Por ejemplo, cada zona con etiquetas puede conectarse con el servidor NFS que se ejecuta en la etiqueta de la zona con etiquetas.

Si el sitio necesita servicios de varios niveles, estos servicios se configuran mejor en un sistema con al menos dos direcciones IP. Los puertos de varios niveles que requiere un servicio de varios niveles se pueden asignar a la dirección IP que está asociada con la zona global. Las zonas con etiquetas pueden usar una dirección `all-zones` para acceder a los servicios.

Consejo – Si los usuarios de zonas con etiquetas no deben tener acceso a los servicios de varios niveles, puede asignar una dirección IP al sistema. Generalmente, esta configuración de Trusted Extensions se utiliza en equipos portátiles.

Planificación del servicio de nombres LDAP en Trusted Extensions

Si no tiene pensado instalar una red de sistemas con etiquetas, puede omitir esta sección. Si planea utilizar LDAP, sus sistemas se deben configurar como clientes LDAP antes de agregar la primera zona con etiquetas.

Si piensa ejecutar Trusted Extensions en una red de sistemas, utilice LDAP como servicio de nombres. Para Trusted Extensions se requiere un servidor LDAP (Oracle Directory Server Enterprise Edition) rellenado en el momento de configurar una red de sistemas. Si su sitio tiene un servidor LDAP existente, puede rellenar el servidor con bases de datos de Trusted Extensions. Para acceder al servidor, configure un proxy LDAP en un sistema Trusted Extensions.

Si su sitio no tiene un servidor LDAP existente, debe crear un servidor LDAP en un sistema en el que se ejecute el software Trusted Extensions. Los procedimientos se describen en el Capítulo 5, "Configuración de LDAP para Trusted Extensions (tareas)".

Planificación de la auditoría en Trusted Extensions

De manera predeterminada, la auditoría se habilita cuando se inicia Trusted Extensions por primera vez. Por lo tanto, de manera predeterminada, se auditan todos los eventos de la clase `login/logout`. Para auditar a los usuarios que están configurando el sistema, puede crear roles en una fase temprana del proceso de configuración. Cuando estos roles configuran el sistema, los registros de auditoría incluyen al usuario de inicio de sesión que asume el rol. Consulte "Creación de roles y usuarios en Trusted Extensions" en la página 67.

La planificación de la auditoría en Trusted Extensions es igual que en el SO Oracle Solaris. Para obtener detalles, consulte la Parte VII, "Auditoría en Oracle Solaris" de *Administración de Oracle Solaris: servicios de seguridad*. Mientras que Trusted Extensions agrega tokens de clases, eventos y auditoría, el software no cambia el modo en que se administra la auditoría. Para obtener información sobre las adiciones de Trusted Extensions a la auditoría, consulte el Capítulo 22, "Auditoría de Trusted Extensions (descripción general)".

Planificación de la seguridad del usuario en Trusted Extensions

El software Trusted Extensions proporciona valores predeterminados de seguridad razonable para los usuarios. Estos valores predeterminados de seguridad se muestran en la Tabla 1–2. Cuando se muestran dos valores, el primero es el valor predeterminado. El administrador de la seguridad puede modificar estos valores predeterminados para reflejar la política de seguridad del sitio. Una vez que el administrador de la seguridad define los valores predeterminados, el administrador del sistema puede crear todos los usuarios, que heredan los valores predeterminados establecidos. Para obtener descripciones de las palabras clave y los valores predeterminados, consulte las páginas del comando man `label_encodings(4)` y `policy.conf(4)`.

TABLA 1–2 Valores predeterminados de seguridad de Trusted Extensions para las cuentas de usuario

Nombre del archivo	Palabra clave	Valor
`/etc/security/policy.conf`	`IDLECMD`	`lock | logout`
	`IDLETIME`	`30`
	`CRYPT_ALGORITHMS_ALLOW`	`1,2a,md5,5,6`
	`CRYPT_DEFAULT`	`sha256`
	`LOCK_AFTER_RETRIES`	`no | yes`
	`PRIV_DEFAULT`	`basic`
	`PRIV_LIMIT`	`all`
	`AUTHS_GRANTED`	`solaris.device.cdrw`
	`CONSOLE_USER`	`Console User`
	`PROFS_GRANTED`	`Basic Solaris User`
Sección LOCAL DEFINITIONS de `/etc/security/tsol/label_encodings`	Espacio de usuario predeterminado	`CNF INTERNAL USE ONLY`
	Etiqueta de sensibilidad de usuario predeterminado	`PUBLIC`

Nota – Las variables `IDLECMD` e `IDLETIME` se aplican a la sesión del usuario de inicio de sesión. Si el usuario de inicio de sesión asume un rol, los valores `IDLECMD` e `IDLETIME` del usuario están en vigencia para ese rol.

El administrador del sistema puede configurar una plantilla de usuario estándar que defina los valores predeterminados del sistema adecuados para cada usuario. Por ejemplo, de manera predeterminada, el shell inicial de cada usuario es un shell bash. El administrador del sistema puede configurar una plantilla que proporcione un shell pfbash a cada usuario.

Diseño de una estrategia de configuración para Trusted Extensions

A continuación se describen las estrategias de configuración, de la estrategia más segura a la menos segura:

- Un equipo de dos personas configura el software. El proceso de configuración es auditado.

  Dos personas están en el equipo cuando se habilita el software. En una fase temprana del proceso de configuración, este equipo crea roles discretos y usuarios locales que puedan asumir dichos roles. El equipo también configura la auditoría para auditar los eventos ejecutados por los roles. Una vez se asignan los roles a los usuarios y se reinicia el equipo, los usuarios inician sesión y asumen un rol limitado. El software aplica la división de tareas por rol. La pista de auditoría proporciona un registro del proceso de configuración. Para ver una ilustración de un proceso de configuración seguro, consulte la Figura 1–1.

- Una persona habilita y configura el software asumiendo el rol adecuado. El proceso de configuración es auditado.

  En una fase temprana del proceso de configuración, el rol de usuario `root` crea roles adicionales. El rol de usuario `root` también configura la auditoría para auditar los eventos ejecutados por los roles. Una vez asignados estos roles adicionales al usuario inicial y reiniciado el equipo, el usuario inicia sesión y asume el rol adecuado para la tarea actual. La pista de auditoría proporciona un registro del proceso de configuración.

- Una persona asume el rol de usuario `root` para habilitar y configurar el software. El proceso de configuración no es auditado.

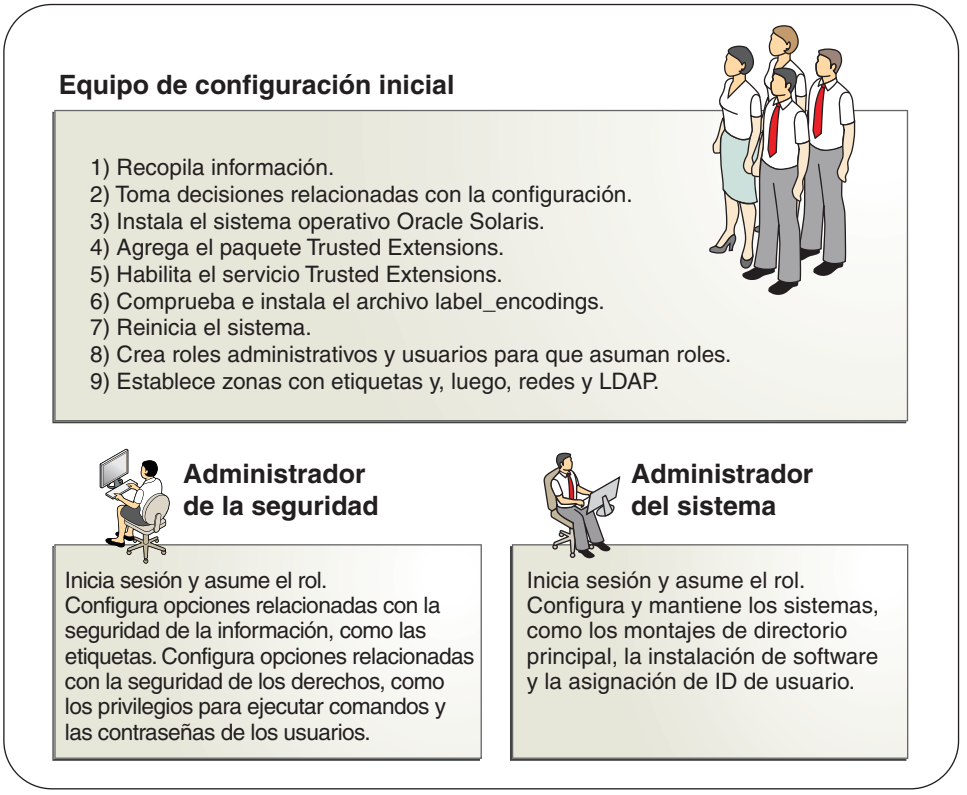
  Mediante esta estrategia, no se conserva ningún registro del proceso de configuración.

- El equipo de configuración inicial cambia el rol `root` a un usuario.

  No se conserva ningún registro en el software del nombre del usuario que actúa como `root`. Esta configuración puede ser necesaria para la administración remota de un sistema sin periféricos.

En la figura siguiente se muestra la división de tareas por rol. El administrador de la seguridad configura la auditoría, protege los sistemas de archivos, establece la política de dispositivos, determina qué programas requieren privilegio para la ejecución y protege a los usuarios, entre otras tareas. El administrador del sistema comparte y monta sistemas de archivos, instala paquetes de software y crea usuarios, entre otras tareas.

FIGURA 1–1 Administración de un sistema Trusted Extensions: división de tareas por rol



Resolución de problemas adicionales antes de habilitar Trusted Extensions

Antes de configurar Trusted Extensions, debe proteger físicamente los sistemas, decidir qué etiquetas conectará a las zonas y resolver otras cuestiones de seguridad. Para conocer los procedimientos, consulte "Resolución de problemas de seguridad antes de habilitar Trusted Extensions" en la página 46.

Realización de copia de seguridad del sistema antes de habilitar Trusted Extensions

Si el sistema tiene archivos que se deben guardar, realice una copia de seguridad antes de habilitar el servicio Trusted Extensions. La forma más segura de realizar una copia de seguridad

de los archivos es realizar un volcado de nivel 0. Si no tiene un procedimiento de copia de seguridad en el lugar, consulte la guía del administrador de su sistema operativo actual para obtener instrucciones.

Resultados de la habilitación de Trusted Extensions desde la perspectiva de un administrador

Una vez que se haya habilitado el software Trusted Extensions y se haya reiniciado el sistema, las siguientes funciones de seguridad estarán en su lugar. Muchas de las funciones pueden ser configuradas por el administrador de la seguridad.

- Se instala y configura un archivo label_encodings de Oracle.
- Un escritorio de confianza, Solaris Trusted Extensions (GNOME), crea un entorno de ventanas con etiquetas que proporciona espacios de trabajo administrativos en la zona global. Estos espacios de trabajo están protegidos por Trusted Path, visible en la banda de confianza.
- Como en el SO Oracle Solaris, los perfiles de derechos para los roles están definidos. Como en el SO Oracle Solaris, `root` es el único rol definido.

  Para utilizar roles adicionales para administrar Trusted Extensions, debe crear los roles. Durante la configuración, debe crear el rol de administrador de la seguridad.
- Se agregan tres bases de datos de red de Trusted Extensions, `tnrhdb`, `tnrhtp` y `tnzonecfg`. El comando `tncfg` permite a los administradores ver y modificar estas bases de datos de confianza.
- Trusted Extensions proporciona las interfaces gráficas de usuario para administrar el sistema. Para obtener una lista completa, consulte el Capítulo 7, “Herramientas de administración de Trusted Extensions”.
  - La secuencia de comandos `txzonemgr` permite a los administradores configurar las zonas y las redes de Trusted Extensions. Para obtener más información, consulte la página del comando man `txzonemgr(1M)`.
  - Device Manager gestiona la asignación y el etiquetado de los dispositivos conectados.

◆ ◆ ◆ CAPÍTULO 2

Guía básica de configuración de Trusted Extensions

Este capítulo describe las tareas para habilitar y configurar la función Trusted Extensions de Oracle Solaris.

Precaución – Si desea habilitar y configurar Trusted Extensions de manera remota, lea atentamente el Capítulo 12, "Administración remota en Trusted Extensions (tareas)" antes de iniciar el entorno Trusted Extensions.

Mapa de tareas: preparación y habilitación de Trusted Extensions

Para preparar el sistema y habilitar Trusted Extensions, complete las siguientes tareas.

Tarea	Para obtener instrucciones
■ Preparar una instalación existente de Oracle Solaris para Trusted Extensions. ■ Instalar el SO Oracle Solaris con Trusted Extensions en mente.	■ "Preparación de un sistema Oracle Solaris instalado para Trusted Extensions" en la página 45 ■ "Instalación segura de un sistema Oracle Solaris" en la página 44
Reunir información y tomar decisiones relacionadas con el sistema y la red de Trusted Extensions.	"Resolución de problemas de seguridad antes de habilitar Trusted Extensions" en la página 46
Habilitar Trusted Extensions.	"Habilitación de Trusted Extensions y reinicio" en la página 48

Mapa de tareas: selección de una configuración de Trusted Extensions

Configure Trusted Extensions en el sistema mediante uno de los métodos mencionados en el siguiente mapa de tareas.

Tarea	Para obtener instrucciones
Crear un sistema Trusted Extensions de demostración.	"Mapa de tareas: configuración de Trusted Extensions con los valores predeterminados proporcionados" en la página 40
Crear un sistema Trusted Extensions empresarial.	"Mapa de tareas: configuración de Trusted Extensions para cumplir los requisitos del sitio" en la página 41
Configurar Trusted Extensions en un sistema remoto.	Habilite Trusted Extensions sin reiniciar. Siga las instrucciones descritas en el Capítulo 12, "Administración remota en Trusted Extensions (tareas)". Luego, continúe con las instrucciones para sistemas con monitores.

Mapa de tareas: configuración de Trusted Extensions con los valores predeterminados proporcionados

Para una configuración predeterminada, realice las siguientes tareas en orden.

Tarea	Para obtener instrucciones
Cargar los paquetes de Trusted Extensions.	"Adición de paquetes de Trusted Extensions a un sistema Oracle Solaris" en la página 45
Habilitar Trusted Extensions y reiniciar.	"Habilitación de Trusted Extensions y reinicio" en la página 48
Iniciar sesión.	"Inicio de sesión en Trusted Extensions" en la página 49
Crear dos zonas con etiquetas.	"Cómo crear un sistema Trusted Extensions predeterminado" en la página 56 O bien, "Cómo crear zonas con etiquetas de forma interactiva" en la página 57
Crear espacios de trabajo con etiquetas para las zonas.	"Cómo asignar etiquetas a dos espacios de trabajo con zonas" en la página 59

Mapa de tareas: configuración de Trusted Extensions para cumplir los requisitos del sitio

Consejo – Para un proceso de configuración seguro, cree roles en una fase temprana del proceso.

El orden de tareas se muestra en el siguiente mapa de tareas.

- Las tareas descritas en "Creación de zonas con etiquetas" en la página 56 son obligatorias.
- En función de los requisitos del sitio, realice otras tareas de configuración.

Tarea	Para obtener instrucciones
Configurar la zona global.	"Configuración de la zona global en Trusted Extensions" en la página 51
Configurar las zonas con etiquetas.	"Creación de zonas con etiquetas" en la página 56
Configurar redes para la comunicación con otros sistemas.	"Configuración de las interfaces de red en Trusted Extensions" en la página 61
Configurar el servicio de nombres LDAP. **Nota –** Omita esta tarea si no se utiliza LDAP.	Capítulo 5, "Configuración de LDAP para Trusted Extensions (tareas)"
Completar la configuración del sistema.	Parte II

◆ ◆ ◆ CAPÍTULO 3

Adición de la función Trusted Extensions a Oracle Solaris (tareas)

En este capítulo, se describe cómo preparar y habilitar el servicio Trusted Extensions en un sistema Oracle Solaris. En este capítulo, se tratan los siguientes temas:

Responsabilidades del equipo de configuración inicial

El software Trusted Extensions está diseñado para ser configurado por dos personas con distintas responsabilidades. Esta división de tareas puede aplicarse mediante roles. Como los roles discretos y los usuarios adicionales se crean después de la instalación, se recomienda que un equipo de configuración inicial de al menos dos personas esté presente para habilitar y configurar el software Trusted Extensions.

Preparación de un sistema Oracle Solaris y adición de Trusted Extensions

La elección de las opciones de instalación de Oracle Solaris puede afectar el uso y la seguridad de Trusted Extensions:

- Para obtener una compatibilidad adecuada para Trusted Extensions, debe instalar el SO Solaris subyacente de manera segura. Para conocer las opciones de instalación de Oracle Solaris que afectan a Trusted Extensions, consulte "Instalación segura de un sistema Oracle Solaris" en la página 44.
- Si ha utilizado el SO Solaris, compare la configuración actual con los requisitos de Trusted Extensions. Para conocer los factores que afectan a Trusted Extensions, consulte "Preparación de un sistema Oracle Solaris instalado para Trusted Extensions" en la página 45.

▼ Instalación segura de un sistema Oracle Solaris

Esta tarea se aplica a las instalaciones realizadas desde cero de Oracle Solaris. Si desea realizar una actualización, consulte "Preparación de un sistema Oracle Solaris instalado para Trusted Extensions" en la página 45.

1 Al instalar el SO Oracle Solaris, cree una cuenta de usuario y la cuenta del rol de usuario `root`.

En Trusted Extensions, puede utilizar el rol de usuario `root`, además de los roles que cree, para configurar el sistema.

2 Al iniciar sesión en Oracle Solaris por primera vez, asigne una contraseña a la cuenta del rol de usuario `root`.

a. Abra una ventana de terminal.

b. Asuma el rol de usuario root.

Cuando se solicite, proporcione una contraseña que sea diferente de la contraseña de la cuenta de usuario.

```
% su -
Your password has expired. Create a new password.
Enter new password:      Type a password for root
Retype the password:      Retype the root password
#
```

Asigne una contraseña de seis caracteres alfanuméricos como mínimo. La contraseña debe ser difícil de adivinar, a fin de reducir la posibilidad de que un adversario obtenga acceso no autorizado al intentar adivinar la contraseña.

Pasos siguientes Continúe con "Adición de paquetes de Trusted Extensions a un sistema Oracle Solaris" en la página 45.

▼ Preparación de un sistema Oracle Solaris instalado para Trusted Extensions

Esta tarea se aplica a los sistemas Oracle Solaris que han estado en uso y en los que tiene previsto ejecutar Trusted Extensions.

Antes de empezar Debe estar con el rol de usuario `root` en la zona global.

1 Si hay zonas no globales instaladas en el sistema, elimínelas.

La marca con etiquetas de Trusted Extensions es una marca de zonas exclusiva. Consulte las páginas del comando man `brands(5)` y `trusted_extensions(5)`.

2 Si el sistema no tiene una contraseña de usuario root, cree una.

Nota – Los usuarios no deben revelar sus contraseñas a otra persona, ya que esa persona podría acceder a los datos del usuario sin que se la pueda identificar claramente ni responsabilizar. Tenga en cuenta que la divulgación puede ser directa, si el usuario revela su contraseña deliberadamente a otra persona, o indirecta, si el usuario escribe la contraseña o selecciona una contraseña insegura. Oracle Solaris ofrece protección contra contraseñas inseguras, pero no puede evitar que el usuario revele su contraseña o la escriba.

Pasos siguientes Continúe con "Adición de paquetes de Trusted Extensions a un sistema Oracle Solaris" en la página 45.

▼ Adición de paquetes de Trusted Extensions a un sistema Oracle Solaris

Antes de empezar Ha completado los pasos descritos en "Preparación de un sistema Oracle Solaris instalado para Trusted Extensions" en la página 45 o "Instalación segura de un sistema Oracle Solaris" en la página 44.

Debe tener asignado el perfil de derechos de instalación de software.

1 Después de iniciar sesión como usuario inicial, asuma el rol de usuario `root` en una ventana de terminal.

```
% su -
Enter Password:      Type root password
#
```

2. **Descargue e instale el paquete Trusted Extensions.**

   Utilice la línea de comandos o la interfaz gráfica de usuario Package Manager.

   - **En la ventana de terminal, use el comando `pkg install`.**

     ```
     $ pkg install system/trusted/trusted-extensions
     ```

     Para instalar configuraciones regionales de confianza, especifique el nombre corto de la configuración regional. Por ejemplo, el siguiente comando instala la configuración regional para Japón:

     ```
     $ pkg install system/trusted/locale/ja &
     ```

   - **En la ventana de terminal, inicie la interfaz gráfica de usuario Package Manager.**

     ```
     $ packagemanager &
     ```

     a. **Seleccione los paquetes de Trusted Extensions.**

        i. **Visualice las categorías de la categoría Escritorio (GNOME).**

        ii. **Seleccione la categoría Trusted Extensions.**

        iii. **En la lista de paquetes, haga clic en la casilla de trusted-extensions.**

        iv. **(Opcional) En la lista de paquetes, haga clic en la casilla de cualquier configuración regional que desee instalar.**

     b. **Para agregar los paquetes, haga clic en el icono Instalar/Actualizar.**

Resolución de problemas de seguridad antes de habilitar Trusted Extensions

En cada sistema en el que se configurará Trusted Extensions, deberá tomar algunas decisiones respecto de la configuración. Por ejemplo, debe decidir si instalará la configuración predeterminada de Trusted Extensions o si personalizará la configuración.

▼ Protección del hardware del sistema y toma de decisiones relacionadas con la seguridad antes de habilitar Trusted Extensions

En cada sistema en el que se va a configura Trusted Extensions, tome estas decisiones de configuración antes de habilitar el software.

1 **Decida el grado de seguridad con el que se debe proteger el hardware del sistema.**

En un sitio seguro, este paso se realiza en cada sistema Oracle Solaris.

- En los sistemas SPARC, seleccione un nivel de seguridad PROM y proporcione una contraseña.
- En los sistemas x86, proteja el BIOS.
- En todos los sistemas, proteja `root` con una contraseña.

2 **Prepare el archivo `label_encodings`.**

Si tiene un archivo `label_encodings` específico del sitio, el archivo se debe comprobar e instalar antes de iniciar otras tareas de configuración. Si su sitio no tiene un archivo `label_encodings`, puede usar el archivo predeterminado que suministra Oracle. Oracle también suministra otros archivos `label_encodings`, que puede encontrar en el directorio `/etc/security/tsol`. Los archivos de Oracle son archivos de demostración. Es posible que no sean adecuados para los sistemas de producción.

Para personalizar un archivo para su sitio, consulte *Trusted Extensions Label Administration*.

3 **A partir de la lista de etiquetas del archivo `label_encodings`, realice una lista de las zonas con etiquetas que planea crear.**

En el archivo `label_encodings` predeterminado, las etiquetas son las siguientes y los nombres de las zonas pueden ser similares a los siguientes:

Nombre de etiqueta completo	Nombre de zona propuesto
`PUBLIC`	`public`
`CONFIDENTIAL: INTERNAL USE ONLY`	`internal`
`CONFIDENTIAL : NEED TO KNOW`	`needtoknow`
`CONFIDENTIAL : RESTRICTED`	`restricted`

Nota – El método de configuración automático crea las zonas `public` e `internal`.

4 **Decida cuándo crear roles.**

Según la política de seguridad del sitio, es posible que deba asumir un rol para administrar Trusted Extensions. Si es así, o si desea configurar el sistema para cumplir con los criterios de una configuración evaluada, debe crear estos roles en una fase temprana del proceso de configuración.

Si no es necesario que configure el sistema mediante el uso de roles discretos, puede configurar el sistema con el rol de usuario `root`. Este método de configuración es menos seguro. El rol de usuario `root` puede realizar todas las tareas del sistema, mientras que otros roles normalmente

realizan un conjunto más limitado de tareas. Por lo tanto, la configuración está más controlada cuando se realiza mediante los roles que usted crea.

5 **Decida otras cuestiones de seguridad para cada sistema y para la red.**

Por ejemplo, se recomienda considerar los siguientes temas de seguridad:

- Determinar qué dispositivos se pueden conectar al sistema y asignar para su uso.
- Identificar a qué impresoras de qué etiquetas se puede acceder desde el sistema.
- Identificar los sistemas que tienen un rango de etiquetas limitado, como un sistema de puerta de enlace o un quiosco público.
- Identificar qué sistemas con etiquetas se pueden comunicar con determinados sistemas sin etiquetas.

Habilitación del servicio Trusted Extensions e inicio de sesión

En el SO Oracle Solaris, Trusted Extensions es un servicio gestionado por la utilidad de gestión de servicios (SMF, Service Management Facility). El nombre del servicio es `svc:/system/labeld:default`. De manera predeterminada, el servicio `labeld` está deshabilitado.

Nota – El sistema Trusted Extensions no necesita una red para ejecutar un escritorio con una pantalla de mapa de bits con conexión directa, como un equipo portátil o una estación de trabajo. Se requiere una configuración de red para la comunicación con otros sistemas.

▼ Habilitación de Trusted Extensions y reinicio

El servicio `labeld` anexa etiquetas a puntos finales de comunicación. Por ejemplo, se etiqueta lo siguiente:

- Todas las zonas, y los directorios y archivos de cada zona
- Todos los procesos, incluidos los procesos de ventana
- Todas las comunicaciones de red

Antes de empezar Ha completado las tareas descritas en "Preparación de un sistema Oracle Solaris y adición de Trusted Extensions" en la página 44 y "Resolución de problemas de seguridad antes de habilitar Trusted Extensions" en la página 46.

Debe estar con el rol de usuario `root` en la zona global.

1 **Mueva el panel de la parte superior de la pantalla a la parte inferior de la pantalla.**

Precaución – Si no mueve el panel, es posible que no pueda acceder al menú principal o los paneles del escritorio al iniciar sesión en Trusted Extensions.

a. En el panel superior, haga clic con el botón derecho y seleccione Propiedades.

b. Cambie la orientación del panel superior a inferior.

2 Abra una ventana de terminal y habilite el servicio `labeld`.

```
# svcadm enable -s labeld
```

El servicio `labeld` agrega etiquetas al sistema e inicia los servicios de asignación de dispositivos.

Precaución – No realice ninguna otra tarea en el sistema hasta que el cursor regrese al indicador.

3 Compruebe que el servicio esté habilitado.

```
# svcs -x labeld
svc:/system/labeld:default (Trusted Extensions)
 State: online since weekday month date hour:minute:second year
   See: labeld(1M)
Impact: None.
```

Precaución – Si desea habilitar y configurar Trusted Extensions de manera remota, lea atentamente el Capítulo 12, “Administración remota en Trusted Extensions (tareas)”. No reinicie el sistema hasta que haya configurado el sistema para permitir la administración remota. Si no configura el sistema Trusted Extensions para la administración remota, no podrá acceder a él desde un sistema remoto.

4 Reinicie el sistema.

```
# /usr/sbin/reboot
```

Pasos siguientes Continúe con “Inicio de sesión en Trusted Extensions” en la página 49.

▼ Inicio de sesión en Trusted Extensions

Al iniciar sesión, accede a la zona global, que es un entorno que reconoce y aplica el control de acceso obligatorio (MAC).

En la mayoría de los sitios, dos o más administradores conforman el equipo de configuración inicial y están presentes durante la configuración del sistema.

Antes de empezar Ha completado los pasos descritos en "Habilitación de Trusted Extensions y reinicio" en la página 48.

1 Inicie sesión con la cuenta de usuario que creó durante la instalación.

En el cuadro de diálogo de inicio de sesión, escriba *nombre_usuario* y luego la contraseña.

Los usuarios no deben revelar sus contraseñas a otra persona, ya que esa persona podría acceder a los datos del usuario sin que se la pueda identificar claramente ni responsabilizar. Tenga en cuenta que la divulgación puede ser directa, si el usuario revela su contraseña deliberadamente a otra persona, o indirecta, si el usuario escribe la contraseña o selecciona una contraseña insegura. El software Trusted Extensions ofrece protección contra contraseñas inseguras, pero no puede evitar que el usuario revele su contraseña o la escriba.

2 Utilice el mouse para cerrar la ventana Status y la ventana Clearance.

3 Cierre el cuadro de diálogo que indica que la etiqueta `PUBLIC` no tiene ninguna zona coincidente.

Creará la zona después de asumir el rol de usuario `root`.

4 Asuma el rol de usuario `root`.

a. Haga clic en su nombre en la banda de confianza.

El rol de usuario `root` aparece en un menú desplegable.

b. Seleccione el rol de usuario `root`.

Si se solicita, cree una nueva contraseña para el rol.

Nota – Antes de dejar el sistema desatendido, debe cerrar la sesión o bloquear la pantalla. De lo contrario, una persona puede acceder al sistema sin la necesidad de una identificación o autenticación, y esa persona no se podría identificar claramente ni responsabilizar.

Pasos siguientes Continúe con uno de los siguientes pasos:

- Para configurar un sistema predeterminado, vaya a "Creación de zonas con etiquetas" en la página 56.
- Para personalizar el sistema antes de crear zonas con etiquetas, vaya a "Configuración de la zona global en Trusted Extensions" en la página 51.
- Si el sistema no tiene una pantalla gráfica, vaya al Capítulo 12, "Administración remota en Trusted Extensions (tareas)".

◆ ◆ ◆ CAPÍTULO 4

Configuración de Trusted Extensions (tareas)

En este capítulo, se explica cómo configurar Trusted Extensions en un sistema con un monitor. Para un funcionamiento correcto, el software Trusted Extensions requiere la configuración de etiquetas y zonas. También puede configurar comunicaciones de red, roles y usuarios que pueden asumir roles.

Para otras tareas de configuración, consulte la Parte II.

Configuración de la zona global en Trusted Extensions

Para personalizar la configuración de Trusted Extensions, realice los procedimientos descritos en el siguiente mapa de tareas. Para instalar la configuración predeterminada, vaya a "Creación de zonas con etiquetas" en la página 56.

Tarea	Descripción	Para obtener instrucciones
Proteger el hardware.	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*
Configurar etiquetas.	Se *deben* configurar etiquetas para el sitio. Si tiene previsto utilizar el archivo `label_encodings` predeterminado, puede omitir este paso.	"Cómo comprobar e instalar el archivo de codificaciones de etiquetas" en la página 52
Habilitar una red IPv6.	Se habilita IP para que reconozca paquetes con etiquetas en una red IPv6.	"Cómo habilitar redes IPv6 en Trusted Extensions" en la página 54

Tarea	Descripción	Para obtener instrucciones
Cambiar el dominio de interpretación.	Se especifica un dominio de interpretación (DOI) diferente de 1.	"Cómo configurar el dominio de interpretación" en la página 55
Configurar el servidor LDAP.	Se configura un servidor de directorios LDAP de Trusted Extensions.	Capítulo 5, "Configuración de LDAP para Trusted Extensions (tareas)"
Configurar los clientes LDAP.	Este sistema se convierte en cliente del servidor de directorios LDAP de Trusted Extensions.	"Conversión de la zona global en un cliente LDAP en Trusted Extensions" en la página 94

▼ Cómo comprobar e instalar el archivo de codificaciones de etiquetas

El archivo de codificaciones debe ser compatible con cualquier host de Trusted Extensions con el que se esté comunicando.

Nota – Trusted Extensions instala un archivo `label_encodings` predeterminado. Este archivo predeterminado es útil para las demostraciones. Sin embargo, es posible que este archivo no sea una buena opción para usted. Si tiene previsto usar el archivo predeterminado, puede omitir este procedimiento.

- Si está familiarizado con los archivos de codificaciones, puede utilizar el siguiente procedimiento.
- Si no está familiarizado con los archivos de codificaciones, consulte *Trusted Extensions Label Administration* para ver los requisitos, los procedimientos y los ejemplos.

Precaución – Antes de continuar, *debe* instalar correctamente las etiquetas o la configuración fallará.

Antes de empezar

Debe ser el administrador de la seguridad. El administrador de la seguridad es el responsable de la edición, la comprobación y el mantenimiento del archivo `label_encodings`. Si piensa editar el archivo `label_encodings`, asegúrese de que el archivo se pueda escribir. Para obtener más información, consulte la página del comando man `label_encodings(4)`.

Para editar el archivo `label_encodings`, debe tener el rol de usuario `root`.

1 Copie el archivo `label_encodings` en el disco.

Para copiar desde medios portátiles, consulte "Cómo copiar archivos desde medios portátiles en Trusted Extensions" en la página 79.

2. **En una ventana de terminal, compruebe la sintaxis del archivo.**

   a. **Ejecute el comando `chk_encodings`.**

      ```
      # /usr/sbin/chk_encodings /full-pathname-of-label-encodings-file
      ```

   b. **Lea el resultado y realice una de las siguientes acciones:**

      - **Corrija los errores.**

        Si el comando informa errores, éstos se *deben* corregir antes de continuar. Para obtener ayuda, consulte el Capítulo 3, "Creating a Label Encodings File (Tasks)" de *Trusted Extensions Label Administration*.

      - **Convierta el archivo en el archivo `label_encodings` activo.**

        ```
        # cp /full-pathname-of-label-encodings-file \
         /etc/security/tsol/label.encodings.site
        # cd /etc/security/tsol
        # cp label_encodings label_encodings.tx.orig
        # cp label.encodings.site label_encodings
        ```

Precaución – Para poder continuar, su archivo `label_encodings` *debe* aprobar la prueba de comprobación de codificaciones.

Ejemplo 4–1 Comprobación de la sintaxis de label_encodings en la línea de comandos

En este ejemplo, el administrador prueba varios archivos `label_encodings` mediante la línea de comandos.

```
# /usr/sbin/chk_encodings /var/encodings/label_encodings1
No errors found in /var/encodings/label_encodings1
# /usr/sbin/chk_encodings /var/encodings/label_encodings2
No errors found in /var/encodings/label_encodings2
```

Cuando la administración decide utilizar el archivo `label_encodings2`, el administrador ejecuta un análisis semántico del archivo.

```
# /usr/sbin/chk_encodings -a /var/encodings/label_encodings2
No errors found in /var/encodings/label_encodings2

---> VERSION = MYCOMPANY LABEL ENCODINGS  2.0 10/10/2010

---> CLASSIFICATIONS <---

   Classification 1: PUBLIC
   Initial Compartment bits: 10
   Initial Markings bits: NONE

---> COMPARTMENTS AND MARKINGS USAGE ANALYSIS <---
...
```

```
---> SENSITIVITY LABEL to COLOR MAPPING <---
...
```

El administrador imprime una copia del análisis semántico para sus registros y, a continuación, mueve el archivo al directorio `/etc/security/tsol`.

```
# cp /var/encodings/label_encodings2 /etc/security/tsol/label.encodings.10.10.10
# cd /etc/security/tsol
# cp label_encodings label_encodings.tx.orig
# cp label.encodings.10.10.10 label_encodings
```

Por último, el administrador verifica que el archivo `label_encodings` sea el archivo de la compañía.

```
# /usr/sbin/chk_encodings -a /etc/security/tsol/label_encodings | head -4
No errors found in /etc/security/tsol/label_encodings

---> VERSION = MYCOMPANY LABEL ENCODINGS  2.0 10/10/2010
```

Pasos siguientes Debe reiniciar el sistema antes de crear zonas con etiquetas.

▼ Cómo habilitar redes IPv6 en Trusted Extensions

Precaución – La secuencia de comandos `txzonemgr` no admite la sintaxis de direcciones IPv6. Por lo tanto, puede utilizar el comando `tncfg` para agregar hosts IPv6 a la red de Trusted Extensions. Para ver ejemplos, consulte "Mecanismo de reserva de la red de confianza" en la página 203 y el Ejemplo 16–11.

Las opciones de CIPSO no tienen un número de Autoridad de números asignados de Internet (IANA) para utilizar en el campo de tipo de opción IPv6 de un paquete. La entrada que defina en este procedimiento proporcionará un número para utilizar en la red local hasta que IANA asigne un número para esta opción. Si este número no se define, Trusted Extensions deshabilita las redes IPv6.

Para habilitar una red IPv6 en Trusted Extensions, debe agregar una entrada en el archivo `/etc/system`.

Antes de empezar Tiene el rol de usuario `root` en la zona global.

- **Escriba la siguiente entrada en el archivo `/etc/system`:**

```
set ip:ip6opt_ls = 0x0a
```

Errores más frecuentes

- Si los mensajes de error durante el inicio indican que la configuración de IPv6 es incorrecta, corrija la entrada:

- Verifique que la entrada esté escrita correctamente.
- Verifique que el sistema se haya reiniciado después de agregar la entrada correcta al archivo `/etc/system`.

- Si agrega Trusted Extensions en un sistema Oracle Solaris que actualmente tiene IPv6 habilitado, pero no agrega la entrada de IP en `/etc/system`, aparecerá un mensaje de error similar siguiente: `t_optmgmt: Error de sistema: No es posible asignar la dirección solicitada` *indicación de hora*.

Pasos siguientes Debe reiniciar el sistema antes de crear zonas con etiquetas.

▼ Cómo configurar el dominio de interpretación

Todas las comunicaciones en las que participe un sistema en el que esté configurado Trusted Extensions deben seguir las reglas de etiquetado de un solo dominio de interpretación (DOI) de CIPSO. El dominio de interpretación que se usa en cada mensaje se identifica mediante un número entero en el encabezado de la opción IP de CIPSO. De manera predeterminada, el dominio de interpretación en Trusted Extensions es `1`.

Si su sitio no utiliza un dominio de interpretación con el valor `1`, debe modificar el valor `doi` en cada plantilla de seguridad.

Antes de empezar Tiene el rol de usuario `root` en la zona global.

- **Especifique el valor del dominio de interpretación en las plantillas de seguridad predeterminadas.**

```
# tncfg -t cipso set doi=n
# tncfg -t admin_low set doi=n
```

Nota – Cada plantilla de seguridad debe especificar el valor del dominio de interpretación.

Véase también
- "Atributos de seguridad de red en Trusted Extensions" en la página 200
- "Cómo crear plantillas de seguridad" en la página 219

Pasos siguientes Si tiene previsto utilizar LDAP, vaya al Capítulo 5, "Configuración de LDAP para Trusted Extensions (tareas)". Debe configurar LDAP antes de crear zonas con etiquetas.

De lo contrario, continúe con "Creación de zonas con etiquetas" en la página 56.

Creación de zonas con etiquetas

Las instrucciones de esta sección permiten configurar zonas con etiquetas. Tiene la posibilidad de crear dos zonas con etiquetas de manera automática o crear zonas de forma manual.

Nota – Si tiene previsto utilizar LDAP, vaya al Capítulo 5, "Configuración de LDAP para Trusted Extensions (tareas)". Debe configurar LDAP antes de crear zonas con etiquetas.

Tarea	Descripción	Para obtener instrucciones
1a. Crear una configuración predeterminada de Trusted Extensions.	El comando `txzonemgr -c` crea dos zonas con etiquetas a partir del archivo `label_encodings`.	"Cómo crear un sistema Trusted Extensions predeterminado" en la página 56
1b. Crear una configuración predeterminada de Trusted Extensions mediante una interfaz gráfica de usuario.	La secuencia de comandos `txzonemgr` crea una interfaz gráfica de usuario que presenta las tareas correspondientes a medida que configura el sistema.	"Cómo crear zonas con etiquetas de forma interactiva" en la página 57
1c. Avanzar manualmente por la creación de zonas.	La secuencia de comandos `txzonemgr` crea una interfaz gráfica de usuario que presenta las tareas correspondientes a medida que configura el sistema.	"Cómo crear zonas con etiquetas de forma interactiva" en la página 57
2. Crear un entorno con etiquetas activo.	En la configuración predeterminada, se etiquetan dos espacios de trabajo como `PUBLIC` e `INTERNAL USE ONLY`.	"Cómo asignar etiquetas a dos espacios de trabajo con zonas" en la página 59
3. (Opcional) Establecer un enlace con otros sistemas de la red.	Se configuran las interfaces de red de las zona con etiquetas y se conecta la zona global y las zonas con etiquetas con otros sistemas.	"Configuración de las interfaces de red en Trusted Extensions" en la página 61

▼ Cómo crear un sistema Trusted Extensions predeterminado

Este procedimiento crea un sistema Trusted Extensions activo con dos zonas con etiquetas. Los hosts remotos no se asignaron a las plantillas de seguridad del sistema, de modo que este sistema no se puede comunicar con ningún host remoto.

Antes de empezar Ha completado los pasos descritos en "Inicio de sesión en Trusted Extensions" en la página 49. Ha asumido el rol de usuario `root`.

1 Abra una ventana de terminal en el cuarto espacio de trabajo.

2 (Opcional) Revise la página del comando man `txzonemgr`.

```
# man txzonemgr
```

3 **Cree una configuración predeterminada.**

```
# /usr/sbin/txzonemgr -c
```

Este comando copia el SO Oracle Solaris y el software Trusted Extensions en una zona, crea una instantánea de la zona, etiqueta la zona original y luego utiliza la instantánea para crear una segunda zona con etiquetas. Se inician las zonas.

- La primera zona con etiquetas se basa en el valor de `Default User Sensitivity Label` del archivo `label_encodings`.
- La segunda zona con etiquetas se basa en el valor de `Default User Clearance` del archivo `label_encodings`.

Este paso puede tardar cerca de 20 minutos. Para instalar las zonas, la secuencia de comandos utiliza la contraseña de usuario root de la zona global para la las zonas con etiquetas.

Pasos siguientes Para utilizar su configuración de Trusted Extensions, vaya a "Cómo asignar etiquetas a dos espacios de trabajo con zonas" en la página 59.

▼ Cómo crear zonas con etiquetas de forma interactiva

No es necesario que cree una zona para cada la etiqueta del archivo `label_encodings`, pero puede hacerlo. Las interfaces gráficas de usuario administrativas enumeran las etiquetas para las que se pueden crear zonas en este sistema. En este procedimiento, se crean dos zonas con etiquetas. Si se utiliza el archivo `label_encodings` de Trusted Extensions, se crea la configuración predeterminada de Trusted Extensions.

Antes de empezar Ha completado los pasos descritos en "Inicio de sesión en Trusted Extensions" en la página 49. Ha asumido el rol de usuario `root`.

No ha creado aún ninguna zona.

1 **Ejecute el comando `txzonemgr` sin ninguna opción.**

```
# txzonemgr &
```

La secuencia de comandos abre el cuadro de diálogo `Labeled Zone Manager`. Este cuadro de diálogo de `zenity` le solicita que realice las tareas correspondientes, según el estado actual de su configuración.

Para realizar una tarea, seleccione la opción de menú, a continuación, presione la tecla de retorno o haga clic en OK. Cuando se le pida que introduzca texto, escriba el texto y, a continuación, presione la tecla de retorno o haga clic en OK.

Consejo – Para ver el estado actual de finalización de la zona, haga clic en Return to Main Menu, en Labeled Zone Manager. O bien, puede hacer clic en el botón Cancel.

2 Seleccione uno de los siguientes métodos para instalar las zonas:

- **Para crear dos zonas con etiquetas, seleccione `public` and `internal` zones en el cuadro de diálogo.**
  - La primera zona con etiquetas se basa en el valor de `Default User Sensitivity Label` del archivo `label_encodings`.
  - La segunda zona con etiquetas se basa en el valor de `Default User Clearance` del archivo `label_encodings`.

  a. Responda la petición de datos para identificar el sistema.

  Si la zona `public` utiliza una pila de IP exclusiva, o si tiene una dirección IP definida en DNS, utilice el nombre de host como se define en DNS. De lo contrario, utilice el nombre del sistema.

  b. No responda la petición de una contraseña de usuario root.

  La contraseña de usuario root se definió en la instalación del sistema. La introducción de datos para esta petición fallará.

  c. En la petición de datos de inicio de sesión de la zona, escriba su usuario y contraseña.

  A continuación, verifique que todos los servicios estén configurados mediante la ejecución del comando `svcs -x`. Si no se muestra ningún mensaje, todos los servicios están configurados.

  d. Salga de la zona y cierre la ventana.

  Escriba exit en la petición de datos y seleccione Close window en Zone Console.

  En otra ventana, se completa la instalación de la segunda zona. Esta zona se crea a partir de una instantánea, por lo que se crea rápidamente.

  e. Inicie sesión en la segunda consola de zona y verifique que todos los servicios estén en ejecución.

  ```
  # svcs -x
  #
  ```

  Si no se muestra ningún mensaje, todos los servicios están configurados. Se visualiza Labeled Zone Manager.

f. Haga doble clic en la zona interna en Labeled Zone Manager.

Seleccione Reboot y, a continuación, haga clic en el botón Cancel para volver a la pantalla principal. Todas las zonas están en ejecución. La instantánea sin etiquetas no está en ejecución.

- **Para crear zonas manualmente, seleccione el menú principal y, a continuación, Create a Zone.**

  Siga las indicaciones. La interfaz gráfica de usuario lo guía a través de la creación de zonas.

  Una vez que se crea y se inicia la zona, puede volver a la zona global para crear más zonas. Estas zonas se crean a partir de una instantánea.

Ejemplo 4–2 Creación de otra zona con etiquetas

En este ejemplo, el administrador crea una zona restringida a partir del archivo `label_encodings` predeterminado.

En primer lugar, el administrador abre la secuencia de comandos `txzonemgr` en modo interactivo.

```
# txzonemgr &
```

A continuación, el administrador navega hasta la zona global y crea una zona con el nombre `restricted`.

```
Create a new zone:restricted
```

Luego, el administrador aplica la etiqueta correcta.

```
Select label:CNF : RESTRICTED
```

En la lista, el administrador selecciona la opción Clone y, a continuación, selecciona `snapshot` como plantilla para la nueva zona.

Una vez que la zona `restricted` está disponible, el administrador hace clic en Boot para iniciar la segunda zona.

Para permitir el acceso a la zona `restricted`, el administrador cambia el valor `Default User Clearance` del archivo `label_encodings` a `CNF RESTRICTED`.

▼ Cómo asignar etiquetas a dos espacios de trabajo con zonas

Este procedimiento crea dos espacios de trabajo con etiquetas y abre una ventana con etiquetas en cada espacio de trabajo etiquetado. Cuando finalice esta tarea, tendrá un sistema Trusted Extensions activo sin conexión en red.

Antes de empezar Ha completado los pasos descritos en "Cómo crear un sistema Trusted Extensions predeterminado" en la página 56 o en "Cómo crear zonas con etiquetas de forma interactiva" en la página 57.

Es el usuario inicial.

1 Cree un espacio de trabajo `PUBLIC`.

La etiqueta del espacio de trabajo `PUBLIC` se corresponde con el valor de `Default User Sensitivity Label`.

a. Cambie al segundo espacio de trabajo.

b. Haga clic con el botón derecho y seleccione Change Workspace Label.

c. Seleccione PUBLIC y haga clic en OK.

2 Indique su contraseña cuando se solicite.

Se encuentra en un espacio de trabajo `PUBLIC`.

3 Abra una ventana de terminal.

La ventana tiene la etiqueta `PUBLIC`.

4 Cree un espacio de trabajo INTERNAL USE ONLY.

Si se utiliza un archivo `label_encodings` específico del sitio, se crea un espacio de trabajo a partir del valor de `Default User Clearance`.

a. Cambie al tercer espacio de trabajo.

b. Haga clic con el botón derecho y seleccione Change Workspace Label.

c. Seleccione INTERNAL USE ONLY y haga clic en OK.

5 Indique su contraseña cuando se solicite.

Se encuentra en espacio de trabajo `INTERNAL`.

6 Abra una ventana de terminal.

La ventana tiene la etiqueta `CONFIDENTIAL : INTERNAL USE ONLY`.

El sistema está listo para usar. Tiene dos espacios de trabajo de usuario y un espacio de trabajo de rol. En esta configuración, las zonas con etiquetas utilizan la misma dirección IP que la zona global para comunicarse con otros sistemas. Pueden hacerlo porque, de forma predeterminada, comparten la dirección IP como una interfaz `all-zones`.

Pasos siguientes Si planea que el sistema Trusted Extensions se comunique con otros sistemas, vaya a "Configuración de las interfaces de red en Trusted Extensions" en la página 61.

Configuración de las interfaces de red en Trusted Extensions

El sistema Trusted Extensions no necesita una red para ejecutar un escritorio con una pantalla de mapa de bits con conexión directa, como un equipo portátil o una estación de trabajo. Sin embargo, se requiere una configuración de red para la comunicación con otros sistemas. Mediante la interfaz gráfica de usuario `txzonemgr`, puede configurar de forma sencilla las zonas con etiquetas y la zona global para la conexión con otros sistemas. Para obtener una descripción de las opciones de configuración para las zonas con etiquetas, consulte "Acceso a zonas con etiquetas" en la página 32. En el siguiente mapa de tareas, se describen las tareas de configuración de red y se incluyen enlaces a ellas.

Tarea	Descripción	Para obtener instrucciones
Configurar un sistema predeterminado para los usuarios comunes.	El sistema tiene una dirección IP y utiliza una interfaz `all-zones` para la comunicación entre las zonas con etiquetas y la zona global. La misma dirección IP se utiliza para la comunicación con sistemas remotos.	"Cómo compartir una única dirección IP con todas las zonas" en la página 62
Agregar una dirección IP a la zona global.	El sistema tiene más de una dirección IP y utiliza la dirección IP exclusiva de la zona global para acceder a una subred privada. Las zonas con etiquetas no pueden acceder a esta subred.	"Cómo compartir una única dirección IP con todas las zonas" en la página 62
Asignar una dirección IP a cada zona, donde las zonas comparten la pila de IP.	El sistema tiene más de una dirección IP. En el caso más sencillo, las zonas comparten una interfaz física.	"Cómo agregar una instancia de IP para una zona con etiquetas" en la página 63
Agregar una interfaz `all-zones` a la instancia de IP por zona.	El sistema puede ofrecer a sus zonas con etiquetas servicios con privilegios que están protegidos contra ataques remotos.	"Cómo agregar una instancia de IP para una zona con etiquetas" en la página 63
Asignar una dirección IP a cada zona, donde la pila de IP es exclusiva.	Se asigna una dirección IP a cada zona, incluida la zona global. Se crea una tarjeta de interfaz de red virtual (VNIC) para cada zona con etiquetas.	"Cómo agregar una interfaz de red virtual a una zona con etiquetas" en la página 64
Conectar las zonas con zonas remotas.	Esta tarea configura las interfaces de red de las zonas con etiquetas y la zona global para acceder a sistemas remotos en la misma etiqueta.	"Cómo conectar un sistema Trusted Extensions con otros sistemas Trusted Extensions" en la página 65
Ejecutar un daemon `nscd` independiente por zona.	En un entorno en el que cada subred tiene su propio servidor de nombres, esta tarea configura un daemon `nscd` por zona.	"Cómo configurar un servicio de nombres independiente para cada zona con etiquetas" en la página 65

▼ Cómo compartir una única dirección IP con todas las zonas

Este procedimiento permite a cada zona del sistema utilizar una dirección IP, la dirección IP de la zona global, para acceder a otros hosts o zonas con etiquetas idénticas. Ésta es la configuración predeterminada. Debe completar este procedimiento si ha configurado las interfaces de red de forma diferente y desea restablecer el sistema a la configuración de red predeterminada.

Antes de empezar Debe estar con el rol de usuario `root` en la zona global.

1. **Ejecute el comando `txzonemgr` sin ninguna opción.**

   ```
   # txzonemgr &
   ```

   La lista de zonas se muestra en Labeled Zone Manager. Para obtener información sobre esta interfaz gráfica de usuario, consulte "Cómo crear zonas con etiquetas de forma interactiva" en la página 57.

2. **Haga doble clic en la zona global.**

3. **Haga doble clic en Configure Network Interfaces.**

   Aparece una lista de interfaces. Busque una interfaz en la lista con las siguientes características:

   - Tipo de `phys`
   - Dirección IP de su nombre de host
   - Estado de `up`

4. **Seleccione la interfaz que coincide con su nombre de host.**

5. **De la lista de comandos, seleccione Share with Shared-IP Zones.**

   Todas las zonas pueden utilizar esta dirección IP compartida para la comunicación con sistemas remotos en su etiqueta.

6. **Haga clic en Cancel para volver a la lista de comandos de zonas.**

Pasos siguientes Para configurar la red externa del sistema, vaya a "Cómo conectar un sistema Trusted Extensions con otros sistemas Trusted Extensions" en la página 65.

▼ Cómo agregar una instancia de IP para una zona con etiquetas

Este procedimiento resulta necesario si utiliza una pila de IP compartida y direcciones por zona, y desea conectar las zonas con etiquetas a zonas con etiquetas de otros sistemas de la red.

En este procedimiento, se crea una instancia de IP, es decir, una dirección por zona, para una o varias zonas con etiquetas. Las zonas con etiquetas utilizan su dirección por zona para comunicarse con zonas con etiquetas idénticas en la red.

Antes de empezar

Debe estar con el rol de usuario `root` en la zona global.

La lista de zonas se muestra en Labeled Zone Manager. Para abrir esta interfaz gráfica de usuario, consulte "Cómo crear zonas con etiquetas de forma interactiva" en la página 57. Se debe detener la zona con etiquetas que desea configurar.

1. **En Labeled Zone Manager, haga doble clic en una zona con etiquetas a la que desea agregar una instancia de IP.**
2. **Haga doble clic en Configure Network Interfaces.**

   Aparece una lista de opciones de configuración.
3. **Seleccione Add an IP instance.**
4. **Si el sistema tiene más de una dirección IP, seleccione la entrada con la interfaz deseada.**
5. **Para esta zona con etiquetas, proporcione una dirección IP y un recuento de prefijos.**

   Por ejemplo, escriba `192.168.1.2/24`. Si no anexa el recuento de prefijos, se le solicitará una máscara de red. La máscara de red equivalente para este ejemplo es `255.255.255.0`.
6. **Haga clic en OK.**
7. **Para agregar un enrutador predeterminado, haga doble clic en la entrada que acaba de agregar.**

   Cuando se solicite, escriba la dirección IP del enrutador y haga clic en OK.

   Nota – Para eliminar o modificar el enrutador predeterminado, elimine la entrada y, a continuación, cree la instancia de IP de nuevo.
8. **Haga clic en Cancel para volver a la lista de comandos de zonas.**

Pasos siguientes

Para configurar la red externa del sistema, vaya a "Cómo conectar un sistema Trusted Extensions con otros sistemas Trusted Extensions" en la página 65.

▼ Cómo agregar una interfaz de red virtual a una zona con etiquetas

Este procedimiento resulta necesario si utiliza una pila de IP exclusiva y direcciones por zona, y planea conectar las zonas con etiquetas a zonas con etiquetas de otros sistemas de la red.

En este procedimiento, se crea una VNIC y se la asigna a una zona con etiquetas.

Antes de empezar

Debe estar con el rol de usuario `root` en la zona global.

La lista de zonas se muestra en Labeled Zone Manager. Para abrir esta interfaz gráfica de usuario, consulte "Cómo crear zonas con etiquetas de forma interactiva" en la página 57. Se debe detener la zona con etiquetas que desea configurar.

1. **En Labeled Zone Manager, haga doble clic en la zona con etiquetas a la que desea agregar una interfaz virtual.**

2. **Haga doble clic en Configure Network Interfaces.**

   Aparece una lista de opciones de configuración.

3. **Haga doble clic en Add a virtual interface (VNIC).**

   Si el sistema tiene más de una tarjeta VNIC, se muestra más de una opción. Seleccione la entrada con la interfaz deseada.

4. **Asigne un nombre de host o asigne una dirección IP y un recuento de prefijos.**

   Por ejemplo, escriba `192.168.1.2/24`. Si no anexa el recuento de prefijos, se le solicitará una máscara de red. La máscara de red equivalente para este ejemplo es `255.255.255.0`.

5. **Para agregar un enrutador predeterminado, haga doble clic en la entrada que acaba de agregar.**

   Cuando se solicite, escriba la dirección IP del enrutador y haga clic en OK.

   Nota – Para eliminar o modificar el enrutador predeterminado, elimine la entrada y, a continuación, cree la VNIC de nuevo.

6. **Haga clic en Cancel para volver a la lista de comandos de zonas.**

   Se muestra la entrada de VNIC. El sistema asigna el nombre *nombre_zona_n*, como en `internal_0`.

Pasos siguientes

Para configurar la red externa del sistema, vaya a "Cómo conectar un sistema Trusted Extensions con otros sistemas Trusted Extensions" en la página 65.

▼ Cómo conectar un sistema Trusted Extensions con otros sistemas Trusted Extensions

En este procedimiento, se define la red de Trusted Extensions mediante la adición de hosts remotos a los que el sistema Trusted Extensions se puede conectar.

Antes de empezar Aparece Labeled Zone Manager. Para abrir esta interfaz gráfica de usuario, consulte "Cómo crear zonas con etiquetas de forma interactiva" en la página 57. Debe estar con el rol de usuario `root` en la zona global.

1. **En Labeled Zone Manager, haga doble clic en la zona global.**
2. **Seleccione Add Multilevel Access to Remote Host.**
   a. **Escriba la dirección IP de otro sistema Trusted Extensions.**
   b. **Ejecute los comandos correspondientes en el otro sistema Trusted Extensions.**
3. **Haga clic en Cancel para volver a la lista de comandos de zonas.**
4. **En Labeled Zone Manager, haga doble clic en una zona con etiquetas.**
5. **Seleccione Add Access to Remote Host.**
   a. **Escriba la dirección IP de la zona con etiquetas idénticas en otro sistema Trusted Extensions.**
   b. **Ejecute los comandos correspondientes en la zona del otro a sistema Trusted Extensions.**

Véase también
- Capítulo 15, "Redes de confianza (descripción general)"
- "Etiquetado de hosts y redes (mapa de tareas)" en la página 216

▼ Cómo configurar un servicio de nombres independiente para cada zona con etiquetas

Este procedimiento permite configurar por separado un daemon de servicio de nombres (`nscd`) en cada zona con etiquetas. Esta configuración no cumple con los criterios de una configuración evaluada. En una configuración evaluada, el daemon `nscd` sólo se ejecuta en la zona global. Las puertas de cada zona con etiquetas conectan la zona al daemon `nscd` global.

Esta configuración admite entornos donde cada zona está conectada a una subred que se ejecuta en la etiqueta de la zona y la subred tiene su propio servidor de nombres para esa etiqueta.

Nota – Para utilizar esta configuración, es necesario tener conocimientos avanzados sobre redes.

Antes de empezar Aparece Labeled Zone Manager. Para abrir esta interfaz gráfica de usuario, consulte "Cómo crear zonas con etiquetas de forma interactiva" en la página 57. Debe estar con el rol de usuario `root` en la zona global.

1 En Labeled Zone Manager, seleccione Configure per-zone name service y haga clic en OK.

Nota – Esta opción está diseñada que ser utilizada una vez, durante configuración inicial del sistema.

2 Configure el servicio `nscd` de cada zona.

Para obtener ayuda, consulte la página del comando man `nscd(1M)`.

3 Reinicie el sistema.

```
# /usr/sbin/reboot
```

4 Para cada zona, verifique la ruta y el daemon de servicio de nombres.

a. En la consola de zona, muestre el servicio `nscd`.

```
zone-name # svcs -x name-service/cache
svc:/system/name-service/cache:default (name service cache)
 State: online since September 10, 2011  10:10:11 AM PDT
   See: nscd(1M)
   See: /var/svc/log/system-name-service-cache:default.log
Impact: None.
```

b. Verifique la ruta a la subred.

```
zone-name # netstat -rn
```

Ejemplo 4–3 Eliminación de una antememoria de servicio de nombres en cada zona con etiquetas

Después de probar un daemon de servicio de nombres por zona, el administrador del sistema decide eliminar los daemons de servicio de nombres de las zonas con etiquetas y ejecutar el daemon sólo en la zona global. Para restablecer el sistema a la configuración predeterminada del servicio de nombres, el administrador abre la interfaz gráfica de usuario `txzonemgr`, selecciona la zona global y, a continuación, selecciona `Unconfigure per-zone name service` y `OK`. Esta selección elimina el daemon `nscd` de cada zona con etiquetas. A continuación, el administrador reinicia el sistema.

Pasos siguientes Al configurar las cuentas de usuario y de rol para cada zona, cuenta con tres opciones.

- Puede crear cuentas LDAP en un servidor de directorios LDAP de varios niveles.
- Puede crear cuentas LDAP en servidores de directorios LDAP separados (un servidor por etiqueta).
- Puede crear cuentas locales.

La configuración por separado de un daemon de servicio de nombres en cada zona con etiquetas tiene consecuencias en las contraseñas para todos los usuarios. Los usuarios deben autenticarse para obtener acceso a cualquiera de sus zonas con etiquetas, incluida la zona que corresponde a su etiqueta predeterminada. Además, el administrador debe crear cuentas de manera local en cada zona, o bien las cuentas deben existir en un directorio LDAP en donde la zona es un cliente LDAP.

En el caso especial en que una cuenta de la zona global ejecuta Labeled Zone Manager, `txzonemgr`, la información de la cuenta se copia en las zonas con etiquetas para que al menos esa cuenta pueda iniciar sesión en cada zona. De manera predeterminada, esta cuenta es la cuenta de usuario inicial.

Creación de roles y usuarios en Trusted Extensions

La creación de roles en Trusted Extensions es idéntica a la creación de roles en Oracle Solaris. No obstante, para una configuración evaluada, se requiere un rol de administrador de la seguridad.

Tarea	Descripción	Para obtener instrucciones
Crear un rol de administrador de la seguridad.	Se crea un rol para gestionar las tareas relacionadas con la seguridad.	"Cómo crear el rol de administrador de la seguridad en Trusted Extensions" en la página 68
Crear un rol de administrador del sistema.	Se crea un rol para gestionar las tareas de administración del sistema que no están relacionadas con la seguridad.	"Cómo crear un rol de administrador del sistema" en la página 69
Crear usuarios para que asuman roles administrativos.	Se crean uno o varios usuarios que pueden asumir roles.	"Cómo crear usuarios que puedan asumir roles en Trusted Extensions" en la página 70
Verificar que los roles puedan realizar sus tareas.	Se prueban los roles.	"Cómo verificar que los roles de Trusted Extensions funcionan" en la página 72
Permitir que los usuarios inicien sesión en una zona con etiquetas.	Se inicia el servicio `zones` para que los usuarios comunes puedan iniciar sesión.	"Cómo permitir que los usuarios inicien sesión en una zona con etiquetas" en la página 73

▼ Cómo crear el rol de administrador de la seguridad en Trusted Extensions

Antes de empezar Tiene el rol de usuario `root` en la zona global.

1 Para crear el rol, utilice el comando `roleadd`.

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

Utilice la siguiente información como guía:

- Nombre del rol: `secadmin`
- `-c` Local Security Officer

  No proporcione información de propiedad exclusiva.
- `-m` *directorio principal*
- `-u` *UID de rol*
- `-S` *depósito*
- `-K` *clave=valor*

  Asigne los perfiles de derechos de seguridad de la información y seguridad de usuarios.

Nota – Para todos los roles administrativos, utilice las etiquetas administrativas para el rango de etiquetas, audite los usos del comando `pfexec`, defina `lock_after_retries=no` y no establezca fechas de caducidad para las contraseñas.

```
# roleadd -c "Local Security Officer" -m \
-u 110 -K profiles="Information Security,User Security" -S files \
-K lock_after_retries=no \
-K min_label=ADMIN_LOW -K clearance=ADMIN_HIGH secadmin
```

2 Proporcione una contraseña inicial para el rol.

```
# passwd -r files secadmin
New Password:            <Type password>
Re-enter new Password:     <Retype password>
passwd: password successfully changed for secadmin
#
```

Asigne una contraseña de seis caracteres alfanuméricos como mínimo. Al igual que todas las contraseñas, la contraseña del rol de administrador de la seguridad debe ser difícil de adivinar, a fin de reducir la posibilidad de que un adversario obtenga acceso no autorizado al intentar adivinar la contraseña.

3 Utilice el rol de administrador de la seguridad como guía al crear otros roles.

Entre los posibles roles se incluyen los siguientes:

- Rol de administrador: perfil de derechos `System Administrator`
- Rol de operador: perfil de derechos `Operator`

Ejemplo 4–4 Creación del rol de administrador de la seguridad en LDAP

Después de configurar el primer sistema con un rol de administrador de la seguridad local, el administrador crea el rol de administrador de la seguridad en el depósito LDAP. En este caso, el rol de administrador de la seguridad definido en LDAP puede administrar los clientes LDAP.

```
# roleadd -c "Site Security Officer" -d server1:/rpool/pool1/BayArea/secadmin
-u 111 -K profiles="Information Security,User Security" -S ldap \
-K lock_after_retries=no -K audit_flags=lo,ex:no \
-K min_label=ADMIN_LOW -K clearance=ADMIN_HIGH secadmin
```

El administrador proporciona una contraseña inicial para el rol.

```
# passwd -r ldap secadmin
New Password:            <Type password>
Re-enter new Password:     <Retype password>
passwd: password successfully changed for secadmin
#
```

Pasos siguientes Para asignar el rol local a un usuario local, consulte "Cómo crear usuarios que puedan asumir roles en Trusted Extensions" en la página 70.

▼ Cómo crear un rol de administrador del sistema

Antes de empezar Tiene el rol de usuario `root` en la zona global.

1 Asigne el perfil de derechos de administrador del sistema al rol.

```
# roleadd -c "Local System Administrator" -m -u 111  -K audit_flags=lo,ex:no\
-K profiles="System Administrator" -K lock_after_retries=no \
-K min_label=ADMIN_LOW -K clearance=ADMIN_HIGH sysadmin
```

2 Proporcione una contraseña inicial para el rol.

```
# passwd -r files sysadmin
New Password:            <Type password>
Re-enter new Password:     <Retype password>
passwd: password successfully changed for sysadmin
#
```

▼ Cómo crear usuarios que puedan asumir roles en Trusted Extensions

Si la política de seguridad del sitio lo permite, puede elegir crear un usuario que pueda asumir más de un rol administrativo.

Para una creación segura de los usuarios, el rol de administrador del sistema crea el usuario y asigna la contraseña inicial, y el rol de administrador de la seguridad asigna los atributos relacionados con la seguridad, por ejemplo, un rol.

Antes de empezar Debe estar con el rol de usuario `root` en la zona global. O bien, si se aplica la separación de tareas, los usuarios que pueden asumir los roles de administrador de la seguridad y administrador del sistema deben estar presentes para asumir sus roles y llevar a cabo los pasos apropiados en este procedimiento.

1 Cree un usuario.

El rol de usuario `root` o el rol de administrador del sistema realizan este paso.

No incluya información de propiedad exclusiva en el comentario.

```
# useradd -c "Second User" -u 1201 -d /home/jdoe jdoe
```

2 Después de crear el usuario, modifique los atributos de seguridad del usuario.

El rol de usuario `root` o el rol de administrador de la seguridad realizan este paso.

Nota – Para los usuarios que pueden asumir roles, desactive el bloqueo de cuentas y no establezca fechas de caducidad para las contraseñas. Además, audite los usos del comando `pfexec`.

```
# usermod -K lock_after_retries=no -K idletime=5 -K idlecmd=lock \
-K audit_flags=lo,ex:no jdoe
```

Nota – Los valores de `idletime` e `idlecmd` siguen vigentes cuando el usuario asume un rol. Para obtener más información, consulte "Valores predeterminados del archivo `policy.conf` en Trusted Extensions" en la página 138.

---

3 Asigne una contraseña de seis caracteres alfanuméricos como mínimo.

```
# passwd jdoe
New Password:       Type password
Re-enter new Password:      Retype password
```

Nota – Cuando el equipo de configuración inicial elige una contraseña, debe seleccionar una contraseña que sea difícil de adivinar. De esta manera, se reduce la posibilidad de que un adversario obtenga acceso no autorizado al intentar adivinar las contraseñas.

4 **Asigne un rol al usuario.**

El rol de usuario `root` o el rol de administrador de la seguridad realizan este paso.

```
# usermod -R oper jdoe
```

5 **Personalice el entorno del usuario.**

a. **Asigne autorizaciones convenientes.**

Después de comprobar la política de seguridad del sitio, es posible que desee otorgar a los primeros usuarios el perfil de derechos de autorizaciones convenientes. Con este perfil, los usuarios pueden asignar dispositivos, imprimir archivos PostScript, imprimir sin etiquetas, iniciar sesión de manera remota y apagar el sistema. Para crear el perfil, consulte "Cómo crear perfiles de derechos para autorizaciones convenientes" en la página 151.

b. **Personalice los archivos de inicialización de usuario.**

Consulte "Personalización del entorno de usuario para la seguridad (mapa de tareas)" en la página 143.

c. **Cree archivos de copia y enlace de varios niveles.**

En un sistema de varios niveles, los usuarios y los roles se pueden configurar mediante archivos que contienen los archivos de inicialización de usuario que se copiarán o enlazarán a otras etiquetas. Para obtener más información, consulte "Archivos `.copy_files` y `.link_files`" en la página 141.

Ejemplo 4–5 Uso del comando useradd para crear un usuario local

En este ejemplo, el rol de usuario `root` crea un usuario local que puede asumir el rol de administrador de la seguridad. Para obtener detalles, consulte las páginas del comando man `useradd`(1M) y `atohexlabel`(1M).

Este usuario tendrá un rango de etiquetas más amplio que el rango de etiquetas predeterminado. Entonces, el rol de usuario `root` determina el formato hexadecimal de la etiqueta mínima y la etiqueta de acreditación del usuario.

```
# atohexlabel public
0x0002-08-08
# atohexlabel -c "confidential restricted"
0x0004-08-78
```

Luego, el rol de usuario `root` consulta la Tabla 1–2 y crea el usuario. El administrador coloca el directorio principal del usuario en `/export/home1` en lugar del directorio predeterminado `/export/home`.

```
# useradd -c "Local user for Security Admin" -d /export/home1/jandoe \
-K  idletime=10 -K idlecmd=logout -K lock_after_retries=no
-K min_label=0x0002-08-08 -K clearance=0x0004-08-78 jandoe
```

A continuación, el rol de usuario `root` proporciona una contraseña inicial.

```
# passwd -r files jandoe
New Password:         <Type password>
Re-enter new Password:      <Retype password>
passwd: password successfully changed for jandoe
#
```

Por último, el rol de usuario `root` agrega el rol de administrador de la seguridad a la definición del usuario. El rol se creó en la sección "Cómo crear el rol de administrador de la seguridad en Trusted Extensions" en la página 68.

```
# usermod -R secadmin jandoe
```

▼ Cómo verificar que los roles de Trusted Extensions funcionan

Para verificar cada rol, asuma el rol. A continuación, realice tareas que sólo ese rol puede llevar a cabo e intente efectuar tareas para las que el rol no tiene autorización.

Antes de empezar Si ha configurado DNS o rutas, debe reiniciar después de haber creado los roles y antes de verificar que los roles funcionen.

1. **Para cada rol, inicie sesión como un usuario que pueda asumir el rol.**
2. **Asuma el rol.**

   En la siguiente banda de confianza, el nombre de usuario es `tester`.

   a. **Haga clic en su nombre de usuario, en la banda de confianza.**

   b. **De la lista de roles asignados, seleccione un rol.**

3. **Pruebe el rol.**

   Para las autorizaciones que son necesarias para cambiar las propiedades de usuario, consulte la página del comando man `passwd(1)`.

- El rol de administrador del sistema debe ser capaz de crear un usuario y modificar las propiedades de usuario que requieren la autorización `solaris.user.manage`, como el shell de inicio de sesión del usuario. El rol de administrador del sistema no debe tener permiso para cambiar las propiedades de usuario que requieren la autorización `solaris.account.setpolicy`.
- El rol de administrador de la seguridad debe ser capaz de cambiar las propiedades de usuario que requieren la autorización `solaris.account.setpolicy`. El administrador de la seguridad no debe tener permiso para crear un usuario o cambiar el shell de inicio de sesión de un usuario.

▼ Cómo permitir que los usuarios inicien sesión en una zona con etiquetas

Cuando se reinicia el sistema, la asociación entre los dispositivos y el almacenamiento subyacente se debe volver a establecer.

Antes de empezar Debe haber creado al menos una zona con etiquetas. Reinicie el sistema después de configurarlo. Puede asumir el rol de usuario `root`.

1. **Inicie sesión y asuma el rol de usuario `root`.**
2. **Compruebe el estado del servicio de zonas.**

```
# svcs zones
STATE          STIME    FMRI
offline        -        svc:/system/zones:default
```

3. **Reinicie el servicio.**

```
# svcadm restart svc:/system/zones:default
```

4. **Cierre la sesión.**

   Ahora los usuarios comunes pueden iniciar sesión. Su sesión está en una zona con etiquetas.

Creación de directorios principales centralizados en Trusted Extensions

En Trusted Extensions, los usuarios necesitan tener acceso a sus directorios principales en cada etiqueta en la que trabajan. De manera predeterminada, los directorios principales se crean automáticamente mediante el montador automático que se ejecuta en cada zona. Sin embargo, si utiliza un servidor NFS para centralizar los directorios principales, debe habilitar el acceso a directorios principales en cada etiqueta para los usuarios.

▼ Cómo crear el servidor de directorio principal en Trusted Extensions

Antes de empezar Tiene el rol de usuario `root` en la zona global.

1. **Agregue el software Trusted Extensions al servidor de directorio principal y configure sus zonas con etiquetas.**
   - Debido a que los usuarios necesitan un directorio principal en cada etiqueta en las que pueden iniciar sesión, cree un servidor de directorio principal en cada etiqueta de usuario. Por ejemplo, si crea una configuración predeterminada, debe crear un servidor de directorio principal para la etiqueta `PUBLIC` y un servidor para la etiqueta `INTERNAL`.
2. **Para cada zona con etiquetas, siga el procedimiento de montaje automático detallado en "Cómo montar archivos en NFS en una zona con etiquetas" en la página 191. A continuación, regrese a este procedimiento.**
3. **Verifique que se hayan creado los directorios principales.**
   a. **Cierre la sesión del servidor de directorio principal.**
   b. **Como usuario común, inicie sesión en el servidor de directorio principal.**
   c. **En la zona de inicio de sesión, abra un terminal.**
   d. **En la ventana de terminal, verifique que el directorio principal del usuario exista.**
   e. **Cree espacios de trabajo para cada zona en la que el usuario puede trabajar.**
   f. **En cada zona, abra una ventana de terminal para verificar que el directorio principal del usuario exista.**
4. **Cierre la sesión del servidor de directorio principal.**

▼ Cómo permitir que los usuarios accedan a sus directorios principales remotos en cada etiqueta mediante el inicio de sesión en cada servidor NFS

En este procedimiento, se permite a los usuarios crear un directorio principal en cada etiqueta. Para ello, se les permite iniciar sesión directamente en cada servidor de directorio principal. Después de crear cada directorio principal en el servidor central, los usuarios pueden acceder a sus directorios principales desde cualquier sistema.

Como alternativa, usted, como administrador, puede crear un punto de montaje en cada servidor de directorio principal mediante la ejecución de una secuencia de comandos y la posterior modificación del montador automático. Para obtener detalles sobre este método, consulte "Cómo permitir que los usuarios accedan a sus directorios principales remotos mediante la configuración del montador automático en cada servidor" en la página 75.

Antes de empezar Los servidores de directorio principal para su dominio de Trusted Extensions deben estar configurados.

- **Permita a los usuarios iniciar sesión directamente en el servidor de directorio principal.**

  Normalmente, se ha creado un servidor NFS por etiqueta.

  a. **Indique a los usuarios que inicien sesión en cada servidor NFS en la etiqueta del servidor.**

  b. **Una vez que el inicio de sesión finaliza correctamente, indique al usuario que se desconecte del servidor.**

     Hay un directorio principal para el usuario disponible en la etiqueta del servidor cuando el inicio de sesión es correcto.

  c. **Indique a los usuarios que inicien sesión desde su estación de trabajo habitual.**

     El directorio principal para su etiqueta predeterminada está disponible en el servidor de directorio principal. Cuando un usuario cambia la etiqueta de una sesión o agrega un espacio de trabajo en una etiqueta diferente, el directorio principal del usuario para esa etiqueta se monta.

Pasos siguientes Los usuarios pueden iniciar sesión en una etiqueta diferente de su etiqueta predeterminada. Para ello, deben seleccionar una etiqueta diferente en el generador de etiquetas durante el inicio de sesión.

▼ Cómo permitir que los usuarios accedan a sus directorios principales remotos mediante la configuración del montador automático en cada servidor

En este procedimiento, se ejecuta una secuencia de comandos que crea un punto de montaje para los directorios principales en cada servidor NFS. A continuación, se modifica la entrada `auto_home` en la etiqueta del servidor para agregar el punto de montaje. Luego, los usuarios pueden iniciar sesión.

Antes de empezar Los servidores de directorio principal para su dominio de Trusted Extensions deben estar configurados como clientes LDAP. Las cuentas de usuario se crearon en el servidor LDAP mediante el comando `useradd` con la opción `-S ldap`. Debe estar con el rol de usuario `root`.

1 **Escriba una secuencia de comandos que cree un punto de montaje de directorio principal para cada usuario.**

La secuencia de comandos de ejemplo parte de los siguientes supuestos:

- El servidor LDAP es un servidor diferente del servidor de directorio principal NFS.
- Los sistemas cliente también son sistemas diferentes.
- La entrada `hostname` especifica la dirección IP externa de la zona, es decir, el servidor de directorio principal NFS para su etiqueta.
- La secuencia de comandos se ejecutará en el servidor NFS, en la zona que presta servicios a clientes en esa etiqueta.

```
#!/bin/sh
hostname=$(hostname)
scope=ldap

for j in $(getent passwd|tr ' ' _); do
    uid=$(echo $j|cut -d: -f3)
    if [ $uid -ge 100 ]; then
        home=$(echo $j|cut -d: -f6)
        if [[ $home == /home/* ]]; then
            user=$(echo $j|cut -d: -f1)
            echo Updating home directory for $user
            homedir=/export/home/$user
            usermod -md ${hostname}:$homedir -S $scope $user
            mp=$(mount -p|grep  " $homedir zfs" )
            dataset=$(echo $mp|cut -d" " -f1)
            if [[ -n $dataset ]]; then
                zfs set sharenfs=on $dataset
            fi
        fi
    fi
done
```

2 **En cada servidor NFS, ejecute la secuencia de comandos anterior en la zona con etiquetas que presta servicios a clientes en esa etiqueta.**

Resolución de los problemas de configuración de Trusted Extensions

Un escritorio con una configuración incorrecta puede impedir el uso del sistema.

▼ Cómo mover los paneles de escritorio a la parte inferior de la pantalla

Nota – La posición predeterminada para los paneles de escritorio es la parte superior de la pantalla. Sin embargo, en Trusted Extensions, la banda de confianza abarca la parte superior de la pantalla. Por lo tanto, los paneles debe estar en la parte lateral o inferior del espacio de trabajo. Un espacio de trabajo predeterminado tiene dos paneles de escritorio.

Antes de empezar Debe estar con el rol de usuario `root` para cambiar la ubicación de los paneles de escritorio del sistema.

1 Si hay un panel de escritorio visible en la parte inferior de la pantalla, realice una de las siguientes acciones:

- **Utilice el botón derecho del mouse para agregar applets al panel visible.**
- **Mueva el segundo panel de escritorio oculto a la parte inferior de la pantalla mediante el siguiente paso.**

2 De lo contrario, cree un panel de escritorio inferior para su inicio de sesión solamente o para todos los usuarios del sistema.

- **Si desea mover los paneles para su inicio de sesión solamente, edite el archivo `top_panel_screen`*n* en el directorio principal.**

  a. Cambie al directorio que contiene el archivo que define la ubicación de los paneles.

  ```
  % cd $HOME/.gconf/apps/panel/toplevels
  % ls
  %gconf.xml    bottom_panel_screen0/   top_panel_screen0/
  % cd top_panel_screen0
  % ls
  %gconf.xml             top_panel_screen0/
  ```

  b. Edite el archivo `%gconf.xml`, que define la ubicación de los paneles superiores.

  ```
  % vi %gconf.xml
  ```

  c. Busque todas las líneas de orientación y reemplace la cadena `top` con `bottom`.

  Por ejemplo, la línea de orientación podría ser similar a la siguiente:

  ```
  /toplevels/orientation" type="string">
                  <stringvalue>bottom</stringvalue>
  ```

- **Si desea mover los paneles para todos los usuarios del sistema, modifique la configuración del escritorio.**

  En una ventana de terminal con el rol de usuario `root`, ejecute los siguientes comandos:

  ```
  # export SETUPPANEL="/etc/gconf/schemas/panel-default-setup.entries"
  # export TMPPANEL="/tmp/panel-default-setup.entries"
  # sed 's/<string>top<\/string>/<string>bottom<\/string>/' $SETUPPANEL > $TMPPANEL
  # cp $TMPPANEL $SETUPPANEL
  # svcadm restart gconf-cache
  ```

3 **Cierre la sesión del sistema y vuelva a iniciar sesión.**

Si tiene más de un panel de escritorio, los paneles se apilan en la parte inferior de la pantalla.

Tareas adicionales de configuración de Trusted Extensions

Las dos tareas siguientes permiten transferir copias exactas de los archivos de configuración a todos los sistemas Trusted Extensions del sitio. La tarea final permite eliminar las personalizaciones de Trusted Extensions de un sistema Oracle Solaris.

▼ Cómo copiar archivos en medios portátiles en Trusted Extensions

Cuando copie a medios portátiles, etiquete los medios con la etiqueta de sensibilidad de la información.

Nota – Durante la configuración de Trusted Extensions, el rol de usuario `root` puede utilizar medios portátiles para transferir los archivos `label_encodings` a todos los sistemas. Etiquete los medios con `Trusted Path`.

Antes de empezar Para copiar archivos administrativos, debe tener el rol de usuario `root` en la zona global.

1 **Asigne el dispositivo adecuado.**

Utilice Device Manager e inserte un medio vacío. Para obtener detalles, consulte "Cómo asignar un dispositivo en Trusted Extensions" de *Guía del usuario de Oracle Solaris Trusted Extensions*.

El explorador de archivos muestra el contenido del medio vacío.

2 **Abra un segundo explorador de archivos.**

3 **Navegue hasta la carpeta que contiene los archivos que se van a copiar.**

4. **Para cada archivo, realice lo siguiente:**

   a. **Resalte el icono para el archivo.**

   b. **Arrastre el archivo hasta el explorador de archivos para el medio portátil.**

5. **Desasigne el dispositivo.**

   Para obtener detalles, consulte "Cómo desasignar un dispositivo en Trusted Extensions" de *Guía del usuario de Oracle Solaris Trusted Extensions*.

6. **En el explorador de archivos para el medio portátil, seleccione Eject en el menú File.**

Nota – Recuerde colocar una etiqueta a los medios con la etiqueta de sensibilidad de los archivos copiados.

Ejemplo 4–6 Mantenimiento de los mismos archivos de configuración en todos los sistemas

El administrador del sistema desea comprobar que todos los sistemas estén configurados con los mismos valores. Por lo tanto, en el primer sistema que se configura, el administrador crea un directorio que no se puede suprimir entre reinicios. En ese directorio, el administrador coloca los archivos, que deben ser idénticos o muy similares en todos los sistemas.

Por ejemplo, el administrador modifica el archivo `policy.conf` y los archivos `login` y `passwd` predeterminados para este sitio. Por lo tanto, el administrador copia los siguientes archivos al directorio permanente.

```
# mkdir /export/commonfiles
# cp  /etc/security/policy.conf \
# cp  /etc/default/login \
# cp  /etc/default/passwd \
# cp  /etc/security/tsol/label_encodings \
/export/commonfiles
```

El administrador utiliza Device Manager para asignar un CD-ROM en la zona global, transfiere los archivos al CD y coloca una etiqueta `Trusted Path`.

▼ Cómo copiar archivos desde medios portátiles en Trusted Extensions

Se recomienda, como una práctica segura, cambiar el nombre del archivo original de Trusted Extensions antes de reemplazarlo. Al configurar un sistema, el rol de usuario `root` copia los archivos administrativos y les cambia el nombre.

Antes de empezar Para copiar archivos administrativos, debe tener el rol de usuario `root` en la zona global.

1. **Asigne el dispositivo adecuado.**

   Para obtener detalles, consulte "Cómo asignar un dispositivo en Trusted Extensions" de *Guía del usuario de Oracle Solaris Trusted Extensions*.

   El explorador de archivos muestra el contenido.

2. **Inserte el medio que contiene los archivos administrativos.**

3. **Si el sistema tiene un archivo con el mismo nombre, copie el archivo original y asígnele un nombre nuevo.**

   Por ejemplo, agregue `.orig` al final del archivo original:

   ```
   # cp /etc/security/tsol/label_encodings /etc/security/tsol/label_encodings.orig
   ```

4. **Abra un explorador de archivos.**

5. **Navegue hasta el directorio de destino deseado, por ejemplo `/etc/security/tsol`.**

6. **Para cada archivo que desee copiar, realice lo siguiente:**

   a. **En el explorador de archivos para los medios montados, resalte el icono del archivo.**

   b. **A continuación, arrastre el archivo hasta el directorio de destino en el segundo explorador de archivos.**

7. **Desasigne el dispositivo.**

   Para obtener detalles, consulte "Cómo desasignar un dispositivo en Trusted Extensions" de *Guía del usuario de Oracle Solaris Trusted Extensions*.

8. **Cuando se solicite, expulse y retire el medio.**

▼ Cómo eliminar Trusted Extensions del sistema

Debe realizar pasos específicos para eliminar la función Trusted Extensions de un sistema Oracle Solaris.

Antes de empezar Tiene el rol de usuario `root` en la zona global.

1. **Archive todos los datos en las zonas con etiquetas que desee conservar.**

   Para los medios portátiles, coloque un adhesivo con la etiqueta de sensibilidad de la zona en cada zona archivada.

2. **Elimine las zonas con etiquetas del sistema.**

   Para obtener detalles, consulte "Cómo eliminar una zona no global" de *Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*.

3. **Deshabilite el servicio de Trusted Extensions.**

   ```
   # svcadm disable labeld
   ```

4. **Deshabilite la asignación de dispositivos.**

   ```
   # svcadm disable allocate
   ```

5. **(Opcional) Reinicie el sistema.**

6. **Configure el sistema.**

   Es posible que se deban configurar varios servicios para el sistema Oracle Solaris. Entre las posibilidades, se incluyen las funciones básicas de redes, los servicios de nombres y los montajes de sistemas de archivos.

◆ ◆ ◆ CAPÍTULO 5

Configuración de LDAP para Trusted Extensions (tareas)

En este capítulo, se describe cómo configurar Oracle Directory Server Enterprise Edition (servidor de directorios) para su uso con Trusted Extensions. El servidor de directorios proporciona los servicios LDAP. LDAP es el servicio de nombres admitido para Trusted Extensions. En la sección final, "Creación de un cliente LDAP de Trusted Extensions" en la página 94, se explica cómo configurar un cliente LDAP.

Al configurar el servidor de directorios, dispone de dos opciones. Puede configurar un servidor LDAP en un sistema Trusted Extensions, o puede utilizar un servidor existente y conectarse a él mediante un servidor proxy Trusted Extensions.

Para configurar el servidor LDAP, siga las instrucciones de *uno* de los siguientes mapas de tareas:

- "Configuración de LDAP en una red de Trusted Extensions (mapa de tareas)" en la página 84
- "Configuración de un servidor proxy LDAP en un sistema Trusted Extensions (mapa de tareas)" en la página 84

Configuración de LDAP en una red de Trusted Extensions (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Configurar un servidor LDAP de Trusted Extensions.	Si no tiene un servidor Oracle Directory Server Enterprise Edition existente, convierta su primer sistema Trusted Extensions en el servidor de directorios. Este sistema no tiene zonas con etiquetas. Los demás sistemas Trusted Extensions son clientes de este servidor.	"Recopilación de información para el servidor de directorios para LDAP" en la página 85 "Instalación de Oracle Directory Server Enterprise Edition" en la página 86 "Configuración de los registros para Oracle Directory Server Enterprise Edition" en la página 89
Agregar bases de datos de Trusted Extensions al servidor.	Rellene el servidor LDAP con datos de los archivos del sistema Trusted Extensions.	"Rellenado de Oracle Directory Server Enterprise Edition" en la página 91
Configurar todos los demás sistemas Trusted Extensions como clientes de este servidor.	Al configurar Trusted Extensions en otro sistema, convierta el sistema en un cliente de este servidor LDAP.	"Conversión de la zona global en un cliente LDAP en Trusted Extensions" en la página 94

Configuración de un servidor proxy LDAP en un sistema Trusted Extensions (mapa de tareas)

Utilice este mapa de tareas si tiene un servidor Oracle Directory Server Enterprise Edition existente que se ejecuta en un sistema Oracle Solaris.

Tarea	Descripción	Para obtener instrucciones
Agregar bases de datos de Trusted Extensions al servidor.	Las bases de datos de red de Trusted Extensions, `tnrhdb` y `tnrhtp`, se deben agregar al servidor LDAP.	"Rellenado de Oracle Directory Server Enterprise Edition" en la página 91
Configurar un servidor proxy LDAP.	Convierta un sistema Trusted Extensions en el servidor proxy de los demás sistemas Trusted Extensions. Los otros sistemas utilizan este servidor proxy para acceder al servidor LDAP.	"Creación de un servidor proxy LDAP" en la página 93
Configurar el servidor proxy para que tenga un puerto de varios niveles para LDAP.	Habilite el servidor proxy de Trusted Extensions para que se pueda comunicar con el servidor LDAP en etiquetas específicas.	"Configuración de puerto de varios niveles para Oracle Directory Server Enterprise Edition" en la página 91

Tarea	Descripción	Para obtener instrucciones
Configurar todos los demás sistemas Trusted Extensions como clientes del servidor proxy LDAP.	Al configurar Trusted Extensions en otro sistema, convierta el sistema en un cliente del servidor proxy LDAP.	"Conversión de la zona global en un cliente LDAP en Trusted Extensions" en la página 94

Configuración de Oracle Directory Server Enterprise Edition en un sistema Trusted Extensions

El servicio de nombres LDAP es el servicio de nombres admitido para Trusted Extensions. Si en su sitio aún no se ejecuta el servicio de nombres LDAP, configure Oracle Directory Server Enterprise Edition (servidor de directorios) en un sistema en el que esté configurado Trusted Extensions.

Si en su sitio ya se está ejecuta un servidor de directorios, debe agregar las bases de datos de Trusted Extensions al servidor. Para acceder al servidor de directorios, debe configurar un proxy LDAP en un sistema Trusted Extensions.

Nota – Si no utiliza este servidor LDAP como servidor NFS, no necesita instalar ninguna zona con etiquetas en este servidor.

▼ Recopilación de información para el servidor de directorios para LDAP

- **Determine los valores para los siguientes elementos.**

  Los elementos se muestran en el orden en el que aparecen en el asistente de instalación de Sun Java Enterprise System.

Petición de datos del asistente de instalación	Acción o información
Oracle Directory Server Enterprise Edition *versión*	
ID de usuario de administrador	El valor predeterminado es `admin`.
Contraseña de administrador	Cree una contraseña, como `admin123`.
DN del gestor de directorios	El valor predeterminado es `cn=Directory Manager`.
Contraseña del gestor de directorios	Cree una contraseña, como `dirmgr89`.

Petición de datos del asistente de instalación	Acción o información
Root de servidor de directorios	El valor predeterminado es `/var/Sun/mps`. Esta ruta también se utiliza posteriormente si se instala el software de proxy.
Identificador del servidor	El valor predeterminado es el sistema local.
Puerto del servidor	Si tiene previsto usar el servidor de directorios para proporcionar servicios de nombres LDAP estándar a sistemas cliente, utilice el valor predeterminado, `389`. Si tiene previsto utilizar el servidor de directorios para admitir una instalación posterior de un servidor proxy, introduzca un puerto no estándar, como `10389`.
Sufijo	Incluya el componente de dominio, como en `dc=example-domain,dc=com`.
Dominio de administración	Cree un dominio que corresponda al sufijo, como en `example-domain.com`.
Usuario del sistema	El valor predeterminado es `root`.
Grupo del sistema	El valor predeterminado es `root`.
Ubicación del almacenamiento de datos	El valor predeterminado es `Store configuration data on this server`.
Ubicación del almacenamiento de datos	El valor predeterminado es `Store user data and group data on this server`.
Puerto de administración	El valor predeterminado es el puerto del servidor. La convención sugerida para cambiar el valor predeterminado es multiplicar *versión_software* por `1000`. Para la versión de software `5.2`, esta convención da como resultado el puerto `5200`.

▼ Instalación de Oracle Directory Server Enterprise Edition

Los paquetes del servidor de directorios están disponibles en el sitio web de Oracle para productos de software de Sun (`http://www.oracle.com/us/sun/sun-products-map-075562.html`).

Antes de empezar

Debe estar en un sistema Trusted Extensions con una zona global. El sistema no debe tener zonas con etiquetas. Debe estar con el rol de usuario `root` en la zona global.

Los servidores LDAP de Trusted Extensions están configurados para los clientes que usan `pam_unix` para autenticarse en el depósito LDAP. Con `pam_unix`, las operaciones de contraseña y, por consiguiente, las directivas de contraseña son determinadas por el cliente. En concreto, la

política establecida por el servidor LDAP no se utiliza. Para conocer los parámetros de contraseña que puede establecer en el cliente, consulte "Gestión de información de contraseñas" de *Administración de Oracle Solaris: servicios de seguridad*. Para obtener información sobre `pam_unix`, consulte la página del comando man `pam.conf(4)`.

Nota – El uso de `pam_ldap` en un cliente LDAP no es una configuración evaluada para Trusted Extensions.

---

1 **Antes de instalar los paquetes del servidor de directorios, agregue el nombre de dominio completo (FQDN) a la entrada del nombre de host del sistema.**

El FQDN es el nombre de dominio completo. Este nombre es una combinación del nombre de host y el dominio de administración, como en el siguiente ejemplo:

```
## /etc/hosts
...
192.168.5.5 myhost myhost.example-domain.com
```

2 **Descargue los paquetes de Oracle Directory Server Enterprise Edition del sitio web de Oracle para productos de software de Sun (`http://www.oracle.com/us/sun/sun-products-map-075562.html`).**

Seleccione el software más reciente adecuado para su plataforma.

3 **Instale los paquetes del servidor de directorios.**

Responda a las preguntas utilizando la información de "Recopilación de información para el servidor de directorios para LDAP" en la página 85. Para obtener una lista completa de las preguntas, los valores predeterminados y las respuestas sugeridas, consulte el Capítulo 11, "Setting Up Oracle Directory Server Enterprise Edition With LDAP Clients (Tasks)" de *Oracle Solaris Administration: Naming and Directory Services* y el Capítulo 12, "Setting Up LDAP Clients (Tasks)" de *Oracle Solaris Administration: Naming and Directory Services*.

4 **(Opcional) Agregue las variables de entorno para el servidor de directorios a la ruta.**

```
# $PATH
/usr/sbin:.../opt/SUNWdsee/dsee6/bin:/opt/SUNWdsee/dscc6/bin:/opt/SUNWdsee/ds6/bin:
/opt/SUNWdsee/dps6/bin
```

5 **(Opcional) Agregue las páginas del comando man del servidor de directorios a su `MANPATH`.**

```
/opt/SUNWdsee/dsee6/man
```

6 **Habilite el programa `cacaoadm` y verifique que el programa esté habilitado.**

```
# /usr/sbin/cacaoadm enable
# /usr/sbin/cacaoadm start
start: server (pid n) already running
```

7 Asegúrese de que el servidor de directorios se inicie en cada inicio.

Las plantillas de los servicios SMF para el servidor de directorios están en los paquetes de Oracle Directory Server Enterprise Edition.

- **Para un servidor de directorios de Trusted Extensions, habilite el servicio.**

```
# dsadm stop /export/home/ds/instances/your-instance
# dsadm enable-service -T SMF /export/home/ds/instances/your-instance
# dsadm start /export/home/ds/instances/your-instance
```

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

- **Para un servidor de directorios proxy, habilite el servicio.**

```
# dpadm stop /export/home/ds/instances/your-instance
# dpadm enable-service -T SMF /export/home/ds/instances/your-instance
# dpadm start /export/home/ds/instances/your-instance
```

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

8 Verifique la instalación.

```
# dsadm info /export/home/ds/instances/your-instance
Instance Path:         /export/home/ds/instances/your-instance
Owner:                 root(root)
Non-secure port:       389
Secure port:           636
Bit format:            32-bit
State:                 Running
Server PID:            298
DSCC url:              -
SMF application name:  ds--export-home-ds-instances-your-instance
Instance version:      D-A00
```

Errores más frecuentes

Para conocer las estrategias para resolver problemas de configuración de LDAP, consulte el Capítulo 13, "LDAP Troubleshooting (Reference)" de *Oracle Solaris Administration: Naming and Directory Services*.

▼ Creación de un cliente LDAP para el servidor de directorios

Puede utilizar este cliente para rellenar su servidor de directorios para LDAP. Debe realizar esta tarea antes rellenar el servidor de directorios.

Puede crear el cliente temporalmente en el servidor de directorios de Trusted Extensions y, a continuación, eliminar el cliente del servidor, o bien puede crear un cliente independiente.

Antes de empezar

Tiene el rol de usuario `root` en la zona global.

1. **Agregue el software Trusted Extensions a un sistema.**

   Puede utilizar el servidor de directorios de Trusted Extensions o agregar Trusted Extensions en un sistema diferente.

2. **En el cliente, configurar LDAP en el servicio `name-service/switch`.**

   a. **Visualice la configuración actual.**

   ```
   # svccfg -s name-service/switch listprop config
   config                        application
   config/value_authorization    astring       solaris.smf.value.name-service.switch
   config/default                astring       "files ldap"
   config/host                   astring       "files dns"
   config/netgroup               astring       ldap
   config/printer                astring       "user files ldap"
   ```

   b. **Cambie el valor predeterminado de la siguiente propiedad:**

   ```
   # svccfg -s name-service/switch setprop config/host = astring: "files ldap dns"
   ```

3. **En la zona global, ejecute el comando `ldapclient init`.**

   En este ejemplo, el cliente LDAP está en el dominio `example-domain.com`. La dirección IP del servidor es `192.168.5.5`.

   ```
   # ldapclient init -a domainName=example-domain.com -a profileName=default \
   > -a proxyDN=cn=proxyagent,ou=profile,dc=example-domain,dc=com \
   > -a proxyDN=cn=proxyPassword={NS1}ecc423aad0 192.168.5.5
   System successfully configured
   ```

4. **Establezca el parámetro `enableShadowUpdate` del servidor en `TRUE`.**

   ```
   # ldapclient -v mod -a enableShadowUpdate=TRUE \
   > -a adminDN=cn=admin,ou=profile,dc=example-domain,dc=com
   System successfully configured
   ```

   Para obtener información sobre el parámetro `enableShadowUpdate`, consulte "enableShadowUpdate Switch" de *Oracle Solaris Administration: Naming and Directory Services* y la página del comando man `ldapclient`(1M).

▼ Configuración de los registros para Oracle Directory Server Enterprise Edition

Mediante este procedimiento se configuran tres tipos de registros: registros de acceso, registros de auditoría y registros de errores. Los siguientes valores predeterminados no se modifican:

- Todos los registros se habilitan y almacenan en la memoria intermedia.
- Los registros se colocan en el directorio `/export/home/ds/instances/`*your-instance*`/logs/`*LOG_TYPE* adecuado.
- Los eventos se registran en el nivel de registro 256.

- Los registros están protegidos por `600` permisos de archivo.
- Los registros de acceso rotan diariamente.
- Los registros de errores rotan semanalmente.

La configuración de este procedimiento cumple con los siguientes requisitos:

- Los registros de auditoría rotan diariamente.
- Los archivos de registro anteriores a 3 meses caducan.
- Todos los archivos de registro utilizan un máximo de 20.000 MB de espacio de disco.
- Se conserva un máximo de 100 archivos de registro, y cada archivo tiene como máximo 500 MB.
- Los registros más antiguos se suprimen si hay menos de 500 MB de espacio libre en el disco.
- Se recopila información adicional en los registros de errores.

Antes de empezar Debe estar con el rol de usuario `root` en la zona global.

1 Configure los registros de acceso.

El *LOG_TYPE* para el acceso es `ACCESS`. La sintaxis para la configuración de registros es la siguiente:

`dsconf set-log-prop` *LOG_TYPE property*:*value*

```
# dsconf set-log-prop ACCESS max-age:3M
# dsconf set-log-prop ACCESS max-disk-space-size:20000M
# dsconf set-log-prop ACCESS max-file-count:100
# dsconf set-log-prop ACCESS max-size:500M
# dsconf set-log-prop ACCESS min-free-disk-space:500M
```

2 Configure los registros de auditoría.

```
# dsconf set-log-prop AUDIT max-age:3M
# dsconf set-log-prop AUDIT max-disk-space-size:20000M
# dsconf set-log-prop AUDIT max-file-count:100
# dsconf set-log-prop AUDIT max-size:500M
# dsconf set-log-prop AUDIT min-free-disk-space:500M
# dsconf set-log-prop AUDIT rotation-interval:1d
```

De manera predeterminada, el intervalo de rotación de registros de auditoría es de una semana.

3 Configure los registros de errores.

En esta configuración, puede especificar los datos adicionales que se van a recopilar en el registro de errores.

```
# dsconf set-log-prop ERROR max-age:3M
# dsconf set-log-prop ERROR max-disk-space-size:20000M
# dsconf set-log-prop ERROR max-file-count:30
# dsconf set-log-prop ERROR max-size:500M
# dsconf set-log-prop ERROR min-free-disk-space:500M
# dsconf set-log-prop ERROR verbose-enabled:on
```

4 **(Opcional) Configure más valores para los registros.**

También puede configurar los siguientes valores de configuración para cada registro:

```
# dsconf set-log-prop LOG_TYPE rotation-min-file-size:undefined
# dsconf set-log-prop LOG_TYPE rotation-time:undefined
```

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

▼ Configuración de puerto de varios niveles para Oracle Directory Server Enterprise Edition

Para trabajar en Trusted Extensions, el puerto de servidor del servidor de directorios debe estar configurado como un puerto de varios niveles (MLP) en la zona global.

Antes de empezar Debe estar con el rol de usuario `root` en la zona global.

1 **Inicie `txzonemgr`.**

```
# /usr/sbin/txzonemgr &
```

2 **Agregue un puerto de varios niveles para el protocolo TCP en la zona global.**

El número de puerto es 389.

3 **Agregue un puerto de varios niveles para el protocolo UDP en la zona global.**

El número de puerto es 389.

▼ Rellenado de Oracle Directory Server Enterprise Edition

Se han creado o modificado varias bases de datos LDAP para contener los datos de Trusted Extensions sobre la configuración de etiquetas, los usuarios y los sistemas remotos. Mediante este procedimiento, se rellenan las bases de datos del servidor de directorios con la información de Trusted Extensions.

Antes de empezar Debe estar con el rol de usuario `root` en la zona global. Se encuentra en un cliente LDAP en el que está habilitada la actualización de shadow. Para conocer los requisitos previos, consulte "Creación de un cliente LDAP para el servidor de directorios" en la página 88.

1 **Cree un área temporal para los archivos que piensa utilizar para rellenar las bases de datos del servicio de nombres.**

```
# mkdir -p /setup/files
```

2 Copie los archivos `/etc` de ejemplo en el área temporal.

```
# cd /etc
# cp aliases group networks netmasks protocols /setup/files
# cp rpc services auto_master /setup/files

# cd /etc/security/tsol
# cp tnrhdb tnrhtp /setup/files
```

Precaución – No copie los archivos `*attr`. En su lugar, utilice la opción `-S ldap` para los comandos que agregan usuarios, roles y perfiles de derechos en el depósito LDAP. Estos comandos agregan entradas para las bases de datos `user_attr`, `auth_attr`, `exec_attr` y `prof_attr`. Para obtener más información, consulte las páginas del comando man `user_attr(4)` y `useradd(1M)`.

3 Elimine la entrada `+auto_master` del archivo `/setup/files/auto_master`.

4 Cree los mapas automáticos de zona en el área temporal.

```
# cp /zone/public/root/etc/auto_home_public /setup/files
# cp /zone/internal/root/etc/auto_home_internal /setup/files
# cp /zone/needtoknow/root/etc/auto_home_needtoknow /setup/files
# cp /zone/restricted/root/etc/auto_home_restricted /setup/files
```

En la siguiente lista de mapas automáticos, el primero de cada par de líneas muestra el nombre del archivo. La segunda línea de cada par muestra el contenido del archivo. Los nombres de zona identifican etiquetas del archivo `label_encodings` predeterminado que se incluye con el software Trusted Extensions.

- Sustituya los nombres de zona por los nombres de zona de estas líneas.
- *myNFSserver* identifica el servidor NFS para los directorios principales.

```
/setup/files/auto_home_public
 * myNFSserver_FQDN:/zone/public/root/export/home/&

/setup/files/auto_home_internal
 * myNFSserver_FQDN:/zone/internal/root/export/home/&

/setup/files/auto_home_needtoknow
 * myNFSserver_FQDN:/zone/needtoknow/root/export/home/&

/setup/files/auto_home_restricted
 * myNFSserver_FQDN:/zone/restricted/root/export/home/&
```

5 Utilice el comando `ldapaddent` para rellenar el servidor de directorios con cada archivo del área temporal.

Por ejemplo, el siguiente comando rellena el servidor del archivo `hosts` del área temporal.

```
# /usr/sbin/ldapaddent -D "cn=directory manager" \
-w dirmgr123 -a simple -f /setup/files/hosts hosts
```

6 **Si ejecutó el comando `ldapclient` en el servidor de directorios Trusted Extensions, deshabilite el cliente en ese sistema.**

En la zona global, ejecute el comando `ldapclient uninit`. Utilice el resultado detallado para verificar que el sistema ya no sea un cliente LDAP.

```
# ldapclient -v uninit
```

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

7 **Para rellenar las bases de datos de red de Trusted Extensions en LDAP, utilice el comando `tncfg` con la opción `-S ldap`.**

Para obtener instrucciones, consulte "Etiquetado de hosts y redes (mapa de tareas)" en la página 216.

Creación de un proxy de Trusted Extensions para un servidor Oracle Directory Server Enterprise Edition existente

En primer lugar, debe agregar las bases de datos de Trusted Extensions al servidor de directorios existente en un sistema Oracle Solaris. En segundo lugar, debe habilitar los sistemas Trusted Extensions para el acceso al servidor de directorios y, a continuación, configurar un sistema Trusted Extensions para que sea el servidor proxy LDAP.

▼ Creación de un servidor proxy LDAP

Si un servidor LDAP ya existe en su sitio, cree un servidor proxy en un sistema Trusted Extensions.

Antes de empezar

Debe haber rellenado el servidor LDAP a partir de un cliente que haya sido modificado para establecer el parámetro `enableShadowUpdate` en `TRUE`. Para conocer los requisitos, consulte "Creación de un cliente LDAP para el servidor de directorios" en la página 88.

Además, debe haber agregado las bases de datos que contengan la información de Trusted Extensions al servidor LDAP desde un cliente en el que el parámetro `enableShadowUpdate` esté establecido en `TRUE`. Para obtener detalles, consulte "Rellenado de Oracle Directory Server Enterprise Edition" en la página 91.

Debe estar con el rol de usuario `root` en la zona global.

1 **Cree un servidor proxy en un sistema en el que esté configurado Trusted Extensions.**

Nota – Debe ejecutar dos comandos `ldapclient`. Después de ejecutar el comando `ldapclient init`, ejecute el comando `ldapclient modify` para establecer el parámetro `enableShadowUpdate` en `TRUE`.

Los siguientes son comandos de ejemplo. El comando `ldapclient init` define los valores de proxy.

```
# ldapclient init \
-a proxyDN=cn=proxyagent,ou=profile,dc=west,dc=example,dc=com \
-a domainName=west.example.com \
-a profileName=pit1 \
-a proxyPassword=test1234 192.168.0.1
System successfully configured
```

El comando `ldapclient mod` habilita la actualización de shadow.

```
# ldapclient mod -a enableShadowUpdate=TRUE \
-a adminDN=cn=admin,ou=profile,dc=west,dc=example,dc=com \
-a adminPassword=admin-password
System successfully configured
```

Para obtener detalles, consulte el Capítulo 12, "Setting Up LDAP Clients (Tasks)" de *Oracle Solaris Administration: Naming and Directory Services*.

2 Verifique que las bases de datos de Trusted Extensions se puedan ver en el servidor proxy.

```
# ldaplist -l database
```

Errores más frecuentes

Para conocer las estrategias para resolver problemas de configuración de LDAP, consulte el Capítulo 13, "LDAP Troubleshooting (Reference)" de *Oracle Solaris Administration: Naming and Directory Services*.

Creación de un cliente LDAP de Trusted Extensions

El siguiente procedimiento crea un cliente LDAP para un servidor de directorios existente de Trusted Extensions.

▼ Conversión de la zona global en un cliente LDAP en Trusted Extensions

Este procedimiento establece la configuración del servicio de nombres LDAP para la zona global en un cliente LDAP.

Utilice la secuencia de comandos `txzonemgr`.

Nota – Si tiene previsto configurar un servidor de nombres en cada zona con etiquetas, debe establecer la conexión entre el cliente LDAP y cada zona con etiquetas.

Antes de empezar

Oracle Directory Server Enterprise Edition, es decir, el servidor de directorios, debe existir. El servidor se debe rellenar con las bases de datos de Trusted Extensions, y este sistema cliente debe poder establecer contacto con el servidor. Por lo tanto, el servidor de directorios debe tener asignada una plantilla de seguridad para este cliente. No se necesita una asignación específica; una asignación comodín es suficiente.

Debe estar con el rol de usuario `root` en la zona global.

1 Si utiliza DNS, agregue `dns` a la configuración `name-service/switch`.

El archivo de cambio de servicio de nombres estándar para LDAP es demasiado restrictivo para Trusted Extensions.

a. Visualice la configuración actual.

```
# svccfg -s name-service/switch listprop config
config                      application
config/value_authorization  astring       solaris.smf.value.name-service.switch
config/default              astring       files ldap
config/netgroup             astring       ldap
config/printer              astring       "user files ldap"
```

b. Agregue `dns` a la propiedad `host` y refresque el servicio.

```
# svccfg -s name-service/switch setprop config/host = astring: "files dns ldap"
# svccfg -s name-service/switch:default refresh
```

c. Verifique la nueva configuración.

```
# svccfg -s name-service/switch listprop config
config                      application
config/value_authorization  astring       solaris.smf.value.name-service.switch
config/default              astring       files ldap
config/host                 astring       files dns ldap
config/netgroup             astring       ldap
config/printer              astring       "user files ldap"
```

Las bases de datos de Trusted Extensions utilizan la configuración predeterminada `files ldap` y, por lo tanto, no se muestran.

2 Para crear un cliente LDAP, ejecute el comando `txzonemgr` sin ninguna opción.

```
# txzonemgr &
```

a. Haga doble clic en la zona global.

b. Seleccione Create LDAP Client.

c. Responda a las siguientes peticiones de datos y haga clic en OK después de cada respuesta:

```
Enter Domain Name:                          Type the domain name
Enter Hostname of LDAP Server:              Type the name of the server
Enter IP Address of LDAP Server servername:     Type the IP address
Enter LDAP Proxy Password:                  Type the password to the server
Confirm LDAP Proxy Password:                Retype the password to the server
Enter LDAP Profile Name:                    Type the profile name
```

d. Confirme o cancele los valores mostrados.

```
Proceed to create LDAP Client?
```

Al confirmar, la secuencia de comandos `txzonemgr` ejecuta el comando `ldapclient init`.

3 Complete la configuración de cliente mediante la habilitación de las actualizaciones de shadow.

```
# ldapclient -v mod -a enableShadowUpdate=TRUE \
> -a adminDN=cn=admin,ou=profile,dc=domain,dc=suffix
System successfully configured
```

4 Verifique que la información del servidor es correcta.

a. Abra una ventana de terminal y consulte el servidor LDAP.

```
# ldapclient list
```

El resultado es similar al siguiente:

```
NS_LDAP_FILE_VERSION= 2.0
NS_LDAP_BINDDN= cn=proxyagent,ou=profile,dc=domain-name
...
NS_LDAP_BIND_TIME= number
```

b. Corrija los errores.

Si se produce un error, vuelva a realizar el Paso 2 al Paso 4. Por ejemplo, el siguiente error puede indicar que el sistema no tiene una entrada en el servidor LDAP:

```
LDAP ERROR (91): Can't connect to the LDAP server.
Failed to find defaultSearchBase for domain domain-name
```

Para corregir este error, debe revisar el servidor LDAP.

PARTE II

Administración de Trusted Extensions

En los capítulos incluidos en esta parte, se describe cómo administrar Trusted Extensions.

Capítulo 6, "Conceptos de la administración de Trusted Extensions": presenta la función Trusted Extensions.

Capítulo 7, "Herramientas de administración de Trusted Extensions": describe los programas administrativos que son específicos de Trusted Extensions.

Capítulo 8, "Requisitos de seguridad del sistema Trusted Extensions (descripción general)": describe los requisitos de seguridad necesarios y configurables en Trusted Extensions.

Capítulo 9, "Realización de tareas comunes en Trusted Extensions (tareas)": presenta la administración de Trusted Extensions.

Capítulo 10, "Usuarios, derechos y roles en Trusted Extensions (descripción general)": presenta el control de acceso basado en roles (RBAC) en Trusted Extensions.

Capítulo 11, "Gestión de usuarios, derechos y roles en Trusted Extensions (tareas)": proporciona instrucciones sobre la gestión de usuarios comunes de Trusted Extensions.

Capítulo 12, "Administración remota en Trusted Extensions (tareas)": proporciona instrucciones sobre la administración remota de Trusted Extensions.

Capítulo 13, "Gestión de zonas en Trusted Extensions (tareas)": proporciona instrucciones sobre la gestión de zonas con etiquetas.

Capítulo 14, “Gestión y montaje de archivos en Trusted Extensions (tareas)”: proporciona instrucciones sobre la gestión del montaje, la realización de copias de seguridad del sistema y otras tareas relacionadas con archivos en Trusted Extensions.

Capítulo 15, “Redes de confianza (descripción general)”: proporciona una descripción general del enrutamiento y las bases de datos de red en Trusted Extensions.

Capítulo 16, “Gestión de redes en Trusted Extensions (tareas)”: proporciona instrucciones sobre la gestión del enrutamiento y las bases de datos de red en Trusted Extensions.

Capítulo 18, “Correo de varios niveles en Trusted Extensions (descripción general)”: describe cuestiones específicas del correo en Trusted Extensions.

Capítulo 19, “Gestión de impresión con etiquetas (tareas)”: proporciona instrucciones sobre la gestión de la impresión en Trusted Extensions.

Capítulo 20, “Dispositivos en Trusted Extensions (descripción general)”: describe las extensiones que Trusted Extensions proporciona para la protección de dispositivos en Oracle Solaris.

Capítulo 21, “Gestión de dispositivos para Trusted Extensions (tareas)”: proporciona instrucciones sobre la gestión de dispositivos mediante Device Manager.

Capítulo 22, “Auditoría de Trusted Extensions (descripción general)”: proporciona información específica de Trusted Extensions sobre la auditoría.

Capítulo 23, “Gestión de software en Trusted Extensions (referencia)”: describe cómo administrar aplicaciones en un sistema Trusted Extensions.

◆ ◆ ◆ CAPÍTULO 6

Conceptos de la administración de Trusted Extensions

Este capítulo brinda una introducción a la administración de sistemas configurados con la función Trusted Extensions.

Trusted Extensions y el SO Oracle Solaris

El software Trusted Extensions agrega etiquetas a un sistema que ejecuta el SO Oracle Solaris. Las etiquetas implementan el *control de acceso obligatorio* (MAC, Mandatory Access Control). El MAC, junto con el control de acceso discrecional (DAC, Discretionary Access Control), protege los sujetos (procesos) y objetos (datos) del sistema. El software Trusted Extensions proporciona interfaces para gestionar la configuración, la asignación y la política de etiquetas.

Similitudes entre Trusted Extensions y el SO Oracle Solaris

El software Trusted Extensions utiliza perfiles de derechos, roles, auditoría, privilegios y otras funciones de seguridad de Oracle Solaris. Puede utilizar las funciones Secure Shell, BART, estructura criptográfica, IPsec y filtro IP con Trusted Extensions. Todas las funciones del sistema de archivos ZFS están disponibles en Trusted Extensions, incluidas las instantáneas y el cifrado.

Diferencias entre Trusted Extensions y el SO Oracle Solaris

El software Trusted Extensions amplía el SO Oracle Solaris. La siguiente lista proporciona una descripción general. Consulte también el Apéndice C, "Referencia rápida a la administración de Trusted Extensions".

- Trusted Extensions controla el acceso a los datos mediante marcas de seguridad especiales que se denominan *etiquetas*. Las etiquetas proporcionan el *control de acceso obligatorio* (MAC). Se brinda la protección de MAC además de los permisos de archivos UNIX o el control de acceso discrecional (DAC). Las etiquetas se asignan directamente a los usuarios, las zonas, los dispositivos, las ventanas y los puntos finales de red. De manera implícita, las etiquetas se asignan a los procesos, los archivos y otros objetos del sistema.

  Los usuarios comunes no pueden invalidar el MAC. Trusted Extensions requiere que los usuarios comunes operen en las zonas con etiquetas. De manera predeterminada, ningún usuario o proceso de las zonas con etiquetas puede invalidar el MAC.

  Como en el SO Oracle Solaris, la capacidad de invalidar la política de seguridad puede asignarse a procesos o usuarios específicos en los casos en que puede invalidarse el MAC. Por ejemplo, los usuarios pueden estar autorizados para cambiar la etiqueta de un archivo. Este tipo de acciones aumentan o disminuyen el nivel de sensibilidad de la información en dicho archivo.
- Trusted Extensions complementa los comandos y los archivos de configuración existentes. Por ejemplo, Trusted Extensions agrega eventos de auditoría, autorizaciones, privilegios y perfiles de derechos.
- Algunas funciones que son opcionales en un sistema Oracle Solaris son obligatorias en un sistema Trusted Extensions. Por ejemplo, las zonas y los roles son necesarios en un sistema que esté configurado con Trusted Extensions.
- Algunas funciones que son opcionales en un sistema Oracle Solaris están habilitadas en un sistema Trusted Extensions. Por ejemplo, muchos sitios que configuran Trusted Extensions exigen la separación de tareas al crear usuarios y asignar atributos de seguridad.
- Trusted Extensions puede cambiar el comportamiento predeterminado de Oracle Solaris. Por ejemplo, en un sistema configurado con Trusted Extensions, la asignación de dispositivo es obligatoria.
- Trusted Extensions puede reducir las opciones que están disponibles en Oracle Solaris. Por ejemplo, en Trusted Extensions, todas las zonas son zonas con etiquetas. A diferencia de Oracle Solaris, las zonas con etiquetas deben utilizar la misma agrupación de ID de usuario e ID de grupo. Asimismo, en Trusted Extensions, las zonas con etiquetas pueden compartir una dirección IP.
- Trusted Extensions ofrece un versión de varios niveles del escritorio Oracle Solaris, Solaris Trusted Extensions (GNOME). El nombre se puede abreviar como Trusted GNOME.

- Trusted Extensions proporciona interfaces gráficas de usuario (GUI) e interfaces de la línea de comandos (CLI) adicionales. Por ejemplo, Trusted Extensions proporciona la interfaz gráfica de usuario Device Manager para administrar dispositivos. Además, el comando `updatehome` se utiliza para colocar los archivos de inicio en los directorios principales de los usuarios en cada etiqueta.
- Trusted Extensions requiere el uso de determinadas interfaces gráficas de usuario para la administración. Por ejemplo, en un sistema configurado con Trusted Extensions, Labeled Zone Manager se utiliza para administrar las zonas con etiquetas, además del comando `zonecfg`.
- Trusted Extensions limita lo que pueden visualizar los usuarios. Por ejemplo, el usuario que no puede asignar un dispositivo tampoco puede visualizarlo.
- Trusted Extensions limita las opciones de escritorio de los usuarios. Por ejemplo, los usuarios disponen de un tiempo limitado de inactividad de la estación de trabajo antes de que se bloquee la pantalla. De manera predeterminada, los usuarios comunes no pueden apagar el sistema.

Sistemas de varios periféricos y escritorio de Trusted Extensions

Cuando los monitores de un sistema de varios periféricos de Trusted Extensions están configurados de forma horizontal, la banda de confianza abarca todos los monitores. Cuando los monitores están configurados de forma vertical, la banda de confianza aparece en el monitor ubicado en el extremo inferior.

Cuando se visualizan diferentes espacios de trabajo en los monitores de un sistema de varios periféricos, Trusted GNOME muestra una banda de confianza en cada monitor.

Conceptos básicos de Trusted Extensions

El software Trusted Extensions agrega etiquetas a un sistema Oracle Solaris. También se agregan espacios de trabajo con etiquetas y aplicaciones de confianza, como Device Manager y el generador de etiquetas. Los conceptos de esta sección son necesarios para que los usuarios y los administradores comprendan Trusted Extensions. En la *Guía del usuario de Oracle Solaris Trusted Extensions*, se presentan estos conceptos para los usuarios.

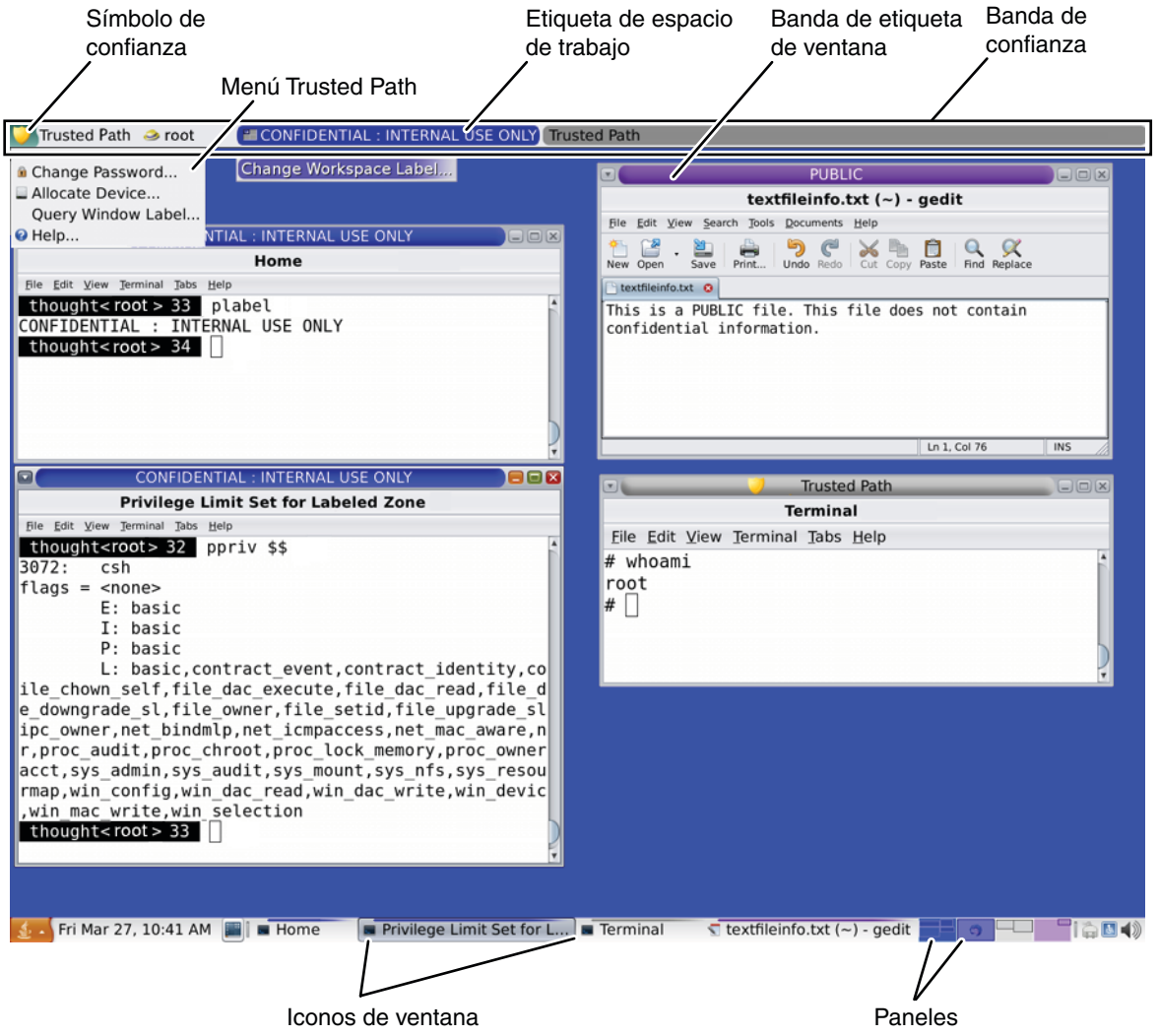
Protecciones de Trusted Extensions

El software Trusted Extensions mejora la protección del SO Oracle Solaris. Oracle Solaris protege el acceso al sistema mediante cuentas de usuario que requieren contraseñas. Se puede exigir que las contraseñas deban cambiarse con regularidad, que tengan una extensión

determinada, etc. Los roles requieren contraseñas adicionales para realizar tareas administrativas, y no se pueden utilizar como cuentas de inicio de sesión. El software Trusted Extensions mejora aún más este aspecto al restringir a los usuarios y los roles a un rango de etiquetas aprobado. Este rango de etiquetas limita la información a la que pueden acceder los usuarios y los roles.

El software Trusted Extensions muestra el símbolo de Trusted Path, un emblema inconfundible y a prueba de falsificaciones que aparece a la izquierda de la banda de confianza. En Trusted GNOME, la banda se muestra en la parte superior de la pantalla. El símbolo de Trusted Path les indica a los usuarios que están utilizando partes del sistema relacionadas con la seguridad. Si este símbolo no aparece cuando el usuario está ejecutando una aplicación de confianza, debe comprobarse inmediatamente la autenticidad de esa versión de la aplicación. Si la banda de confianza no aparece, el escritorio no es de confianza. Para ver un ejemplo de la visualización del escritorio, consulte la Figura 6–1.

FIGURA 6–1 Escritorio de varios niveles de Trusted Extensions



La mayor parte del software relacionado con la seguridad, es decir, la base de computación de confianza (TCB, Trusted Computing Base), se ejecuta en la zona global. Los usuarios comunes no pueden entrar en la zona global ni visualizar sus recursos. Los usuarios pueden interactuar con el software TCB, por ejemplo, al cambiar las contraseñas. El símbolo de Trusted Path se muestra cuando el usuario interactúa con la TCB.

Trusted Extensions y el control de acceso

El software Trusted Extensions protege la información y otros recursos mediante el control de acceso discrecional (DAC) y el control de acceso obligatorio (MAC). El DAC corresponde a las listas de control de acceso y los bits de permiso tradicionales de UNIX que están configurados según el criterio del propietario. El MAC es un mecanismo que el sistema pone en funcionamiento automáticamente. El MAC controla todas las transacciones mediante la comprobación de las etiquetas de los procesos y los datos de la transacción.

La *etiqueta* del usuario representa el nivel de sensibilidad en que el usuario tiene permitido operar y que, a la vez, elige para operar. Las etiquetas típicas son `Secret` o `Public`. La etiqueta determina la información a la que puede acceder el usuario. Tanto MAC como DAC se pueden sustituir mediante permisos especiales que proporciona Oracle Solaris. Los *privilegios* son permisos especiales que pueden otorgarse a los procesos. Las *autorizaciones* son permisos especiales que puede otorgar el administrador a los usuarios y los roles.

Como administrador, debe brindar a los usuarios formación sobre los procedimientos adecuados para proteger los archivos y los directorios, en función de la política de seguridad del sitio. Además, debe indicar a los usuarios que estén autorizados a subir o bajar el nivel de las etiquetas cuál es el momento adecuado para hacerlo.

Etiquetas en el software Trusted Extensions

Las etiquetas y las acreditaciones son fundamentales para el control de acceso obligatorio (MAC) en Trusted Extensions. Determinan qué usuarios pueden acceder a qué programas, archivos y directorios. Las etiquetas y las acreditaciones contienen un componente de *clasificación* y, además, puede que no contengan ningún componente de *compartimiento* o que contengan algunos. El componente de clasificación indica un nivel jerárquico de seguridad, por ejemplo, de `TOP SECRET` a `SECRET` y `PUBLIC`. El componente de compartimiento representa un grupo de usuarios que podrían necesitar acceso a un cuerpo común de información. Algunos de los ejemplos de tipos de compartimientos más comunes son los proyectos, los departamentos o las ubicaciones físicas. Las etiquetas son legibles para los usuarios autorizados, pero internamente se las manipula como números. En el archivo `label_encodings`, se definen los números y las versiones legibles correspondientes.

Trusted Extensions media en todas las transacciones relacionadas con la seguridad que se hayan intentado realizar. El software compara las etiquetas de la entidad de acceso (por lo general, un proceso) y la entidad a la que se accede (normalmente, un objeto del sistema de archivos). Luego, el software permite o no realizar la transacción según qué etiqueta sea *dominante*. Las etiquetas también se utilizan para determinar el acceso a otros recursos del sistema, como dispositivos asignables, redes, búferes de trama y otros sistemas.

Relaciones de dominio entre etiquetas

Se dice que la etiqueta de una entidad *domina* otra etiqueta si se cumplen las dos condiciones siguientes:

- El componente de clasificación de la etiqueta de la primera entidad es mayor o igual que la clasificación de la segunda entidad. El administrador de la seguridad asigna números a las clasificaciones en el archivo `label_encodings`. El software compara estos números para determinar el dominio.
- El conjunto de compartimientos de la primera entidad incluye todos los compartimientos de la segunda entidad.

Se dice que dos etiquetas son *iguales* si tienen la misma clasificación y el mismo conjunto de compartimientos. Si las etiquetas son iguales, se dominan entre sí, y se permite el acceso.

Si una etiqueta tiene una clasificación superior o tiene la misma clasificación y los compartimientos son un superconjunto de los compartimientos de la segunda etiqueta, o si se cumplen ambas condiciones, se dice que la primera etiqueta *domina estrictamente* la segunda etiqueta.

Se dice que dos etiquetas están *separadas* o *no son comparables* si ninguna de ellas domina la otra.

La siguiente tabla presenta algunos ejemplos sobre comparaciones de etiquetas con relación al dominio. En el ejemplo, `NEED_TO_KNOW` es una clasificación superior a `INTERNAL`. Hay tres compartimientos: Eng, Mkt y Fin.

TABLA 6–1 Ejemplos de relaciones de etiquetas

Etiqueta 1	Relación	Etiqueta 2
`NEED_TO_KNOW Eng Mkt`	domina (estrictamente)	`INTERNAL Eng Mkt`
`NEED_TO_KNOW Eng Mkt`	domina (estrictamente)	`NEED_TO_KNOW Eng`
`NEED_TO_KNOW Eng Mkt`	domina (estrictamente)	`INTERNAL Eng`
`NEED_TO_KNOW Eng Mkt`	domina (de igual modo)	`NEED_TO_KNOW Eng Mkt`
`NEED_TO_KNOW Eng Mkt`	está separada de	`NEED_TO_KNOW Eng Fin`
`NEED_TO_KNOW Eng Mkt`	está separada de	`NEED_TO_KNOW Fin`
`NEED_TO_KNOW Eng Mkt`	está separada de	`INTERNAL Eng Mkt Fin`

Etiquetas administrativas

Trusted Extensions proporciona dos etiquetas administrativas especiales que se utilizan como etiquetas o acreditaciones: `ADMIN_HIGH` y `ADMIN_LOW`. Estas etiquetas se utilizan para proteger los recursos del sistema y no están diseñadas para los usuarios comunes, sino para los administradores.

ADMIN_HIGH es la etiqueta máxima. ADMIN_HIGH domina el resto de las etiquetas del sistema y se utiliza para evitar la lectura de los datos del sistema, como las bases de datos de administración o las pistas de auditoría. Debe estar en la zona global para leer los datos con la etiqueta ADMIN_HIGH.

ADMIN_LOW es la etiqueta mínima. ADMIN_LOW está dominada por el resto de las etiquetas de un sistema, incluidas las etiquetas de los usuarios comunes. El control de acceso obligatorio no permite que los usuarios escriban datos en los archivos con etiquetas de un nivel inferior al de la etiqueta del usuario. Por lo tanto, los usuarios comunes pueden leer un archivo con la etiqueta ADMIN_LOW, pero no pueden modificarlo. ADMIN_LOW se utiliza normalmente para proteger los archivos ejecutables que son públicos y están compartidos, como los archivos de /usr/bin.

Archivo de codificaciones de etiqueta

Todos los componentes de etiqueta de un sistema, es decir, las clasificaciones, los compartimientos y las reglas asociadas, se almacenan en un archivo ADMIN_HIGH: el archivo label_encodings. Este archivo se encuentra en el directorio /etc/security/tsol. El administrador de la seguridad configura el archivo label_encodings para el sitio. Un archivo de codificaciones de etiqueta contiene lo siguiente:

- **Definiciones de componente**: son las definiciones de clasificaciones, compartimientos, etiquetas y acreditaciones, incluidas las reglas para las restricciones y las combinaciones necesarias
- **Definiciones de rangos de acreditación**: es la especificación de las acreditaciones y las etiquetas mínimas que definen los conjuntos de etiquetas disponibles para todo el sistema y los usuarios comunes
- **Especificaciones de impresión**: representan la identificación y el tratamiento de la información para imprimir carátulas, ubicadores, encabezados, pies de página y otras funciones de seguridad en el resultado de la impresión
- **Personalizaciones**: son las definiciones locales que incluyen los códigos de color de etiquetas y otros valores predeterminados

Para obtener más información, consulte la página del comando man label_encodings(4). También se puede encontrar información detallada en *Trusted Extensions Label Administration* y *Compartmented Mode Workstation Labeling: Encodings Format* .

Rangos de etiquetas

Un *rango de etiquetas* es el conjunto de etiquetas potencialmente utilizables en que pueden operar los usuarios. Tanto los usuarios como los recursos tienen rangos de etiquetas. Los rangos de etiquetas pueden proteger recursos que incluyen elementos como dispositivos asignables, redes, interfaces, búferes de trama y comandos. Un rango de etiquetas está definido por una acreditación en la parte superior del rango y una etiqueta mínima en la parte inferior.

Un rango no incluye necesariamente todas las combinaciones de etiquetas que se ubican entre una etiqueta máxima y una etiqueta mínima. Las reglas del archivo `label_encodings` pueden descartar determinadas combinaciones. Una etiqueta debe estar *bien formada*, es decir, deben permitirla todas las reglas aplicables del archivo de codificaciones de etiqueta a fin de que pueda incluirse en un rango.

No obstante, no es necesario que una acreditación esté bien formada. Imagine, por ejemplo, que un archivo `label_encodings` prohíbe todas las combinaciones de los compartimientos `Eng`, `Mkt` y `Fin` de una etiqueta. `INTERNAL Eng Mkt Fin` sería una acreditación válida, pero no una etiqueta válida. Como acreditación, esta combinación permitiría al usuario acceder a los archivos con las etiquetas `INTERNAL Eng`, `INTERNAL Mkt` e `INTERNAL Fin`.

Rango de etiquetas de cuenta

Cuando se asigna una acreditación y una etiqueta mínima a un usuario, se definen los límites superiores e inferiores del *rango de etiquetas de cuenta* en que puede operar el usuario. La siguiente ecuación describe el rango de etiquetas de cuenta, utilizando ≤ para indicar "dominada por o igual a":

etiqueta mínima ≤ etiqueta permitida ≤ acreditación

De este modo, el usuario puede operar en cualquier etiqueta que la acreditación domine, siempre que esa etiqueta domine la etiqueta mínima. Cuando no se define expresamente la acreditación o la etiqueta mínima del usuario, se aplican los valores predeterminados que están definidos en el archivo `label_encodings`.

Se pueden asignar una acreditación y una etiqueta mínima a los usuarios que los habiliten a operar en más de una etiqueta o en una sola etiqueta. Cuando la acreditación y la etiqueta mínima del usuario son iguales, el usuario sólo puede operar en una etiqueta.

Rango de sesión

El *rango de sesión* es el conjunto de etiquetas que están disponibles para un usuario durante una sesión de Trusted Extensions. El rango de sesión deberá estar dentro del rango de etiquetas de cuenta del usuario y el conjunto de rangos de etiquetas del sistema. En el inicio de sesión, si el usuario selecciona el modo de sesión de una sola etiqueta, el rango de sesión se limita a esa etiqueta. Si el usuario selecciona el modo de sesión de varias etiquetas, la etiqueta que el usuario selecciona se convierte en la acreditación de sesión. La acreditación de sesión define el límite superior del rango de sesión. La etiqueta mínima del usuario define el límite inferior. El usuario inicia la sesión en un espacio de trabajo ubicado en la etiqueta mínima. Durante la sesión, el usuario puede cambiar a un espacio de trabajo que se encuentre en cualquier etiqueta dentro del rango de sesión.

Qué protegen las etiquetas y dónde aparecen

Las etiquetas aparecen en el escritorio y en el resultado que se ejecuta en el escritorio, como el resultado de la impresión.

- **Aplicaciones**: son las aplicaciones que inician los procesos. Dichos procesos se ejecutan en la etiqueta del espacio de trabajo en que se inicia la aplicación. Una aplicación de una zona con etiquetas, como un archivo, se etiqueta en la etiqueta de la zona.
- **Dispositivos**: la asignación de dispositivos y los rangos de etiquetas de dispositivos se utilizan para controlar los datos que se transfieren entre dispositivos. Para utilizar un dispositivo, los usuarios deben ubicarse dentro del rango de etiquetas del dispositivo y estar autorizados para asignar el dispositivo.
- **Puntos de montaje del sistema de archivos**: cada punto de montaje tiene una etiqueta. Se puede visualizar la etiqueta con el comando `getlabel`.
- **IPsec e IKE**: las asociaciones de seguridad IPsec y las reglas IKE tienen etiquetas.
- **Interfaces de red**: las direcciones IP (hosts) tienen asignadas plantillas de seguridad que describen sus rangos de etiquetas. El sistema Trusted Extensions implicado en la comunicación asigna también una etiqueta predeterminada a los hosts sin etiquetas.
- **Impresoras e impresión**: las impresoras tienen rangos de etiquetas. Las etiquetas se imprimen en las páginas del cuerpo. Las etiquetas, el tratamiento de la información y otros datos de seguridad se imprimen en las páginas de la carátula y del ubicador. Para configurar la impresión en Trusted Extensions, consulte el Capítulo 19, "Gestión de impresión con etiquetas (tareas)" y "Labels on Printed Output" de *Trusted Extensions Label Administration*.
- **Procesos**: los procesos tienen etiquetas. Los procesos se ejecutan en la etiqueta del espacio de trabajo en que se origina cada proceso. Se puede visualizar la etiqueta de un proceso con el comando `plabel`.
- **Usuarios**: se les asignan una etiqueta predeterminada y un rango de etiquetas. La etiqueta del espacio de trabajo del usuario señala la etiqueta de los procesos del usuario.
- **Ventanas**: se pueden visualizar las etiquetas en la parte superior de las ventanas del escritorio. La etiqueta del escritorio también se señala por color. El color aparece en el panel del espacio de trabajo y arriba de las barras de título de las ventanas, como se muestra en la Figura 6–1.

  Cuando se mueve una ventana a un escritorio de trabajo con etiquetas diferentes, la ventana conserva la etiqueta original. Los procesos que se inician en la ventana se ejecutan en la etiqueta original.
- **Zonas**: cada zona tiene una sola etiqueta. Los archivos y los directorios que son propiedad de una zona se encuentran en la etiqueta de la zona. Para obtener más información, consulte la página del comando man `getzonepath(1)`.

Roles y Trusted Extensions

En un sistema que ejecuta el software Oracle Solaris sin Trusted Extensions, los roles son opcionales. En un sistema que está configurado con Trusted Extensions, los roles son

necesarios. Los roles de administrador del sistema y de administrador de la seguridad administran el sistema. En algunos casos, se utiliza el rol `root`.

Los programas que están disponibles para un rol en Trusted Extensions tienen una propiedad especial: el *atributo de la ruta de confianza*. Este atributo indica que el programa es parte de la TCB. El atributo de la ruta de confianza está disponible cuando un programa se inicia desde la zona global.

Como en Oracle Solaris, los perfiles de derechos representan la base de las capacidades de un rol. Para obtener información acerca de los derechos los perfiles y los roles, consulte el Capítulo 8, "Uso de roles y privilegios (descripción general)" de *Administración de Oracle Solaris: servicios de seguridad*.

◆ ◆ ◆ CAPÍTULO 7

Herramientas de administración de Trusted Extensions

En este capítulo, se describen las herramientas que están disponibles en Trusted Extensions, la ubicación de dichas herramientas y las bases de datos en las que operan.

Herramientas de administración para Trusted Extensions

La administración en los sistemas configurados con Trusted Extensions emplea muchas de las herramientas que se encuentran disponibles en el SO Oracle Solaris. Asimismo, Trusted Extensions ofrece herramientas con mejoras en la seguridad. Los roles pueden acceder a las herramientas de administración únicamente en un espacio de trabajo de rol.

En un espacio de trabajo de rol, puede acceder a los comandos, las aplicaciones y las secuencias de comandos que son de confianza. La siguiente tabla proporciona un resumen de estas herramientas administrativas.

TABLA 7–1 Herramientas administrativas de Trusted Extensions

Herramienta	Descripción	Para obtener más información
`/usr/sbin/txzonemgr`	Permite crear la interfaz gráfica de usuario Labeled Zone Manager para la creación y configuración de zonas con etiquetas, incluidas las redes. Las opciones de la línea de comandos permiten la creación automática de zonas con nombre de usuario.	Consulte "Creación de zonas con etiquetas" en la página 56 y la página del comando man `txzonemgr(1M)`. `txzonemgr` es una secuencia de comandos `zenity` (1).
Device Manager	Se utiliza para administrar los rangos de etiquetas de los dispositivos, y para asignar y desasignar dispositivos.	Consulte "Device Manager" en la página 113 y "Control de dispositivos en Trusted Extensions (mapa de tareas)" en la página 275.
Generador de etiquetas	Es otra herramienta de usuario. Aparece cuando un programa le solicita que seleccione una etiqueta.	Para ver un ejemplo, consulte "Cómo modificar el rango de etiquetas de un usuario" en la página 150.
Selection Manager	Es una herramienta para los usuarios que están autorizados a cambiar el nivel de seguridad de los datos. Aparece cuando un programa le solicita que cambie el nivel de seguridad de los datos.	Para autorizar usuarios, consulte "Cómo habilitar a un usuario para que cambie el nivel de seguridad de los datos" en la página 155. Para ver una ilustración, consulte "Cómo mover datos entre etiquetas" de *Guía del usuario de Oracle Solaris Trusted Extensions*.
Comandos de Trusted Extensions	Se utilizan para realizar tareas administrativas.	Para conocer la lista de comandos administrativos y archivos de configuración, consulte el Apéndice D, "Lista de las páginas del comando man de Trusted Extensions".

Secuencia de comandos txzonemgr

El comando `/usr/sbin/txzonemgr` ofrece dos modos.

- Como interfaz de la línea de comandos, el comando crea zonas con etiquetas a partir de los archivos existentes. Cuando se ejecuta con la opción de comando `-c`, la interfaz de la línea de comandos crea e inicia dos zonas con etiquetas. La opción `-d` suprime todas las zonas con etiquetas.
- Como interfaz gráfica de usuario, la secuencia de comandos muestra un cuadro de diálogo con el título Labeled Zone Manager. Esta interfaz gráfica de usuario lo guiará a través del proceso de creación e inicio de zonas con etiquetas. La secuencia de comandos incluye la clonación de una zona para crear una instantánea. Además, la interfaz gráfica de usuario proporciona menús de configuración de LDAP, servicio de nombres y redes.

El comando `txzonemgr` ejecuta una secuencia de comandos `zenity`(1). El cuadro de diálogo Labeled Zone Manager muestra sólo las opciones válidas para el estado de configuración actual de una zona con etiquetas. Por ejemplo, si una zona ya tiene etiquetas, la opción de menú Label no aparece.

Device Manager

Un *dispositivo* es un periférico físico que está conectado a un equipo o un dispositivo simulado mediante software que se llama *pseudodispositivo*. Dado que los dispositivos proporcionan un medio para la importación y la exportación de datos de un sistema a otro, estos deben controlarse a fin de proteger los datos de manera adecuada. Trusted Extensions utiliza rangos de etiquetas de dispositivos y asignación de dispositivos para controlar los datos que fluyen por los dispositivos.

Entre los dispositivos que tienen rangos de etiquetas se encuentran los búferes de trama, las unidades de cinta, las unidades de disquetes y CD-ROM, las impresoras y los dispositivos USB.

Los usuarios asignan dispositivos mediante Device Manager. Device Manager monta el dispositivo, ejecuta una secuencia de comandos clean para preparar el dispositivo y realiza la asignación. Una vez finalizadas estas tareas, el usuario desasigna el dispositivo mediante Device Manager, que ejecuta otra secuencia de comandos clean, y desmonta y desasigna el dispositivo.

Puede gestionar dispositivos con la herramienta Device Administration de Device Manager. Los usuarios comunes no tienen acceso a Device Allocation Manager.

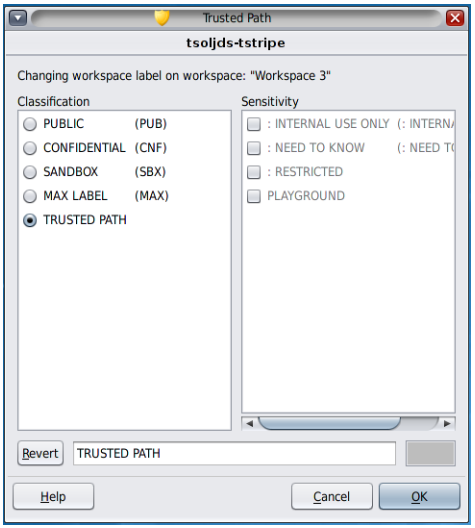
Para obtener más información sobre la protección de dispositivos en Trusted Extensions, consulte el Capítulo 21, “Gestión de dispositivos para Trusted Extensions (tareas)”.

Selection Manager en Trusted Extensions

La interfaz gráfica de usuario Selection Manager aparece cuando intenta cambiar la etiqueta de un objeto o una selección. Para obtener más información, consulte “Reglas para cambiar el nivel de seguridad de los datos” en la página 122.

Generador de etiquetas en Trusted Extensions

La interfaz gráfica de usuario del generador de etiquetas proporciona una acreditación o etiqueta válida de su elección cuando un programa le solicita que asigne una etiqueta. Por ejemplo, un generador de etiquetas aparece durante el inicio de sesión (consulte el Capítulo 2, “Inicio de sesión en Trusted Extensions (tareas)” de *Guía del usuario de Oracle Solaris Trusted Extensions*). El generador de etiquetas también aparece cuando cambia la etiqueta de un espacio de trabajo o cuando asigna una etiqueta a un usuario, una zona o una interfaz de red. El siguiente generador de etiquetas aparece cuando asigna un rango de etiquetas a un nuevo dispositivo.



En el generador de etiquetas, los nombres de los componentes en la columna Classification corresponden a la sección `CLASSIFICATIONS` del archivo `label_encodings`. Los nombres de los componentes de la columna Sensitivity corresponden a la sección `WORDS` ubicada en la sección `SENSITIVITY` del archivo `label_encodings`.

Los desarrolladores pueden crear generadores de etiquetas para sus aplicaciones mediante el comando `tgnome-selectlabel`. Escriba `tgnome-selectlabel -h` para ver la ayuda en pantalla. Asimismo, consulte el Capítulo 6, "Label Builder GUI" de *Trusted Extensions Developer's Guide*.

Herramientas de la línea de comandos en Trusted Extensions

Los comandos exclusivos de Trusted Extensions y los comandos modificados por Trusted Extensions se incluyen en el *Manual de referencia de Oracle Solaris*. El comando `man` busca todos los comandos. Para obtener una descripción de los comandos, enlaces a ejemplos en el conjunto de documentos de Trusted Extensions y un enlace a las páginas del comando man, consulte el Apéndice D, "Lista de las páginas del comando man de Trusted Extensions".

Archivos de configuración en Trusted Extensions

El archivo `/etc/inet/ike/config` se amplía en Trusted Extensions para incluir información de etiquetas. La página del comando man `ike.config(4)` describe el parámetro global `label_aware` y tres parámetros de transformación de fase 1, `single_label`, `multi_label` y `wire_label`.

Nota – El archivo de configuración de IKE contiene una palabra clave, `label`, que se utiliza para hacer que una regla IKE de fase 1 sea exclusiva. La palabra clave `label` de IKE es distinta de las etiquetas de Trusted Extensions.

◆ ◆ ◆ CAPÍTULO 8

Requisitos de seguridad del sistema Trusted Extensions (descripción general)

En este capítulo, se describen las funciones de seguridad que pueden configurarse en un sistema con Trusted Extensions.

Funciones de seguridad configurables

Trusted Extensions utiliza las mismas funciones de seguridad que proporciona Oracle Solaris y agrega otras funciones. Por ejemplo, el SO Oracle Solaris proporciona protección `eeprom`, algoritmos de contraseña complejos y requisitos de contraseña, protección del sistema mediante el bloqueo del usuario, y protección frente a la interrupción del teclado.

Trusted Extensions difiere de Oracle Solaris en que normalmente asume un rol para administrar los sistemas. Como en el SO Oracle Solaris, los archivos de configuración se modifican mediante el rol de usuario `root`.

Roles en Trusted Extensions

En Trusted Extensions, los roles son el medio convencional para administrar el sistema. El superusuario es el rol `root`, y es necesario para algunas tareas, como la definición de indicadores de auditoría, la modificación de la contraseña de una cuenta y la edición de archivos del sistema. Los roles se crean de la misma manera que en Oracle Solaris.

Los siguientes son los roles típicos de un sitio de Trusted Extensions:

- **Rol de usuario** `root`: creado en la instalación de Oracle Solaris.
- **Rol de administrador de la seguridad**: creado por el equipo de configuración inicial durante, o una vez finalizada, la configuración inicial.

- **Rol de administrador del sistema**: creado por el equipo de configuración inicial durante, o una vez finalizada, la configuración inicial.

Creación de roles en Trusted Extensions

Para administrar Trusted Extensions, puede crear roles que dividan las funciones del sistema y de la seguridad.

El proceso de creación de roles en Trusted Extensions es idéntico al proceso de Oracle Solaris. De manera predeterminada, se asigna a los roles un rango de etiquetas administrativas entre `ADMIN_HIGH` y `ADMIN_LOW`.

- Para obtener una descripción general de la creación de roles, consulte "Uso de RBAC (tareas)" de *Administración de Oracle Solaris: servicios de seguridad*.
- Para crear roles, consulte "Cómo crear un rol" de *Administración de Oracle Solaris: servicios de seguridad*.

Asunción de roles en Trusted Extensions

En el escritorio de confianza, puede asumir un rol asignado haciendo clic en su nombre de usuario, en la banda de confianza para las opciones de rol. Después de confirmar la contraseña del rol, el espacio de trabajo actual cambia a un espacio de trabajo de rol. Los espacios de trabajo de rol están en la zona global y tienen el atributo de ruta de confianza. Los espacios de trabajo de rol son espacios de trabajo administrativos.

Interfaces de Trusted Extensions para configurar las funciones de seguridad

En Trusted Extensions, puede ampliar las funciones de seguridad existentes. Además, Trusted Extensions proporciona funciones de seguridad exclusivas.

Ampliación de las funciones de seguridad de Oracle Solaris mediante Trusted Extensions

Los siguientes mecanismos de seguridad que proporciona Oracle Solaris pueden ampliarse en Trusted Extensions al igual que en Oracle Solaris:

- **Clases de auditoría**: la adición de clases de auditoría se describe en el Capítulo 28, "Gestión de auditoría (tareas)" de *Administración de Oracle Solaris: servicios de seguridad*.

Nota – Los proveedores que desean agregar *eventos de auditoría* necesitan ponerse en contacto con un representante de Oracle Solaris para reservar números de evento y obtener acceso a las interfaces de auditoría.

- **Roles y perfiles de derechos**: la adición de roles y perfiles de derechos se describe en el Capítulo 9, "Uso del control de acceso basado en roles (tareas)" de *Administración de Oracle Solaris: servicios de seguridad*.
- **Autorizaciones**: para ver un ejemplo de adición de una nueva autorización, consulte "Personalización de autorizaciones para dispositivos en Trusted Extensions (mapa de tareas)" en la página 284.

Como en Oracle Solaris, los privilegios no se pueden ampliar.

Funciones de seguridad exclusivas de Trusted Extensions

Trusted Extensions proporciona las siguientes funciones de seguridad exclusivas:

- **Etiquetas**: los sujetos y los objetos tienen etiquetas. Los procesos tienen etiquetas. Las zonas y la red tienen etiquetas. Los espacios de trabajo y sus objetos tienen etiquetas.
- **Device Manager**: de manera predeterminada, los dispositivos se encuentran protegidos por los requisitos de asignación. La interfaz gráfica de usuario Device Manager es la interfaz para administradores y para usuarios comunes.
- **Menú Change Password**: este menú permite cambiar la contraseña de usuario o de rol.
- **Menú Change Workspace Label**: los usuarios de sesiones de varios niveles pueden cambiar la etiqueta del espacio de trabajo. Es posible que se solicite a los usuarios que proporcionen una contraseña al acceder a un espacio de trabajo de una etiqueta diferente.

Aplicación de los requisitos de seguridad

A fin de garantizar que la seguridad del sistema no se vea comprometida, los administradores necesitan proteger las contraseñas, los archivos y los datos de auditoría. Los usuarios deben estar capacitados para hacer su parte del trabajo. Para cumplir con los requisitos de una configuración evaluada, siga las directrices descritas de esta sección.

Usuarios y requisitos de seguridad

Cada administrador de la seguridad del sitio debe garantizar que los usuarios reciban la formación necesaria sobre procedimientos de seguridad. El administrador de la seguridad necesita comunicar las siguientes reglas a los empleados nuevos y recordarlas a los empleados existentes con regularidad:

- No diga a nadie la contraseña.

  Cualquiera que conozca su contraseña puede acceder a la misma información que usted sin identificarse y, por lo tanto, sin tener que responsabilizarse.
- No escriba su contraseña en un papel ni la incluya en un correo electrónico.
- Elija contraseñas que sean difíciles de adivinar.
- No envíe su contraseña a nadie por correo electrónico.
- No deje su equipo desatendido sin bloquear la pantalla o cerrar sesión.
- Recuerde que los administradores no dependen del correo electrónico para enviar instrucciones a los usuarios. Nunca siga las instrucciones enviadas mediante correo electrónico por un administrador sin antes confirmar con el administrador.

  Tenga en cuenta que la información del remitente en el correo electrónico puede falsificarse.
- Dado que es responsable de los permisos de acceso a los archivos y directorios que crea, asegúrese de que los permisos de los archivos y directorios se hayan definido correctamente. No permita que los usuarios no autorizados lean o modifiquen un archivo, enumeren los contenidos de un directorio, o aumenten un directorio.

Es posible que su sitio proporcione sugerencias adicionales.

Uso del correo electrónico

Utilizar el correo electrónico para dar instrucciones a los usuarios de que realicen alguna acción resulta una práctica insegura.

Advierta a los usuarios que no confíen en los correos electrónicos que contienen instrucciones que provienen presuntamente de un administrador. De este modo, se evita la posibilidad de que se envíen mensajes de correo electrónico falsos con el objeto de engañar a los usuarios para que cambien la contraseña a un valor determinado o para que la divulguen, lo que posteriormente podría ser utilizado para iniciar sesión y poner en riesgo el sistema.

Aplicación de la contraseña

El rol de administrador del sistema debe especificar un nombre de usuario y un ID de usuario únicos al crear una nueva cuenta. Cuando selecciona el nombre y el ID de una nueva cuenta, debe asegurarse de que tanto el nombre de usuario como el ID asociado no estén duplicados en ninguna parte de la red ni se hayan utilizado previamente.

El rol de administrador de la seguridad tiene la responsabilidad de especificar la contraseña original para cada cuenta y de comunicar las contraseñas a los usuarios de cuentas nuevas. Debe tener en cuenta la siguiente información al administrar las contraseñas:

- Asegúrese de que las cuentas para los usuarios que pueden asumir el rol de administrador de la seguridad se hayan configurado de manera que la cuenta no se pueda bloquear. Esta práctica garantiza que al menos una cuenta siempre pueda iniciar sesión y asumir el rol de administrador de la seguridad para volver a abrir las cuentas de todos los demás si estas se bloquean.
- Comunique la contraseña al usuario de una cuenta nueva de modo tal que nadie más pueda enterarse de cuál es la contraseña.
- Cambie la contraseña de una cuenta ante la más mínima sospecha de que alguien que no debiera conocer la contraseña la haya descubierto.
- Nunca use los nombres de usuario o los ID de usuario más de una vez durante la vida útil del sistema.

  Al asegurarse de que los nombres de usuario y los ID de usuario no se vuelvan a utilizar, se evitan posibles confusiones respecto de lo siguiente:

  - Las acciones que realizó cada usuario en el análisis de los registros de auditoría
  - Los archivos que posee cada usuario en la restauración de archivos

Protección de la información

Como administrador, tiene la responsabilidad de configurar y mantener correctamente la protección del control de acceso discrecional (DAC) y del control de acceso obligatorio (MAC) para los archivos cuya seguridad es crítica. Entre los archivos críticos, se incluyen los siguientes:

- **Archivo** `shadow`: contiene contraseñas cifradas. Consulte la página del comando man `shadow`(4).
- **Archivo** `auth_attr`: contiene autorizaciones personalizadas. Consulte la página del comando man `auth_attr`(4).
- **Archivo** `prof_attr`: contiene perfiles de derechos personalizados. Consulte la página del comando man `prof_attr`(4).
- **Archivo** `exec_attr`: contiene comandos con atributos de seguridad que el sitio agregó a los perfiles de derechos. Consulte la página del comando man `exec_attr`(4).
- **Pista de auditoría**: contiene los registros de auditoría que recopiló el servicio de auditoría. Consulte la página del comando man `audit.log`(4).

Protección de contraseña

En los archivos locales, la protección que evita la visualización de las contraseñas se realiza mediante DAC, y la que evita su modificación, mediante DAC y MAC. Las contraseñas de las cuentas locales se actualizan en el archivo `/etc/shadow`, que solamente el superusuario puede leer. Para obtener más información, consulte la página del comando man `shadow(4)`.

Administración de grupos

El rol de administrador del sistema necesita comprobar, en el sistema local y en la red, que todos los grupos tengan un único ID de grupo (GID, Group ID).

Cuando se suprime del sistema un grupo local, el rol de administrador del sistema debe garantizar que:

- Todos los objetos con el GID del grupo eliminado se deben suprimir o asignar a otro grupo.
- A todos los usuarios que tienen el grupo eliminado como grupo principal se les asigna otro grupo principal.

Prácticas de eliminación de usuarios

Cuando se suprime una cuenta del sistema, el rol de administrador del sistema y el rol de administrador de la seguridad deben realizar las siguientes acciones:

- Suprimir los directorios principales de la cuenta en cada zona.
- Suprimir cualquier proceso o trabajo que pertenezca a la cuenta eliminada:
  - Suprimir cualquier objeto que pertenezca a la cuenta o asignar la propiedad a otro usuario.
  - Suprimir cualquier trabajo de `at` o `batch` planificado en nombre del usuario. Para obtener detalles, consulte las páginas del comando man `at(1)` y `crontab(1)`.
- Nunca vuelva a usar el nombre de usuario ni el ID de usuario.

Reglas para cambiar el nivel de seguridad de los datos

De manera predeterminada, los usuarios comunes pueden emplear las operaciones de cortar y pegar, copiar y pegar, y arrastrar y soltar en los archivos y en las selecciones. El origen y el destino deben estar en la misma etiqueta.

Para cambiar la etiqueta de los archivos o la etiqueta de la información dentro de los archivos se requiere autorización. Cuando los usuarios están autorizados a cambiar el nivel de seguridad de los datos, la aplicación Selection Manager media en la transferencia. El archivo

`/usr/share/gnome/sel_config` controla las acciones para volver a etiquetar archivos, y para cortar o copiar información y pegarla en una etiqueta diferente. La aplicación `/usr/bin/tsoljdsselmgr` controla las operaciones de arrastrar y soltar entre ventanas. Como se muestra en las siguientes tablas, hay más restricciones para volver a etiquetar una selección que un archivo.

La siguiente tabla muestra un resumen de las reglas para volver a etiquetar archivos. Las reglas incluyen las operaciones de cortar y pegar, copiar y pegar, y arrastrar y soltar.

TABLA 8–1 Condiciones para mover archivos a una etiqueta nueva

Descripción de la transacción	Relaciones de etiquetas	Relaciones de propietarios	Autorización requerida
Copiar y pegar, cortar y pegar, o arrastrar y soltar archivos entre exploradores de archivos	Misma etiqueta	Mismo UID	Ninguna
	Degradar información	Mismo UID	`solaris.label.file.downgrade`
	Actualizar información	Mismo UID	`solaris.label.file.upgrade`
	Degradar información	Diferentes UID	`solaris.label.file.downgrade`
	Actualizar información	Diferentes UID	`solaris.label.file.upgrade`

Se aplican reglas diferentes a las selecciones en una ventana que en un archivo. La acción de arrastrar y soltar *selecciones* siempre requiere que exista igualdad de etiquetas y propiedad. La acción de arrastrar y soltar entre ventanas es mediada por la aplicación Selection Manager, no por el archivo `sel_config`.

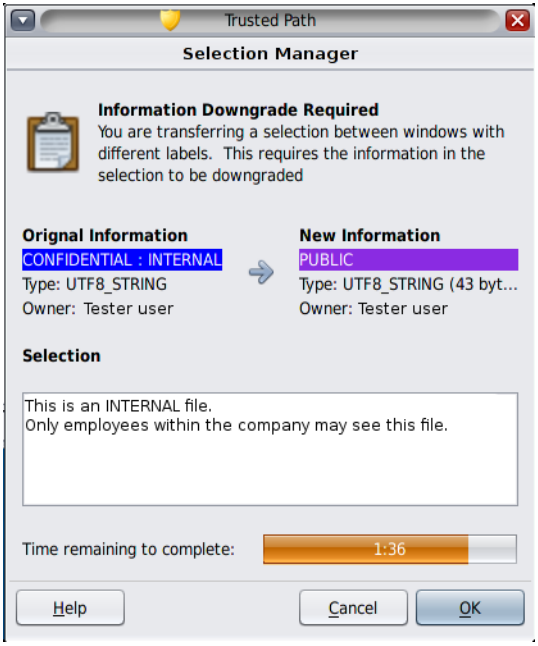
Las reglas para cambiar la etiqueta de selecciones se resumen en la siguiente tabla.

TABLA 8–2 Condiciones para mover selecciones a una etiqueta nueva

Descripción de la transacción	Relaciones de etiquetas	Relaciones de propietarios	Autorización requerida
Copiar y pegar, o cortar y pegar selecciones entre ventanas	Misma etiqueta	Mismo UID	Ninguna
	Degradar información	Mismo UID	`solaris.label.win.downgrade`
	Actualizar información	Mismo UID	`solaris.label.win.upgrade`
	Degradar información	Diferentes UID	`solaris.label.win.downgrade`
	Actualizar información	Diferentes UID	`solaris.label.win.upgrade`
Arrastrar y soltar las selecciones entre las ventanas	Misma etiqueta	Mismo UID	Ninguna

Trusted Extensions proporciona un confirmador de selección para que medie en los cambios de etiquetas. Esta ventana aparece cuando un usuario autorizado intenta cambiar la etiqueta de un archivo o selección. El usuario tiene 120 segundos para confirmar la operación. Para cambiar el

nivel de seguridad de datos sin esta ventana, se requiere la autorización `solaris.label.win.noview` además de que se vuelvan a etiquetar las autorizaciones. La siguiente ilustración muestra una selección, de dos líneas, en la ventana.



De manera predeterminada, el confirmador de selección aparece cuando se transfieren datos a una etiqueta diferente. Si una selección requiere varias decisiones de transferencia, el mecanismo de respuesta automático proporciona un modo de responder una sola vez a todas las transferencias. Para obtener más información, consulte la página del comando man `sel_config(4)` y la sección siguiente.

Archivo sel_config

El archivo `/usr/share/gnome/sel_config` se verifica a fin de determinar el comportamiento del confirmador de selección cuando una operación aumenta o disminuye el nivel de una etiqueta.

El archivo `sel_config` define lo siguiente:

- Qué tipos de selecciones obtienen respuestas automáticas
- Qué tipos de operaciones pueden confirmarse automáticamente
- Cuándo se muestra un cuadro de diálogo del confirmador de selección

◆ ◆ ◆ CAPÍTULO 9

Realización de tareas comunes en Trusted Extensions (tareas)

En este capítulo, se presenta la administración de los sistemas de Trusted Extensions y se incluyen tareas que se realizan comúnmente en estos sistemas.

Introducción para administradores de Trusted Extensions (mapa de tareas)

Familiarícese con los siguientes procedimientos antes de administrar Trusted Extensions.

Tarea	Descripción	Para obtener instrucciones
Iniciar sesión en un sistema Trusted Extensions.	Permite iniciar sesión de manera segura.	"Inicio de sesión en Trusted Extensions" de *Guía del usuario de Oracle Solaris Trusted Extensions*
Realizar tareas de usuario comunes en un escritorio.	Las tareas incluyen: ■ Configurar los espacios de trabajo ■ Usar espacios de trabajo en diferentes etiquetas ■ Usar las páginas del comando man de Trusted Extensions	"Trabajo en un sistema con etiquetas" de *Guía del usuario de Oracle Solaris Trusted Extensions*
Realizar tareas que requieren la ruta de confianza.	Las tareas incluyen: ■ Asignar un dispositivo ■ Cambiar la contraseña ■ Cambiar la etiqueta de un espacio de trabajo	"Realizar acciones de confianza" de *Guía del usuario de Oracle Solaris Trusted Extensions*

Tarea	Descripción	Para obtener instrucciones
Asumir un rol.	Permite acceder a la zona global con un rol. Todas las tareas administrativas se realizan en la zona global.	"Cómo entrar en la zona global en Trusted Extensions" en la página 126
Seleccionar un espacio de trabajo de usuario.	Permite salir de la zona global.	"Cómo salir de la zona global en Trusted Extensions" en la página 126

▼ Cómo entrar en la zona global en Trusted Extensions

Cuando asume un rol, entra en la zona global en Trusted Extensions. Es posible administrar todo el sistema solamente desde la zona global.

Para la resolución de problemas, también puede entrar en la zona global si inicia una sesión en modo a prueba de fallos. Para obtener detalles, consulte "Cómo iniciar una sesión en modo a prueba de fallos en Trusted Extensions" en la página 149.

Antes de empezar Se le asigna un rol administrativo. Para obtener referencias, consulte "Creación de roles en Trusted Extensions" en la página 118.

1. **Haga clic en *account-name* en la banda de confianza.**

   Seleccione un rol de la lista.

   Para conocer la ubicación de las funciones del escritorio de Trusted Extensions, consulte la Figura 6–1. Para obtener una explicación de estas funciones, consulte el Capítulo 4, "Elementos de Trusted Extensions (referencia)" de *Guía del usuario de Oracle Solaris Trusted Extensions*.

2. **Cuando se solicite, escriba la contraseña de rol.**

   Tras la autenticación, el espacio de trabajo actual cambia al espacio de trabajo de rol.

▼ Cómo salir de la zona global en Trusted Extensions

Antes de empezar Debe encontrarse en la zona global.

1. **Seleccione un espacio de trabajo de usuario en el panel del escritorio ubicado en la parte inferior de la pantalla.**

2. **O bien, haga clic en el nombre del rol en la banda de confianza y, a continuación, seleccione su nombre de usuario.**

   El espacio de trabajo actual cambia a un espacio de trabajo de usuario. Todas las ventanas que cree posteriormente en este espacio de trabajo se crearán en la etiqueta del usuario.

Las ventanas creadas en el espacio de trabajo de rol siguen admitiendo procesos en la etiqueta del rol. Los procesos iniciados en esas ventanas se ejecutan en la zona global con privilegios administrativos.

Para obtener más información, consulte "Trabajo en un sistema con etiquetas" de *Guía del usuario de Oracle Solaris Trusted Extensions*.

Tareas comunes en Trusted Extensions (mapa de tareas)

En el siguiente mapa de tareas, se describen los procedimientos administrativos comunes en Trusted Extensions.

Tarea	Descripción	Para obtener instrucciones
Cambiar la contraseña de `root`.	Se especifica una contraseña nueva para el rol de usuario `root`.	"Cómo cambiar la contraseña de `root`" en la página 128
Reflejar un cambio de contraseña en una zona con etiquetas.	Se reinicia la zona para actualizar la zona que una contraseña ha cambiado.	"Cómo aplicar una nueva contraseña de usuario local en una zona con etiquetas" en la página 128
Utilizar la combinación de teclas de aviso de seguridad.	Permite obtener control del mouse o el teclado. Además, permite probar si el mouse o el teclado son de confianza.	"Cómo recuperar el control del enfoque actual del escritorio" en la página 129
Determinar el número hexadecimal de una etiqueta.	Muestra la representación interna de una etiqueta de texto.	"Cómo obtener el equivalente hexadecimal de una etiqueta" en la página 130
Determinar la representación de texto de una etiqueta.	Muestra la representación de texto de una etiqueta hexadecimal.	"Cómo obtener una etiqueta legible de su forma hexadecimal" en la página 131
Asignar un dispositivo.	Permite a los usuarios asignar dispositivos. Utiliza un dispositivo periférico para agregar o eliminar información en el sistema.	"Cómo autorizar a usuarios para que asignen un dispositivo" de *Administración de Oracle Solaris: servicios de seguridad* "Cómo asignar un dispositivo en Trusted Extensions" de *Guía del usuario de Oracle Solaris Trusted Extensions*
Administrar un sistema de manera remota.	Permite administrar los sistemas Trusted Extensions desde un sistema remoto.	Capítulo 12, "Administración remota en Trusted Extensions (tareas)"

▼ Cómo cambiar la contraseña de root

Trusted Extensions proporciona una interfaz gráfica de usuario para cambiar la contraseña.

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

   Para conocer los pasos, consulte "Cómo entrar en la zona global en Trusted Extensions" en la página 126.

2. **Abra el menú Trusted Path. Para ello, haga clic en el símbolo de confianza en la banda de confianza.**

3. **Seleccione Change Login Password.**

   Si se crean contraseñas independientes por zona, el menú puede indicar Change Workspace Password.

4. **Cambie la contraseña y confirme el cambio.**

▼ Cómo aplicar una nueva contraseña de usuario local en una zona con etiquetas

Se deben reiniciar las zonas con etiquetas en los siguientes casos:

- Uno o varios usuarios locales han cambiado sus contraseñas.
- Todas las zonas utilizan una sola instancia del daemon de antememoria de servicio de nombres (`nscd`).
- El sistema se administra con archivos, no con LDAP.

Antes de empezar Debe tener asignado el perfil de derechos de seguridad de la zona.

- **Para aplicar el cambio de contraseña, reinicie las zonas con etiquetas a las que pueden acceder los usuarios.**

  Utilice uno de los métodos siguientes:

  - **Utilice la interfaz gráfica de usuario `txzonemgr`.**

    ```
    # txzonemgr &
    ```

    En Labeled Zone Manager, navegue hasta la zona con etiquetas y, en la lista de comandos, seleccione Halt y luego Boot.

  - **En una ventana de terminal de la zona global, utilice los comandos de administración de zonas.**

    Puede optar por apagar o detener el sistema.

- El comando `zlogin` apaga la zona correctamente.

  ```
  # zlogin labeled-zone shutdown -i 0
  # zoneadm -z labeled-zone boot
  ```

- El subcomando `halt` omite las secuencias de comandos de apagado.

  ```
  # zoneadm -z labeled-zone halt
  # zoneadm -z labeled-zone boot
  ```

Errores más frecuentes

Para actualizar automáticamente las contraseñas de usuario de las zonas con etiquetas, debe configurar LDAP o un servicio de nombres por zona. También puede configurar ambos.

- Para configurar LDAP, consulte el Capítulo 5, "Configuración de LDAP para Trusted Extensions (tareas)".
- La configuración de un servicio de nombres por zona requiere conocimientos avanzados sobre redes. Para conocer el procedimiento, consulte "Cómo configurar un servicio de nombres independiente para cada zona con etiquetas" en la página 65.

▼ Cómo recuperar el control del enfoque actual del escritorio

La combinación de teclas de aviso de seguridad se puede utilizar para interrumpir un arrastre del puntero o del teclado que provenga de una aplicación que no sea de confianza. Esta combinación de teclas también puede utilizarse para verificar si un arrastre del puntero o del teclado proviene de una aplicación de confianza. En un sistema de varios periféricos que se ha suplantado para que se muestre más de una banda de confianza, esta combinación de teclas dirige el puntero hacia la banda de confianza autorizada.

1 Para recuperar el control de un teclado de Sun, utilice la siguiente combinación de teclas.

Presione las teclas simultáneamente para recuperar el control del enfoque actual del escritorio. En el teclado de Sun, el rombo es la tecla Meta.

```
<Meta> <Stop>
```

Si el arrastre, como un puntero, no es de confianza, el puntero se mueve hacia la banda. Si el puntero es de confianza, no se pasa a la banda de confianza.

2 Si no utiliza un teclado de Sun, use la siguiente combinación de teclas.

```
<Alt> <Break>
```

Presione las teclas simultáneamente para recuperar el control del enfoque del escritorio actual de su equipo portátil.

Ejemplo 9–1 Comprobar si la petición de contraseña es de confianza

En un sistema x86 que se usa con un teclado de Sun, se le solicita una contraseña al usuario. Se arrastra el puntero y se lo ubica en el cuadro de diálogo de contraseña. Para comprobar si el indicador es de confianza, el usuario presiona simultáneamente las teclas <Meta> y <Stop>. Cuando el puntero permanece en el cuadro de diálogo, el usuario sabe que la petición de contraseña es de confianza.

Si el puntero se mueve a la banda de confianza, el usuario se da cuenta de que la petición de contraseña no es de confianza, por lo que debe ponerse en contacto con el administrador.

Ejemplo 9–2 Forzar el puntero hacia la banda de confianza

En este ejemplo, un usuario no está ejecutando ningún proceso de confianza, pero no puede ver el puntero del mouse. Para ubicar el puntero en el centro de la banda de confianza, el usuario presiona simultáneamente las teclas <Meta> y <Stop>.

▼ Cómo obtener el equivalente hexadecimal de una etiqueta

Este procedimiento proporciona la representación hexadecimal interna de una etiqueta. Esta representación se puede almacenar con seguridad en un directorio público. Para obtener más información, consulte la página del comando man `atohexlabel(1M)`.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global. Para obtener detalles, consulte "Cómo entrar en la zona global en Trusted Extensions" en la página 126.

- **Para obtener el valor hexadecimal de una etiqueta, realice una de las acciones siguientes:**

  - **Para obtener el valor hexadecimal de una etiqueta de sensibilidad, pase la etiqueta al comando.**

    ```
    $ atohexlabel "CONFIDENTIAL : INTERNAL USE ONLY"
    0x0004-08-48
    ```

    La cadena no distingue mayúsculas de minúsculas, pero los espacios en blanco deben ser exactos. Por ejemplo, las siguientes cadenas entre comillas devuelven una etiqueta hexadecimal:

    - `"CONFIDENTIAL : INTERNAL USE ONLY"`
    - `"cnf : Internal"`
    - `"confidential : internal"`

    Las siguientes cadenas entre comillas devuelven un error de análisis:

    - `"confidential:internal"`

- `"confidential: internal"`

- **Para obtener el valor hexadecimal de una acreditación, utilice la opción `-c`.**

```
$ atohexlabel -c "CONFIDENTIAL NEED TO KNOW"
0x0004-08-68
```

Nota – Las etiquetas de sensibilidad y de acreditación en lenguaje natural se forman según las reglas del archivo `label_encodings`. Cada tipo de etiqueta utiliza reglas de una sección independiente de este archivo. Cuando la etiqueta de sensibilidad y la etiqueta de acreditación expresan el mismo nivel de sensibilidad subyacente, ambas tienen una forma hexadecimal idéntica. Sin embargo, las etiquetas pueden tener diferentes formas en lenguaje natural. Las interfaces del sistema que aceptan etiquetas en lenguaje natural como entrada esperan un tipo de etiqueta. Si las cadenas de texto de los tipos de etiquetas difieren, estas cadenas de texto no se pueden intercambiar.

En el archivo `label_encodings`, el equivalente de texto de una etiqueta de acreditación no incluye dos puntos (:).

Ejemplo 9–3 Uso del comando atohexlabel

Cuando pasa una etiqueta válida en formato hexadecimal, el comando devuelve el argumento.

```
$ atohexlabel 0x0004-08-68
0x0004-08-68
```

Cuando pasa una etiqueta administrativa, el comando devuelve el argumento.

```
$ atohexlabel admin_high
ADMIN_HIGH
atohexlabel admin_low
ADMIN_LOW
```

Errores más frecuentes

El mensaje de error `atohexlabel parsing error found in <string> at position 0` indica que el argumento `<string>` que pasó a `atohexlabel` no es una etiqueta o acreditación válidas. Verifique que no haya errores de escritura y compruebe que la etiqueta exista en el archivo `label_encodings` que tiene instalado.

▼ Cómo obtener una etiqueta legible de su forma hexadecimal

Este procedimiento proporciona un modo de reparar las etiquetas almacenadas en las bases de datos internas. Para obtener más información, consulte la página del comando man `hextoalabel(1M)`.

Antes de empezar

Debe estar con el rol de administrador de la seguridad en la zona global.

- **Para obtener el equivalente de texto de la representación interna de una etiqueta, realice una de las acciones siguientes.**

  - **Para obtener el equivalente de texto de una etiqueta de sensibilidad, pase la forma hexadecimal de la etiqueta.**

    ```
    $ hextoalabel 0x0004-08-68
    CONFIDENTIAL : NEED TO KNOW
    ```

  - **Para obtener el equivalente de texto de una acreditación, utilice la opción `-c`.**

    ```
    $ hextoalabel -c 0x0004-08-68
    CONFIDENTIAL NEED TO KNOW
    ```

▼ Cómo cambiar los valores predeterminados de seguridad en los archivos del sistema

Como en Oracle Solaris, en Trusted Extensions, la cuenta `root` puede cambiar los valores de seguridad predeterminados en un sistema.

Los archivos de los directorios `/etc/security` y `/etc/default` contienen valores de seguridad. Para obtener más información, consulte el Capítulo 3, "Control de acceso a sistemas (tareas)" de *Administración de Oracle Solaris: servicios de seguridad*.

Precaución – Reduzca los valores predeterminados de seguridad del sistema únicamente si la política de seguridad del sitio lo permite.

Antes de empezar Debe estar con el rol de usuario `root` en la zona global.

- **Edite el archivo del sistema.**

  La siguiente tabla muestra los archivos de seguridad y los valores de seguridad que es posible cambiar en los archivos.

Archivo	Tarea	Para obtener más información
`/etc/default/login`	Reducir el número permitido de intentos de introducción de contraseña.	Consulte el ejemplo de "Cómo supervisar todos los intentos de inicio de sesión fallidos" de *Administración de Oracle Solaris: servicios de seguridad*. Página del comando man `passwd(1)`

Archivo	Tarea	Para obtener más información
`/etc/default/kbd`	Deshabilitar la interrupción del teclado.	"Cómo deshabilitar una secuencia de interrupción del sistema" de *Administración de Oracle Solaris: servicios de seguridad* **Nota –** En los hosts que los administradores utilizan para realizar la depuración, la configuración predeterminada para `KEYBOARD_ABORT` permite el acceso al depurador del núcleo `kadb`. Página del comando man `kadb(1M)`
`/etc/security/policy.conf`	Solicitar un algoritmo más potente para las contraseñas de usuario. Eliminar un privilegio básico de todos los usuarios de este host. Restringir a los usuarios de este host a las autorizaciones de usuario de Solaris básico.	Página del comando man `policy.conf(4)`
`/etc/default/passwd`	Solicitar a los usuarios que cambien las contraseñas con frecuencia. Solicitar a los usuarios que creen contraseñas que sean extremadamente diferentes. Solicitar una contraseña de usuario más larga. Solicitar una contraseña que no se pueda encontrar en el diccionario.	Página del comando man `passwd(1)`

◆ ◆ ◆ CAPÍTULO 10

Usuarios, derechos y roles en Trusted Extensions (descripción general)

En este capítulo, se explican las decisiones fundamentales que debe tomar antes de crear usuarios comunes y se proporciona información básica adicional para administrar las cuentas de usuario. En el capítulo, se supone que el equipo de configuración inicial ya configuró los roles y un número determinado de cuentas de usuario. Estos usuarios pueden asumir los roles que se utilizan para configurar y administrar Trusted Extensions. Para obtener detalles, consulte·"Creación de roles y usuarios en Trusted Extensions" en la página 67.

Funciones de seguridad del usuario en Trusted Extensions

El software Trusted Extensions agrega las siguientes funciones de seguridad a usuarios, roles o perfiles de derechos:

- Los usuarios tienen un rango de etiquetas dentro del que pueden utilizar el sistema.
- Hay un rango de etiquetas dentro del que pueden utilizarse los roles para realizar tareas administrativas.
- Los comandos de un perfil de derechos de Trusted Extensions tienen un atributo de etiqueta. El comando se debe realizar dentro de un rango de etiquetas o en una etiqueta en particular.
- El software Trusted Extensions agrega privilegios y autorizaciones al conjunto de privilegios y autorizaciones definidos por Oracle Solaris.

Responsabilidades del administrador para los usuarios

El rol de administrador del sistema crea las cuentas de usuarios. El rol de administrador de la seguridad configura los aspectos de seguridad de una cuenta.

Para obtener detalles sobre la configuración de los usuarios y los roles, consulte lo siguiente:

- "Configuración y administración de cuentas de usuario (mapa de tareas)" de *Administración de Oracle Solaris: tareas comunes*
- Parte III, "Roles, perfiles de derechos y privilegios" de *Administración de Oracle Solaris: servicios de seguridad*

Responsabilidades del administrador del sistema para los usuarios

En Trusted Extensions, el rol de administrador del sistema es responsable de determinar quién puede acceder al sistema. El administrador del sistema es responsable de las siguientes tareas:

- Agregar y suprimir usuarios
- Agregar y suprimir roles
- Asignar la contraseña inicial
- Modificar las propiedades de rol y de usuario que no sean atributos de seguridad

Responsabilidades del administrador de la seguridad para los usuarios

En Trusted Extensions, el rol de administrador de la seguridad es responsable de todos los atributos de seguridad de un usuario o rol. El administrador de la seguridad tiene a su cargo las siguientes tareas:

- Asignar y modificar los atributos de seguridad de un usuario, rol o perfil de derechos
- Crear y modificar perfiles de derechos
- Asignar perfiles de derechos a un usuario o rol
- Asignar privilegios a un usuario, rol o perfil de derechos
- Asignar autorizaciones a un usuario, rol o perfil de derechos
- Eliminar privilegios de un usuario, rol o perfil de derechos
- Eliminar autorizaciones de un usuario, rol o perfil de derechos

Normalmente, el rol de administrador de la seguridad crea perfiles de derechos. Sin embargo, si un perfil necesita capacidades que el rol de administrador de la seguridad no puede otorgar, el rol de usuario `root` puede crear el perfil.

Antes de crear un perfil de derechos, el administrador de la seguridad tiene que analizar si alguno de los comandos del nuevo perfil necesita un privilegio o una autorización para ejecutarse correctamente. Las páginas del comando man para los comandos individuales enumeran las autorizaciones y los privilegios que pueden necesitarse.

Decisiones que deben tomarse antes de crear usuarios en Trusted Extensions

Las siguientes decisiones afectan las acciones que los usuarios pueden realizar en Trusted Extensions y la cantidad de esfuerzo que se necesita. Algunas decisiones son las mismas que deben tomarse cuando se instala el SO Oracle Solaris. Sin embargo, las decisiones que son específicas de Trusted Extensions pueden afectar la seguridad del sitio y la facilidad de uso.

- Decida si se cambian los atributos de seguridad del usuario predeterminados en el archivo `policy.conf`. Los valores predeterminados de usuario del archivo `label_encodings` fueron configurados originalmente por el equipo de configuración inicial. Para obtener una descripción de los valores predeterminados, consulte "Atributos de seguridad del usuario predeterminados en Trusted Extensions" en la página 137.
- Decida qué archivos de inicio se copiarán o enlazarán del directorio principal de etiqueta mínima del usuario a los directorios principales de nivel superior del usuario. Para conocer el procedimiento, consulte "Cómo configurar los archivos de inicio para los usuarios en Trusted Extensions" en la página 146.
- Decida si los usuarios pueden acceder a los dispositivos periféricos, como el micrófono, la unidad de CD-ROM y los dispositivos USB.

  Si a algunos usuarios se les permite el acceso, decida si el sitio requiere autorizaciones adicionales a fin de garantizar la seguridad del sitio. Para obtener una lista predeterminada con las autorizaciones relacionadas con los dispositivos, consulte "Cómo asignar autorizaciones para dispositivos" en la página 288. Para crear un conjunto de autorizaciones para dispositivos más específico, consulte "Personalización de autorizaciones para dispositivos en Trusted Extensions (mapa de tareas)" en la página 284.

Atributos de seguridad del usuario predeterminados en Trusted Extensions

Las configuraciones de los archivos `label_encodings` y `policy.conf` definen conjuntamente los atributos de seguridad predeterminados para las cuentas de usuario. Los valores que establece explícitamente para un usuario sustituyen estos valores de sistema. Algunos valores que se establecen en estos archivos también se aplican a las cuentas de rol. Para conocer los atributos de seguridad que puede establecer explícitamente, consulte "Atributos de usuario que pueden configurarse en Trusted Extensions" en la página 139.

Valores predeterminados del archivo label_encodings

El archivo `label_encodings` define la visualización de la etiqueta predeterminada, la etiqueta mínima y la acreditación del usuario. Para obtener detalles sobre el archivo, consulte la página del comando man `label_encodings(4)`. El archivo `label_encodings` fue instalado por el equipo de configuración inicial. Las decisiones se basaron en "Diseño de una estrategia de etiqueta" en la página 29 y en los ejemplos de *Trusted Extensions Label Administration*.

Los valores de etiquetas que el administrador de la seguridad establece explícitamente para los usuarios individuales sustituyen los valores del archivo `label_encodings`.

Valores predeterminados del archivo policy.conf en Trusted Extensions

El archivo `/etc/security/policy.conf` contiene los valores de seguridad predeterminados del sistema. Trusted Extensions agrega dos palabras clave a este archivo. Para cambiar los valores en todo el sistema, agregue los pares *palabra clave=valor* en el archivo. La siguiente tabla muestra los valores predeterminados y los valores posibles para esas palabras claves.

TABLA 10–1 Valores predeterminados de seguridad de Trusted Extensions en el archivo policy.conf

Palabra clave	Valor predeterminado	Valores posibles	Notas
`IDLECMD`	`LOCK`	`LOCK` | `LOGOUT`	Se aplica al usuario de inicio de sesión.
`IDLETIME`	`30`	De `0` a `120` minutos	Se aplica al usuario de inicio de sesión.

Las autorizaciones y los perfiles de derechos que se definen en el archivo `policy.conf` son *adicionales* de cualquier autorización o perfil que se asigne a las cuentas individuales. Para los demás campos, el valor del usuario individual valor sustituye el valor del sistema.

En "Planificación de la seguridad del usuario en Trusted Extensions" en la página 34, se incluye una tabla de cada palabra clave de `policy.conf`. También, puede consultar la página del comando man `policy.conf(4)`.

Atributos de usuario que pueden configurarse en Trusted Extensions

Para los usuarios que pueden iniciar sesión en más de una etiqueta, se recomienda configurar dos archivos auxiliares, `.copy_files` y `.link_files`, en el directorio principal de la etiqueta mínima de cada usuario. Para obtener más información, consulte "Archivos `.copy_files` y `.link_files`" en la página 141.

Atributos de seguridad que deben asignarse a los usuarios

El administrador de la seguridad puede modificar los atributos de seguridad de los usuarios nuevos. Para obtener información acerca de los archivos que contienen los valores predeterminados, consulte "Atributos de seguridad del usuario predeterminados en Trusted Extensions" en la página 137. La siguiente tabla muestra los atributos de seguridad que se pueden asignar a los usuarios y el efecto de cada asignación.

TABLA 10–2 Atributos de seguridad que se asignan después la creación del usuario

Atributo de usuario	Ubicación de valor predeterminado	Condición de la acción	Efecto de la asignación
Contraseña	Ninguno	Necesaria	El usuario tiene contraseña
Roles	Ninguno	Opcional	El usuario puede asumir un rol
Autorizaciones	Archivo `policy.conf`	Opcional	El usuario tiene autorizaciones adicionales
Perfiles de derechos	Archivo `policy.conf`	Opcional	El usuario tiene perfiles de derechos adicionales
Etiquetas	Archivo `label_encodings`	Opcional	El usuario tiene un rango de acreditación o etiqueta predeterminado que es diferente
Privilegios	Archivo `policy.conf`	Opcional	El usuario tiene un conjunto de privilegios diferente
Uso de la cuenta	Archivo `policy.conf`	Opcional	El usuario tiene una configuración diferente para cuando el equipo está inactivo
Auditoría	Núcleo	Opcional	El usuario no se audita de la misma forma que los valores predeterminados del sistema

Asignación de atributos de seguridad a los usuarios en Trusted Extensions

El administrador de la seguridad asigna atributos de seguridad a los usuarios una vez que se crean las cuentas de usuario. Si estableció los valores predeterminados correctos, el siguiente paso consiste en asignar los atributos de seguridad únicamente a los usuarios que necesiten excepciones a los valores predeterminados.

Al asignar atributos de seguridad a los usuarios, tenga en cuenta la siguiente información:

Asignación de contraseñas
El administrador del sistema puede asignar contraseñas a cuentas de usuario durante la creación de cuentas. Después de esta asignación inicial, el administrador de la seguridad o el usuario pueden cambiar la contraseña.

Como en Oracle Solaris, se puede exigir a los usuarios que cambien sus contraseñas periódicamente. Las opciones de caducidad de las contraseñas limitan el período durante el que un intruso capaz de adivinar o robar la contraseña puede acceder al sistema. Además, al establecer que transcurra un período mínimo antes de poder cambiar la contraseña, se impide que el usuario reemplace inmediatamente la contraseña nueva por la contraseña anterior. Para obtener detalles, consulte la página del comando man `passwd(1)`.

Nota – Las contraseñas de los usuarios que pueden asumir roles no deben estar sujetas a ninguna limitación por caducidad.

Asignación de roles
No es obligatorio que los usuarios tengan roles. Se puede asignar más de un rol a un usuario si esto coincide con la política de seguridad del sitio.

Asignación de autorizaciones
Como en el SO Oracle Solaris, al asignar autorizaciones a un usuario, se agregan esas autorizaciones a las existentes. Se recomienda agregar las autorizaciones a un perfil de derechos y luego asignar el perfil al usuario.

Asignación de perfiles de derechos
Como en el SO Oracle Solaris, el orden de los perfiles de derechos es importante. Con la excepción de las autorizaciones, el mecanismo de perfiles utiliza el valor de la primera instancia de un atributo de seguridad asignado. Para obtener más información, consulte "Orden de búsqueda para atributos de seguridad asignados" de *Administración de Oracle Solaris: servicios de seguridad*.

Puede utilizar el orden de clasificación de perfiles para su beneficio. Si desea que un comando se ejecute con atributos de seguridad diferentes de los que se definen para el comando de un perfil existente, cree un perfil nuevo con las asignaciones preferidas para el comando. Luego, inserte ese perfil nuevo antes del perfil existente.

Nota – No asigne perfiles de derechos que incluyan comandos administrativos a un usuario común. El perfil de derechos no funciona porque el usuario común no puede acceder a la zona global.

Cambio de valores predeterminados de privilegios
El conjunto de privilegios predeterminado puede ser demasiado liberal para varios sitios. A fin de restringir el conjunto de privilegios para cualquier usuario común en el sistema, cambie la configuración del archivo `policy.conf`. Para cambiar el conjunto de privilegios para usuarios individuales, consulte "Cómo restringir el conjunto de privilegios de un usuario" en la página 154.

Cambio de valores predeterminados de etiquetas
El cambio de los valores predeterminados de una etiqueta del usuario crea una excepción a los valores predeterminados del usuario en el archivo `label_encodings`.

Cambio de valores predeterminados de auditoría
Como en el SO Oracle Solaris, la asignación de clases de auditoría a un usuario modifica la máscara de preselección del usuario. Para obtener más información acerca de la auditoría, consulte la Parte VII, "Auditoría en Oracle Solaris" de *Administración de Oracle Solaris: servicios de seguridad* y el Capítulo 22, "Auditoría de Trusted Extensions (descripción general)".

Archivos .copy_files y .link_files

En Trusted Extensions, los archivos se copian automáticamente del directorio de estructura básica *sólo* en la zona que contiene la etiqueta mínima de la cuenta. A fin de garantizar que las zonas de las etiquetas superiores puedan usar los archivos de inicio, el usuario o el administrador deben crear los archivos `.copy_files` y `.link_files`.

Los archivos `.copy_files` y `.link_files` de Trusted Extensions ayudan a automatizar los procedimientos para copiar o enlazar los archivos de inicio en cada etiqueta del directorio principal de una cuenta. Siempre que un usuario crea un espacio de trabajo en una etiqueta nueva, el comando `updatehome` lee el contenido de `.copy_files` y `.link_files` en la etiqueta mínima de la cuenta. A continuación, el comando enlaza o copia cada archivo enumerado en el espacio de trabajo con etiquetas superiores.

El archivo `.copy_files` resulta útil cuando un usuario quiere que los archivos de inicio sean diferentes en las etiquetas diferentes. Se prefiere copiar, por ejemplo, cuando los usuarios utilizan alias de correo diferentes en etiquetas diferentes. El archivo `.link_files` resulta útil cuando el archivo de inicio debe ser idéntico en cualquier etiqueta que se invoque. Se prefiere enlazar, por ejemplo, cuando una impresora se utiliza para todos los trabajos de impresión con etiquetas. Para ver archivos de ejemplo, consulte "Cómo configurar los archivos de inicio para los usuarios en Trusted Extensions" en la página 146.

La lista siguiente enumera algunos archivos de inicio que quizás quiera que los usuarios puedan enlazar o copiar en etiquetas superiores:

```
.acrorc                 .cshrc                  .mime_types
.aliases                .emacs                  .newsrc
.bashrc                 .login                  .signature
.bashrc.user            .mailrc                 .soffice
```

◆ ◆ ◆ CAPÍTULO 11

Gestión de usuarios, derechos y roles en Trusted Extensions (tareas)

En este capítulo se explican los procedimientos de Trusted Extensions para configurar y gestionar usuarios, cuentas de usuario y perfiles de derechos.

Personalización del entorno de usuario para la seguridad (mapa de tareas)

En el siguiente mapa de tareas se describen las tareas comunes que puede llevar a cabo para personalizar un sistema para todos los usuarios o una cuenta de usuario individual. Muchas de estas tareas se llevan a cabo antes de que los usuarios comunes puedan iniciar sesión.

Tarea	Descripción	Para obtener instrucciones
Cambiar los atributos de etiquetas.	Se modifican los atributos de etiquetas, como la vista de la etiqueta mínima y la etiqueta predeterminada, para una cuenta de usuario.	"Cómo modificar atributos de etiquetas de usuarios predeterminados" en la página 144
Cambiar la política de Trusted Extensions para todos los usuarios de un sistema.	Se modifica el archivo `policy.conf`.	"Cómo modificar los valores predeterminados de `policy.conf`" en la página 145
	Se activa el protector de pantalla o se cierra la sesión del usuario después de que el sistema permanece inactivo por un tiempo determinado.	Ejemplo 11–1
	Se eliminan los privilegios innecesarios de todos los usuarios comunes de un sistema.	Ejemplo 11–2
	Impide que las etiquetas aparezcan en la salida impresa en un quiosco público.	Ejemplo 11–3

Tarea	Descripción	Para obtener instrucciones
Configurar los archivos de inicialización para los usuarios.	Se configuran los archivos de inicio, como `.bashrc`, `.cshrc`, `.copy_files` y `.soffice`, para todos los usuarios.	"Cómo configurar los archivos de inicio para los usuarios en Trusted Extensions" en la página 146
Iniciar sesión en modo a prueba de fallos.	Se corrigen los archivos de inicialización de usuario defectuosos.	"Cómo iniciar una sesión en modo a prueba de fallos en Trusted Extensions" en la página 149

▼ Cómo modificar atributos de etiquetas de usuarios predeterminados

Puede modificar los atributos de etiquetas de usuarios predeterminados durante la configuración del primer sistema. Los cambios se deben copiar en cada sistema Trusted Extensions.

Precaución – Debe completar esta tarea antes de que los usuarios comunes accedan al sistema.

Antes de empezar

Debe estar con el rol de administrador de la seguridad en la zona global. Para obtener detalles, consulte "Cómo entrar en la zona global en Trusted Extensions" en la página 126.

1. **Revise la configuración predeterminada de los atributos de usuario en el archivo `/etc/security/tsol/label_encodings`.**

   Para conocer los valores predeterminados, consulte la Tabla 1–2 en "Planificación de la seguridad del usuario en Trusted Extensions" en la página 34.

2. **Modifique la configuración de los atributos de usuario en el archivo `label_encodings`.**

3. **Distribuya una copia del archivo en cada sistema Trusted Extensions.**

Precaución – El archivo `label_encodings` debe ser igual en todos los sistemas. Para conocer un método de distribución, consulte "Cómo copiar archivos en medios portátiles en Trusted Extensions" en la página 78 y "Cómo copiar archivos desde medios portátiles en Trusted Extensions" en la página 79.

▼ Cómo modificar los valores predeterminados de policy.conf

La modificación de los valores predeterminados de `policy.conf` en Trusted Extensions es idéntica a la modificación de cualquier archivo del sistema relacionado con la seguridad en Oracle Solaris. Utilice este procedimiento para cambiar los valores predeterminados para todos los usuarios de un sistema.

Antes de empezar Debe estar con el rol de usuario `root` en la zona global. Para obtener detalles, consulte "Cómo entrar en la zona global en Trusted Extensions" en la página 126.

1 Revise los valores predeterminados en el archivo `/etc/security/policy.conf`.

Para conocer las palabras clave de Trusted Extensions consulte la Tabla 10–1.

2 Modifique la configuración.

Ejemplo 11–1 Cambio de la configuración del tiempo de inactividad del sistema

En este ejemplo, el administrador de la seguridad desea que los sistemas inactivos regresen a la pantalla de inicio de sesión. El valor predeterminado bloquea los sistemas inactivos. Por lo tanto, el rol de usuario `root` agrega el par `IDLECMD` *palabra clave=valor* al archivo `/etc/security/policy.conf` de la siguiente manera:

```
IDLECMD=LOGOUT
```

El administrador también desea que los sistemas permanezcan inactivos durante un período más corto antes de que se cierre la sesión. Por lo tanto, el rol de usuario `root` agrega el par `IDLETIME` *palabra clave=valor* al archivo `policy.conf` de la siguiente manera:

```
IDLETIME=10
```

Así, el sistema cierra la sesión del usuario si el sistema permanece inactivo durante 10 minutos.

Tenga en cuenta que si el usuario de inicio de sesión asume un rol, los valores `IDLECMD` e `IDLETIME` del usuario están vigentes para ese rol.

Ejemplo 11–2 Modificación del conjunto de privilegios básico de cada usuario

En este ejemplo, el administrador de la seguridad de una instalación grande no desea que los usuarios comunes vean los procesos de otros usuarios. Por lo tanto, en todos los sistemas que estén configurados con Trusted Extensions, el rol de usuario `root` elimina `proc_info` del conjunto básico de privilegios. La configuración `PRIV_DEFAULT` del archivo `/etc/policy.conf` no tiene comentarios y se modifica de la siguiente manera:

```
PRIV_DEFAULT=basic,!proc_info
```

Ejemplo 11–3 Asignación de las autorizaciones relacionadas con la impresión a todos los usuarios de un sistema

En este ejemplo, la seguridad del sitio permite que un equipo de quiosco público imprima sin etiquetas. En el quiosco público, el rol `root` modifica el valor para `AUTHS_GRANTED` en el archivo `/etc/security/policy.conf`. La próxima vez que inicie, los trabajos de impresión de todos los usuarios de este quiosco se imprimen sin las etiquetas de las páginas.

```
AUTHS_GRANTED=solaris.print.unlabeled
```

A continuación, el administrador decide quitar las páginas de la carátula y del ubicador para ahorrar papel. El administrador modifica la entrada `policy.conf`.

```
AUTHS_GRANTED=solaris.print.unlabeled,solaris.print.nobanner
```

Después de reiniciar el quiosco público, se quitan todas las etiquetas de los trabajos de impresión y no cuentan con carátulas ni páginas de ubicador.

▼ Cómo configurar los archivos de inicio para los usuarios en Trusted Extensions

Los usuarios pueden introducir los archivos `.copy_files` y `.link_files` en el directorio principal en la etiqueta que corresponde a la etiqueta de sensibilidad mínima. Los usuarios también pueden modificar los archivos `.copy_files` y `.link_files` que ya existen en la etiqueta mínima de los usuarios. Este procedimiento sirve para que el rol de administrador automatice la configuración del sitio.

Antes de empezar Debe estar con el rol de administrador del sistema en la zona global. Para obtener detalles, consulte "Cómo entrar en la zona global en Trusted Extensions" en la página 126.

1 Cree dos archivos de inicio de Trusted Extensions.

Agregará los archivos `.copy_files` y `.link_files` a la lista de archivos de inicio.

```
# cd /etc/skel
# touch .copy_files .link_files
```

2 Personalice el archivo `.copy_files`.

a. En un editor, escriba el nombre completo de la ruta del archivo `.copy_files`.

```
# vi /etc/skel/.copy_files
```

b. Escriba en `.copy_files`, uno por línea, los archivos que se copiarán en el directorio principal del usuario en todas las etiquetas.

Consulte "Archivos `.copy_files` y `.link_files`" en la página 141 para obtener ideas. Para ver archivos de muestra, consulte el Ejemplo 11–4.

3. **Personalice el archivo `.link_files`.**

   a. **En un editor, escriba el nombre completo de la ruta de `.link_files`.**

      ```
      # vi /etc/skel/.link_files
      ```

   b. **Escriba en `.link_files`, uno por línea, los archivos que se enlazarán con el directorio principal del usuario en todas las etiquetas.**

4. **Personalice los otros archivos de inicio para sus usuarios.**

   - Para ver una explicación de los archivos que se deben incluir en los archivos de inicio, consulte "Personalización de un entorno de trabajo del usuario" de *Administración de Oracle Solaris: tareas comunes*.
   - Para obtener detalles, consulte "Cómo personalizar los archivos de inicialización de usuario" de *Administración de Oracle Solaris: tareas comunes*.

5. **(Opcional) Cree un subdirectorio `skelP` para los usuarios cuyo shell predeterminado sea un shell del perfil.**

   `P` indica el shell Profile.

6. **Copie los archivos de inicio personalizados en el directorio de estructura básica apropiado.**

7. **Utilice el nombre de ruta `skel`*X* apropiado cuando cree el usuario.**

   X representa la letra con la que comienza el nombre del shell; por ejemplo, `B` para un shell Bourne, `K` para un shell Korn, `C` para un shell C y `P` para un shell Profile.

Ejemplo 11–4 Personalización de los archivos de inicio para los usuarios

En este ejemplo, el administrador del sistema configura archivos para el directorio principal de cada usuario. Los archivos se encuentran en su lugar antes de que cualquier usuario inicie sesión. Los archivos están en la etiqueta mínima del usuario. En este sitio, el shell predeterminado de los usuarios es el shell C.

El administrador del sistema crea un archivo `.copy_files` y un archivo `.link_files` con el siguiente contenido:

```
## .copy_files for regular users
## Copy these files to my home directory in every zone
.mailrc
.mozilla
.soffice
:wq

## .link_files for regular users with C shells
## Link these files to my home directory in every zone
.bashrc
```

```
.bashrc.user
.cshrc
.login
:wq

## .link_files for regular users with Korn shells
# Link these files to my home directory in every zone
.ksh
.profile
:wq
```

En los archivos de inicialización del shell, el administrador garantiza que los trabajos de impresión de los usuarios se dirijan a una impresora con etiquetas.

```
## .cshrc file
setenv PRINTER conf-printer1
setenv LPDEST  conf-printer1

## .ksh file
export PRINTER conf-printer1
export LPDEST  conf-printer1
```

Los archivos personalizados se copian en el directorio de estructura básica apropiado.

```
$ cp .copy_files .link_files .bashrc .bashrc.user .cshrc \
.login .profile .mailrc /etc/skelC
$ cp .copy_files .link_files .ksh .profile .mailrc \
/etc/skelK
```

Errores más frecuentes

Si crea archivos `.copy_files` en la etiqueta más baja y, a continuación, inicia sesión en una zona superior para ejecutar el comando `updatehome`, y el comando falla con un error de acceso, intente realizar lo siguiente:

- Verifique que desde la zona de nivel superior pueda ver el directorio de nivel inferior.

  ```
  higher-level zone# ls /zone/lower-level-zone/home/username
  ACCESS ERROR: there are no files under that directory
  ```

- Si no puede ver el directorio, reinicie el servicio de montaje automático en la zona de nivel superior:

  ```
  higher-level zone# svcadm restart autofs
  ```

Salvo que use montajes de NFS para los directorios principales, el montador automático de la zona de nivel superior debe montar en bucle de retorno de `/zone/`*lower-level-zone*`/export/home/`*username* a `/zone/`*lower-level-zone*`/home/`*username*.

▼ Cómo iniciar una sesión en modo a prueba de fallos en Trusted Extensions

En Trusted Extensions, el inicio de sesión en modo a prueba de fallos está protegido. Si un usuario común personalizó los archivos de inicialización del shell y ahora no puede iniciar sesión, puede utilizar el inicio de sesión en modo a prueba de fallos para reparar los archivos del usuario.

Antes de empezar Debe conocer la contraseña de usuario root.

1. **Escriba su nombre de usuario en la pantalla de inicio de sesión.**
2. **En la parte inferior de la pantalla, seleccione Solaris Trusted Extensions Failsafe Session del menú de escritorio.**
3. **Cuando se solicite, escriba su contraseña.**
4. **Cuando se solicite una contraseña adicional, escriba la contraseña de usuario root.**

   Ya puede depurar los archivos de inicialización del usuario.

Gestión de usuarios y derechos (mapa de tareas)

En Trusted Extensions, asume el rol de administrador de la seguridad para administrar usuarios, autorizaciones, derechos y roles. El siguiente mapa de tareas describe las tareas comunes que debe realizar para los usuarios que operan en un entorno con etiquetas.

Tarea	Descripción	Para obtener instrucciones
Modificar el rango de etiquetas de un usuario.	Se modifican las etiquetas en las que el usuario puede trabajar. Es posible que las modificaciones restrinjan o amplíen el rango que el archivo `label_encodings` permite.	"Cómo modificar el rango de etiquetas de un usuario" en la página 150
Crear un perfil de derechos para las autorizaciones convenientes.	Existen varias autorizaciones que pueden ser útiles para los usuarios comunes. Se crea un perfil para los usuarios que cumplen los requisitos para tener estas autorizaciones.	"Cómo crear perfiles de derechos para autorizaciones convenientes" en la página 151
Crear un escritorio que restrinja el acceso de un usuario a algunas aplicaciones.	Se asignan perfiles de derechos que permiten a los usuarios abrir sólo las aplicaciones que aparece en el escritorio. La línea de comandos no está disponible o, de manera opcional, acepta algunos comandos.	"Cómo limitar el acceso de un usuario a las aplicaciones de escritorio" en la página 152

Tarea	Descripción	Para obtener instrucciones
Modificar el conjunto de privilegios predeterminado del usuario.	Se elimina un privilegio del conjunto de privilegios predeterminado del usuario.	"Cómo restringir el conjunto de privilegios de un usuario" en la página 154
Impedir el bloqueo de cuentas para usuarios concretos.	Los usuarios que pueden asumir un rol deben tener desactivado el bloqueo de cuentas.	"Cómo impedir el bloqueo de cuentas de los usuarios" en la página 154
Permitir que un usuario vuelva a etiquetar datos.	Se autoriza a un usuario a reducir o aumentar el nivel de la información.	"Cómo habilitar a un usuario para que cambie el nivel de seguridad de los datos" en la página 155
Eliminar a un usuario del sistema.	Se elimina por completo a un usuario y sus procesos.	"Cómo suprimir una cuenta de usuario de un sistema Trusted Extensions" en la página 156

▼ Cómo modificar el rango de etiquetas de un usuario

Puede que desee ampliar el rango de etiquetas de un usuario para proporcionarle acceso de lectura a una aplicación administrativa. Por ejemplo, un usuario que puede iniciar sesión en la zona global puede ver una lista de los sistemas que se ejecutan en una determinada etiqueta. El usuario puede ver el contenido, pero no puede modificarlo.

Como alternativa, es posible que desee restringir el rango de etiquetas del usuario. Por ejemplo, un usuario invitado puede estar limitado a una etiqueta.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

- **Realice una de las siguientes acciones:**

  - **Para ampliar el rango de etiquetas del usuario, asigne una acreditación superior.**

    ```
    # usermod -K min_label=INTERNAL -K clearance=ADMIN_HIGH jdoe
    ```

    También puede ampliar el rango de etiquetas del usuario disminuyendo la etiqueta mínima.

    ```
    # usermod -K min_label=PUBLIC -K clearance=INTERNAL jdoe
    ```

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

  - **Para restringir el rango de etiquetas a una etiqueta, haga la acreditación igual que la etiqueta mínima.**

    ```
    # usermod -K min_label=INTERNAL -K clearance=INTERNAL jdoe
    ```

▼ Cómo crear perfiles de derechos para autorizaciones convenientes

Cuando la política de seguridad del sitio lo permita, quizás desee crear un perfil de derechos que contenga las autorizaciones para los usuarios que pueden realizar tareas que requieren autorización. Para habilitar a todos los usuarios de un sistema en particular que se van a autorizar, consulte "Cómo modificar los valores predeterminados de `policy.conf`" en la página 145.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1 Cree un perfil de derechos que contenga una o más de las siguientes autorizaciones.

Para conocer el procedimiento paso a paso, consulte "Cómo crear o cambiar un perfil de derechos" de *Administración de Oracle Solaris: servicios de seguridad*.

Las siguientes autorizaciones pueden ser convenientes para los usuarios:

- `solaris.device.allocate`: autoriza a un usuario a asignar un dispositivo periférico, como un micrófono o un CD-ROM.

  De manera predeterminada, los usuarios de Oracle Solaris pueden leer y escribir en un CD-ROM. Sin embargo, en Trusted Extensions, solamente los usuarios que pueden asignar un dispositivo pueden acceder a la unidad de CD-ROM. Para asignar la unidad para su uso se requiere autorización. Por lo tanto, para leer y escribir en un CD-ROM en Trusted Extensions, los usuarios necesitan la autorización Allocate Device.
- `solaris.label.file.downgrade`: autoriza a un usuario a disminuir el nivel de seguridad de un archivo.
- `solaris.label.file.upgrade`: autoriza a un usuario a aumentar el nivel de seguridad de un archivo.
- `solaris.label.win.downgrade`: autoriza a un usuario a seleccionar información de un archivo de nivel superior y colocarla en un archivo de nivel inferior.
- `solaris.label.win.noview`: autoriza a un usuario a mover información sin ver la información que se mueve.
- `solaris.label.win.upgrade`: autoriza a un usuario a seleccionar información de un archivo de nivel inferior y colocarla en un archivo de nivel superior.
- `solaris.login.remote`: autoriza a un usuario a iniciar sesión de manera remota.
- `solaris.print.ps`: autoriza a que un usuario imprima archivos de PostScript.
- `solaris.print.nobanner`: autoriza a un usuario a que haga copias impresas sin la página de la carátula.
- `solaris.print.unlabeled` : autoriza a un usuario a que haga copias impresas que no muestren etiquetas.
- `solaris.system.shutdown`: autoriza a un usuario a apagar el sistema y cerrar una zona.

2 **Asigne el perfil de derechos a un usuario o a un rol.**

Para conocer el procedimiento paso a paso, consulte "Cómo cambiar las propiedades RBAC de un usuario" de *Administración de Oracle Solaris: servicios de seguridad*.

▼ Cómo limitar el acceso de un usuario a las aplicaciones de escritorio

La seguridad del sitio puede requerir que los usuarios sólo tengan acceso a las aplicaciones que pueden abrir desde un icono de escritorio. Este procedimiento asigna perfiles de derechos que limitan el acceso de los usuarios solamente a las aplicaciones requeridas.

Nota – En el escritorio de Trusted Extensions, la ejecución de comandos siempre se basa en los perfiles de derechos.

Para permitir que todos los usuarios de un sistema en particular tengan dicha autorización, consulte "Cómo modificar los valores predeterminados de `policy.conf`" en la página 145.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1 **Cree un perfil de derechos denominado perfil de derechos Desktop Applets que permita a los usuarios de Oracle Solaris ejecutar los applets básicos en su escritorio.**

Para conocer el procedimiento, consulte "Cómo restringir a un usuario a las aplicaciones de escritorio" de *Administración de Oracle Solaris: servicios de seguridad*.

2 **Cree otro perfil de derechos que permita a los usuarios de Trusted Extensions ejecutar los applets de confianza requeridos en su escritorio.**

Las líneas se ajustaron con fines de visualización.

```
# profiles -p "Trusted Desktop Applets"
profiles:Trusted Desktop Applets>
set desc="Can use trusted desktop applications except terminal"
profiles:Trusted Desktop Applets> add cmd=/usr/dt/config/tsoljds-migration;end
profiles:Trusted Desktop Applets> add cmd=/usr/bin/tsoljds-xagent;end
profiles:Trusted Desktop Applets> commit
```

3 **Agregue el perfil Desktop Applets como un perfil de derechos complementario del perfil Trusted Desktop Applets.**

Ha creado este perfil de derechos en el Paso 2.

```
profiles:Trusted Desktop Applets> add profiles="Desktop Applets"
profiles:Trusted Desktop Applets> commit
profiles:Trusted Desktop Applets> exit
```

4 **Verifique que el perfil de derechos Trusted Desktop Applets contenga las entradas correctas.**

Revise las entradas en busca de errores, por ejemplo, errores ortográficos, omisiones o repeticiones.

```
# profiles -p "Trusted Desktop Applets" info
Found profile in files repository.
name=Trusted Desktop Applets
desc=Can use trusted desktop applications except terminal
profiles=Desktop Applets
cmd=/usr/dt/config/tsoljds-migration
cmd=/usr/bin/tsoljds-xagent
```

Consejo – Puede crear un perfil de derechos para una aplicación o una clase de aplicaciones que tengan iconos de escritorio. A continuación, agregue el perfil de derechos Trusted Desktop Applets como un perfil de derechos complementario para el acceso al escritorio.

5 **Asigne al usuario los perfiles de derechos `Trusted Desktop Applets` y `Stop`.**

```
# usermod -P "Trusted Desktop Applets,Stop" username
```

Este usuario puede utilizar el escritorio de confianza, pero no puede iniciar una ventana de terminal, actuar como usuario de consola ni tener ninguno de los derechos incluidos en el perfil de derechos de usuario de Solaris básico.

Ejemplo 11–5 Cómo permitir que un usuario del escritorio abra una ventana de terminal

En este ejemplo, el administrador permite a un usuario del escritorio abrir una ventana de terminal. El administrador ya creó el perfil de derechos Desktop Applets para los usuarios del escritorio de Oracle Solaris y el perfil de derechos Trusted Desktop Applets para los usuarios del escritorio de Trusted Extensions en el depósito LDAP.

En primer lugar, el administrador crea el perfil de derechos Terminal Window y verifica su contenido.

```
# profiles -p "Terminal Window" -S ldap
profiles:Terminal Window> set desc="Can open a terminal window"
profiles:Terminal Window> add cmd=/usr/bin/gnome-terminal;end
profiles:Terminal Window> commit
profiles:Terminal Window> exit
# profiles -p "Terminal Window" info
Found profile in ldap repository.
name=Terminal Window
desc=Can open a terminal window
cmd=/usr/bin/gnome-terminal
```

A continuación, el administrador asigna este perfil de derechos y el perfil de derechos All a los usuarios del escritorio que necesitan ventanas de terminal para realizar sus tareas. Sin el perfil de derechos All, los usuarios no podrán ejecutar los comandos UNIX que no requieren privilegios, como `ls` y `cat`.

```
# usermod -P "Trusted Desktop Applets,Terminal Window,All,Stop" -S ldap jdoe
```

Con este conjunto de perfiles de derechos, el usuario `jdoe` puede utilizar el escritorio y las ventanas de terminal, pero no puede actuar como usuario de consola ni tener ninguno de los derechos incluidos en el perfil de derechos de usuario de Solaris básico.

▼ Cómo restringir el conjunto de privilegios de un usuario

Puede que la seguridad del sitio requiera que a los usuarios se les otorgue menos privilegios que los asignados de manera predeterminada.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

- **Elimine uno o varios de los privilegios del conjunto `basic`.**

Precaución – No elimine los privilegios `proc_fork` o `proc_exec`. Sin estos privilegios, los usuarios no pueden utilizar el sistema.

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

Al eliminar el privilegio `proc_info`, impide que el usuario examine los procesos que no se originan desde el usuario. Con la eliminación del privilegio `proc_session`, se impide que el usuario examine cualquier proceso que se encuentre fuera de su sesión actual. Con la eliminación del privilegio `file_link_any`, se impide que el usuario establezca enlaces físicos con archivos que no sean de su propiedad.

Véase también Para ver un ejemplo de la recopilación de restricciones de privilegios en un perfil de derechos, consulte los ejemplos que aparecen a continuación de "Cómo crear o cambiar un perfil de derechos" de *Administración de Oracle Solaris: servicios de seguridad*.

Para restringir los privilegios de todos los usuarios en un sistema, consulte el Ejemplo 11–2.

▼ Cómo impedir el bloqueo de cuentas de los usuarios

Realice este procedimiento para todos los usuarios que pueden asumir un rol.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

- **Desactive el bloqueo de cuentas para un usuario local.**

```
# usermod -K lock_after_retries=no jdoe
```

Para desactivar el bloqueo de cuentas para un usuario LDAP, especifique el depósito LDAP.

```
# usermod -S ldap -K lock_after_retries=no jdoe
```

▼ Cómo habilitar a un usuario para que cambie el nivel de seguridad de los datos

Se puede autorizar a un usuario común o a un rol a cambiar el nivel de seguridad, o las etiquetas, de los archivos y los directorios o del texto seleccionado. El usuario o el rol, además de tener la autorización, deben estar configurados para trabajar en más de una etiqueta. Las zonas con etiquetas deben estar configuradas de modo que se permita volver a etiquetar. Para conocer el procedimiento, consulte "Cómo permitir que los archivos se vuelvan a etiquetar desde una zona con etiquetas" en la página 180.

Precaución – El cambio del nivel de seguridad de los datos es una operación privilegiada. Esta tarea la deben realizar únicamente los usuarios de confianza.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1. **Siga el procedimiento "Cómo crear perfiles de derechos para autorizaciones convenientes" en la página 151 para crear un perfil de derechos.**

   Las siguientes autorizaciones habilitan al usuario para que vuelva a etiquetar un archivo:

   - Downgrade File Label
   - Upgrade File Label

   Las siguientes autorizaciones habilitan al usuario para que vuelva a etiquetar la información de un archivo:

   - Downgrade DragNDrop or CutPaste Info
   - DragNDrop or CutPaste Info Without Viewing
   - Upgrade DragNDrop or CutPaste Info

2. **Asigne el perfil a los usuarios y los roles adecuados.**

   Para conocer el procedimiento paso a paso, consulte "Cómo cambiar las propiedades RBAC de un usuario" de *Administración de Oracle Solaris: servicios de seguridad*.

▼ Cómo suprimir una cuenta de usuario de un sistema Trusted Extensions

Cuando se elimina del sistema a un usuario, debe asegurarse de que también se supriman el directorio principal del usuario y cualquier otro objeto que sea propiedad del usuario. Como alternativa a la eliminación de objetos que sean propiedad del usuario, puede transferir la propiedad de estos objetos a un usuario válido.

También debe asegurarse de que se supriman todos los trabajos por lotes que estén asociados con el usuario. Ningún objeto o proceso que pertenezca a un usuario eliminado puede permanecer en el sistema.

Antes de empezar Debe estar con el rol de administrador del sistema en la zona global.

1. **Archive el directorio principal del usuario en cada etiqueta.**
2. **Archive los archivos de correo del usuario en cada etiqueta.**
3. **Suprima la cuenta de usuario.**

   ```
   # userdel -r jdoe
   ```

4. **En cada zona con etiquetas, suprima manualmente los directorios del usuario y sus archivos de correo.**

Nota – Deberá buscar y suprimir los archivos temporales del usuario en todas las etiquetas, como los archivos de los directorios `/tmp`.

Para conocer otras consideraciones, consulte "Prácticas de eliminación de usuarios" en la página 122.

◆ ◆ ◆ CAPÍTULO 12

Administración remota en Trusted Extensions (tareas)

En este capítulo, se describe cómo configurar un sistema Trusted Extensions para administrarlo de manera remota, y cómo realizar las tareas de inicio de sesión y administración.

Nota – Los métodos de configuración que requieren los sistemas remotos y sin periféricos no cumplen con los criterios de una configuración evaluada. Para obtener más información, consulte "Comprensión de la política de seguridad del sitio" en la página 28.

Administración remota en Trusted Extensions

La administración remota presenta un riesgo considerable para la seguridad, en particular, en el caso de los usuarios de sistemas que no son de confianza. De manera predeterminada, Trusted Extensions no permite la administración remota desde ningún sistema.

Hasta que se configura la red, se asigna la plantilla de seguridad `admin_low` a todos los hosts remotos, es decir, se los reconoce como hosts sin etiquetas. Hasta que se configuran las zonas con etiquetas, la única zona disponible es la zona global. En Trusted Extensions, la zona global es la zona administrativa. Sólo un rol puede acceder a ella. En concreto, una cuenta debe tener un rango de etiquetas entre `ADMIN_LOW` y `ADMIN_HIGH` para acceder a la zona global.

En este estado inicial, los sistemas Trusted Extensions permanecen protegidos frente a los ataques remotos mediante varios mecanismos. Entre los mecanismos, se incluyen los valores `netservices`, la política `ssh` predeterminada, la política de inicio de sesión predeterminada y la política PAM predeterminada.

- En la instalación, ningún servicio remoto excepto el shell seguro tiene permiso para escuchar en la red.

  Sin embargo, el servicio `ssh` no se puede utilizar para el inicio de sesión remoto mediante `root` o un rol debido a las políticas `ssh`, de inicio de sesión y PAM.
- La cuenta de usuario `root` no se puede utilizar para los inicios de sesión remotos porque `root` es un rol. Los roles no pueden iniciar sesión, de acuerdo con PAM.

  Incluso si `root` se modifica a una cuenta de usuario, las políticas `ssh` y de inicio de sesión predeterminadas impiden los inicios de sesión remotos por parte del usuario `root`.
- Dos valores predeterminados de PAM impiden los inicios de sesión remotos.

  El módulo `pam_roles` rechaza los inicios de sesión locales y remotos desde las cuentas de tipo `role`.

  Un módulo PAM de Trusted Extensions, `pam_tsol_account`, rechaza los inicios de sesión remotos en la zona global, a menos que se utilice el protocolo CIPSO. Esta política tiene por objeto que la administración remota se realice por medio de otro sistema Trusted Extensions.

Por lo tanto, al igual que en un sistema Oracle Solaris, se debe configurar la administración remota. Trusted Extensions agrega dos requisitos de configuración, el rango de etiquetas necesario para acceder a la zona global y el módulo `pam_tsol_account`.

Métodos para administrar sistemas remotos en Trusted Extensions

En Trusted Extensions, debe utilizar el protocolo `ssh` con autenticación basada en host para acceder al sistema remoto y administrarlo. La autenticación basada en host permite que una cuenta de usuario con nombre idéntico asuma un rol en el sistema Trusted Extensions remoto.

Cuando se utiliza la autenticación basada en host, el cliente `ssh` envía el nombre de usuario original y el nombre de rol al sistema remoto, es decir, el servidor. Con esta información, el servidor puede transferir suficiente contenido al módulo `pam_roles` para permitir que se asuma un rol sin que se inicie sesión en el servidor con la cuenta de usuario.

Los siguientes métodos de administración remota son posibles en Trusted Extensions:

- **Administración desde un sistema Trusted Extensions**: para contar con la administración remota más segura, ambos sistemas asignan su igual a una plantilla de seguridad CIPSO. Consulte el Ejemplo 12–1.
- **Administración desde un sistema sin etiquetas**: si la administración mediante un sistema Trusted Extensions no es práctica, la política del protocolo de red se puede hacer menos estricta mediante la especificación de la opción `allow_unlabeled` para el módulo `pam_tsol_account` en el archivo `pam.conf`.

  Si esta política se hace menos estricta, la plantilla de seguridad predeterminada se debe cambiar para que los sistemas arbitrarios no puedan acceder a la zona global. La plantilla `admin_low` debe usarse con moderación, y la dirección comodín `0.0.0.0` no se debe establecer de manera predetermina en la etiqueta `ADMIN_LOW`. Para obtener detalles, consulte "Cómo limitar los hosts que se pueden contactar en la red de confianza" en la página 229.

En cualquier escenario administrativo, si desea utilizar el rol de usuario `root` para el inicio de sesión remoto, debe hacer más flexible la política PAM mediante la especificación de la opción `allow_remote` para el módulo `pam_roles`.

Por lo general, los administradores utilizan el comando `ssh` para administrar sistemas remotos desde la línea de comandos. Con la opción `-X`, se pueden usar las interfaces gráficas de usuario administrativas de Trusted Extensions.

Además, puede configurar el sistema Trusted Extensions remoto con el servidor Xvnc. Luego, se puede usar una conexión de informática en red virtual (VNC, Virtual Network Computing) para visualizar el escritorio remoto de varios niveles y administrar el sistema. Consulte "Cómo configurar un sistema Trusted Extensions con Xvnc para el acceso remoto" en la página 162.

Configuración y administración de sistemas remotos en Trusted Extensions (mapa de tareas)

Tras habilitar la administración remota antes de reiniciar el sistema remoto en Trusted Extensions, puede configurar el sistema mediante la informática en red virtual (VNC) o el protocolo `ssh`.

Tarea	Descripción	Para obtener instrucciones
Habilitar la administración remota de un sistema Trusted Extensions.	Permite la administración de sistemas Trusted Extensions desde clientes `ssh` especificados.	"Cómo habilitar la administración remota de un sistema Trusted Extensions remoto" en la página 160
Habilitar la informática en red virtual (VNC).	Desde cualquier cliente, se utiliza el servidor Xvnc en un sistema Trusted Extensions remoto para mostrar la sesión de varios niveles del servidor al cliente.	"Cómo configurar un sistema Trusted Extensions con Xvnc para el acceso remoto" en la página 162

Tarea	Descripción	Para obtener instrucciones
Iniciar sesión de manera remota en un sistema Trusted Extensions.	Se asume un rol en el sistema remoto para administrarlo.	"Cómo realizar las tareas de inicio de sesión y administración en un sistema Trusted Extensions remoto" en la página 164

Nota – Consulte su política de seguridad para determinar qué métodos de administración remota están permitidos en su sitio.

▼ Cómo habilitar la administración remota de un sistema Trusted Extensions remoto

En este procedimiento, se habilita la autenticación basada en host en un sistema remoto Oracle Solaris antes de agregar la función Trusted Extensions. El sistema remoto es el servidor `ssh`.

Antes de empezar El sistema remoto se instala con Oracle Solaris, y es posible acceder a ese sistema.

1 En ambos sistemas, habilite la autenticación basada en host.

Para conocer el procedimiento, consulte "Cómo configurar la autenticación basada en host para Secure Shell" de *Administración de Oracle Solaris: servicios de seguridad*.

Nota – No utilice el comando `cat`. Copie y pegue la clave pública mediante una conexión `ssh`. Si su cliente ssh no es un sistema Oracle Solaris, siga las instrucciones de la plataforma para la configuración de un cliente `ssh` con autenticación basada en host.

Después de completar este paso, tendrá una cuenta de usuario en ambos sistemas que puede asumir el rol de usuario `root`. Se asigna el mismo UID, GID y asignación de rol a las cuentas. También ha generado pares de claves públicas/privadas y tiene claves públicas compartidas.

2 En el servidor `ssh`, haga más flexible la política `ssh` para permitir que `root` inicie sesión de manera remota.

```
# vi /etc/ssh/sshd_config
## Permit remote login by root
PermitRootLogin yes
```

Un paso posterior limita el inicio de sesión de `root` a un sistema y un usuario concretos.

Nota – Dado que el administrador asumirá el rol de usuario `root`, no necesita hacer menos estricta la política de inicio de sesión que impide que `root` inicie sesión de manera remota.

3 En el servidor `ssh`, reinicie el servicio `ssh`.

```
# svcadm restart ssh
```

4 En el servidor `ssh`, en el directorio principal de `root`, especifique el host y el usuario para la autenticación basada en host.

```
# cd
# vi .shosts
client-host username
```

El archivo `.shosts` permite que *username* en el sistema *client-host* asuma el rol de usuario `root` en el servidor, cuando se comparte una clave pública/privada.

5 En el servidor `ssh`, haga menos estrictas las dos políticas PAM.

a. Permita el inicio de sesión remoto mediante roles.

```
# vi /etc/pam.conf
...
# Default definition for Account management
# Used when service name is not explicitly mentioned for account management
#
# other   account requisite    pam_roles.so.1
# Enable remote role assumption
other   account requisite    pam_roles.so.1   allow_remote
...
```

Esta política permite que *username* en el sistema *client-host* asuma un rol en el servidor.

b. Permita que los hosts sin etiquetas establezcan contacto con el sistema remoto Trusted Extensions.

```
# vi /etc/pam.conf
# Default definition for Account management
# Used when service name is not explicitly mentioned for account management
#
# other   account requisite    pam_roles.so.1
# Enable remote role assumption
other   account requisite    pam_roles.so.1   allow_remote
#
other   account required     pam_unix_account.so.1
# other   account required     pam_tsol_account.so.1
# Enable unlabeled access to TX system
other   account required     pam_tsol_account.so.1  allow_unlabeled
```

c. Copie el archivo `pam.conf` modificado en `pam.conf.site`.

```
# cp /etc/pam.conf /etc/pam.conf.site
```

6 Pruebe la configuración.

a. Abra un nuevo terminal en el sistema remoto.

b. En *client-host*, en una ventana de *username*, asuma el rol de usuario `root` en el sistema remoto.

```
% ssh -l root remote-system
```

7 Después de comprobar que la configuración funciona, habilite Trusted Extensions en el sistema remoto y reinicie el sistema.

```
# svcadm enable -s labeld
# /usr/sbin/reboot
```

Ejemplo 12–1 Asignación del tipo de host CIPSO para la administración remota

En este ejemplo, el administrador utiliza un sistema Trusted Extensions para configurar un host Trusted Extensions remoto. Para ello, el administrador utiliza el comando `tncfg` en cada sistema con el fin de definir el tipo de host del sistema equivalente.

remote-system `# tncfg -t cipso add host=192.168.1.12` *Client-host*

client-host `# tncfg -t cipso add host=192.168.1.22` *Remote system*

Dado que un sistema sin etiquetas también puede configurar el host Trusted Extensions remoto, el administrador deja la opción `allow_unlabeled` en el archivo `pam.conf` del host remoto.

Errores más frecuentes Cuando el administrador realiza una actualización a una nueva versión del SO Oracle Solaris, no se instala un nuevo archivo `pam.conf`. Para obtener una descripción de la acción de archivo `preserve=true` en la actualización, consulte la página del comando man `pkg`(5).

▼ Cómo configurar un sistema Trusted Extensions con Xvnc para el acceso remoto

La tecnología de informática en red virtual (VNC) conecta un cliente a un servidor remoto y, luego, muestra el escritorio del servidor remoto en una ventana en el cliente. Xvnc es la versión UNIX de VNC, que se basa en un servidor X estándar. En Trusted Extensions, un cliente de cualquier plataforma puede conectarse a un servidor Xvnc que ejecuta Trusted Extensions, iniciar sesión en el servidor Xvnc y, luego, visualizar un escritorio de varios niveles y trabajar en él.

Para obtener más información, consulte las páginas del comando man `Xvnc`(1) y `vncconfig`(1).

Antes de empezar Debe tener instalado y configurado Trusted Extensions en este sistema que se utilizará como servidor Xvnc. La zona global de este sistema tiene una dirección IP fija, es decir, no utiliza el perfil de configuración de red automático, como se describe en la página del comando man `netcfg(1M)`.

Este sistema reconoce los clientes VNC por nombre de host o por dirección IP. En concreto, la plantilla de seguridad `admin_low` identifica de forma explícita o mediante un comodín los sistemas que pueden ser clientes VNC de este servidor. Para obtener más información sobre cómo configurar la conexión de manera segura, consulte "Cómo limitar los hosts que se pueden contactar en la red de confianza" en la página 229.

Si actualmente ejecuta una sesión GNOME en la consola del futuro servidor Xvnc de Trusted Extensions, no tiene habilitado el uso compartido del escritorio.

Tiene el rol de usuario `root` en la zona global del futuro servidor Xvnc de Trusted Extensions.

1 Cargue o actualice el software Xvnc.

```
# packagemanager &
```

En la interfaz gráfica de usuario Package Manager, busque "vnc" y elija entre los servidores disponibles. Una opción es el software de servidor TigerVNC X11/VNC.

2 Habilite X Display Manager Control Protocol.

Modifique el archivo de configuración personalizado de GNOME Display Manager (gdm). En el archivo `/etc/gdm/custom.conf`, escriba `Enable=true` en el encabezado `[xdmcp]`.

```
[xdmcp]
Enable=true
```

3 Inserte la siguiente línea en el archivo `/etc/gdm/Xsession` cerca de la línea 27.

```
DISPLAY=unix:$(echo $DISPLAY|sed -e s/::ffff://|cut -d: -f2)
```

4 Habilite el servicio del servidor Xvnc.

```
# svcadm enable xvnc-inetd
```

5 Cierre todas las sesiones GNOME activas en este servidor.

```
# svcadm restart gdm
```

Espere aproximadamente un minuto para que se reinicie el administrador del escritorio. A continuación, puede conectarse un cliente VNC.

6 Verifique que el software Xvnc esté habilitado.

```
# svcs | grep vnc
```

7 En cada cliente VNC del servidor Xvnc, instale el software del cliente VNC.

Para el sistema cliente, puede elegir el software. Puede utilizar el software VNC desde el depósito de Oracle Solaris.

8 Para visualizar el espacio de trabajo del servidor Xvnc en un cliente VNC, lleve a cabo los siguientes pasos:

a. En una ventana de terminal del cliente, conéctese al servidor.

```
% /usr/bin/vncviewer Xvnc-server-hostname
```

Para conocer las opciones de comandos, consulte la página del comando man `vncviewer`(1).

b. En la ventana que aparece, escriba su nombre de usuario y contraseña.

Continúe con el proceso de inicio de sesión. Para obtener una descripción del resto de los pasos, consulte "Inicio de sesión en Trusted Extensions" de *Guía del usuario de Oracle Solaris Trusted Extensions*.

▼ Cómo realizar las tareas de inicio de sesión y administración en un sistema Trusted Extensions remoto

Este procedimiento permite utilizar la línea de comandos y la interfaz gráfica de usuario `txzonemgr` para administrar un sistema Trusted Extensions remoto.

Antes de empezar El usuario, el rol y la asignación de rol se definen de manera idéntica en los sistemas locales y remotos, como se describe en "Cómo habilitar la administración remota de un sistema Trusted Extensions remoto" en la página 160.

1 En el sistema de escritorio, habilite la visualización de los procesos del sistema remoto.

```
desktop $ xhost + remote-sys
```

2 Asegúrese de ser el usuario que está nombrado de la misma manera en ambos sistemas.

3 Desde una ventana de terminal, inicie sesión en el sistema remoto.

Utilice el comando `ssh` para iniciar sesión.

```
desktop $ ssh -X -l identical-username remote-sys
Password:       Type the user's password
remote-sys $
```

La opción `-X` permite la visualización de las interfaces gráficas de usuario.

4 En la misma ventana de terminal, asuma el rol que se define de forma idéntica en ambos sistemas.

Por ejemplo, asuma el rol de usuario `root`.

```
remote-sys $ su - root
Password:       Type the root password
```

Ahora está en la zona global. Ahora puede utilizar esta ventana de terminal para administrar el sistema remoto desde la línea de comandos. Las interfaces gráficas de usuario se mostrarán en la pantalla. Para ver un ejemplo, consulte el Ejemplo 12–2.

Ejemplo 12–2 Configuración de zonas con etiquetas en un sistema remoto

En este ejemplo, el administrador utiliza la interfaz gráfica de usuario `txzonemgr` para configurar zonas con etiquetas en un sistema remoto con etiquetas desde un sistema de escritorio con etiquetas. Como en Oracle Solaris, el administrador habilita el acceso del sistema de escritorio al servidor X mediante la opción `-X` para el comando `ssh`. El usuario `jandoe` está definido de la misma manera en ambos sistemas y puede asumir el rol `remoterole`.

```
TXdesk1 $ xhost + TXnohead4

TXdesk1 $ ssh -X -l jandoe TXnohead4
Password: Ins1PwD1
TXnohead4 $
```

Para acceder a la zona global, el administrador utiliza la cuenta `jandoe` para asumir el rol `remoterole`. Este rol está definido de la misma manera en ambos sistemas.

```
TXnohead4 # su - remoterole
Password: abcd1EFG
```

En el mismo terminal, el administrador con el rol `remoterole` inicia la interfaz gráfica de usuario `txzonemgr`.

```
TXnohead4 $ /usr/sbin/txzonemgr &
```

Labeled Zone Manager se ejecuta en el sistema remoto y se visualiza en el sistema local.

Ejemplo 12–3 Inicio de sesión en una zona con etiquetas remota

El administrador desea cambiar un archivo de configuración de un sistema remoto en la etiqueta `PUBLIC`.

El administrador tiene dos opciones.

- Puede iniciar sesión de manera remota en la zona global, mostrar la zona global remota y, a continuación, cambiar a la etiqueta `PUBLIC`, abrir una ventana de terminal y editar el archivo.
- Puede iniciar sesión de manera remota en la zona `PUBLIC` mediante el comando `ssh` desde una ventana de terminal `PUBLIC` y, a continuación, editar el archivo.

Tenga en cuenta que si el sistema remoto ejecuta un daemon de servicio de nombres (`nscd`) para todas las zonas *y* el sistema remoto utiliza el servicio de nombres de archivos, la contraseña de la zona remota es la contraseña que estaba vigente cuando se inició la zona por última vez. Si se modificó la contraseña de la zona `PUBLIC`, pero no se inició la zona después del cambio, la contraseña original permite el acceso.

Errores más frecuentes

Si la opción `-X` no funciona, es posible que deba instalar un paquete. El reenvío de X11 se deshabilita cuando no se instala el binario `xauth`. El siguiente comando carga el binario: **`pkg install pkg:/x11/session/xauth`**.

◆ ◆ ◆ CAPÍTULO 13

Gestión de zonas en Trusted Extensions (tareas)

En este capítulo, se describe cómo funcionan las zonas no globales, o *con etiquetas*, en un sistema Trusted Extensions. También se incluyen procedimientos que son exclusivos de las zonas con etiquetas.

Zonas en Trusted Extensions

El sistema Trusted Extensions bien configurado consta de una zona global, que es la instancia del sistema operativo, y una o más zonas no globales con etiquetas. Durante la configuración, Trusted Extensions anexa una sola etiqueta a cada zona; lo que crea las zonas con etiquetas. Las etiquetas proceden del archivo `label_encodings`. Puede crear una zona para cada etiqueta, pero esto no es obligatorio. Es posible tener más etiquetas que zonas con etiquetas en un sistema. No es posible tener más zonas con etiquetas que etiquetas.

En un sistema Trusted Extensions, la zona global es únicamente una zona administrativa. Las zonas con etiquetas son para los usuarios comunes. Los usuarios pueden trabajar en una zona cuya etiqueta se encuentre dentro del rango de acreditación del usuario.

En un sistema Trusted Extensions, los sistemas de archivos de una zona suelen montarse en la zona global como un sistema de archivos de bucle de retorno (LOFS, Loopback File System). Todos los archivos y directorios que se pueden escribir en una zona con etiquetas se encuentran en la etiqueta de la zona. De manera predeterminada, el usuario puede visualizar los archivos que están en una zona de una etiqueta inferior a la etiqueta actual del usuario. Esta configuración permite a los usuarios ver sus directorios principales en las etiquetas inferiores a la etiqueta del espacio de trabajo actual. Aunque los usuarios pueden ver los archivos en una etiqueta inferior, no pueden modificarlos. Los usuarios pueden modificar solamente los archivos de un proceso que tenga la misma etiqueta que el archivo.

Cada zona es un sistema de archivos ZFS discreto. Cada zona tiene una dirección IP y atributos de seguridad asociados. Las zonas pueden configurarse con puertos de varios niveles (MLP, Multilevel Ports). Asimismo, las zonas se pueden configurar con una política para la difusión del protocolo de mensajes de control de Internet (ICMP, Internet Control Message Protocol), como `ping`.

Para obtener información sobre cómo compartir directorios desde una zona con etiquetas y cómo montar directorios desde zonas con etiquetas de manera remota, consulte el Capítulo 14, "Gestión y montaje de archivos en Trusted Extensions (tareas)" y "Montaje de conjuntos de datos ZFS con etiquetas" en la página 186.

Las zonas de Trusted Extensions, están integradas en el producto Oracle Solaris Zones. Para obtener información de referencia, consulte la Parte II, "Zonas de Oracle Solaris" de *Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*.

Zonas y direcciones IP en Trusted Extensions

El equipo de configuración inicial asignó direcciones IP a la zona global y a las zonas con etiquetas. Consideraron tres tipos de configuraciones como se describe en "Acceso a zonas con etiquetas" en la página 32 y que se resumen de la siguiente manera:

- El sistema tiene una dirección IP para la zona global y todas las zonas con etiquetas.

  Esta configuración predeterminada es útil para los sistemas que utilizan software DHCP para obtener su dirección IP.

- El sistema tiene una dirección IP para la zona global y otra dirección IP que comparten todas las zonas, incluida la zona global. Cualquier zona puede tener una combinación de una dirección exclusiva y una dirección compartida.

  Esta configuración es útil para los sistemas en red en que los usuarios comunes iniciarán sesión. También se puede utilizar para una impresora o un servidor NFS. Esta configuración conserva las direcciones IP.

- El sistema tiene una dirección IP para la zona global, y cada zona con etiquetas tiene una dirección IP exclusiva.

  Esta configuración sirve para proporcionar acceso a redes físicas separadas de sistemas de un solo nivel. Normalmente, cada zona tiene una dirección IP en una red física diferente de las demás zonas con etiquetas. Debido a que esta configuración se implementa con una sola instancia de IP, la zona global controla las interfaces físicas y gestiona los recursos globales, como la tabla de enrutamiento.

Existe un cuarto tipo de configuración para una zona no global disponible en Oracle Solaris: las instancias de IP exclusivas. En esta configuración, se asigna a una zona no global su propia instancia de IP y la zona gestiona sus propias interfaces físicas. Cada zona funciona como si

fuera un sistema distinto. Para obtener una descripción, consulte "Interfaces de red de zona" de *Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*.

Si configura instancias de IP exclusivas en Trusted Extensions, cada zona con etiquetas funciona como si fuera un sistema *de un solo nivel* distinto. Las funciones de redes de varios niveles de Trusted Extensions se basan en las funciones de una pila de IP compartida. En esta guía, se asume que la red está controlada totalmente por la zona global. Por lo tanto, si el equipo de configuración inicial instaló zonas con etiquetas con instancias de IP exclusivas, debe proporcionar o consultar documentación específica del sitio.

Zonas y puertos de varios niveles

De manera predeterminada, las zonas no pueden enviar paquetes a ninguna otra zona ni recibir paquetes de ninguna otra zona. Los puertos de varios niveles habilitan servicios concretos en un puerto para aceptar solicitudes dentro de un rango de etiquetas o de un conjunto de etiquetas. Estos servicios con privilegios pueden responder en la etiqueta de la solicitud. Por ejemplo, quizás desee crear un puerto de explorador web con privilegios que pueda recibir todas las etiquetas, pero cuyas respuestas estén restringidas por etiqueta. De manera predeterminada, las zonas con etiquetas no tienen puertos de varios niveles.

El rango o el conjunto de etiquetas que restringe los paquetes que el puerto de varios niveles puede aceptar se basan en la dirección IP de la zona. Se asigna una plantilla de seguridad a la dirección IP mediante la comunicación de los sistemas Trusted Extensions. El rango o el conjunto de etiquetas de la plantilla de seguridad restringe los paquetes que el puerto de varios niveles puede aceptar.

Las restricciones en los puertos de varios niveles para las configuraciones de direcciones IP diferentes son las siguientes:

- En los sistemas en que la zona global tiene una dirección IP y cada zona con etiquetas tiene una sola dirección IP, se puede agregar un puerto de varios niveles para un servicio en particular a cada zona. Por ejemplo, el sistema podría configurarse para que el servicio `ssh`, mediante el puerto TCP `22`, sea un puerto de varios niveles en la zona global y en cada zona con etiquetas.
- En una configuración típica, a la zona global se le asigna una dirección IP, y las zonas con etiquetas comparten una segunda dirección IP con la zona global. Cuando se agrega un puerto de varios niveles a una interfaz compartida, el paquete de servicio se enruta hacia la zona con etiquetas donde se define el puerto de varios niveles. El paquete se acepta únicamente si el rango de etiquetas de la plantilla de host remoto para la zona con etiquetas incluye la etiqueta del paquete. Si el rango es `ADMIN_LOW` a `ADMIN_HIGH`, se aceptan todos los paquetes. Si el rango fuera menor, se descartarían los paquetes que no estén dentro del rango.

  En la mayoría de los casos, una zona puede definir un puerto determinado para que actúe como puerto de varios niveles en una interfaz compartida. En la situación anterior, donde el puerto `ssh` está configurado como puerto de varios niveles compartido en una zona no global, ninguna otra zona puede recibir conexiones `ssh` en la dirección compartida. Sin embargo, la zona global podría definir el puerto `ssh` como puerto de varios niveles privado para la recepción de conexiones en su dirección específica de la zona.
- En la configuración predeterminada, en donde la zona global y las zonas con etiquetas comparten una dirección IP, se puede agregar un puerto de varios niveles para el servicio `ssh` en una zona. Si el puerto de varios niveles para `ssh` se agrega a la zona global, ninguna zona con etiquetas puede agregar un puerto de varios niveles para el servicio `ssh`. De manera similar, si el puerto de varios niveles para el servicio `ssh` se agrega a una zona con etiquetas, la zona global no se puede configurar con un puerto de varios niveles `ssh`.

Para ver un ejemplo, consulte "Cómo crear un puerto de varios niveles para una zona" en la página 233.

Zonas e ICMP en Trusted Extensions

Las redes transmiten mensajes de difusión y envían paquetes de ICMP a los sistemas de la red. En un sistema de varios niveles, estas transmisiones pueden colapsar el sistema en cada etiqueta. De manera predeterminada, la política de red para las zonas con etiquetas requiere que los paquetes de ICMP se reciban únicamente en la etiqueta que coincide.

Procesos de la zona global y de las zonas con etiquetas

En Trusted Extensions, la política de MAC se aplica a todos los procesos, incluso los procesos de la zona global. Los procesos de la zona global se ejecutan en la etiqueta `ADMIN_HIGH`. Cuando se comparten los archivos de una zona global, se comparten en la etiqueta `ADMIN_LOW`. Por lo tanto, dado que MAC impide que un proceso con una etiqueta superior modifique un objeto de nivel inferior, generalmente la zona global no puede escribir en un sistema montado en NFS.

Sin embargo, en un número limitado de los casos, las acciones en una zona con etiquetas puede requerir que un proceso de la zona global modifique un archivo en dicha zona.

A fin de habilitar un proceso de la zona global para que monte un sistema de archivos remoto con permisos de lectura y escritura, el montaje debe estar en la ruta de la zona cuya etiqueta corresponde a la del sistema de archivos remoto. El montaje no debe estar en la ruta root de la zona.

- El sistema de montaje debe tener una zona en la etiqueta idéntica como el sistema de archivos remoto.
- El sistema debe montar el sistema de archivos remoto en la ruta de la zona que tiene etiquetas idénticas.

  El sistema *no* debe montar el sistema de archivos remoto en la *ruta root de la zona* de la zona que tiene etiquetas idénticas.

Tenga en cuenta una zona que esté denominada como `public` en la etiqueta `PUBLIC`. La *ruta de la zona* es `/zone/public/`. Todos los directorios de la ruta de la zona se encuentran en la etiqueta `PUBLIC`; por ejemplo:

```
/zone/public/dev
/zone/public/etc
/zone/public/home/username
/zone/public/root
/zone/public/usr
```

De los directorios de la ruta de la zona, solamente los archivos que se encuentran en `/zone/public/root` son visibles desde la zona public. A los demás directorios y archivos en la etiqueta `PUBLIC` se puede acceder solamente desde la zona global. La ruta `/zone/public/root` es la *ruta root de la zona*.

Desde la perspectiva del administrador de la zona public, la ruta root de la zona se ve como `/`. De manera similar, el administrador de la zona public no puede acceder a un directorio principal del usuario en la ruta de la zona (directorio `/zone/public/home/`*username*). Dicho directorio se ve solamente desde la zona global. La zona public monta ese directorio en la ruta root de la zona como `/home/`*username*. Desde la perspectiva de la zona global, este montaje se ve como `/zone/public/root/home/`*username*.

El administrador de la zona public puede modificar `/home/`*username*. Cuando los archivos del directorio principal del usuario deben modificarse, el proceso de la zona global no utiliza dicha ruta. La zona global utiliza el directorio principal del usuario en la ruta de la zona, `/zone/public/home/`*username*.

- Los archivos y directorios que se encuentran en la ruta de la zona, `/zone/`*zonename*`/`, pero no en la ruta root de la zona, directorio `/zone/`*zonename*`/root` , pueden modificarse mediante un proceso de la zona global que se ejecute en la etiqueta `ADMIN_HIGH`.
- El administrador de la zona con etiquetas puede modificar los archivos y directorios de la ruta root de la zona, `/zone/public/root`.

Por ejemplo, cuando un usuario asigna un dispositivo en la zona public, un proceso de la zona global que se ejecuta en la etiqueta `ADMIN_HIGH` modifica el directorio `dev` en la ruta de la zona, `/zone/public/dev`. De manera similar, cuando un usuario guarda una configuración del escritorio, un proceso de la zona global de `/zone/public/home/`*username* modifica el archivo de la configuración del escritorio. Para compartir un sistema de archivos con etiquetas, consulte "Cómo compartir sistemas de archivos de una zona con etiquetas" en la página 189.

Utilidades de administración de zonas en Trusted Extensions

Las tareas de administración de zonas se pueden realizar desde la línea de comandos. Sin embargo, la forma más sencilla de administrar zonas es utilizar la secuencia de comandos de shell, `/usr/sbin/txzonemgr`, que proporciona Trusted Extensions. Esta secuencia de comandos proporciona un asistente basado en menús para crear, instalar, inicializar e iniciar las zonas. `txzonemgr` utiliza el comando `zenity`. Para obtener detalles, consulte las páginas del comando man `txzonemgr(1M)` y `zenity`(1).

Gestión de zonas (mapa de tareas)

El mapa de tareas siguiente describe las tareas de gestión de zonas que son específicas de Trusted Extensions. El mapa también incluye enlaces a los procedimientos comunes que se realizan en Trusted Extensions de la misma manera que en un sistema Oracle Solaris.

Tarea	Descripción	Para obtener instrucciones
Ver todas las zonas.	En cualquier etiqueta, se visualizan las zonas dominadas por la zona actual.	"Cómo visualizar las zonas que están preparadas o en ejecución" en la página 174
Ver directorios montados.	En cualquier etiqueta, se visualizan los directorios dominados por la etiqueta actual.	"Cómo visualizar las etiquetas de los archivos montados" en la página 174

Tarea	Descripción	Para obtener instrucciones
Permitir que los usuarios comunes vean un archivo `/etc`.	Se monta en bucle de retorno un directorio o archivo de la zona global que no es visible de manera predeterminada en una zona con etiquetas.	"Cómo montar en bucle de retorno un archivo que no suele estar visible en una zona con etiquetas" en la página 175
Impedir que los usuarios comunes visualicen un directorio principal de nivel inferior desde una etiqueta de nivel superior.	De manera predeterminada, los directorios de nivel inferior son visibles desde las zonas de nivel superior. Cuando deshabilita el montaje de una zona de nivel inferior, puede deshabilitar todos los montajes de las zonas de nivel inferior.	"Cómo deshabilitar el montaje de archivos de nivel inferior" en la página 176
Configurar una zona para permitir el cambio de las etiquetas en los archivos.	Las zonas con etiquetas tienen privilegios limitados. De manera predeterminada, las zonas con etiquetas no tienen el privilegio que habilita a un usuario autorizado para volver a etiquetar un archivo. Se debe modificar la configuración de zona para agregar el privilegio.	"Cómo permitir que los archivos se vuelvan a etiquetar desde una zona con etiquetas" en la página 180
Anexar un conjunto de datos ZFS a una zona con etiquetas y compartirlo.	Se monta un conjunto de datos ZFS con permisos de lectura y escritura en una zona con etiquetas y se comparte la parte de sólo lectura del conjunto de datos con una zona superior.	"Cómo compartir un conjunto de datos ZFS desde una zona con etiquetas" en la página 178.
Configurar una zona nueva.	Se crea una zona en una etiqueta que no se esté utilizando actualmente para etiquetar una zona en este sistema.	Consulte "Cómo crear zonas con etiquetas de forma interactiva" en la página 57.
Crear un puerto de varios niveles para una aplicación.	Los puertos de varios niveles son útiles para los programas que requieren un avance de varios niveles en una zona con etiquetas.	"Cómo crear un puerto de varios niveles para una zona" en la página 233 Ejemplo 16–19
Resolver problemas de acceso y montaje NFS.	Se depuran los problemas de acceso generales para los montajes y, quizás, para las zonas.	"Cómo resolver problemas por fallos de montaje en Trusted Extensions" en la página 192
Eliminar una zona con etiquetas.	Se elimina por completo una zona con etiquetas del sistema.	"Cómo eliminar una zona no global" de *Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*

▼ Cómo visualizar las zonas que están preparadas o en ejecución

Antes de empezar Debe estar con el rol de administrador del sistema en la zona global.

1 Ejecute el comando `txzonemgr &`.

Los nombres de las zonas, su estado y sus etiquetas se muestran en una interfaz gráfica de usuario.

2 O bien, utilice el comando `zoneadm list -v`.

```
# zoneadm list -v
ID NAME       STATUS     PATH              BRAND       IP
 0 global     running    /                 ipkg        shared
 5 internal   running    /zone/internal    labeled     shared
 6 public     running    /zone/public      labeled     shared
```

La salida no muestra las etiquetas de las zonas.

▼ Cómo visualizar las etiquetas de los archivos montados

Este procedimiento crea una secuencia de comandos de shell que muestra los sistemas de archivos montados de la zona actual. Cuando la secuencia de comandos se ejecuta desde la zona global, muestra las etiquetas de todos los sistemas de archivos montados en cada zona.

Antes de empezar Debe estar con el rol de administrador del sistema en la zona global.

1 En un editor, cree la secuencia de comandos `getmounts`.

Proporcione el nombre de la ruta de la secuencia de comandos; por ejemplo, `/usr/local/scripts/getmounts`.

2 Agregue el siguiente contenido y guarde el archivo:

```
#!/bin/sh
#
for i in ‘/usr/sbin/mount -p | cut -d " " -f3‘ ; do
        /usr/bin/getlabel $i
done
```

3 Pruebe la secuencia de comandos en la zona global.

```
# /usr/local/scripts/getmounts
/:      ADMIN_HIGH
/dev:   ADMIN_HIGH
/system/contract:       ADMIN_HIGH
/proc:                  ADMIN_HIGH
```

```
/system/volatile:        ADMIN_HIGH
/system/object:          ADMIN_HIGH
/lib/libc.so.1:          ADMIN_HIGH
/dev/fd:        ADMIN_HIGH
/tmp:           ADMIN_HIGH
/etc/mnttab:    ADMIN_HIGH
/export:        ADMIN_HIGH
/export/home:   ADMIN_HIGH
/export/home/jdoe:   ADMIN_HIGH
/zone/public:        ADMIN_HIGH
/rpool:              ADMIN_HIGH
/zone:               ADMIN_HIGH
/home/jdoe:          ADMIN_HIGH
/zone/public:        ADMIN_HIGH
/zone/snapshot:      ADMIN_HIGH
/zone/internal:      ADMIN_HIGH
...
```

Ejemplo 13–1 Visualización de las etiquetas de los sistemas de archivos en la zona restricted

Cuando un usuario común ejecuta la secuencia de comandos desde una zona con etiquetas, la secuencia de comandos `getmounts` muestra las etiquetas de todos los sistemas de archivos montados en dicha zona. En un sistema en el que las zonas se crean para cada etiqueta en el archivo `label_encodings` predeterminado, la salida de muestra de la zona `restricted` es la siguiente:

```
# /usr/local/scripts/getmounts
/:      CONFIDENTIAL : RESTRICTED
/dev:   CONFIDENTIAL : RESTRICTED
/kernel:        ADMIN_LOW
/lib:   ADMIN_LOW
/opt:   ADMIN_LOW
/platform:      ADMIN_LOW
/sbin:  ADMIN_LOW
/usr:   ADMIN_LOW
/var/tsol/doors:        ADMIN_LOW
/zone/needtoknow/export/home:   CONFIDENTIAL : NEED TO KNOW
/zone/internal/export/home:     CONFIDENTIAL : INTERNAL USE ONLY
/proc:  CONFIDENTIAL : RESTRICTED
/system/contract:       CONFIDENTIAL : RESTRICTED
/etc/svc/volatile:      CONFIDENTIAL : RESTRICTED
/etc/mnttab:    CONFIDENTIAL : RESTRICTED
/dev/fd:        CONFIDENTIAL : RESTRICTED
/tmp:   CONFIDENTIAL : RESTRICTED
/var/run:       CONFIDENTIAL : RESTRICTED
/zone/public/export/home:       PUBLIC
/home/jdoe:   CONFIDENTIAL : RESTRICTED
```

▼ Cómo montar en bucle de retorno un archivo que no suele estar visible en una zona con etiquetas

Este procedimiento habilita a un usuario en una zona con etiquetas especificada para que vea los archivos que no se exportaron desde la zona global de manera predeterminada.

Antes de empezar Debe estar con el rol de administrador del sistema en la zona global.

1 Detenga la zona cuya configuración desea cambiar.

```
# zoneadm -z zone-name halt
```

2 Monte en bucle de retorno un archivo o directorio.

Por ejemplo, habilite a los usuarios comunes para que vean un archivo en el directorio `/etc`.

```
# zonecfg -z zone-name
 add filesystem
 set special=/etc/filename
 set directory=/etc/filename
 set type=lofs
 add options [ro,nodevices,nosetuid]
 end
 exit
```

3 Inicie la zona.

```
# zoneadm -z zone-name boot
```

Ejemplo 13–2 Montaje en bucle de retorno del archivo /etc/passwd

En este ejemplo, el administrador de la seguridad desea habilitar a los evaluadores y a los programadores para que verifiquen si sus contraseñas locales se encuentran establecidas. Después de que se detiene la zona `sandbox`, esta se configura para montar en bucle de retorno el archivo `passwd`. A continuación, la zona se reinicia.

```
# zoneadm -z sandbox halt
# zonecfg -z sandbox
 add filesystem
    set special=/etc/passwd
    set directory=/etc/passwd
    set type=lofs
    add options [ro,nodevices,nosetuid]
 end
 exit
# zoneadm -z sandbox boot
```

▼ Cómo deshabilitar el montaje de archivos de nivel inferior

De manera predeterminada, los usuarios pueden ver los archivos de nivel inferior. Eliminar el privilegio `net_mac_aware` para impedir la visualización de todos los archivos de nivel inferior de una zona en particular. Para obtener una descripción del privilegio `net_mac_aware`, consulte la página del comando man `privileges(5)`.

Antes de empezar Debe estar con el rol de administrador del sistema en la zona global.

1. **Detenga la zona cuya configuración desea cambiar.**

   ```
   # zoneadm -z zone-name halt
   ```

2. **Configure la zona para impedir la visualización de los archivos de nivel inferior.**

   Elimine el privilegio `net_mac_aware` de la zona.

   ```
   # zonecfg -z zone-name
    set limitpriv=default,!net_mac_aware
    exit
   ```

3. **Reinicie la zona.**

   ```
   # zoneadm -z zone-name boot
   ```

Ejemplo 13–3 Cómo impedir que los usuarios vean los archivos de nivel inferior

En este ejemplo, el administrador de la seguridad desea impedir que los usuarios en un sistema se confundan. Por lo tanto, los usuarios pueden ver únicamente los archivos de la etiqueta en la que están trabajando. Entonces, el administrador de la seguridad impide la visualización de todos los archivos de nivel inferior. En este sistema, los usuarios no pueden ver los archivos que se encuentran disponibles públicamente, a menos que estén trabajando en la etiqueta `PUBLIC`. Además, los usuarios sólo pueden montar archivos en NFS en la etiqueta de las zonas.

```
# zoneadm -z restricted halt
# zonecfg -z restricted
 set limitpriv=default,!net_mac_aware
 exit
# zoneadm -z restricted boot

# zoneadm -z needtoknow halt
# zonecfg -z needtoknow
 set limitpriv=default,!net_mac_aware
 exit
# zoneadm -z needtoknow boot

# zoneadm -z internal halt
# zonecfg -z internal
 set limitpriv=default,!net_mac_aware
 exit
# zoneadm -z internal boot
```

Dado que `PUBLIC` es la etiqueta mínima, el administrador de la seguridad no ejecuta los comandos para la zona `PUBLIC`.

▼ Cómo compartir un conjunto de datos ZFS desde una zona con etiquetas

En este procedimiento, monta un conjunto de datos ZFS con permisos de lectura y escritura en una zona con etiquetas. Ya que todos los comandos se ejecutan en la zona global, el administrador de la zona global controla la adición de conjuntos de datos ZFS a las zonas con etiquetas.

Como mínimo, la zona con etiquetas debe estar en el estado `ready` para compartir un conjunto de datos. La zona puede estar en el estado `running`.

Antes de empezar Para configurar la zona con el conjunto de datos, primero debe detener la zona. Debe estar con el rol de usuario `root` en la zona global.

1 Cree el conjunto de datos ZFS.

```
# zfs create datasetdir/subdir
```

El nombre del conjunto de datos puede incluir un directorio, como `zone/data`.

2 En la zona global, detenga la zona con etiquetas.

```
# zoneadm -z labeled-zone-name halt
```

3 Defina el punto de montaje del conjunto de datos.

```
# zfs set mountpoint=legacy datasetdir/subdir
```

La configuración de la propiedad ZFS `mountpoint` establece la etiqueta del punto de montaje cuando el punto de montaje corresponde a una zona con etiquetas.

4 Habilite el uso compartido del conjunto de datos.

```
# zfs set sharenfs=on datasetdir/subdir
```

5 Agregue el conjunto de datos a la zona como un sistema de archivos.

```
# zonecfg -z labeled-zone-name
# zonecfg:labeled-zone-name> add fs
# zonecfg:labeled-zone-name:dataset> set dir=/subdir
# zonecfg:labeled-zone-name:dataset> set special=datasetdir/subdir
# zonecfg:labeled-zone-name:dataset> set type=zfs
# zonecfg:labeled-zone-name:dataset> end
# zonecfg:labeled-zone-name> exit
```

Si se agrega el conjunto de datos como un sistema de archivos, el conjunto de datos se monta en `/data`, en la zona. Este paso garantiza que el conjunto de datos no se monte antes de que se inicie la zona.

6 Inicie la zona con etiquetas.

```
# zoneadm -z labeled-zone-name boot
```

Cuando se inicia la zona, se monta el conjunto de datos automáticamente como punto de montaje de lectura y escritura en la zona *labeled-zone-name* con la etiqueta de la zona *labeled-zone-name*.

Ejemplo 13–4 Uso compartido y montaje de un conjunto de datos ZFS desde zonas con etiquetas

En este ejemplo, el administrador agrega un conjunto de datos ZFS a la zona `needtoknow` y, luego, lo comparte. El conjunto de datos, `zone/data`, se encuentra asignado al punto de montaje `/mnt`. Los usuarios de la zona `restricted` pueden ver el conjunto de datos.

En primer lugar, el administrador detiene la zona.

```
# zoneadm -z needtoknow halt
```

Dado que el conjunto de datos se encuentra asignado a un punto de montaje diferente, el administrador elimina la asignación anterior y, a continuación, establece el nuevo punto de montaje.

```
# zfs set zoned=off zone/data
# zfs set mountpoint=legacy zone/data
```

Luego, el administrador comparte el conjunto de datos.

```
# zfs set sharenfs=on zone/data
```

A continuación, en la interfaz interactiva `zonecfg`, el administrador agrega explícitamente el conjunto de datos a la zona `needtoknow`.

```
# zonecfg -z needtoknow
# zonecfg:needtoknow> add fs
# zonecfg:needtoknow:dataset> set dir=/data
# zonecfg:needtoknow:dataset> set special=zone/data
# zonecfg:needtoknow:dataset> set type=zfs
# zonecfg:needtoknow:dataset> end
# zonecfg:needtoknow> exit
```

Luego, el administrador inicia la zona `needtoknow`.

```
# zoneadm -z needtoknow boot
```

Finalmente se podrá acceder al conjunto de datos.

Los usuarios de la zona `restricted`, que domina la zona `needtoknow`, pueden ver el conjunto de datos montado. Para ello, deben cambiar al directorio `/data`. Deben usar la ruta completa para acceder al conjunto de datos montado desde la perspectiva de la zona global. En este ejemplo, `machine1` es el nombre de host del sistema que incluye la zona con etiquetas. El administrador asignó este nombre de host a una dirección IP no compartida.

```
# cd /net/machine1/zone/needtoknow/root/data
```

Errores más frecuentes Si el intento de acceder al conjunto de datos desde la etiqueta superior devuelve los mensajes de error `not found` o `No such file or directory`, el administrador debe reiniciar el servicio del montador automático mediante la ejecución del comando `svcadm restart autofs`.

▼ Cómo permitir que los archivos se vuelvan a etiquetar desde una zona con etiquetas

Este procedimiento es un requisito previo para que un usuario pueda volver a etiquetar archivos.

Antes de empezar La zona que planea configurar debe estar detenida. Debe estar con el rol de administrador de la seguridad en la zona global.

1. **Abra Labeled Zone Manager.**

   ```
   # /usr/sbin/txzonemgr &
   ```

2. **Configure la zona para habilitar la opción de volver a etiquetar.**

   a. **Haga doble clic en la zona**

   b. **En la lista, seleccione Permit Relabeling.**

3. **Seleccione Boot para reiniciar la zona.**

4. **Haga clic en Cancel para volver a la lista de zonas.**

   Para conocer los requisitos del proceso y del usuario que permiten volver a etiquetar, consulte la página del comando man `setflabel`(3TSOL). Para saber cómo autorizar a un usuario a que vuelva a etiquetar archivos, consulte "Cómo habilitar a un usuario para que cambie el nivel de seguridad de los datos" en la página 155.

Ejemplo 13–5 Cómo evitar las disminuciones de nivel desde la zona internal

En este ejemplo, el administrador de la seguridad desea evitar la disminución del nivel de los archivos `CNF: INTERNAL USE ONLY` en un sistema que anteriormente se utilizaba para disminuir el nivel de los archivos.

El administrador utiliza Labeled Zone Manager para detener la zona `internal` y, a continuación, selecciona Deny Relabeling en el menú de la zona `internal`.

◆ ◆ ◆ CAPÍTULO 14

Gestión y montaje de archivos en Trusted Extensions (tareas)

En este capítulo, se describe el funcionamiento de los montajes LOFS, NFS y ZFS en un sistema configurado con Trusted Extensions. Además, se explica cómo realizar copias de seguridad de los archivos y cómo restaurarlos.

Uso compartido y montaje de archivos en Trusted Extensions

El software Trusted Extensions admite los mismos sistemas de archivos y comandos de gestión de sistemas de archivos que Oracle Solaris. Dado que Trusted Extensions anexa una etiqueta única a cada zona no global, todos los archivos y sistemas de archivos que pertenecen a esa zona están montados en la etiqueta de la zona. Cualquier sistema de archivos compartido que pertenezca a otras zonas o a servidores NFS se monta en la etiqueta del propietario. Trusted Extensions impide cualquier montaje que pueda infringir las políticas del control de acceso obligatorio (MAC) sobre el uso de etiquetas. Por ejemplo, la etiqueta de una zona debe dominar todas las etiquetas de su sistema de archivos montado, y solamente los sistemas de archivos con etiquetas iguales pueden montarse con permisos de lectura y escritura.

Montajes NFS en Trusted Extensions

Los montajes NFS de Trusted Extensions son similares a los montajes de Oracle Solaris. Las diferencias se producen en la aplicación de la política MAC. Además, la secuencia de comandos `txzonemgr` asume que los directorios principales se montan como `/export/home`.

Lo recursos compartidos NFS de Trusted Extensions son similares a los recursos compartidos de Oracle Solaris en una zona global. Sin embargo, el uso compartido de una zona con etiquetas en un sistema de varios niveles es exclusivo de Trusted Extensions:

- **Recursos compartidos y montajes en la zona global** : el uso compartido y el montaje de archivos en la zona global de un sistema Trusted Extensions es casi idéntico al procedimiento de Oracle Solaris. Para montar archivos, se pueden utilizar el montador automático y el comando `mount`. Para compartir archivos, se utiliza la propiedad `sharenfs` de los conjuntos de datos ZFS.
- **Montaje en zonas con etiquetas**: el montaje de archivos en las zonas con etiquetas de Trusted Extensions es casi idéntico al montaje de archivos en las zonas no globales de Oracle Solaris. Para montar archivos, se pueden utilizar el montador automático y el comando `mount`. En Trusted Extensions, existe un único archivo de configuración `auto_home_`*nombre_zona* para cada zona con etiquetas.
- **Recursos compartidos en zonas con etiquetas**: los archivos de una zona con etiquetas se pueden compartir en la etiqueta de la zona mediante las propiedades de recursos compartidos ZFS. Para obtener más información, consulte "Procesos de la zona global y de las zonas con etiquetas" en la página 171.

Las etiquetas determinan qué archivos se pueden montar. Los archivos se comparten y se montan en una etiqueta determinada.

- Para que un sistema Trusted Extensions monte un sistema de archivos en otro sistema Trusted Extensions, el servidor y el cliente deben tener plantillas de host remoto compatibles del tipo `cipso`.

  Para que un cliente de Trusted Extensions escriba un sistema de archivos que está montado en NFS, el sistema de archivos debe estar montado con permisos de lectura y escritura *y* debe estar en la misma etiqueta que el cliente.
- Para que un sistema Trusted Extensions monte un sistema de archivos de un sistema sin etiquetas, la etiqueta única asignada al sistema sin etiquetas por el sistema Trusted Extensions debe coincidir con la etiqueta del sistema Trusted Extensions.

  De forma similar, para que una zona con etiquetas monte un sistema de archivos de un sistema sin etiquetas, la etiqueta única asignada al sistema sin etiquetas por el sistema Trusted Extensions debe coincidir con la etiqueta de la zona con etiquetas.
- Los sistemas de archivos cuyas etiquetas difieren de la zona de montaje y están montados con LOFS se pueden visualizar, pero no se pueden modificar. Para obtener detalles sobre los montajes NFS, consulte "Acceso a los sistemas de archivos montados en NFS en Trusted Extensions" en la página 183.

Las etiquetas también determinan qué directorios y archivos pueden verse. De manera predeterminada, los objetos de nivel inferior están disponibles en un entorno de usuario. Por lo tanto, en la configuración predeterminada, los usuarios comunes pueden ver los archivos que están en la zona de un nivel inferior a su nivel actual. Por ejemplo, los usuarios pueden ver sus directorios principales de nivel inferior desde una etiqueta superior. Para obtener detalles, consulte "Creación de directorios principales en Trusted Extensions" en la página 184.

Si la seguridad del sitio prohíbe la visualización de objetos de nivel inferior, puede ocultar los sistemas de archivos de nivel inferior para los usuarios. Para obtener detalles, consulte "Cómo deshabilitar el montaje de archivos de nivel inferior" en la página 176.

La política de montaje en Trusted Extensions no incluye invalidaciones de MAC. Un proceso de etiqueta superior nunca puede modificar los archivos montados que pueden verse en una etiqueta inferior. Esta política de MAC también se aplica en la zona global. Un proceso de zona global `ADMIN_HIGH` no puede modificar un archivo montado en NFS en una etiqueta inferior, como un archivo `PUBLIC` o un archivo `ADMIN_LOW`. Las políticas de MAC aplican la configuración predeterminada y no están visibles para los usuarios comunes. Los usuarios comunes no pueden ver objetos, salvo que tengan acceso MAC.

Uso compartido de archivos desde una zona con etiquetas

En Oracle Solaris, una zona no global puede compartir sistemas de archivos. Del mismo modo, en Trusted Extensions, una zona con etiquetas puede compartir sistemas de archivos. Para compartir sistemas de archivos de una zona con etiquetas, se activan las propiedades de recursos compartidos ZFS del sistema de archivos.

Cuando el estado de la zona con etiquetas es `ready` o `running`, el sistema de archivos se comparte en la etiqueta de la zona. Para conocer el procedimiento, consulte "Cómo compartir sistemas de archivos de una zona con etiquetas" en la página 189.

Acceso a los sistemas de archivos montados en NFS en Trusted Extensions

Para hacer que los directorios de nivel inferior montados en NFS estén visibles para los usuarios en una zona de nivel superior, se deben llevar a cabo los siguientes pasos:

- **Configuración del servidor**: en el servidor NFS, se debe exportar el sistema de archivos ZFS mediante la definición de las propiedades de recursos compartidos. Para conocer el procedimiento, consulte "Cómo compartir sistemas de archivos de una zona con etiquetas" en la página 189.
- **Configuración del cliente**: el privilegio `net_mac_aware` debe especificarse en el archivo de configuración de la zona que se utiliza durante la etapa inicial de configuración de la zona. Por lo tanto, el usuario que tenga permiso para ver todos los directorios principales de nivel

inferior también debe tener el privilegio `net_mac_aware` en cada zona, excepto en la zona más inferior. Para ver un ejemplo, consulte "Cómo montar archivos en NFS en una zona con etiquetas" en la página 191.

Creación de directorios principales en Trusted Extensions

Los directorios principales son un caso especial en Trusted Extensions. Debe asegurarse de que se creen los directorios principales en cada zona que los usuarios pueden utilizar. Además, deben crearse los puntos de montaje del directorio principal en las zonas del sistema del usuario. Para que los directorios principales montados en NFS funcionen correctamente, se debe usar la ubicación convencional de los directorios, `/export/home`. En Trusted Extensions, se cambió el montador automático para manejar los directorios principales en cada zona, es decir, en cada etiqueta. Para obtener detalles, consulte "Cambios en el montador automático en Trusted Extensions" en la página 184.

Los directorios principales se generan cuando se crean los usuarios. Sin embargo, los directorios principales se crean en la zona global del servidor de directorio principal. En ese servidor, los directorios están montados con LOFS. Los directorios principales se crean automáticamente con el montador automático si se encuentran especificados como montajes LOFS.

Nota – Cuando se suprime un usuario, solamente se suprime el directorio principal del usuario en la zona global. Los directorios principales del usuario en las zonas con etiquetas no se suprimen. Usted debe encargarse de archivar y suprimir los directorios principales en las zonas con etiquetas. Para conocer el procedimiento, consulte "Cómo suprimir una cuenta de usuario de un sistema Trusted Extensions" en la página 156.

Sin embargo, el montador automático no puede crear directorios principales en servidores NFS remotos de manera automática. Primero el usuario debe iniciar sesión en el servidor NFS, o se requiere intervención administrativa. Para crear directorios principales para los usuarios, consulte "Cómo permitir que los usuarios accedan a sus directorios principales remotos en cada etiqueta mediante el inicio de sesión en cada servidor NFS" en la página 74.

Cambios en el montador automático en Trusted Extensions

En Trusted Extensions, cada una de las etiquetas requiere un montaje de directorio principal separado. Se modificó el comando `automount` a fin de gestionar los montajes automáticos con etiquetas. Para cada zona, el montador automático `autofs` monta un archivo `auto_home_`*nombre_zona*. Por ejemplo, a continuación se muestra la entrada para la zona global en el archivo `auto_home_global`:

```
+auto_home_global
*       -fstype=lofs    :/export/home/&
```

Cuando se inicia una zona que permite montar zonas de nivel inferior, sucede lo siguiente. Los directorios principales de las zonas de nivel inferior se montan como de sólo lectura en `/zone/`*nombre_zona*`/export/home`. El mapa `auto_home_`*nombre_zona* especifica la ruta `/zone` como directorio de origen para un nuevo montaje de `lofs` en `/zone/`*nombre_zona*`/home/`*nombre_usuario*.

Por ejemplo, a continuación se muestra una entrada `auto_home_public` en un mapa `auto_home_`*zona_nivel_superior* que se genera a partir de una zona de nivel superior:

```
+auto_home_public
*    public-zone-IP-address:/export/home/&
```

La secuencia de comandos `txzonemgr` configura esta entrada `PUBLIC` en el archivo `auto_master` en la zona global:

```
+auto_master
/net        -hosts        -nosuid,nobrowse
/home        auto_home    -nobrowse
/zone/public/home      auto_home_public      -nobrowse
```

Cuando se hace referencia a un directorio principal y el nombre no coincide con ninguna de las entradas del mapa `auto_home_`*nombre_zona*, el mapa intenta asociar esta especificación de montaje en bucle de retorno. El software crea el directorio principal cuando se cumplen las dos condiciones siguientes:

1. El mapa encuentra la coincidencia con la especificación de montaje en bucle de retorno.
2. El nombre del directorio principal coincide con un usuario válido cuyo directorio principal todavía no existe en *nombre_zona*.

Para obtener detalles sobre los cambios en el montador automático, consulte la página del comando man `automount(1M)`.

Software Trusted Extensions y versiones del protocolo NFS

El software Trusted Extensions reconoce las etiquetas en NFS versión 3 (NFSv3) y NFSv4. Puede utilizar una de las siguientes opciones de conjuntos de montaje:

```
vers=4 proto=tcp
vers=3 proto=tcp
vers=3 proto=udp
```

Trusted Extensions no tiene restricciones para los montajes realizados en protocolo `tcp`. En NFSv3 y NFSv4, el protocolo `tcp` puede usarse para los montajes de una misma etiqueta y los montajes de lectura en sentido descendente. Los montajes de lectura en sentido descendente requieren un puerto de varios niveles (MLP).

En NFSv3, Trusted Extensions se comporta igual que Oracle Solaris. El protocolo `udp` es el que está predeterminado para NFSv3, pero `udp` se usa solamente para la operación de montaje inicial. Para las operaciones de NFS subsiguientes, el sistema utiliza `tcp`. Por lo tanto, los montajes de lectura en sentido descendente funcionan para NFSv3 con la configuración predeterminada.

Si eventualmente llegara a restringir los montajes en NFSv3 para que se use el protocolo udp en las operaciones NFS iniciales y posteriores, debe crear un MLP para las operaciones NFS que usan el protocolo `udp`. Para conocer el procedimiento, consulte el Ejemplo 16–19.

Un sistema Trusted Extensions también puede compartir sus sistemas de archivos con hosts sin etiquetas. Un sistema de archivos que se exporta a un host sin etiquetas *se puede escribir* si su etiqueta es igual a la etiqueta que se asigna al host remoto mediante la exportación de la zona. Un sistema de archivos que se exporta a un host sin etiquetas *se puede leer* únicamente si su etiqueta está dominada por la etiqueta asignada al host remoto.

Las comunicaciones con los sistemas que ejecutan una versión del software Trusted Solaris son posibles en una sola etiqueta. Los sistemas Trusted Extensions y Trusted Solaris deben asignar al su igual una plantilla con el tipo de host sin etiquetas. Los tipos de host sin etiquetas deben especificar la misma etiqueta sola. Como cliente NFS sin etiquetas de un servidor de Trusted Solaris, la etiqueta del cliente no puede ser `ADMIN_LOW`.

El protocolo NFS que se utiliza es independiente del tipo de sistema de archivos local. En realidad, el protocolo depende del tipo de sistema operativo del equipo de uso compartido. El tipo de sistema de archivos especificado en el comando `mount` para los sistemas de archivos remotos siempre es NFS.

Montaje de conjuntos de datos ZFS con etiquetas

ZFS proporciona un atributo de etiqueta de seguridad, `mlslabel`, que contiene la etiqueta de los datos del conjunto de datos. La propiedad `mlslabel` se puede heredar. Cuando un conjunto de datos ZFS tiene una etiqueta explícita, el conjunto de datos no se puede montar en un sistema Oracle Solaris que no está configurado con Trusted Extensions.

Si la propiedad `mlslabel` no está definida, se establece el valor predeterminado `none`, el cual indica que no hay ninguna etiqueta.

Al montar un conjunto de datos ZFS en una zona con etiquetas, se produce lo siguiente:

- Si el conjunto de datos no tiene etiquetas, es decir, la propiedad `mlslabel` no está definida, el valor de la propiedad `mlslabel` se modifica a la etiqueta de la zona de montaje.

  Para la zona global, la propiedad `mlslabel` no se establece automáticamente. Si etiqueta explícitamente el conjunto de datos `admin_low`, el conjunto de datos debe estar montado como de sólo lectura.

- Si el conjunto de datos tiene etiquetas, el núcleo verifica que la etiqueta del conjunto de datos coincida con la etiqueta de la zona de montaje. Si las etiquetas no coinciden, el montaje falla, a menos que la zona permita montajes de lectura en sentido descendente. Si la zona permite montajes de lectura en sentido descendente, un sistema de archivos de nivel inferior se monta como de sólo lectura.

Para definir la propiedad `mlslabel` desde la línea de comandos, escriba algo similar a lo siguiente:

```
# zfs set mlslabel=public export/publicinfo
```

El privilegio `file_upgrade_sl` se necesita para establecer un etiqueta inicial o cambiar una etiqueta no predeterminada a una etiqueta de nivel superior. El privilegio `file_downgrade_sl` se necesita para eliminar una etiqueta, es decir, para establecer la etiqueta en `none`. Este privilegio también es necesario para cambiar una etiqueta no predeterminada a una etiqueta de nivel inferior.

Copia de seguridad, uso compartido y montaje de archivos con etiquetas (mapa de tareas)

En el siguiente mapa de tareas, se describen las tareas comunes que se emplean para realizar copias de seguridad y restaurar los datos de sistemas de archivos con etiquetas, y para compartir y montar sistemas de archivos que tienen etiquetas.

Tarea	Descripción	Para obtener instrucciones
Realizar copias de seguridad de archivos.	Se archivan los datos.	"Cómo realizar copias de seguridad de los archivos en Trusted Extensions" en la página 188
Restaurar datos.	Se restauran los datos a partir de una copia de seguridad.	"Cómo restaurar archivos en Trusted Extensions" en la página 188
Compartir un sistema de archivos con etiquetas.	Permite que los usuarios de otros sistemas accedan al sistema de archivos con etiquetas.	"Cómo compartir sistemas de archivos de una zona con etiquetas" en la página 189
Montar un sistema de archivos compartido por una zona con etiquetas.	Permite montar el contenido de un sistema de archivos como de lectura y escritura en una zona con etiquetas en la misma etiqueta. Cuando una zona de nivel superior monta el directorio compartido, el directorio se monta como de sólo lectura.	"Cómo montar archivos en NFS en una zona con etiquetas" en la página 191

Tarea	Descripción	Para obtener instrucciones
Crear puntos de montaje del directorio principal.	Se crean puntos de montaje para cada usuario en cada etiqueta. Esta tarea permite a los usuarios acceder a su directorio principal en cada etiqueta, en un sistema que no es el servidor de directorio principal NFS.	"Cómo permitir que los usuarios accedan a sus directorios principales remotos en cada etiqueta mediante el inicio de sesión en cada servidor NFS" en la página 74
Ocultar información de nivel inferior a un usuario que trabaja en una etiqueta superior.	Se impide la visualización de información de nivel inferior desde un nivel superior.	"Cómo deshabilitar el montaje de archivos de nivel inferior" en la página 176
Resolver problemas de montaje de sistema de archivos.	Se resuelven los problemas relacionados con el montaje de un sistema de archivos.	"Cómo resolver problemas por fallos de montaje en Trusted Extensions" en la página 192

▼ Cómo realizar copias de seguridad de los archivos en Trusted Extensions

Antes de empezar Debe tener asignado el perfil de derechos de copia de seguridad de medios. Debe encontrarse en la zona global.

- **Para conocer los métodos disponibles, consulte "Envío y recepción de datos ZFS" de *Administración de Oracle Solaris: sistemas de archivos ZFS*.**

Precaución – Sólo los siguientes comandos conservan las etiquetas.

- `/usr/lib/fs/ufs/ufsdump` para las copias principales
- `/usr/sbin/tar cT` para las copias pequeñas
- Una secuencia de comandos que llame a cualquiera de estos comandos

  Consulte la página del comando man `ufsdump(1M)`. Para obtener detalles sobre la opción `T` para el comando `tar`, consulte la página del comando man `tar(1)`.

▼ Cómo restaurar archivos en Trusted Extensions

Antes de empezar Tiene el rol de usuario `root` en la zona global.

- **Para conocer los métodos disponibles, consulte "Envío y recepción de datos ZFS" de *Administración de Oracle Solaris: sistemas de archivos ZFS*.**

Precaución – Sólo los siguientes comandos conservan las etiquetas.

- `/usr/lib/fs/ufs/ufsrestore` para restauraciones principales
- `/usr/sbin/tar xT` para restauraciones pequeñas

Para obtener detalles sobre la opción `T` para el comando `tar`, consulte la página del comando man `tar(1)`.

▼ Cómo compartir sistemas de archivos de una zona con etiquetas

Para montar o compartir directorios que se originan en zonas con etiquetas, defina las propiedades de recursos compartidos ZFS correspondientes en el sistema de archivos y, a continuación, reinicie la zona para compartir los directorios con etiquetas.

Precaución – No utilice nombres propietarios para los sistemas de archivos compartidos. Los nombres de los sistemas de archivos compartidos son visibles para todos los usuarios.

Antes de empezar Debe tener asignado el perfil de derechos de gestión de sistemas de archivos ZFS.

1. **Cree un espacio de trabajo en la etiqueta del sistema de archivos que desea compartir.**

   Para obtener detalles, consulte "Cómo agregar un espacio de trabajo en una etiqueta mínima" de *Guía del usuario de Oracle Solaris Trusted Extensions*.

2. **En la zona, cree el sistema de archivos.**

   ```
   # zfs create rpool/wdocs1
   ```

3. **Comparta el sistema de archivos mediante la definición de las propiedades de recursos compartidos ZFS.**

   Por ejemplo, el siguiente conjunto de comandos comparte un sistema de archivos de documentación para escritores. El sistema de archivos se comparte en modo de lectura y escritura para que los escritores puedan modificar sus documentos en este servidor. Los programas `setuid` no están permitidos.

   ```
   # zfs set share=name=wdocs1,path=/wdocs1,prot=nfs,setuid=off,
   exec=off,devices=off rpool/wdocs1
   # zfs set sharenfs=on rpool/wdocs1
   ```

   La línea de comandos se ajustó con fines de visualización.

4 **Inicie cada zona para compartir los directorios.**

En la zona global, ejecute uno de los siguientes comandos para cada zona. Cada zona puede compartir sus sistemas de archivos de cualquiera de estas maneras. El uso compartido real tiene lugar cuando las zonas están en estado `ready` o `running`.

- **Si la zona no está en estado running, y no desea que los usuarios inicien sesión en el servidor en la etiqueta de la zona, fije el estado de la zona en `ready`.**

  ```
  # zoneadm -z zone-name ready
  ```

- **Si la zona no está en estado running, y los usuarios tienen permiso para iniciar sesión en el servidor en la etiqueta de la zona, dé inicio a la zona.**

  ```
  # zoneadm -z zone-name boot
  ```

- **Si la zona ya está en ejecución, reiníciela.**

  ```
  # zoneadm -z zone-name reboot
  ```

5 **Muestre los sistemas de archivos que se comparten desde el sistema.**

En el rol de usuario `root`, en la zona global, ejecute el siguiente comando:

```
# zfs get all rpool
```

Para obtener más información, consulte "Consulta de información del sistema de archivos ZFS" de *Administración de Oracle Solaris: sistemas de archivos ZFS*.

6 **Para permitir que el cliente monte el sistema de archivos compartido, consulte "Cómo montar archivos en NFS en una zona con etiquetas" en la página 191.**

Ejemplo 14–1 Uso compartido del sistema de archivos /export/share en la etiqueta PUBLIC

Para las aplicaciones que se ejecutan en la etiqueta `PUBLIC`, el administrador del sistema permite a los usuarios leer la documentación del sistema de archivos `/export/share` de la zona `public`.

En primer lugar, el administrador cambia la etiqueta del espacio de trabajo a `public` y abre una ventana de terminal. En la ventana, el administrador define propiedades `share` seleccionadas en el sistema de archivos `/reference`. El siguiente comando se ajustó con fines de visualización.

```
# zfs set share=name=reference,path=/reference,prot=nfs,
setuid=off,exec=off,devices=off,rdonly=on rpool/wdocs1
```

A continuación, el administrador comparte el sistema de archivos.

```
# zfs set sharenfs=on rpool/reference
```

El administrador deja el espacio de trabajo `public` y vuelve al espacio de trabajo de Trusted Path. Dado que los usuarios no tienen permiso para iniciar sesión en este sistema de archivos, el administrador establece la zona en el estado "ready" para compartir el sistema de archivos:

```
# zoneadm -z public ready
```

Los usuarios pueden acceder al sistema de archivos compartido una vez que se monta en los sistemas de los usuarios.

▼ Cómo montar archivos en NFS en una zona con etiquetas

En Trusted Extensions, las zonas con etiquetas gestionan el montaje de los archivos en su zona. Los sistemas de archivos de hosts con etiquetas y sin etiquetas se pueden montar en un sistema Trusted Extensions con etiquetas. El sistema debe tener una ruta al servidor de archivos en la etiqueta de la zona de montaje.

- Para montar los archivos como de lectura y escritura desde un host de una sola etiqueta, la etiqueta asignada del host remoto debe coincidir con la etiqueta de la zona de montaje. Se permiten dos configuraciones de host remoto.
  - Se asigna la misma etiqueta al host remoto que la zona de montaje.
  - El host remoto es un servidor de varios niveles que incluye la etiqueta de la zona de montaje.
- Los sistemas de archivos que se montan mediante una zona de nivel superior son de sólo lectura.
- En Trusted Extensions, el archivo de configuración `auto_home` se personaliza por zona. El archivo se denomina según el nombre de la zona. Por ejemplo, si el sistema tiene una zona global y una zona public, habrá dos archivos `auto_home`: `auto_home_global` y `auto_home_public`.

Trusted Extensions utiliza las mismas interfaces de montaje que Oracle Solaris:

- De manera predeterminada, los sistemas de archivos se montan en el inicio.
- Para montar los sistemas de archivos de manera dinámica, utilice el comando `mount` en la zona con etiquetas.
- Para montar los directorios principales automáticamente, utilice los archivos de `auto_home_`*nombre_zona*.
- Para montar otros directorios automáticamente, use los mapas de montaje automático estándares.

Antes de empezar

Debe estar en el sistema cliente, en la zona de la etiqueta de los archivos que desea montar. Verifique que el sistema de archivos que desea montar esté compartido. A menos que esté utilizando el montador automático, debe tener asignado el perfil de derechos de gestión de sistemas de archivos. Para el montaje desde servidores de nivel inferior, la zona de este cliente debe estar configurada con el privilegio `net_mac_aware`.

- **Para montar archivos en NFS en una zona con etiquetas, aplique los procedimientos siguientes.**

  La mayoría de los procedimientos requieren la creación de un espacio de trabajo en una etiqueta determinada. Para crear un espacio de trabajo, consulte "Cómo agregar un espacio de trabajo en una etiqueta mínima" de *Guía del usuario de Oracle Solaris Trusted Extensions*.

  - **Monte los archivos dinámicamente.**

    En la zona con etiquetas, utilice el comando `mount`.

  - **Monte los archivos cuando se inicie la zona.**

  - **Monte los directorios principales en sistemas que se administran con los archivos.**

    a. **Cree y rellene un archivo `/export/home/auto_home_`*nombre_zona_etiqueta_inferior*.**

    b. **Edite el archivo `/etc/auto_home_`*nombre_zona_etiqueta_inferior* a fin de que señale al archivo que recién se rellenó.**

    c. **Modifique el archivo `/etc/auto_home_`*nombre_zona_etiqueta_inferior* en cada zona de nivel superior a fin de que apunte al archivo que creó en el Paso a.**

▼ Cómo resolver problemas por fallos de montaje en Trusted Extensions

Antes de empezar Debe estar en la zona en la etiqueta del sistema de archivos que desea montar. Debe estar con el rol de usuario `root`.

1. **Verifique que los sistemas de archivos del servidor NFS estén compartidos.**

2. **Compruebe los atributos de seguridad del servidor NFS.**

   a. **Utilice el comando `tninfo` o `tncfg` para buscar la dirección IP del servidor o un rango de direcciones IP que incluya el servidor NFS.**

      La dirección se puede asignar de manera directa o de manera indirecta, mediante un mecanismo comodín. La dirección puede estar en una plantilla con etiquetas o sin etiquetas.

   b. **Revise la etiqueta que la plantilla asigna al servidor NFS.**

      Esta etiqueta debe ser coherente con la etiqueta en la que intenta montar los archivos.

3. **Revise la etiqueta de la zona actual.**

   Si esta etiqueta es superior a la etiqueta del sistema de archivos montados, no podrá escribir en el montaje, aunque el sistema de archivos remoto se exporte con permisos de lectura y escritura. Sólo puede escribir en el sistema de archivos montados, en la etiqueta del montaje.

4 **Para montar los sistemas de archivos desde un servidor NFS que ejecuta versiones anteriores del software Trusted Solaris, realice las siguientes acciones:**

- **Para un servidor NFS de Trusted Solaris 1, use las opciones `vers=2` y `proto=udp` para el comando `mount`.**
- **Para un servidor NFS de Trusted Solaris 2.5.1, use las opciones `vers=2` y `proto=udp` para el comando `mount`.**
- **Para un servidor NFS de Trusted Solaris 8, use las opciones `vers=3` y `proto=udp` para el comando `mount`.**

Para montar sistemas de archivos de cualquiera de estos servidores, el servidor debe estar asignado a una plantilla sin etiquetas.

◆ ◆ ◆ CAPÍTULO 15

Redes de confianza (descripción general)

En este capítulo, se describen los conceptos y los mecanismos de las redes de confianza de Trusted Extensions.

La red de confianza

Trusted Extensions asigna atributos de seguridad a las zonas, los hosts y las redes. Estos atributos garantizan que las siguientes funciones de seguridad se apliquen en la red:

- Los datos tienen las etiquetas correctas en las comunicaciones de red.
- Las reglas de control de acceso obligatorio (MAC) se aplican cuando se envían o se reciben datos mediante una red local, y cuando se montan los sistemas de archivos.
- Las reglas de MAC se aplican cuando se enrutan datos a redes distantes.
- Las reglas de MAC se aplican cuando se enrutan datos a zonas.

En Trusted Extensions, MAC protege los paquetes de red. Las etiquetas se utilizan para las decisiones de MAC. Los datos se etiquetan explícita o implícitamente con una etiqueta de sensibilidad. La etiqueta tiene un campo de ID, un campo de clasificación o "nivel" y un campo de compartimiento o "categoría". Los datos deben someterse a una comprobación de acreditación. Esta comprobación determina si la etiqueta está bien formada y si se encuentra dentro del rango de acreditación del host de recepción. Los paquetes bien formados que están dentro del rango de acreditación del host de recepción obtienen acceso.

Es posible etiquetar los paquetes IP que se intercambian entre los sistemas de confianza. Trusted Extensions admite las etiquetas de opción de seguridad de IP común (CIPSO). La

etiqueta CIPSO de un paquete sirve para clasificar, separar y enrutar paquetes IP. Las decisiones de enrutamiento comparan la etiqueta de sensibilidad de los datos con la etiqueta del destino.

Por lo general, en una red de confianza, el host de envío genera la etiqueta y el host de recepción la procesa. Sin embargo, un enrutador de confianza también puede agregar o filtrar etiquetas cuando reenvía paquetes en una red de confianza. Antes de la transmisión, se asigna una etiqueta de sensibilidad a una etiqueta CIPSO. La etiqueta CIPSO está integrada en el paquete IP. En general, el remitente y el receptor de un paquete operan en la misma etiqueta.

El software de las redes de confianza garantiza que la política de seguridad de Trusted Extensions se aplique incluso cuando los sujetos (procesos) y los objetos (datos) estén en hosts diferentes. Las redes de Trusted Extensions mantienen el MAC en todas las aplicaciones distribuidas.

Paquetes de datos de Trusted Extensions

Los paquetes de datos de Trusted Extensions incluyen una opción de etiqueta CIPSO. Los paquetes de datos pueden enviarse mediante las redes IPv4 o IPv6.

En el formato IPv4 estándar, el encabezado IPv4 con opciones va seguido de un encabezado TCP, UDP o SCTP, y, a continuación, los datos reales. La versión de Trusted Extensions de un paquete IPv4 utiliza la opción CIPSO del encabezado IP para los atributos de seguridad.

En el formato IPv6 estándar, un encabezado IPv6 con extensiones va seguido de un encabezado TCP, UDP o SCTP, y, a continuación, los datos reales. El paquete IPv6 de Trusted Extensions incluye una opción de seguridad de varios niveles en el encabezado con extensiones.

Comunicaciones de la red de confianza

Trusted Extensions admite hosts con etiquetas y sin etiquetas en una red de confianza. La interfaz gráfica de usuario `txzonemgr` y el comando `tncfg` se utilizan para configurar la red.

Los sistemas que ejecutan el software Trusted Extensions admiten las comunicaciones de red entre los sistemas Trusted Extensions y cualquiera de los siguientes tipos de host:

- Otros hosts que ejecutan Trusted Extensions.
- Hosts que ejecutan sistemas operativos que no reconocen atributos de seguridad, pero que admiten TCP/IP, como los sistemas Oracle Solaris, otros sistemas UNIX, sistemas Macintosh OS y Microsoft Windows.
- Hosts que ejecutan otros sistemas operativos de confianza que reconocen etiquetas CIPSO.

Como en el SO Oracle Solaris, el servicio de nombres puede administrar las comunicaciones y los servicios de red de Trusted Extensions. Trusted Extensions agrega las siguientes interfaces a las interfaces de red de Oracle Solaris:

- Trusted Extensions agrega comandos y proporciona una interfaz gráfica de usuario para administrar las redes de confianza. Trusted Extensions también agrega opciones a los comandos de red de Oracle Solaris. Para obtener una descripción de estos comandos, consulte "Comandos de red en Trusted Extensions" en la página 197.

  Las interfaces gestionan tres bases de datos de configuración de red de Trusted Extensions, `tnzonecfg`, `tnrhdb` y `tnrhtp`. Para obtener detalles, consulte "Bases de datos de configuración de red en Trusted Extensions" en la página 199.
- Trusted Extensions agrega las bases de datos `tnrhtp` y `tnrhdb` a las propiedades del servicio SMF de cambio de servicio de nombres, `svc:/system/name-service/switch`.
- En la Parte I, se describe cómo definir zonas y hosts al configurar la red. Para conocer procedimientos adicionales, consulte el Capítulo 16, "Gestión de redes en Trusted Extensions (tareas)".
- Trusted Extensions amplía el archivo de configuración de IKE, `/etc/inet/ike/config`. Para obtener más información, consulte "Administración de IPsec con etiquetas" en la página 211 y la página del comando man `ike.config(4)`.

Comandos de red en Trusted Extensions

Trusted Extensions agrega los siguientes comandos para administrar las redes de confianza:

- `tncfg`: este comando crea, modifica y muestra la configuración de la red de Trusted Extensions. El comando `tncfg -t` se utiliza para ver, crear o modificar una plantilla de seguridad especificada. El comando `tncfg -z` se utiliza para ver o modificar las propiedades de red de una zona especificada. Para obtener detalles, consulte la página del comando man `tncfg(1M)`.
- `tnchkdb`: este comando se utiliza para comprobar la precisión de las bases de datos de la red de confianza. El comando `tnchkdb` se llama cada vez que se cambia una plantilla de seguridad (`tnrhtp`), una asignación de plantilla de seguridad (`tnrhdb`) o la configuración de una zona (`tnzonecfg`) mediante el comando `tncfg` o `txzonemgr`. Para obtener detalles, consulte la página del comando man `tnchkdb(1M)`.

- `tnctl`: este comando puede utilizarse para actualizar la información de la red de confianza en el núcleo. `tnctl` también es un servicio del sistema. Cuando se reinicia con el comando `svcadm restart /network/tnctl`, se refresca la antememoria del núcleo de las bases de datos de la red de confianza en el sistema local. Para obtener detalles, consulte la página del comando man `tnctl`(1M).
- `tnd`: este daemon extrae la información de `tnrhdb` y `tnrhtp` del directorio LDAP y los archivos locales. El orden de búsqueda está determinado por el servicio SMF `name-service/switch`. En el momento del inicio, el servicio `svc:/network/tnd` inicia el daemon `tnd`. Este servicio depende de `svc:/network/ldap/client`.

  En una red LDAP, el comando `tnd` también se puede utilizar para la depuración y para la modificación del intervalo de sondeo. Para obtener detalles, consulte la página del comando man `tnd`(1M).
- `tninfo`: este comando muestra los detalles del estado actual de la antememoria del núcleo de la red de confianza. Es posible filtrar los resultados por zona, plantilla de seguridad o nombre de host. Para obtener detalles, consulte la página del comando man `tninfo`(1M).

Trusted Extensions agrega opciones a los siguientes comandos de red de Oracle Solaris:

- `ipadm`: la propiedad de dirección `all-zones` permite que la interfaz especificada esté disponible para cada zona del sistema. La zona adecuada para entregar los datos se encuentra determinada por la etiqueta que está asociada con los datos. Para obtener detalles, consulte la página del comando man `ipadm`(1M).
- `netstat`: la opción `-R` amplía el uso de `netstat` de Oracle Solaris para mostrar información específica de Trusted Extensions, como los atributos de seguridad para sockets de varios niveles y las entradas de la tabla de enrutamiento. Los atributos de seguridad ampliados incluyen la etiqueta del igual y establecen si el socket es específico para una zona o si está disponible para varias zonas. Para obtener detalles, consulte la página del comando man `netstat`(1M).
- `route`: la opción `-secattr` amplía el uso de `route` de Oracle Solaris para mostrar los atributos de seguridad de la ruta. El valor de la opción tiene el siguiente formato:

  `min_sl=`*label*`,max_sl=`*label*`,doi=`*integer*`,cipso`

  La palabra clave `cipso` es opcional y se establece de manera predeterminada. Para obtener detalles, consulte la página del comando man `route`(1M).
- `snoop`: como en Oracle Solaris, puede utilizarse la opción `-v` de este comando para mostrar los encabezados IP de manera detallada. En Trusted Extensions, los encabezados contienen información de la etiqueta.
- `ipseckey`: en Trusted Extensions, las siguientes extensiones están disponibles para los paquetes de etiquetas protegidos por IPsec: `label` *etiqueta*, `outer-label` *etiqueta* e `implicit-label` *etiqueta*. Para obtener más información, consulte la página del comando man `ipseckey`(1M).

Bases de datos de configuración de red en Trusted Extensions

Trusted Extensions carga tres bases de datos de configuración de red en el núcleo. Estas bases de datos se utilizan en las comprobaciones de acreditaciones cuando se transmiten datos de un host a otro.

- `tnzonecfg`: esta base de datos local almacena atributos de la zona que están relacionados con la seguridad. El comando `tncfg` es la interfaz para acceder a esta base de datos y modificarla.

  Los atributos de cada zona especifican la etiqueta de la zona y el acceso de dicha zona a los puertos de un solo nivel y de varios niveles. Otro atributo gestiona las respuestas a los mensajes de control, como `ping`. Las etiquetas de las zonas se definen en el archivo `label_encodings`. Para obtener más información, consulte la página del comando man `label_encodings(4)`. Para ver una explicación sobre los puertos de varios niveles, consulte "Zonas y puertos de varios niveles" en la página 169.

- `tnrhtp`: esta base de datos almacena plantillas que describen los atributos de seguridad de los hosts y las puertas de enlace. El comando `tncfg` es la interfaz para acceder a esta base de datos y modificarla.

  Los hosts y las puertas de enlace utilizan los atributos del host de destino y la puerta de enlace del próximo salto para aplicar el MAC al enviar tráfico. Cuando el tráfico se recibe, los hosts y las puertas de enlace utilizan los atributos del remitente. Para obtener detalles sobre los atributos de seguridad, consulte "Atributos de seguridad de la red de confianza" en la página 199.

- `tnrhdb`: esta base de datos almacena las direcciones IP y los rangos de direcciones IP que corresponden a todos los hosts que pueden comunicarse con este sistema. El comando `tncfg` es la interfaz para acceder a esta base de datos y modificarla.

  Se asigna una plantilla de seguridad de la base de datos `tnrhtp` a cada host o rango de direcciones IP. Los atributos de la plantilla definen los atributos del host asignado.

Atributos de seguridad de la red de confianza

La administración de redes en Trusted Extensions se basa en plantillas de seguridad. Una plantilla de seguridad describe un conjunto de hosts que tienen protocolos y atributos de seguridad idénticos.

Los atributos de seguridad se asignan de manera administrativa a sistemas remotos, tanto hosts como enrutadores, mediante plantillas. El administrador de la seguridad administra las plantillas y las asigna a sistemas remotos. Si no se asigna ninguna plantilla a un sistema remoto, no se permiten las comunicaciones con ese sistema.

Cada plantilla recibe un nombre e incluye lo siguiente:

- Un tipo de host, que puede ser sin etiquetas o CIPSO. El tipo de host de la plantilla determina el protocolo que se utiliza para las comunicaciones de red.

  El tipo de host se utiliza para determinar si se usan o no las opciones de CIPSO y afecta el MAC. Consulte "Tipo de host y nombre de plantilla en plantillas de seguridad" en la página 201.
- Un conjunto de atributos de seguridad que se aplican a cada tipo de host.

Para obtener más detalles, consulte "Atributos de seguridad de red en Trusted Extensions" en la página 200.

Atributos de seguridad de red en Trusted Extensions

Un sistema Trusted Extensions se instala con un conjunto predeterminado de plantillas de seguridad que se utilizan para definir las propiedades de etiquetas de los hosts remotos. En Trusted Extensions, se asignan atributos de seguridad a los hosts con etiquetas y sin etiquetas de la red mediante una plantilla de seguridad. Los hosts que no tienen una plantilla de seguridad asignada no pueden comunicarse con los hosts que están configurados con Trusted Extensions. Las plantillas se almacenan de manera local.

Los hosts se pueden agregar a una plantilla de seguridad según la dirección IP o como parte de un rango de direcciones IP. Para obtener una explicación más detallada, consulte "Mecanismo de reserva de la red de confianza" en la página 203.

Cada tipo de host tiene su propio conjunto de atributos de seguridad adicionales, tanto necesarios como opcionales. Los siguientes atributos de seguridad están especificados en las plantillas de seguridad:

- **Tipo de host**: define si los paquetes tienen etiquetas de seguridad CIPSO o no tienen ningún tipo de etiquetas.
- **Etiqueta predeterminada**: define el nivel de confianza del host sin etiquetas. En esta etiqueta, el host o la puerta de enlace de recepción de Trusted Extensions leen los paquetes que se envían mediante un host sin etiquetas.

  El atributo de la etiqueta predeterminada es específico del tipo de host `unlabeled`. Para obtener detalles, consulte "Etiqueta predeterminada en plantillas de seguridad" en la página 202.
- **DOI**: es un entero positivo, distinto de cero, que identifica el dominio de interpretación. El DOI se utiliza para indicar qué conjunto de codificaciones de etiqueta se aplica a una comunicación o entidad de red. Las etiquetas con DOI diferentes están separadas, incluso si son idénticas en todo lo demás. En los hosts `unlabeled`, el DOI se aplica a la etiqueta predeterminada. En Trusted Extensions, el valor predeterminado es `1`.

- **Etiqueta mínima**: define el nivel más bajo del rango de acreditación de etiquetas. Los hosts y las puertas de enlace del próximo salto no reciben paquetes que estén por debajo de la etiqueta mínima que está especificada en la plantilla correspondiente.
- **Etiqueta máxima**: define el nivel más alto del rango de acreditación de etiquetas. Los hosts y las puertas de enlace del próximo salto no reciben paquetes que estén por encima de la etiqueta máxima que está especificada en la plantilla correspondiente.
- **Conjunto de etiquetas auxiliares**: es opcional. Especifica un conjunto discreto de etiquetas de seguridad para una plantilla de seguridad. Además su rango de acreditación determinado por la etiqueta máxima y la etiqueta mínima, los hosts que se agregan a una plantilla con un conjunto de etiquetas auxiliares pueden enviar y recibir paquetes que coincidan con cualquiera de las etiquetas del conjunto. El número máximo de etiquetas auxiliares que se puede especificar es cuatro.

Tipo de host y nombre de plantilla en plantillas de seguridad

Trusted Extensions admite dos tipos de host en las bases de datos de la red de confianza y proporciona dos plantillas predeterminadas:

- **Tipo de host CIPSO**: diseñado para los host que ejecutan sistemas operativos de confianza. Trusted Extensions suministra la plantilla denominada `cipso` para este tipo de host.

  El protocolo de opción de seguridad de IP común (CIPSO) se utiliza para especificar las etiquetas de seguridad que se transfieren en el campo de opciones IP. Las etiquetas CIPSO se obtienen automáticamente de la etiqueta de datos. El tipo de etiqueta 1 se utiliza para transferir la etiqueta de seguridad CIPSO. Esta etiqueta se utiliza para realizar comprobaciones de seguridad en el nivel IP y para asignar una etiqueta a los datos del paquete de red.
- **Tipo de host sin etiquetas**: está diseñado para los hosts que utilizan protocolos de redes estándar, pero que no admiten opciones de CIPSO. Trusted Extensions suministra la plantilla denominada `admin_low` para este tipo de host.

  Se asigna este tipo de host a los hosts que ejecutan el SO Oracle Solaris u otros sistemas operativos sin etiquetas. Este tipo de host proporciona una etiqueta y una acreditación predeterminadas para aplicar a las comunicaciones con el host sin etiquetas. Además, se puede especificar un rango de etiquetas o un conjunto de etiquetas discretas para permitir el envío de paquetes a una puerta de enlace sin etiquetas para el posterior reenvío.

Precaución – La plantilla `admin_low` brinda un ejemplo para la creación de plantillas sin etiquetas con etiquetas específicas del sitio. Mientras que la plantilla `admin_low` es necesaria para la instalación de Trusted Extensions, es posible que los atributos de seguridad sean demasiado liberales para el funcionamiento normal del sistema. Conserve las plantillas proporcionadas sin modificaciones para el mantenimiento del sistema y el soporte técnico.

Etiqueta predeterminada en plantillas de seguridad

Las plantillas para el tipo de host sin etiquetas especifican una etiqueta predeterminada. Esta etiqueta se utiliza para controlar las comunicaciones con los hosts cuyos sistemas operativos no reconocen etiquetas, como los sistemas Oracle Solaris. La etiqueta predeterminada que está asignada refleja el nivel de confianza adecuado para el host y los usuarios.

Debido a que las comunicaciones con los hosts sin etiquetas se limitan esencialmente a la etiqueta predeterminada, estos hosts también se denominan *hosts de una sola etiqueta*. Una razón técnica para llamar a estos hosts "de una sola etiqueta" es que estos hosts no tienen etiquetas `admin_high` ni `admin_low`.

Dominio de interpretación en plantillas de seguridad

Las organizaciones que utilizan el mismo dominio de interpretación (DOI) deben acordar entre sí para interpretar la información de la etiqueta y otros atributos de seguridad de la misma manera. Cuando Trusted Extensions realiza una comparación de etiquetas, se efectúa una comprobación para determinar si el DOI es igual.

Un sistema Trusted Extensions aplica la política de etiquetas en un valor DOI. Todas las zonas de un sistema Trusted Extensions deben operar en el mismo DOI. Un sistema Trusted Extensions no proporciona el tratamiento de excepciones en los paquetes que se recibieron de un sistema que utiliza un DOI diferente.

Si su sitio utiliza un valor DOI diferente del valor predeterminado, debe utilizar este valor en cada plantilla de seguridad, como se describe en "Cómo configurar el dominio de interpretación" en la página 55.

Rango de etiquetas en plantillas de seguridad

Los atributos de la etiqueta mínima y la etiqueta máxima se utilizan para establecer el rango de etiquetas para los hosts con etiquetas y sin etiquetas. Estos atributos se utilizan para realizar lo siguiente:

- Establecer el rango de etiquetas que pueden utilizarse cuando se establece la comunicación con un host CIPSO remoto

  Para poder enviar un paquete a un host de destino, la etiqueta del paquete debe estar dentro del rango de etiquetas asignado en la plantilla de seguridad del host de destino.
- Establecer un rango de etiquetas para los paquetes que se reenvían mediante una puerta de enlace CIPSO o una sin etiquetas

  Puede especificarse el rango de etiquetas en la plantilla para un tipo de host sin etiquetas. El rango de etiquetas habilita el host para reenviar los paquetes que no están necesariamente en la etiqueta del host, pero se encuentran dentro de un rango de etiquetas especificado.

Etiquetas auxiliares en plantillas de seguridad

El conjunto de etiquetas auxiliares define un máximo de cuatro etiquetas discretas en que el host remoto puede aceptar, enviar o reenviar paquetes. Este atributo es opcional. De manera predeterminada, no hay ningún conjunto de etiquetas auxiliares definido.

Mecanismo de reserva de la red de confianza

Es posible agregar una dirección IP de un host a una plantilla de seguridad directamente o indirectamente. La asignación directa agrega la dirección IP de un host. La asignación indirecta agrega un rango de direcciones IP que incluye el host. Para asociar un determinado host, el software de la red de confianza busca primero la dirección IP específica. Si la búsqueda no encuentra una entrada específica para el host, busca el "prefijo más extenso de bits coincidentes". Puede asignar indirectamente un host a una plantilla de seguridad cuando la dirección IP del host está comprendida dentro del "prefijo más extenso de bits coincidentes" de una dirección IP que tiene una longitud de prefijo fija.

En IPv4, puede realizar una asignación indirecta mediante la subred. Cuando se realiza una asignación indirecta con 1, 2, 3 ó 4 octetos de cero (0) final, el software calcula una longitud de prefijo de 24, 16, 8 ó 0, respectivamente. Para ver ejemplos, consulte la Tabla 15–1.

También puede determinar una longitud de prefijo fija si agrega una barra diagonal (/) seguida del número de bits fijos. Las direcciones de red IPv4 pueden tener una longitud de prefijo entre 1 y 32. Las direcciones de red IPv6 pueden tener una longitud de prefijo entre 1 y 128.

La siguiente tabla proporciona ejemplos de direcciones de host y de reserva. Si una dirección del conjunto de direcciones de reserva está asignada de manera directa, el mecanismo de reserva no se utiliza para esa dirección.

TABLA 15–1 Entradas del mecanismo de reserva y la dirección de host de Trusted Extensions

Versión de IP	Entrada de host para `host_type=cipso`	Direcciones IP cubiertas
IPv4	`192.168.118.57`	`192.168.118.57`
	`192.168.118.57/32`	`/32` establece una longitud de prefijo de 32 bits fijos.
	`192.168.118.128/26`	De `192.168.118.0` a `192.168.118.63`
	`192.168.118.0`	Todas las direcciones de la subred `192.168.118.`
	`192.168.118.0/24`	
	`192.168.0.0/24`	Todas las direcciones de la subred `192.168.0.`
	`192.168.0.0`	Todas las direcciones de la subred `192.168.`
	`192.168.0.0/16`	
	`192.0.0.0`	Todas las direcciones de la subred `192.`
	`192.0.0.0/8`	
	`192.168.118.0/32`	Dirección de host `192.168.118.0`. No es un rango de direcciones.
	`192.168.0.0/32`	Dirección de host `192.168.0.0`. No es un rango de direcciones.
	`192.0.0.0/32`	Dirección de host `192.0.0.0`. No es un rango de direcciones.
	`0.0.0.0/32`	Dirección de host `0.0.0.0`. No es un rango de direcciones.
	`0.0.0.0`	Todas las direcciones de todas las redes.
IPv6	`2001\:DB8\:22\:5000\:\:21f7`	`2001:DB8:22:5000::21f7`
	`2001\:DB8\:22\:5000\:\:0/52`	De `2001:DB8:22:5000::0` a `2001:DB8:22:5fff:ffff:ffff:ffff:ffff`
	`0\:\:0/0`	Todas las direcciones de todas las redes.

Observe que la dirección `0.0.0.0/32` coincide con la dirección específica, `0.0.0.0`. Al agregar la entrada `0.0.0.0/32` a la plantilla de seguridad sin etiquetas de un sistema, permite que los hosts con la dirección específica, `0.0.0.0`, se comuniquen con el sistema. Por ejemplo, los clientes DHCP se contactan con el servidor DHCP como `0.0.0.0` antes de que el servidor les proporcione una dirección IP.

Para crear una entrada `tnrhdb` para una aplicación que presta servicios a clientes DHCP, consulte el Ejemplo 16–16. La red `0.0.0.0:admin_low` es la entrada predeterminada en plantilla de host sin etiquetas `admin_low`. Consulte "Cómo limitar los hosts que se pueden contactar en la red de confianza" en la página 229 para conocer los temas de seguridad que requieren el cambio de esta opción predeterminada.

Para obtener más información sobre las longitudes de prefijos en las direcciones IPv4 e IPv6, consulte "Cómo decidir el formato de las direcciones IP para la red" de *Administración de Oracle Solaris: servicios IP* y "IPv6 Addressing Overview" de *System Administration Guide: IP Services*.

Descripción general del enrutamiento en Trusted Extensions

En Trusted Extensions, las rutas que unen los hosts de diferentes redes deben preservar la seguridad en cada etapa de la transmisión. Trusted Extensions agrega atributos de seguridad ampliados a los protocolos de enrutamiento en el SO Oracle Solaris. A diferencia de Oracle Solaris, Trusted Extensions no admite el enrutamiento dinámico. Para obtener detalles sobre la especificación del enrutamiento estático, consulte la opción `-p` de la página del comando man `route`(1M).

Paquetes de ruta de enrutadores y puertas de enlace. Aquí se utilizan los términos "puerta de enlace" y "enrutador" de manera intercambiable.

En las comunicaciones entre dos hosts de la misma subred, las comprobaciones de acreditaciones se realizan en los puntos finales sólo porque no participan enrutadores. Las comprobaciones de los rangos de etiquetas se llevan a cabo en el origen. Si el host de recepción ejecuta el software Trusted Extensions, las comprobaciones de los rangos de etiquetas también se efectúan en el destino.

Cuando los hosts de origen y de destino se encuentran en subredes diferentes, el paquete se envía desde el host de origen hasta una puerta de enlace. El rango de etiquetas del destino y la puerta de enlace del primer salto se comprueban en el origen cuando una ruta está seleccionada. La puerta de enlace envía el paquete a la red en que está conectado el host de destino. Es posible que un paquete atraviese varias puertas de enlace antes de llegar al destino.

Conocimientos básicos del enrutamiento

En las puertas de enlace de Trusted Extensions, las comprobaciones de los rangos de etiquetas se llevan a cabo en algunos casos. Un sistema Trusted Extensions que enruta un paquete entre dos hosts sin etiquetas compara la etiqueta predeterminada del host de origen con la etiqueta predeterminada del host de destino. Cuando los hosts sin etiquetas comparten una etiqueta predeterminada, se enruta el paquete.

Cada puerta de enlace mantiene una lista de rutas con todos los destinos. El enrutamiento estándar de Oracle Solaris incluye opciones para optimizar la ruta. Trusted Extensions proporciona software adicional para comprobar los requisitos de seguridad que se aplican a las opciones de ruta. Se omiten las opciones de Oracle Solaris que no cumplen los requisitos de seguridad.

Entradas de la tabla de enrutamiento en Trusted Extensions

Las entradas de la tabla de enrutamiento de Trusted Extensions pueden incorporar atributos de seguridad. Los atributos de seguridad pueden incluir una palabra clave `cipso`. Los atributos de seguridad deben incluir una etiqueta máxima, una etiqueta mínima y un DOI.

En las entradas que no proporcionan atributos de seguridad, se utilizan los atributos de la plantilla de seguridad de la puerta de enlace.

Comprobaciones de acreditaciones de Trusted Extensions

El software Trusted Extensions determina la idoneidad de una ruta por cuestiones de seguridad. El software efectúa una serie de pruebas que se denominan *comprobaciones de acreditaciones* en el host de origen, el host de destino y las puertas de enlace intermedias.

Nota – En la explicación siguiente, la comprobación de acreditación de un rango de etiquetas también implica la comprobación de un conjunto de etiquetas auxiliares.

La comprobación de acreditación controla el rango de etiquetas y la información de la etiqueta CIPSO. Los atributos de seguridad de una ruta se obtienen de la entrada de la tabla de enrutamiento o de la plantilla de seguridad de la puerta de enlace si la entrada no tiene atributos de seguridad.

Para las comunicaciones entrantes, el software Trusted Extensions obtiene etiquetas de los paquetes siempre que sea posible. La obtención de etiquetas de los paquetes sólo es posible cuando los mensajes se envían desde hosts que admiten etiquetas. Cuando una etiqueta no está disponible en el paquete, se asigna una etiqueta predeterminada al mensaje desde la plantilla de seguridad. Estas etiquetas se utilizan posteriormente en las comprobaciones de acreditaciones. Trusted Extensions aplica varias comprobaciones en los mensajes entrantes, salientes y reenviados.

Comprobaciones de acreditaciones del origen

Las siguientes comprobaciones de acreditaciones se realizan en el proceso o la zona de envío:

- En todos los destinos, el DOI de un paquete saliente debe coincidir con el DOI del host de destino. El DOI también debe coincidir con el DOI de todos los saltos de la ruta, incluida la puerta de enlace del primer salto.
- En todos los destinos, la etiqueta del paquete saliente debe estar dentro del rango de etiquetas del próximo salto en la ruta, es decir, el primer salto. Además, la etiqueta debe estar incluida en los atributos de seguridad de la puerta de enlace del primer salto.
- Cuando el host de destino es un host sin etiquetas, debe cumplirse una de las siguientes condiciones:
  - La etiqueta del host de envío debe coincidir con la etiqueta predeterminada del host de destino.
  - El host de envío tiene el privilegio de establecer comunicaciones de etiqueta cruzada, y la etiqueta del remitente domina la etiqueta predeterminada del destino.
  - El host de envío tiene el privilegio de establecer comunicaciones de etiqueta cruzada, y la etiqueta del remitente es `ADMIN_LOW`. Es decir, el remitente realiza el envío desde la zona global.

Nota – Una comprobación del primer salto tiene lugar cuando se envía un mensaje por medio de una puerta de enlace de un host en una red a un host en otra red.

Comprobaciones de acreditaciones de la puerta de enlace

En un sistema de puerta de enlace de Trusted Extensions, se realizan las siguientes comprobaciones de acreditaciones para la puerta de enlace del próximo salto:

- Si el paquete entrante no tiene etiquetas, el paquete hereda la etiqueta predeterminada del host de origen desde la plantilla de seguridad. De lo contrario, el paquete recibe la etiqueta CIPSO indicada.
- Las comprobaciones para el envío de un paquete se efectúan de manera similar a la acreditación de origen:
  - En todos los destinos, el DOI de un paquete saliente debe coincidir con el DOI del host de destino. El DOI también debe coincidir con el DOI del host del próximo salto.
  - En todos los destinos, la etiqueta del paquete saliente debe estar dentro del rango de etiquetas del próximo salto. Además, la etiqueta debe estar incluida en los atributos de seguridad que corresponden al host del próximo salto.
  - La etiqueta de un paquete sin etiquetas debe coincidir con la etiqueta predeterminada del host de destino.
  - La etiqueta de un paquete CIPSO debe estar dentro del rango de etiquetas del host de destino.

Comprobaciones de acreditaciones del destino

Cuando un sistema Trusted Extensions recibe datos, el software realiza las siguientes comprobaciones:

- Si el paquete entrante no tiene etiquetas, el paquete hereda la etiqueta predeterminada del host de origen desde la plantilla de seguridad. De lo contrario, el paquete recibe la etiqueta CIPSO indicada.
- La etiqueta y el DOI del paquete deben ser coherentes con la zona de destino o la etiqueta y el DOI del proceso de destino. La única excepción es cuando el proceso realiza la recepción en un puerto de varios niveles. El proceso que recibe puede obtener un paquete si tiene el privilegio de establecer comunicaciones de etiqueta cruzada y se encuentra en la zona global o tiene una etiqueta que domina la etiqueta del paquete.

Administración del enrutamiento en Trusted Extensions

Trusted Extensions admite varios métodos para el enrutamiento de las comunicaciones entre redes. Puede configurar rutas que apliquen el grado de seguridad que requiere la política de seguridad de su sitio.

Por ejemplo, los sitios pueden restringir las comunicaciones fuera de la red local para una sola etiqueta. Esta etiqueta se aplica a la información disponible públicamente. Las etiquetas como `UNCLASSIFIED` o `PUBLIC` pueden indicar información pública. Para aplicar la restricción, estos sitios agregan la interfaz de red de la puerta de enlace que está conectada con la red externa a una plantilla de una sola etiqueta. Para obtener más detalles sobre TCP/IP y el enrutamiento, consulte lo siguiente:

- "Configuración de un enrutador IPv4" de *Administración de Oracle Solaris: servicios IP*
- "Configuración de los componentes del sistema en la red" de *Administración de Oracle Solaris: servicios IP*
- "Tareas de administración principales de TCP/IP (mapa de tareas)" de *Administración de Oracle Solaris: servicios IP*
- `netcfg`(1M)

Selección de los enrutadores en Trusted Extensions

Los hosts de Trusted Extensions ofrecen el mayor grado de confianza para los enrutadores. Es posible que otros tipos de enrutadores no reconozcan los atributos de seguridad de Trusted Extensions. Sin ninguna acción administrativa, se pueden enrutar los paquetes mediante enrutadores que no proporcionen protección de seguridad del MAC.

- Los enrutadores CIPSO descartan los paquetes cuando no encuentran el tipo correcto de información en la sección de opciones IP del paquete. Por ejemplo, un enrutador CIPSO descarta un paquete si no encuentra una opción CIPSO en las opciones IP cuando la opción es necesaria o cuando el DOI de las opciones IP no es consistente con la acreditación del destino.
- Es posible configurar otros tipos de enrutadores que no ejecutan el software Trusted Extensions para transferir los paquetes o descartar aquellos paquetes que incluyan la opción CIPSO. Sólo las puertas de enlace que reconocen CIPSO, como las que ofrece Trusted Extensions, pueden utilizar el contenido de la opción IP de CIPSO para aplicar el MAC.

Para admitir el enrutamiento de confianza, se ampliaron las tablas de enrutamiento a fin de incluir los atributos de seguridad de Trusted Extensions. En "Entradas de la tabla de enrutamiento en Trusted Extensions" en la página 206, se describen los atributos. Trusted Extensions admite el enrutamiento estático, en el que el administrador crea manualmente las entradas de la tabla de enrutamiento. Para obtener detalles, consulte la opción `-p` en la página del comando man `route(1M)`.

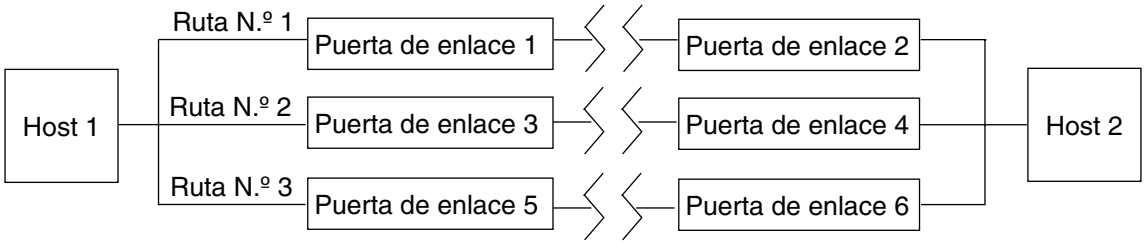
El software de enrutamiento intenta buscar una ruta para el host de destino en las tablas de enrutamiento. Cuando el host no está nombrado de manera explícita, el software de enrutamiento busca una entrada para la subred donde reside el host. Cuando no están definidos ni el host ni la subred, el host envía el paquete a una puerta de enlace predeterminada en caso de que esté definida. Se pueden definir varias puertas de enlace predeterminadas, y todas son tratadas del mismo modo.

En esta versión de Trusted Extensions, el administrador de la seguridad configura manualmente las rutas y, a continuación, cambia manualmente la tabla de enrutamiento cuando cambian las condiciones. Por ejemplo, varios sitios tienen una sola puerta de enlace que comunica con el mundo exterior. En estos casos, se puede definir estadísticamente dicha puerta de enlace como *predeterminada* para cada host de la red.

Puertas de enlace en Trusted Extensions

A continuación, se muestra un ejemplo de enrutamiento en Trusted Extensions. El diagrama y la tabla muestran tres rutas posibles entre el host 1 y el host 2.

FIGURA 15–1 Rutas y entradas de la tabla de enrutamiento típicas de Trusted Extensions



Ruta	Puerta de enlace del primer salto	Etiqueta mínima	Etiqueta máxima	DOI
N.º 1	Puerta de enlace 1	`CONFIDENTIAL`	`SECRET`	1
N.º 2	Puerta de enlace 3	`ADMIN_LOW`	`ADMIN_HIGH`	1
N.º 3	Puerta de enlace 5			

- La ruta N.º 1 puede transmitir paquetes dentro del rango de etiquetas de `CONFIDENTIAL` a `SECRET`.
- La ruta N.º 2 puede transmitir paquetes de `ADMIN_LOW` a `ADMIN_HIGH`.
- La ruta N.º 3 no especifica información del enrutamiento. Por lo tanto, sus atributos de seguridad se derivan de la plantilla de seguridad de la puerta de enlace 5.

Comandos de enrutamiento en Trusted Extensions

Para mostrar etiquetas y atributos de seguridad ampliados para los sockets, Trusted Extensions modifica los siguientes comandos de red de Oracle Solaris:

- El comando `netstat -rR` muestra los atributos de seguridad en las entradas de la tabla de enrutamiento.
- El comando `netstat -aR` muestra los atributos de seguridad para sockets.
- El comando `route -p` con las opciones `add` o `delete` cambia las entradas de la tabla de enrutamiento.

Para obtener detalles, consulte las páginas del comando man `netstat(1M)` y `route(1M)`.

Para cambiar las entradas de la tabla de enrutamiento, Trusted Extensions proporciona las siguientes interfaces:

- La interfaz gráfica de usuario `txzonemgr` se puede utilizar para asignar la ruta predeterminada de una interfaz.
- El comando `route -p` con la opción `add` o `delete` se puede usar para cambiar las entradas de la tabla de enrutamiento.

Para ver ejemplos, consulte "Cómo agregar rutas predeterminadas" en la página 232.

Administración de IPsec con etiquetas

Los sistemas Trusted Extensions pueden proteger los paquetes de red con etiquetas mediante IPsec. Los paquetes IPsec se pueden enviar con etiquetas explícitas o implícitas de Trusted Extensions. Las etiquetas se envían de manera explícita mediante las opciones IP de CIPSO y de manera implícita por medio de las asociaciones de seguridad (SA) de IPsec con etiquetas. Además, los paquetes IPsec cifrados con diferentes etiquetas implícitas se pueden enviar mediante túneles a través de una red sin etiquetas.

Para conocer los procedimientos de configuración y los conceptos generales de IPsec, consulte la Parte III, "Seguridad IP" de *Administración de Oracle Solaris: servicios IP*. Para conocer las modificaciones de Trusted Extensions en los procedimientos de IPsec, consulte "Configuración de IPsec con etiquetas (mapa de tareas)" en la página 236.

Etiquetas para intercambios protegidos por IPsec

Todas las comunicaciones de los sistemas Trusted Extensions, incluidas las comunicaciones protegidas por IPsec, deben cumplir las comprobaciones de acreditaciones de las etiquetas de seguridad. Las comprobaciones se describen en "Comprobaciones de acreditaciones de Trusted Extensions" en la página 206.

Las etiquetas de los paquetes IPsec provenientes de una aplicación en una zona con etiquetas que deben superar estas comprobaciones son la *etiqueta interna*, la *etiqueta de transferencia* y la *etiqueta de gestión de claves*:

- **Etiqueta de seguridad de la aplicación**: la etiqueta de la zona en la que reside la aplicación.
- **Etiqueta interna**: la etiqueta de los datos del mensaje no cifrados antes de aplicar los encabezados AH o ESP de IPsec. Esta etiqueta puede ser diferente de la etiqueta de seguridad de la aplicación cuando se utiliza la opción de socket `SO_MAC_EXEMPT` (exenta de MAC) o las funciones del puerto de varios niveles (MLP). Al seleccionar asociaciones de seguridad (SA) y reglas IKE que están restringidas por etiquetas, IPsec e IKE utilizan esta etiqueta interna.

  De manera predeterminada, la etiqueta interna es igual a la etiqueta de seguridad de la aplicación. Normalmente, las aplicaciones en ambos extremos tienen la misma etiqueta. Sin embargo, para las comunicaciones MLP o exentas de MAC, esta condición puede no ser cierta. Los valores de configuración IPsec pueden definir cómo se transmite la etiqueta interna en la red, es decir, pueden definir la *etiqueta de transferencia*. Los valores de configuración IPsec no pueden definir el valor de la etiqueta interna.
- **Etiqueta de transferencia**: la etiqueta de los datos del mensaje cifrados después de aplicar los encabezados AH o ESP de IPsec. Según los archivos de configuración de IKE e IPsec, la etiqueta de transferencia puede ser diferente de la etiqueta interna.

- **Etiqueta de gestión de claves**: todas las negociaciones IKE entre dos nodos se controlan en una única etiqueta, independientemente de la etiqueta de los mensajes de la aplicación que activan las negociaciones. La etiqueta de las negociaciones IKE se define en el archivo `/etc/inet/ike/config` según la regla IKE.

Extensiones de etiquetas para asociaciones de seguridad IPsec

Las *extensiones de etiquetas* de IPsec se utilizan en los sistemas Trusted Extensions para asociar una etiqueta con el tráfico que se transmite dentro de una asociación de seguridad (SA). De manera predeterminada, IPsec no usa extensiones de etiquetas y, por lo tanto, ignora las etiquetas. Todo el tráfico entre dos sistemas se transporta a través de una asociación de seguridad única, independientemente de la etiqueta de Trusted Extensions.

Las extensiones de etiquetas permiten realizar las siguientes tareas:

- Configurar una asociación de seguridad IPsec diferente para usar con cada etiqueta de Trusted Extensions. Esta configuración proporciona un mecanismo adicional para transmitir la etiqueta del tráfico entre dos sistemas de varios niveles.
- Especificar una etiqueta en la transferencia para el texto del mensaje cifrado de IPsec que sea diferente del formato sin cifrar del texto. Esta configuración admite la transmisión de datos confidenciales cifrados a través de una red menos segura.
- Suprimir el uso de las opciones IP de CIPSO en los paquetes IP. Esta configuración permite que el tráfico con etiquetas atraviese redes que no reconocen CIPSO o hostiles hacia CIPSO.

Puede especificar si desea usar extensiones de etiquetas automáticamente mediante IKE, como se describe en "Extensiones de etiquetas para IKE" en la página 213, o manualmente por medio del comando `ipseckey`. Para obtener detalles sobre las funciones de las extensiones de etiquetas, consulte la página del comando man `ipseckey(1M)`.

Al utilizar extensiones de etiquetas, la selección de la asociación de seguridad para el tráfico saliente incluye la etiqueta de sensibilidad interna como parte de la asociación. La etiqueta de seguridad del tráfico entrante está definida por la etiqueta de seguridad de la asociación de seguridad del paquete recibido.

Extensiones de etiquetas para IKE

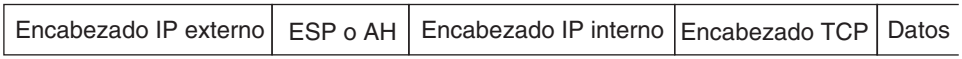
IKE en los sistemas Trusted Extensions admite la negociación de etiquetas para las asociaciones de seguridad con iguales que reconocen etiquetas. Para controlar este mecanismo, puede usar las siguientes palabras clave en el archivo `/etc/inet/ike/config`:

- **label_aware**: permite el uso del daemon `in.iked` de las interfaces de etiquetas de Trusted Extensions y la negociación de etiquetas con iguales.
- **single_label**: indica que el igual no admite la negociación de etiquetas para las asociaciones de seguridad.
- **multi_label**: indica que el igual admite la negociación de etiquetas para las asociaciones de seguridad. IKE crea una nueva asociación de seguridad para cada etiqueta adicional que IKE detecta en el tráfico entre dos nodos.
- **wire_label inner**: hace que el daemon `in.iked` cree asociaciones de seguridad con etiquetas donde la etiqueta de transferencia es igual a la etiqueta interna. La etiqueta de gestión de claves es `ADMIN_LOW` cuando el daemon negocia con iguales `cipso`. La etiqueta de gestión de claves es la etiqueta predeterminada del igual cuando el daemon negocia con iguales sin etiquetas. Se siguen las reglas habituales de Trusted Extensions para la inclusión de opciones IP de CIPSO en los paquetes transmitidos.
- **wire_label** *etiqueta*: hace que el daemon `in.iked` cree asociaciones de seguridad con etiquetas donde la etiqueta de transferencia se definió en *etiqueta*, independientemente del valor de la etiqueta interna. El daemon `in.iked` lleva a cabo negociaciones de gestión de claves en la etiqueta especificada. Se siguen las reglas habituales de Trusted Extensions para la inclusión de opciones IP de CIPSO en los paquetes transmitidos.
- **wire_label none** *etiqueta* : genera un comportamiento similar a `wire_label` *etiqueta*, excepto que las opciones IP de CIPSO se suprimen en los paquetes IKE transmitidos y los paquetes de datos en la asociación de seguridad.

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

Etiquetas y acreditación en IPsec en modo túnel

Cuando los paquetes de datos de la aplicación están protegidos por IPsec en modo túnel, los paquetes contienen varios encabezados IP.



El encabezado IP del protocolo IKE contiene el mismo par de dirección de origen y de destino que el encabezado IP externo del paquete de datos de la aplicación.

Encabezado IP externo	Encabezado UDP	Protocolo de gestión de claves IKE

Trusted Extensions utiliza las direcciones del encabezado IP interno para las comprobaciones de acreditaciones de la etiqueta interna. Trusted Extensions realiza comprobaciones de las etiquetas de transferencia y de gestión de claves mediante las direcciones del encabezado IP externo. Para obtener información sobre las comprobaciones de acreditaciones, consulte "Comprobaciones de acreditaciones de Trusted Extensions" en la página 206.

Protecciones de confidencialidad e integridad con extensiones de etiquetas

La siguiente tabla explica cómo las protecciones de confidencialidad e integridad de IPsec se aplican a la etiqueta de seguridad con distintas configuraciones de extensiones de etiquetas.

Asociación de seguridad	Confidencialidad	Integridad
Sin extensiones de etiquetas	Etiqueta visible en la opción IP de CIPSO.	Etiqueta de mensaje en la opción IP de CIPSO cubierta por AH, no por ESP. Consulte la nota.
Con extensiones de etiquetas	Opción IP de CIPSO visible, pero representa la etiqueta de transferencia, que puede ser diferente de la etiqueta de mensaje interna.	Integridad de etiqueta cubierta de manera implícita por la existencia de una asociación de seguridad específica de la etiqueta. Opción IP de CIPSO en la transferencia cubierta por AH. Consulte la nota.
Con extensiones de etiquetas y opción IP de CIPSO suprimida	Etiqueta de mensaje no visible.	Integridad de etiqueta cubierta de manera implícita por la existencia de una asociación de seguridad específica de la etiqueta.

Nota – No puede utilizar las protecciones de integridad AH de IPsec para proteger la opción IP de CIPSO si los enrutadores que reconocen CIPSO pueden quitar o agregar la opción IP de CIPSO mientras se transmite un mensaje por la red. Cualquier modificación realizada en la opción IP de CIPSO invalidará el mensaje y hará que se descarte un paquete protegido por AH en el destino.

◆ ◆ ◆ CAPÍTULO 16

Gestión de redes en Trusted Extensions (tareas)

En este capítulo se proporcionan detalles y procedimientos de implementación para proteger las redes de Trusted Extensions.

Gestión de la red de confianza (mapa de tareas)

La siguiente tabla contiene enlaces a mapas de tareas para procedimientos de redes comunes en Trusted Extensions.

Tarea	Descripción	Para obtener instrucciones
Asignar etiquetas a hosts y redes.	Se crean plantillas de host remoto y se asignan hosts a las plantillas de seguridad.	"Etiquetado de hosts y redes (mapa de tareas)" en la página 216
Asignar rutas predeterminadas y configurar puertos de varios niveles (MLP).	Se configuran rutas estáticas que permiten que los paquetes con etiquetas alcancen su destino mediante puertas de enlace con etiquetas y sin etiquetas. Se agregan MLP privados y compartidos a las zonas con etiquetas y la zona global.	"Configuración de rutas y puertos de varios niveles (tareas)" en la página 232
Habilitar IPsec para proteger los paquetes con etiquetas.	Se protegen los paquetes con etiquetas mediante IPsec.	"Configuración de IPsec con etiquetas (mapa de tareas)" en la página 236
Resolver problemas de redes.	Pasos que se deben seguir para diagnosticar problemas de redes en los paquetes con etiquetas.	"Resolución de problemas de la red de confianza (mapa de tareas)" en la página 240

Etiquetado de hosts y redes (mapa de tareas)

Un sistema Trusted Extensions puede establecer contacto con otros hosts sólo después de que el sistema ha definido los atributos de seguridad de esos hosts. Debido a que los hosts remotos pueden tener atributos de seguridad similares, Trusted Extensions proporciona plantillas de seguridad a las que es posible agregar hosts.

El siguiente mapa de tareas describe las tareas que puede utilizar para agregar plantillas de seguridad y aplicarlas a los hosts remotos.

Tarea	Descripción	Para obtener instrucciones
Ver las plantillas de seguridad.	Se muestran las plantillas de seguridad disponibles.	"Cómo ver plantillas de seguridad" en la página 217
Determinar si el sitio requiere plantillas de seguridad personalizadas.	Se evalúan las plantillas existentes de acuerdo con los requisitos de seguridad del sitio.	"Cómo determinar si necesita plantillas de seguridad específicas del sitio" en la página 218
Agregar hosts a la red conocida.	Se agregan sistemas y redes a la red de confianza.	"Cómo agregar hosts a la red conocida del sistema" en la página 223
Crear plantillas de seguridad.	Crea plantillas de seguridad que definen los atributos de seguridad de la red de confianza.	"Cómo crear plantillas de seguridad" en la página 219
	Esta plantilla de seguridad cambia el DOI a un valor distinto de 1.	"Cómo configurar el dominio de interpretación" en la página 55
	Esta plantilla de seguridad asigna una etiqueta específica a los hosts remotos.	Ejemplo 16–1
	La plantilla de seguridad es para los hosts remotos que actúan como puertas de enlace con una sola etiqueta.	Ejemplo 16–2
	La plantilla de seguridad es para los hosts remotos que limitan el tráfico a un rango de etiquetas reducido.	Ejemplo 16–3
	La plantilla de seguridad es para hosts remotos con etiquetas discretas.	Ejemplo 16–4
	La plantilla de seguridad es para hosts remotos y redes sin etiquetas.	Ejemplo 16–5
	La plantilla de seguridad es para dos hosts remotos cuyas etiquetas están separadas del resto de la red.	Ejemplo 16–6

Tarea	Descripción	Para obtener instrucciones
Agregar un host a una plantilla de seguridad.	Se agrega una dirección IP a una plantilla de seguridad.	"Cómo agregar un host a una plantilla de seguridad" en la página 223 Ejemplo 16–7 Ejemplo 16–8 Ejemplo 16–9 Ejemplo 16–10
Agregar direcciones IP contiguas a una plantilla de seguridad.	Se agrega un rango de direcciones IP a una plantilla de seguridad.	"Cómo agregar un rango de hosts a una plantilla de seguridad" en la página 226 Ejemplo 16–12 Ejemplo 16–13
Eliminar un host de una plantilla de seguridad.	Se elimina la definición de seguridad de un host.	Ejemplo 16–11
Especificar los hosts que pueden establecer una comunicación en la etiqueta `admin_low`.	Se incrementa la seguridad mediante la definición de los hosts con los que el sistema puede establecer contacto durante el inicio.	"Cómo limitar los hosts que se pueden contactar en la red de confianza" en la página 229
	Se incrementa la seguridad mediante la definición de una red de hosts con etiquetas con la que el sistema puede establecer contacto durante el inicio.	Ejemplo 16–14
Crear una entrada para la dirección de host `0.0.0.0/32`.	Se configura un servidor de aplicaciones para aceptar el contacto inicial de un cliente remoto.	Ejemplo 16–16

▼ Cómo ver plantillas de seguridad

Puede ver la lista de plantillas de seguridad y el contenido de cada plantilla. Los ejemplos que se muestran en este procedimiento hacen referencia a las plantillas de seguridad predeterminadas.

1 Consulte las plantillas de seguridad disponibles.

```
# tncfg list
   cipso
   admin_low
```

2 Vea el contenido de la plantillas mostradas.

```
# tncfg -t cipso info
   name=cipso
   host_type=cipso
   doi=1
```

```
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
   host=127.0.0.1/32
```

La entrada `127.0.0.1/32` de la plantilla de seguridad `cipso` anterior identifica este sistema como un sistema con etiquetas. Cuando un igual asigna este sistema a la plantilla de host remoto del igual con el `host_type` de `cipso`, los dos sistemas pueden intercambiar paquetes con etiquetas.

```
# tncfg -t admin_low info
   name=admin_low
   host_type=unlabeled
   doi=1
   def_label=ADMIN_LOW
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
   host=0.0.0.0/0
```

La entrada `0.0.0.0/0` de la plantilla de seguridad `admin_low` anterior permite que todos los hosts que están asignados explícitamente a una plantilla de seguridad puedan establecer contacto con este sistema. Estos hosts se reconocen como hosts sin etiquetas.

- La ventaja de esta entrada es que se pueden encontrar todos los hosts que este sistema requiere durante el inicio, por ejemplo, servidores y puertas de enlace.
- La desventaja de esta entrada es que cualquier host de la red de este sistema puede establecer contacto con el sistema. Para limitar los hosts que pueden establecer contacto con este sistema, consulte "Cómo limitar los hosts que se pueden contactar en la red de confianza" en la página 229.

▼ Cómo determinar si necesita plantillas de seguridad específicas del sitio

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1 Familiarícese con las plantillas de seguridad de Trusted Extensions.

Siga las instrucciones detalladas en "Cómo ver plantillas de seguridad" en la página 217 para ver las plantillas de seguridad disponibles.

2 Cree nuevas plantillas de seguridad si desea realizar alguna de las siguientes acciones para los hosts con los que establece una comunicación:

- Limite el rango de etiquetas de un host o un grupo de hosts.
- Cree un host de una sola etiqueta en una etiqueta distinta de `ADMIN_LOW`.
- Requiera una etiqueta predeterminada para los hosts sin etiquetas que no sea `ADMIN_LOW`.
- Cree un host que reconozca algunas etiquetas discretas.
- Utilice un dominio de interpretación distinto de `1`.

Pasos siguientes Para agregar hosts a las plantillas de seguridad predeterminadas, vaya a "Cómo agregar un host a una plantilla de seguridad" en la página 223.

De lo contrario, continúe con "Cómo crear plantillas de seguridad" en la página 219.

▼ Cómo crear plantillas de seguridad

Antes de empezar Debe estar en la zona global en un rol que pueda modificar la seguridad de la red. Por ejemplo, los roles que tienen asignados los perfiles de derechos de seguridad de la información o seguridad de la red pueden modificar los valores de seguridad. El rol de administrador de la seguridad incluye estos perfiles de derechos.

1 **(Opcional) Determine la versión hexadecimal de cualquier etiqueta que no sea `ADMIN_HIGH` ni `ADMIN_LOW`.**

Para las etiquetas como `PUBLIC`, puede utilizar la cadena de etiqueta o el valor hexadecimal, `0x0002-08-08`, como valores de etiqueta. El comando `tncfg` acepta ambos formatos.

```
# atohexlabel "confidential : internal use only"
0x0004-08-48
```

Para obtener más información, consulte "Cómo obtener el equivalente hexadecimal de una etiqueta" en la página 130.

2 **No modifique las plantillas de seguridad predeterminadas.**

Por razones de compatibilidad, no suprima las plantillas de seguridad predeterminadas. Puede copiar y modificar estas plantillas. Además, puede agregar y eliminar hosts asignados a estas plantillas. Para obtener un ejemplo, consulte "Cómo limitar los hosts que se pueden contactar en la red de confianza" en la página 229.

3 **Cree una plantilla de seguridad.**

El comando `tncfg -t` proporciona tres maneras de crear plantillas nuevas.

- **Cree una plantilla de seguridad desde el principio.**

  Utilice el comando `tncfg` en modo interactivo. El subcomando `info` muestra los valores que se proporcionan de forma predeterminada. Utilice la tecla de tabulación para completar los valores y las propiedades parciales.

```
# tncfg -t newunlabeled
tncfg:newtemplate> info
   name=newunlabeled
   host_type=unlabeled
   doi=1
   def_label=ADMIN_LOW
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
tncfg:newunlabeled> set m<Tab>
set max_label=" set min_label="
```

```
tncfg:newunlabeled> set ma<Tab>
tncfg:newunlabeled> set max_label=ADMIN_LOW
...
```

También puede proporcionar la lista completa de atributos para una plantilla de seguridad en la línea de comandos. Se utiliza un punto y coma para separar los subcomandos `set`. Una propiedad omitida recibe el valor predeterminado.

```
# tncfg -t newunlabeled set host_type=unlabeled;set doi=1; \
set min_label=ADMIN_LOW;set max_label=ADMIN_LOW
```

- **Copie y modifique una plantilla de seguridad existente.**

```
# tncfg -t cipso
tncfg:cipso> set name=newcipso
tncfg:newcipso> info
name=newcipso
host_type=cipso
doi=1
min_label=ADMIN_LOW
max_label=ADMIN_HIGH
```

Los hosts asignados a la plantilla de seguridad existente no se copian en la nueva plantilla.

- **Utilice un archivo de plantilla creado por el subcomando `export`.**

```
# tncfg -f unlab_1 -f template-file
tncfg: unlab1> set host_type=unlabeled
...
# tncfg -f template-file
```

Para obtener un ejemplo de cómo crear una plantilla de origen para la importación, consulte la página del comando man `tncfg(1M)`.

Ejemplo 16–1 Creación de una plantilla de seguridad para una puerta de enlace que gestiona paquetes en una sola etiqueta

En este ejemplo, el administrador de la seguridad define una puerta de enlace que únicamente puede transferir paquetes en la etiqueta `PUBLIC`.

```
# tncfg -t cipso_public
tncfg:cipso_public> set host_type=cipso
tncfg:cipso_public> set doi=1
tncfg:cipso_public> set min_label="public"
tncfg:cipso_public> set max_label="public"
tncfg:cipso_public> commit
tncfg:cipso_public> exit
```

El administrador de la seguridad luego agrega el host de la puerta de enlace a la plantilla de seguridad. Para obtener detalles sobre la adición, consulte el Ejemplo 16–7.

Ejemplo 16–2 Creación de una plantilla de seguridad para un enrutador sin etiquetas que redirige paquetes con etiquetas

Cualquier enrutador IP puede reenviar los mensajes con etiquetas CIPSO aunque el enrutador no admita etiquetas de manera explícita. Este tipo de enrutador sin etiquetas necesita una etiqueta predeterminada para definir el nivel en el que se deben controlar las conexiones con el enrutador (quizás para la gestión del enrutador). En este ejemplo, el administrador de la seguridad crea un enrutador que puede reenviar tráfico en cualquier etiqueta, pero toda comunicación directa con el enrutador se gestiona en la etiqueta predeterminada, `PUBLIC`.

El administrador de la seguridad crea la plantilla desde el principio.

```
# tncfg -t unl_public
tncfg:unl_public> set host_type=unlabeled
tncfg:unl_public> set doi=1
tncfg:unl_public> set def_label="PUBLIC"
tncfg:unl_public> set min_label=ADMIN_LOW
tncfg:unl_public> set max_label=ADMIN_HIGH
tncfg:unl_public> exit
```

El administrador de la seguridad luego agrega el enrutador a la plantilla de seguridad. Para obtener detalles sobre la adición, consulte el Ejemplo 16–8.

Ejemplo 16–3 Creación de una plantilla de seguridad para una puerta de enlace con un rango de etiquetas limitado

En este ejemplo, el administrador de la seguridad crea una puerta de enlace que limita los paquetes a un rango de etiquetas reducido. El administrador crea una plantilla de seguridad y luego asigna el host de la puerta de enlace a la plantilla de seguridad.

```
# tncfg -t cipso_iuo_rstrct
tncfg:cipso_iuo_rstrct> set host_type=cipso
tncfg:cipso_iuo_rstrct> set doi=1
tncfg:cipso_iuo_rstrct> set min_label=0x0004-08-48
tncfg:cipso_iuo_rstrct> set max_label=0x0004-08-78
tncfg:cipso_iuo_rstrct> add host=192.168.131.78
tncfg:cipso_iuo_rstrct> exit
```

El administrador de la seguridad luego agrega el host de la puerta de enlace a la plantilla de seguridad. Para obtener detalles sobre la adición, consulte el Ejemplo 16–9.

Ejemplo 16–4 Creación de una plantilla de seguridad que tiene etiquetas discretas

En este ejemplo, el administrador de la seguridad crea una plantilla de seguridad que reconoce dos etiquetas solamente, `confidential : internal use only` y `confidential : restricted`. Se rechaza todo el resto del tráfico.

En primer lugar, el administrador escribe las etiquetas con cuidado y precisión. El software reconoce etiquetas en mayúscula y minúsculas y por nombre corto, pero no reconoce etiquetas donde los espacios son inexactos. Por ejemplo, la etiqueta `confidential :restricted` no es una etiqueta válida.

```
# tncfg -t cipso_int_and_rst
tncfg:cipso_int_and_rst> set host_type=cipso
tncfg:cipso_int_and_rst> set doi=1
tncfg:cipso_int_and_rst> set min_label="cnf : internal use only"
tncfg:cipso_int_and_rst> set max_label="cnf : internal use only"
tncfg:cipso_int_and_rst> set aux_label="cnf : restricted"
tncfg:cipso_int_and_rst> exit
```

Ejemplo 16–5 Creación de una plantilla de seguridad sin etiquetas en la etiqueta PUBLIC

En este ejemplo, el administrador de la seguridad crea una plantilla de una sola etiqueta para los hosts que pueden recibir y enviar paquetes en la etiqueta `PUBLIC` únicamente. Esta plantilla se puede asignar a los hosts cuyos sistemas de archivos deben montarse en la etiqueta `PUBLIC` mediante los sistemas Trusted Extensions.

```
# tncfg -t public
tncfg:public> set host_type=unlabeled
tncfg:public> set doi=1
tncfg:public> set def_label="public"
tncfg:public> set min_sl="public"
tncfg:public> set max_sl="public"
tncfg:public> exit
```

El administrador de la seguridad luego agrega los hosts a la plantilla de seguridad. Para obtener detalles sobre la adición, consulte el Ejemplo 16–13.

Ejemplo 16–6 Creación de una plantilla de seguridad con etiquetas para desarrolladores

En este ejemplo, el administrador de la seguridad crea una plantilla `cipso_sandbox`. Esta plantilla de seguridad se asigna a los sistemas que utilizan los desarrolladores de software de confianza. Las pruebas de desarrolladores no afectan a otros hosts con etiquetas, porque la etiqueta `SANDBOX` está separada de las otras etiquetas de la red.

```
# tncfg -t cipso_sandbox
tncfg:cipso_sandbox> set host_type=cipso
tncfg:cipso_sandbox> set doi=1
tncfg:cipso_sandbox> set min_sl="SBX"
tncfg:cipso_sandbox> set max_sl="SBX"
tncfg:cipso_sandbox> exit
```

▼ Cómo agregar hosts a la red conocida del sistema

Después de agregar hosts y grupos de hosts al archivo `/etc/hosts` de un sistema, el sistema reconoce los hosts. Sólo es posible agregar hosts conocidos a una plantilla de seguridad.

Antes de empezar Tiene el rol de usuario `root` en la zona global.

1. **Agregue hosts individuales al archivo `/etc/hosts`.**

```
# vi /etc/hosts

...
192.168.111.121   ahost
```

2. **Agregue un grupo de hosts al archivo `/etc/hosts`.**

```
# vi /etc/hosts

...
192.168.111.0   111-network
```

Pasos siguientes Continúe con "Cómo agregar un host a una plantilla de seguridad" en la página 223.

▼ Cómo agregar un host a una plantilla de seguridad

Antes de empezar Se deben cumplir los siguientes requisitos:

- La plantilla de seguridad debe existir. Para conocer el procedimiento, consulte "Cómo crear plantillas de seguridad" en la página 219.
- Las direcciones IP deben existir en el archivo `/etc/hosts` o DNS debe poder resolverlas.

  Para el archivo `hosts`, consulte "Cómo agregar hosts a la red conocida del sistema" en la página 223.

  Para DNS, consulte el Capítulo 3, "Managing DNS (Tasks)" de *Oracle Solaris Administration: Naming and Directory Services*.
- Los puntos finales de la etiqueta deben coincidir. Para las reglas, consulte "Descripción general del enrutamiento en Trusted Extensions" en la página 205.
- Debe estar con el rol de administrador de la seguridad en la zona global.

1. **Agregue un nombre de host o una dirección IP a una plantilla de seguridad.**

   Por ejemplo, agregue la dirección IP `192.168.1.2`.

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.1.2
```

Si agrega un host que se agregó anteriormente a otra plantilla, se le notificará que está sustituyendo la asignación de plantilla de seguridad. Por ejemplo:

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.1.22
192.168.1.2 previously matched the admin_low template
tncfg:cipso> info
...
host=192.168.1.2/32
tncfg:cipso> exit
```

2 Vea la plantilla de seguridad modificada.

Por ejemplo, a continuación se muestra la dirección `192.168.1.2` que se agregó a la plantilla `cipso`:

```
tncfg:cipso> info
...
   host=192.168.1.2/32
```

La longitud del prefijo de `/32` indica que la dirección es exacta.

3 Confirme el cambio y salga de la plantilla de seguridad.

```
tncfg:cipso> commit
tncfg:cipso> exit
```

Para eliminar una entrada de host, consulte el Ejemplo 16–11.

Ejemplo 16–7 Creación de una puerta de enlace que gestiona paquetes en una sola etiqueta

En el Ejemplo 16–1, el administrador crea una plantilla de seguridad que define una puerta de enlace que sólo puede transferir paquetes en la etiqueta `PUBLIC`. En este ejemplo, el administrador de la seguridad comprueba que se puede resolver la dirección IP del host de la puerta de enlace.

```
# arp 192.168.131.75
gateway-1.example.com (192.168.131.75) at 0:0:0:1:ab:cd
```

El comando `arp` verifica que el host está definido en el archivo `/etc/hosts` del sistema o que DNS puede resolverlo.

A continuación, el administrador agrega el host `gateway-1` a la plantilla de seguridad:

```
# tncfg -t cipso_public
tncfg:cipso_public> add host=192.168.131.75
tncfg:cipso_public> exit
```

El sistema puede enviar y recibir paquetes `public` a través de `gateway-1` de inmediato.

Ejemplo 16–8 Creación de un enrutador sin etiquetas para redirigir paquetes con etiquetas

En el Ejemplo 16–2, el administrador crea la plantilla de seguridad para el enrutador. En este ejemplo, el administrador comprueba que se puede resolver la dirección IP del enrutador.

```
# arp 192.168.131.82
router-1.example.com (192.168.131.82) at 0:0:0:2:ab:cd
```

El comando `arp` indica que el host está definido en el archivo `/etc/hosts` del sistema o que DNS puede resolverlo.

A continuación, el administrador agrega el enrutador a la plantilla de seguridad.

```
# tncfg -t unl_public
tncfg:unl_public> add host=192.168.131.82
tncfg:unl_public> exit
```

El sistema puede enviar y recibir paquetes en todas las etiquetas a través de `router-1` de inmediato.

Ejemplo 16–9 Creación de una puerta de enlace con un rango de etiquetas limitado

En el Ejemplo 16–3, el administrador crea una plantilla de seguridad con un rango de etiquetas limitado. En este ejemplo, el administrador de la seguridad comprueba que se puede resolver la dirección IP del host de la puerta de enlace.

```
# arp 192.168.131.78
gateway-ir.example.com (192.168.131.78) at 0:0:0:3:ab:cd
```

El comando `arp` indica que el host está definido en el archivo `/etc/hosts` del sistema o que DNS puede resolverlo.

A continuación, el administrador agrega la puerta de enlace a la plantilla de seguridad.

```
# tncfg -t cipso_iuo_rstrct
tncfg:cipso_iuo_rstrct> add host=192.168.131.78
tncfg:cipso_iuo_rstrct> exit
```

El sistema puede enviar y recibir paquetes con las etiquetas `internal` y `restricted` a través de `gateway-ir` de inmediato.

Ejemplo 16–10 Creación de un host con etiquetas para desarrolladores

En el Ejemplo 16–6, el administrador crea la plantilla de seguridad `cipso_sandbox`. En este ejemplo, el administrador de la seguridad agrega dos hosts a la plantilla.

```
# tncfg -t cipso_sandbox
tncfg:cipso_sandbox> add host=196.168.129.102
tncfg:cipso_sandbox> add host=196.168.129.129
tncfg:cipso_sandbox> exit
```

Los desarrolladores que utilizan los sistemas `196.168.129.102` y `196.168.129.129` pueden comunicarse entre sí en la etiqueta `SANDBOX`.

Ejemplo 16–11 Eliminación de varios hosts de una plantilla de seguridad

En este ejemplo, el administrador de la seguridad elimina varios hosts de la plantilla de seguridad `cipso`. El administrador utiliza el subcomando `info` para mostrar los hosts, luego escribe `remove` y copia y pega cuatro entradas `host=`.

```
# tncfg -t cipso info
   name=cipso
   host_type=cipso
   doi=1
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
   host=127.0.0.1/32
   host=192.168.1.2/32
   host=192.168.113.0/24
   host=192.168.113.100/25
   host=2001:a08:3903:200::0/56

# tncfg -t cipso
tncfg:cipso> remove host=192.168.1.2/32
tncfg:cipso> remove host=192.168.113.0/24
tncfg:cipso> remove host=192.168.113.100/25
tncfg:cipso> remove host=2001:a08:3903:200::0/56
tncfg:cipso> info
...
   max_label=ADMIN_HIGH
   host=127.0.0.1/32
   host=192.168.75.0/24
```

Después de eliminar los hosts, el administrador confirma los cambios y sale de la plantilla de seguridad.

```
tncfg:cipso> commit
tncfg:cipso> exit
#
```

▼ Cómo agregar un rango de hosts a una plantilla de seguridad

Antes de empezar Para conocer los requisitos, consulte "Cómo agregar un host a una plantilla de seguridad" en la página 223.

1. **Para asignar una plantilla de seguridad a una subred, agregue la dirección de subred a la plantilla.**

   Por ejemplo, agregue dos subredes a la plantilla `cipso` y, a continuación, visualice la plantilla de seguridad.

   ```
   # tncfg -t cipso
   tncfg:cipso> add host=192.168.75.0
   tncfg:cipso> add host=192.168.113.0
   tncfg:cipso> info
   ...
   host=192.168.75.0/24
   host=192.168.113.0/24
   tncfg:cipso> exit
   ```

   La longitud del prefijo de `/24` indica que la dirección, que termina en `.0`, es una subred.

   Nota – Si agrega un rango de hosts que se agregó anteriormente a otra plantilla, se le notificará que está sustituyendo la asignación de plantilla de seguridad.

   ```
   # tncfg -t cipso
   tncfg:cipso> add host=192.168.113.100/25
   192.168.113.100/25 previously matched the admin_low template
   ```

2. **Para asignar una plantilla de seguridad a un grupo de direcciones IP contiguas, especifique la dirección IP y la longitud del prefijo.**

   En el siguiente ejemplo, la longitud del prefijo comprende el rango de direcciones entre `192.168.113.0` y `192.168.113.127`. La dirección incluye `192.168.113.100`.

   ```
   # tncfg -t cipso
   tncfg:cipso> add host=192.168.113.100/25
   tncfg:cipso> exit
   ```

   En el siguiente ejemplo, la longitud del prefijo comprende las direcciones IPv6 contiguas entre `2001:a08:3903:200::0` y `2001:a08:3903:2ff:ffff:ffff:ffff:ffff`. La dirección incluye `2001:a08:3903:201:20e:cff:fe08:58c`.

   ```
   # tncfg -t cipso
   tncfg:cipso> add host=2001:a08:3903:200::0/56
   tncfg:cipso> info
   ...
   host=2001:a08:3903:200::0/56
   tncfg:cipso> exit
   ```

   Si escribe una entrada de manera incorrecta, recibirá un mensaje similar al siguiente:

   ```
   # tncfg -t cipso
   tncfg:cipso> add host=2001:a08:3903::0/56
   Invalid host: 2001:a08:3903::0/56
   ```

Si agrega un host que se agregó anteriormente a otra plantilla, se le notificará que está sustituyendo la asignación de plantilla de seguridad. Por ejemplo:

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.113.100/32
192.168.113.100/32 previously matched the admin_low template
tncfg:cipso> info
...
host=192.168.113.100/32
tncfg:cipso> exit
```

El mecanismo de reserva de Trusted Extensions garantiza que esta asignación explícita sustituya la asignación anterior, como se describe en "Mecanismo de reserva de la red de confianza" en la página 203.

Ejemplo 16–12 Creación de hosts en etiquetas discretas

En el Ejemplo 16–4, el administrador crea una plantilla de seguridad que reconoce dos etiquetas. En este ejemplo, el administrador de la seguridad comprueba que se pueden resolver las direcciones IP de cada host.

```
# arp 192.168.132.21
host-auxset1.example.com (192.168.132.21) at 0:0:0:4:ab:cd
# arp 192.168.132.22
host-auxset2.example.com (192.168.132.22) at 0:0:0:5:ab:cd
# arp 192.168.132.23
host-auxset3.example.com (192.168.132.23) at 0:0:0:6:ab:cd
# arp 192.168.132.24
host-auxset4.example.com (192.168.132.24) at 0:0:0:7:ab:cd
```

El comando `arp` indica que los hosts están definidos en el archivo `/etc/hosts` del sistema o que DNS puede resolverlos.

A continuación, el administrador asigna el rango de direcciones IP a la plantilla de seguridad mediante una longitud de prefijo.

```
# tncfg -t cipso_int_rstrct
tncfg:cipso_int_rstrct> set host=192.168.132.0/24
```

Ejemplo 16–13 Creación de una subred sin etiquetas en la etiqueta PUBLIC

En el Ejemplo 16–5, el administrador crea una plantilla de seguridad que define un host `PUBLIC` de una sola etiqueta. En este ejemplo, el administrador de la seguridad asigna una subred a la etiqueta `PUBLIC`. Los usuarios del sistema de confianza pueden montar sistemas de archivos de esta subred en la etiqueta `PUBLIC`.

```
# tncfg -t public
tncfg:public> add host=10.10.0.0/16
tncfg:public> exit
```

Se puede acceder a la subred de inmediato en la etiqueta `PUBLIC`.

▼ Cómo limitar los hosts que se pueden contactar en la red de confianza

Este procedimiento protege los hosts con etiquetas del contacto de hosts sin etiquetas arbitrarios. Cuando Trusted Extensions está instalado, la plantilla de seguridad predeterminada `admin_low` define cada host de la red. Utilice este procedimiento para enumerar hosts sin etiquetas específicos.

Los valores de la red de confianza local de cada sistema se utilizan para establecer contacto con la red durante el inicio. De manera predeterminada, cada host que no se proporciona con una plantilla `cipso` se define mediante la plantilla `admin_low`. Esta plantilla asigna todos los hosts remotos que no están definidos de ningún otro modo (`0.0.0.0/0`) como sistemas sin etiquetas con la etiqueta predeterminada de `admin_low`.

Precaución – La plantilla `admin_low` predeterminada puede representar un riesgo de seguridad en una red de Trusted Extensions. Si la seguridad del sitio requiere una protección elevada, el administrador de la seguridad puede eliminar la entrada comodín `0.0.0.0/0` una vez instalado el sistema. La entrada se debe reemplazar con entradas para cada host con el que el sistema establece contacto durante el inicio.

Por ejemplo, los servidores DNS, los servidores del directorio principal, los servidores de auditoría, las direcciones de difusión y multidifusión, y los enrutadores se deben agregar de manera explícita a una plantilla una vez que se elimina la entrada comodín `0.0.0.0/0`.

Si una aplicación reconoce inicialmente clientes en la dirección de host `0.0.0.0/32`, debe agregar la entrada de host `0.0.0.0/32` a la plantilla `admin_low`. A continuación, cuando el servidor reconoce los clientes, se proporciona una dirección IP a los clientes y se los conecta como clientes CIPSO.

Antes de empezar

Debe estar con el rol de administrador de la seguridad en la zona global.

Todos los hosts con los que se debe establecer contacto durante el inicio deben existir en el archivo `/etc/hosts`.

1. **Asigne la plantilla `admin_low` a cada host sin etiquetas con el que se debe establecer contacto durante el inicio.**
   - Incluya cada host sin etiquetas con el que se debe establecer contacto durante el inicio.
   - Incluya cada enrutador "on-link" que no ejecute Trusted Extensions, mediante el cual se debe comunicar este sistema.
   - Elimine la asignación `0.0.0.0/0`.
2. **Agregue hosts a la plantilla `cipso`.**

Agregue cada host con etiquetas con el que se debe establecer contacto durante el inicio.

- Incluya cada enrutador "on-link" que ejecute Trusted Extensions, mediante el cual se debe comunicar este sistema.
- Asegúrese de que todas las interfaces de red estén asignadas a la plantilla.
- Incluya las direcciones de difusión.
- Incluya los rangos de hosts con etiquetas con los que se debe establecer contacto durante el inicio.

Consulte el Ejemplo 16–15 para ver una base de datos de ejemplo.

3 Compruebe que las asignaciones de hosts permitan que el sistema se inicie.

Ejemplo 16–14 Cambio de la etiqueta de la dirección IP 0.0.0.0/0

En este ejemplo, el administrador crea un sistema de puerta de enlace pública. El administrador elimina la entrada de host `0.0.0.0/0` de la plantilla `admin_low` y agrega la entrada de host `0.0.0.0/0` a la plantilla `public` sin etiquetas. El sistema luego reconoce cualquier host que no esté asignado específicamente a otra plantilla de seguridad como un sistema sin etiquetas con los atributos de seguridad de la plantilla de seguridad `public`.

```
# tncfg -t admin_low info
tncfg:admin_low> remove host=0.0.0.0      Wildcard address
tncfg:admin_low> exit

# tncfg -t public
tncfg:public> set host_type=unlabeled
tncfg:public> set doi=1
tncfg:public> set def_label="public"
tncfg:public> set min_sl="public"
tncfg:public> set max_sl="public"
tncfg:public> add host=0.0.0.0      Wildcard address
tncfg:public> exit
```

Ejemplo 16–15 Enumeración de los equipos que se deben contactar durante el inicio

En el siguiente ejemplo, el administrador configura la red de confianza de un sistema Trusted Extensions con dos interfaces de red. El sistema se comunica con otra red y con los enrutadores. Los hosts remotos se asignan a una de estas tres plantillas: `cipso`, `admin_low` o `public`. Se anotan los siguientes comandos.

```
# tncfg -t cipso
tncfg:admin_low> add host=127.0.0.1      Loopback address
tncfg:admin_low> add host=192.168.112.111      Interface 1 of this host
tncfg:admin_low> add host=192.168.113.111      Interface 2 of this host
tncfg:admin_low> add host=192.168.113.6      File server
tncfg:admin_low> add host=192.168.112.255      Subnet broadcast address
```

```
tncfg:admin_low> add host=192.168.113.255      Subnet broadcast address
tncfg:admin_low> add host=192.168.113.1     Router
tncfg:admin_low> add host=192.168.117.0/24      Another Trusted Extensions network
tncfg:admin_low> exit

# tncfg -t public
tncfg:public> add host=192.168.112.12      Specific network router
tncfg:public> add host=192.168.113.12      Specific network router
tncfg:public> add host=224.0.0.2     Multicast address
tncfg:admin_low> exit

# tncfg -t admin_low
tncfg:admin_low> add host=255.255.255.255      Broadcast address
tncfg:admin_low> exit
```

Después de especificar los hosts que se deben contactar durante el inicio, el administrador elimina la entrada `0.0.0.0/0` de la plantilla `admin_low`.

```
# tncfg -t admin_low
tncfg:admin_low> remove host=0.0.0.0
tncfg:admin_low> exit
```

Ejemplo 16–16 Cómo hacer que la dirección de host 0.0.0.0/32 sea una dirección inicial válida

En este ejemplo, el administrador de la seguridad configura un servidor de aplicaciones para aceptar las solicitudes de conexión inicial de clientes potenciales.

El administrador configura la red de confianza del servidor. Se anotan las entradas del servidor y el cliente.

```
# tncfg -t cipso info
   name=cipso
   host_type=cipso
   doi=1
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
   host=127.0.0.1/32
   host=192.168.128.1/32       Application server address
   host=192.168.128.0/24       Application's client network
     Other addresses to be contacted at boot time

# tncfg -t admin_low info
   name=cipso
   host_type=cipso
   doi=1
   def_label=ADMIN_LOW
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
   host=192.168.128.0/24       Application's client network
   host=0.0.0.0/0       Wildcard address
     Other addresses to be contacted at boot time
```

Una vez que esta fase de prueba finaliza correctamente, el administrador bloquea la configuración. Para ello, elimina la dirección comodín predeterminada, `0.0.0.0/0`, confirma el cambio y, a continuación, agrega la dirección específica.

```
# tncfg -t admin_low info
tncfg:admin_low> remove host=0.0.0.0
tncfg:admin_low> commit
tncfg:admin_low> add host=0.0.0.0/32      For initial client contact
tncfg:admin_low> exit
```

La configuración `admin_low` final es similar a la siguiente:

```
# tncfg -t admin_low
   name=cipso
   host_type=cipso
   doi=1
   def_label=ADMIN_LOW
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
   192.168.128.0/24      Application's client network
   host=0.0.0.0/32       For initial client contact
     Other addresses to be contacted at boot time
```

La entrada `0.0.0.0/32` sólo permite que los clientes de la aplicación accedan al servidor de aplicaciones.

Configuración de rutas y puertos de varios niveles (tareas)

Las rutas estáticas permiten que los paquetes con etiquetas alcancen su destino mediante puertas de enlace con etiquetas y sin etiquetas. Los puertos de varios niveles permiten que una aplicación utilice un único punto de entrada para acceder a todas las zonas.

▼ Cómo agregar rutas predeterminadas

Antes de empezar

Debe estar con el rol de administrador de la seguridad en la zona global.

Ha agregado cada red, puerta de enlace y host de destino a una plantilla de seguridad. Para obtener detalles, consulte "Cómo agregar un host a una plantilla de seguridad" en la página 223 y "Cómo agregar un rango de hosts a una plantilla de seguridad" en la página 226.

1. **Utilice la interfaz gráfica de usuario `txzonemgr` para crear rutas predeterminadas.**

   ```
   # txzonemgr &
   ```

2. **Haga doble clic en la zona cuya ruta predeterminada desea definir y, a continuación, haga doble clic en la entrada de dirección IP.**

   Si la zona tiene más de una dirección IP, seleccione la entrada con la interfaz deseada.

3 **Cuando se solicite, escriba la dirección IP del enrutador y haga clic en OK.**

Nota – Para eliminar o modificar el enrutador predeterminado, elimine la entrada, cree la entrada de IP de nuevo y agregue el enrutador. Si la zona sólo tiene una dirección IP, debe eliminar la instancia de IP para eliminar la entrada.

Ejemplo 16–17 Uso del comando route para definir la ruta predeterminada de la zona global

En este ejemplo, el administrador utiliza el comando `route` para crear una ruta predeterminada para la zona global.

```
# route add default 192.168.113.1 -static
```

▼ Cómo crear un puerto de varios niveles para una zona

Puede agregar MLP privados y compartidos a las zonas con etiquetas y la zona global.

Este procedimiento se utiliza cuando una aplicación que se ejecuta en una zona con etiquetas necesita un puerto de varios niveles (MLP) para comunicarse con la zona. En este procedimiento, un proxy web se comunica con la zona.

Antes de empezar Debe estar con el rol de usuario `root` en la zona global. El sistema debe tener al menos dos direcciones IP y la zona con etiquetas debe estar detenida.

1 **Agregue el host proxy y los servicios web host al archivo `/etc/hosts`.**

```
## /etc/hosts file
...
proxy-host-name  IP-address
web-service-host-name IP-address
```

2 **Configure la zona.**

Por ejemplo, configure la zona `public` para que reconozca los paquetes explícitamente etiquetados como `PUBLIC`. Para esta configuración, la plantilla de seguridad se denomina `webprox`.

```
# tncfg -t webprox
tncfg:public> set name=webprox
tncfg:public> set host_type=cipso
tncfg:public> set min_label=public
tncfg:public> set max_label=public
tncfg:public> add host=mywebproxy.oracle.com      host name associated with public zone
tncfg:public> add host=10.1.2.3/16      IP address of public zone
tncfg:public> exit
```

3 **Configure el puerto de varios niveles.**

Por ejemplo, el servicio proxy web podría establecer una comunicación con la zona `PUBLIC` a través de la interfaz `8080/tcp`.

```
# tncfg -z public add mlp_shared=8080/tcp
# tncfg -z public add mlp_private=8080/tcp
```

4 **Para agregar el puerto de varios niveles al núcleo, inicie la zona.**

```
# zoneadm -z zone-name boot
```

5 **En la zona global, agregue rutas para las nuevas direcciones.**

Para agregar rutas, consulte "Cómo agregar rutas predeterminadas" en la página 232.

Ejemplo 16–18 Configuración de un puerto de varios niveles con la interfaz gráfica de usuario txzonemgr

Para configurar el servicio proxy web, el administrador abre Labeled Zone Manager.

```
# txzonemgr &
```

El administrador hace doble clic en la zona `PUBLIC` y, a continuación, hace doble clic en `Configure Multilevel Ports`. Luego, el administrador selecciona y hace doble clic en la línea `Private interfaces`. La selección cambia a un campo de entrada similar al siguiente:

```
Private interfaces:111/tcp;111/udp
```

El administrador comienza la entrada del proxy web con un punto y coma como separador.

```
Private interfaces:111/tcp;111/udp;8080/tcp
```

Después de completar la entrada privada, el administrador escribe el proxy web en el campo `Shared interfaces`.

```
Shared interfaces:111/tcp;111/udp;8080/tcp
```

Un mensaje emergente indica que los puertos de varios niveles de la zona `public` estarán activos la próxima vez que se inicie la zona.

Ejemplo 16–19 Configuración de un puerto de varios niveles privado para NFSv3 mediante udp

En este ejemplo, el administrador habilita los montajes de lectura en sentido descendente de NFSv3 mediante `udp`. El administrador tiene la posibilidad de utilizar el comando `tncfg`.

```
# tncfg -z global add mlp_private=2049/udp
```

La interfaz gráfica de usuario `txzonemgr` proporciona otra manera de definir el puerto de varios niveles.

En Labeled Zone Manager, el administrador hace doble clic en la zona `global` y, a continuación, hace doble clic en `Configure Multilevel Ports`. En el menú MLP, el administrador selecciona y hace doble clic en la línea `Private interfaces` y agrega el puerto/protocolo.

```
Private interfaces:111/tcp;111/udp;8080/tcp
```

Un mensaje emergente indica que los puertos de varios niveles de la zona `global` estarán activos la próxima vez que se inicie la zona.

Ejemplo 16–20 Visualización de puertos de varios niveles en un sistema

En este ejemplo, se configura un sistema con varias zonas con etiquetas. Todas las zonas comparten la misma dirección IP. Algunas zonas también se configuran con direcciones específicas de las zonas. En esta configuración, el puerto TCP para navegar por la web (puerto `8080`), es un puerto de varios niveles en una interfaz compartida en la zona public. El administrador también configuró `telnet` (puerto TCP `23`) para que sea un puerto de varios niveles en la zona public. Dado que estos dos puertos de varios niveles están en una interfaz compartida, ninguna otra zona, ni siquiera la zona global, puede recibir paquetes de la interfaz compartida en los puertos `8080` y `23`.

Además, el puerto TCP para `ssh` (puerto `22`) es un puerto de varios niveles por zona en la zona public. El servicio de la zona public `ssh` puede recibir cualquier paquete en su dirección específica de la zona dentro del rango de etiquetas de la etiqueta.

El siguiente comando muestra los puertos de varios niveles para la zona public:

```
$ tninfo -m public
private: 22/tcp
shared:  23/tcp;8080/tcp
```

El siguiente comando muestra los puertos de varios niveles para la zona global. Tenga en cuenta que los puertos `23` y `8080` no pueden ser puertos de varios niveles en la zona global porque dicha zona comparte la misma dirección con la zona public:

```
$ tninfo -m global
private: 111/tcp;111/udp;514/tcp;515/tcp;631/tcp;2049/tcp;
         6000-6003/tcp;38672/tcp;60770/tcp;
shared:  6000-6003/tcp
```

Configuración de IPsec con etiquetas (mapa de tareas)

El siguiente mapa de tareas describe las tareas que se utilizan para agregar etiquetas a las protecciones IPsec.

Tarea	Descripción	Para obtener instrucciones
Utilizar IPsec con Trusted Extensions.	Se agregan etiquetas a las protecciones IPsec.	"Cómo aplicar las protecciones IPsec en una red de Trusted Extensions de varios niveles" en la página 236
Utilizar IPsec con Trusted Extensions en una red que no es de confianza.	Los paquetes IPsec con etiquetas se colocan en túneles en una red sin etiquetas.	"Cómo configurar un túnel en una red que no es de confianza" en la página 238

▼ Cómo aplicar las protecciones IPsec en una red de Trusted Extensions de varios niveles

En este procedimiento, se configura IPsec en dos sistemas Trusted Extensions para manejar las siguientes condiciones:

- Los dos sistemas, `enigma` y `partym`, son sistemas Trusted Extensions de varios niveles que se ejecutan en una red de varios niveles.
- Los datos de aplicación están cifrados y protegidos contra cambios no autorizados en la red.
- La etiqueta de seguridad de los datos se visualiza en forma de una opción IP de CIPSO para su uso en dispositivos de seguridad y enrutadores de varios niveles en la ruta entre los sistemas `enigma` y `partym`.
- La etiquetas de seguridad que `enigma` y `partym` intercambian están protegidas contra cambios no autorizados.

Antes de empezar Tiene el rol de usuario `root` en la zona global.

1. **Agregue los hosts `enigma` y `partym` a una plantilla de seguridad CIPSO.**

   Siga los procedimientos detallados en "Etiquetado de hosts y redes (mapa de tareas)" en la página 216. Utilice una plantilla con un tipo de host CIPSO.

2. **Configure IPsec para los sistemas `enigma` y `partym`.**

   Para conocer el procedimiento, consulte "Cómo proteger el tráfico entre dos sistemas con IPsec" de *Administración de Oracle Solaris: servicios IP*. Utilice IKE para la gestión de claves, como se describe en el siguiente paso.

3 Agregue etiquetas a las negociaciones IKE.

Siga el procedimiento detallado en "Cómo configurar IKE con claves previamente compartidas" de *Administración de Oracle Solaris: servicios IP*, y luego modifique el archivo `ike/config` de la siguiente manera:

a. Agregue las palabras clave `label_aware`, `multi_label` y `wire_label inner` al archivo `/etc/inet/ike/config` del sistema `enigma`.

El archivo resultante tiene el siguiente aspecto. Se resaltan las adiciones de etiquetas.

```
    ### ike/config file on enigma, 192.168.116.16
    ## Global parameters
    #
## Use IKE to exchange security labels.
    label_aware
  #
        ## Defaults that individual rules can override.
    p1_xform
          { auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
    p2_pfs 2
    #
  ## The rule to communicate with partym
      # Label must be unique
    { label "enigma-partym"
          local_addr 192.168.116.16
          remote_addr 192.168.13.213
          multi_label
          wire_label inner
          p1_xform
           { auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
          p2_pfs 5
    }
```

b. Agregue las mismas palabras clave al archivo `ike/config` del sistema `partym`.

```
    ### ike/config file on partym, 192.168.13.213
    ## Global Parameters
    #
## Use IKE to exchange security labels.
    label_aware
    #
        p1_xform
          { auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
    p2_pfs 2
    ## The rule to communicate with enigma
    # Label must be unique
    { label "partym-enigma"
          local_addr 192.168.13.213
          remote_addr 192.168.116.16
          multi_label
          wire_label inner
    p1_xform
           { auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
        p2_pfs 5
    }
```

4 **Si no se puede utilizar la protección AH de las opciones IP de CIPSO en la red, utilice la autenticación ESP.**

Utilice `encr_auth_algs` en lugar de `auth_algs` en el archivo `/etc/inet/ipsecinit.conf` para gestionar la autenticación. La autenticación ESP no abarca el encabezado IP y las opciones IP, pero autenticará toda la información después del encabezado ESP.

```
{laddr enigma raddr partym} ipsec {encr_algs any encr_auth_algs any sa shared}
```

Nota – También puede agregar etiquetas a los sistemas que están protegidos mediante certificados. Los certificados de claves públicas se gestionan en la zona global en los sistemas Trusted Extensions. Modifique el archivo `ike/config` de forma similar al completar los procedimientos detallados en "Configuración de IKE con certificados de clave pública" de *Administración de Oracle Solaris: servicios IP*.

▼ Cómo configurar un túnel en una red que no es de confianza

Este procedimiento configura un túnel IPsec en una red pública entre dos sistemas de puerta de enlace VPN de Trusted Extensions. El ejemplo que se utiliza en este procedimiento se basa en la configuración ilustrada en "Descripción de la topología de red para la protección de una VPN por parte de las tareas de IPsec" de *Administración de Oracle Solaris: servicios IP*.

Supongamos que se realizan las siguientes modificaciones en la ilustración:

- Las `10` subredes son redes de confianza de varios niveles. Las etiquetas de seguridad de las opciones IP de CIPSO se visualizan en estas redes LAN.
- Las subredes `192.168` son redes no de confianza de una sola etiqueta que funcionan en la etiqueta `PUBLIC`. Estas redes no admiten las opciones IP de CIPSO.
- El tráfico con etiquetas entre `euro-vpn` y `calif-vpn` está protegido contra cambios no autorizados.

Antes de empezar Tiene el rol de usuario `root` en la zona global.

1 **Siga los procedimientos detallados en "Etiquetado de hosts y redes (mapa de tareas)" en la página 216 para definir lo siguiente:**

a. **Agregue las direcciones IP `10.0.0.0/8` a una plantilla de seguridad con etiquetas.**

Utilice una plantilla con un tipo de host CIPSO. Conserve el rango de etiquetas predeterminado, de `ADMIN_LOW` a `ADMIN_HIGH`.

b. Agregue las direcciones IP `192.168.0.0/16` a una plantilla de seguridad sin etiquetas en la etiqueta `PUBLIC`.

Utilice una plantilla con un tipo de host sin etiquetas. Defina `PUBLIC` como la etiqueta predeterminada. Conserve el rango de etiquetas predeterminado, de `ADMIN_LOW` a `ADMIN_HIGH`.

c. Agregue las direcciones de Internet de `Calif-vpn` y `Euro-vpn`, `192.168.13.213` y `192.168.116.16`, a una plantilla CIPSO.

Conserve el rango de etiquetas predeterminado.

2 Cree un túnel IPsec.

Siga el procedimiento detallado en "Cómo proteger una VPN con IPsec en modo de túnel" de *Administración de Oracle Solaris: servicios IP*. Utilice IKE para la gestión de claves, como se describe en el siguiente paso.

3 Agregue etiquetas a las negociaciones IKE.

Siga el procedimiento detallado en "Cómo configurar IKE con claves previamente compartidas" de *Administración de Oracle Solaris: servicios IP*, y luego modifique el archivo `ike/config` de la siguiente manera:

a. Agregue las palabras clave `label_aware`, `multi_label` y `wire_label none PUBLIC` al archivo `/etc/inet/ike/config` del sistema `euro-vpn`.

El archivo resultante tiene el siguiente aspecto. Se resaltan las adiciones de etiquetas.

```
        ### ike/config file on euro-vpn, 192.168.116.16
    ## Global parameters
    #
## Use IKE to exchange security labels.
    label_aware
    #
        ## Defaults that individual rules can override.
    p1_xform
          { auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
    p2_pfs 2
    #
   ## The rule to communicate with calif-vpn
       # Label must be unique
    { label "eurovpn-califvpn"
          local_addr 192.168.116.16
          remote_addr 192.168.13.213
          multi_label
          wire_label none PUBLIC
          p1_xform
           { auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
          p2_pfs 5
        }
```

b. Agregue las mismas palabras clave al archivo `ike/config` del sistema `calif-vpn`.

```
    ### ike/config file on calif-vpn, 192.168.13.213
    ## Global Parameters
```

```
    #
## Use IKE to exchange security labels.
    label_aware
    #
        p1_xform
          { auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
    p2_pfs 2
    ## The rule to communicate with euro-vpn
    # Label must be unique
    { label "califvpn-eurovpn"
          local_addr 192.168.13.213
          remote_addr 192.168.116.16
          multi_label
          wire_label none PUBLIC
    p1_xform
           { auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
        p2_pfs 5
    }
```

Nota – También puede agregar etiquetas a los sistemas que están protegidos mediante certificados. Modifique el archivo `ike/config` de forma similar al completar los procedimientos detallados en "Configuración de IKE con certificados de clave pública" de *Administración de Oracle Solaris: servicios IP*.

Resolución de problemas de la red de confianza (mapa de tareas)

El siguiente mapa de tareas describe las tareas que ayudan a depurar la red de Trusted Extensions.

Tarea	Descripción	Para obtener instrucciones
Determinar por qué un sistema y un host remoto no se pueden comunicar.	Se comprueba que las interfaces de un solo sistema estén activas.	"Cómo verificar que las interfaces de un sistema estén activas" en la página 240
	Se utilizan herramientas de depuración cuando un sistema y un host remoto no se pueden comunicar entre sí.	"Cómo depurar la red de Trusted Extensions" en la página 241
Determinar por qué un cliente LDAP no puede acceder al servidor LDAP.	Se resuelven los problemas de pérdida de conexión entre un servidor LDAP y un cliente.	"Cómo depurar la conexión de un cliente con el servidor LDAP" en la página 245

▼ Cómo verificar que las interfaces de un sistema estén activas

Utilice este procedimiento si el sistema no se comunica con otros hosts según lo esperado.

Antes de empezar Debe estar en la zona global en un rol que pueda verificar los valores de atributos de la red. El rol de administrador de la seguridad y el rol de administrador del sistema pueden verificar estos valores.

1 **Verifique que la interfaz de la red del sistema esté activa.**

Puede utilizar la interfaz gráfica de usuario Labeled Zone Manager o el comando `ipadm` para visualizar las interfaces del sistema.

- **Abra Labeled Zone Manager y, a continuación, haga doble clic en la zona de interés.**

```
# txzonemgr &
```

Seleccione Configure Network Interfaces y verifique que el valor de la columna `Status` para la zona sea `Up`.

- **O bien, utilice el comando `ipadm show-addr`.**

```
# ipadm show-addr
...
ADDROBJ           TYPE      STATE        ADDR
lo0/v4            static    ok           127.0.0.1/8
net0/_a           dhcp      down         10.131.132.133/23
net0:0/_a         dhcp      down         10.131.132.175/23
```

Las interfaces `net0` deben tener el valor `ok`. Para obtener más información sobre el comando `ipadm`, consulte la página del comando man `ipadm(1M)`.

2 **Si la interfaz no está activa, actívela.**

a. **En interfaz gráfica de usuario Labeled Zone Manager, haga doble clic en la zona cuya interfaz está inactiva.**

b. **Seleccione Configure Network Interfaces.**

c. **Haga doble clic en la interfaz cuyo estado es `Down`.**

d. **Seleccione Bring Up y luego OK.**

e. **Haga clic en Cancel o en OK.**

▼ Cómo depurar la red de Trusted Extensions

Para depurar dos hosts que deben comunicarse, pero no lo hacen, puede utilizar las herramientas de depuración de Trusted Extensions y Oracle Solaris. Por ejemplo, los comandos de depuración de redes de Oracle Solaris, como `snoop` y `netstat`, se encuentran disponibles. Para obtener detalles, consulte las páginas del comando man `snoop(1M)` y `netstat(1M)`. Para los comandos que son específicos de Trusted Extensions, consulte el Apéndice D, “Lista de las páginas del comando man de Trusted Extensions”.

- Para obtener información sobre los problemas para contactarse con zonas con etiquetas, consulte "Gestión de zonas (mapa de tareas)" en la página 172.
- Para obtener información sobre la depuración de los montajes de NFS, consulte "Cómo resolver problemas por fallos de montaje en Trusted Extensions" en la página 192.

Antes de empezar Debe estar en la zona global en un rol que pueda verificar los valores de atributos de la red. El rol de administrador de la seguridad y el rol de administrador del sistema pueden verificar estos valores. Sólo el rol de usuario `root` puede editar archivos.

1 Compruebe que los hosts que no pueden comunicarse estén utilizando el mismo servicio de nombres.

a. En cada sistema, compruebe los valores de las bases de datos de Trusted Extensions en el servicio SMF `name-service/switch`.

```
# svccfg -s name-service/switch listprop config
config/value_authorization  astring  solaris.smf.value.name-service.switch
config/default              astring  ldap
...
config/tnrhtp               astring  "files ldap"
config/tnrhdb               astring  "files ldap"
```

b. Si los valores son diferentes en los distintos hosts, corrija los valores de los hosts en conflicto.

```
# svccfg -s name-service/switch setprop config/tnrhtp="files ldap"
# svccfg -s name-service/switch setprop config/tnrhdb="files ldap"
```

c. A continuación, reinicie el daemon de servicio de nombres en esos hosts.

```
# svcadm restart name-service/switch
```

2 Verifique que cada host esté definido correctamente. Para ello, visualice los atributos de seguridad de los hosts de origen, de destino y de puerta de enlace en la transmisión.

Utilice la línea de comandos para comprobar que la información de la red es correcta. Verifique que la asignación en cada host coincide con la asignación en los otros hosts de la red. En función de la vista deseada, utilice el comando `tncfg`, el comando `tninfo` o la interfaz gráfica de usuario `txzonemgr`.

- **Visualice una definición de la plantilla.**

  El comando `tninfo -t` muestra las etiquetas en formato de cadena o hexadecimal.

```
$ tninfo -t template-name
template: template-name
host_type: one of CIPSO or UNLABELED
doi: 1
min_sl: minimum-label
hex: minimum-hex-label
max_sl: maximum-label
hex: maximum-hex-label
```

- **Visualice una plantilla y los hosts asignados a ella.**

  El comando `tncfg -t` muestra las etiquetas en formato de cadena y enumera los hosts asignados.

  ```
  $ tncfg -t template info
     name=<template-name>
     host_type=<one of cipso or unlabeled>
     doi=1
     min_label=<minimum-label>
     max_label=<maximum-label>
     host=127.0.0.1/32            /** Localhost **/
     host=192.168.1.2/32          /** LDAP server **/
     host=192.168.1.22/32         /** Gateway to LDAP server **/
     host=192.168.113.0/24        /** Additional network **/
     host=192.168.113.100/25           /** Additional network **/
     host=2001:a08:3903:200::0/56      /** Additional network **/
  ```

- **Visualice la dirección IP y la plantilla de seguridad asignada para un host específico.**

  El comando `tninfo -h` muestra la dirección IP del host especificado y el nombre de la plantilla de seguridad asignada.

  ```
  $ tninfo -h hostname
  IP Address: IP-address
  Template: template-name
  ```

  El comando `tncfg get host=` muestra el nombre de la plantilla de seguridad que define el host especificado.

  ```
  $ tncfg get host=hostname|IP-address[/prefix]
  template-name
  ```

- **Visualice los puertos de varios niveles (MLP) de una zona.**

  El comando `tncfg -z` muestra un MLP por línea.

  ```
  $ tncfg -z zone-name info [mlp_private | mlp_shared]
  mlp_private=<port/protocol-that-is-specific-to-this-zone-only>
  mlp_shared=<port/protocol-that-the-zone-shares-with-other-zones>
  ```

  El comando `tninfo -m` muestra los MLP privados en una línea y los MLP compartidos en una segunda línea. Los MLP se separan con punto y coma.

  ```
  $ tninfo -m zone-name
  private: ports-that-are-specific-to-this-zone-only
  shared: ports-that-the-zone-shares-with-other-zones
  ```

  Para obtener una visualización gráfica de los MLP, utilice el comando `txzonemgr`. Haga doble clic en la zona y, a continuación, seleccione Configure Multilevel Ports.

3 Corrija cualquier información incorrecta.

a. Para cambiar o comprobar la información de seguridad de la red, utilice los comandos administrativos de la red de confianza, `tncfg` y `txzonemgr`. Para verificar la sintaxis de las bases de datos, utilice el comando `tnchkdb`.

Por ejemplo, la siguiente salida muestra que el nombre de una plantilla, `internal_cipso`, no está definido:

```
# tnchkdb
     checking /etc/security/tsol/tnrhtp ...
     checking /etc/security/tsol/tnrhdb ...
tnchkdb: unknown template name: internal_cipso at line 49
tnchkdb: unknown template name: internal_cipso at line 50
tnchkdb: unknown template name: internal_cipso at line 51
     checking /etc/security/tsol/tnzonecfg ...
```

El error indica que los comandos `tncfg` y `txzonemgr` no se utilizaron para crear y asignar la plantilla de seguridad `internal_cipso`.

Para reparar esto, sustituya el archivo `tnrhdb` con el archivo original y luego utilice el comando `tncfg` para crear y asignar plantillas de seguridad.

b. Para borrar la antememoria del núcleo, reinicie el sistema.

Durante el inicio, la antememoria se rellena con información de la base de datos. El servicio SMF, `name-service/switch`, determina si se utilizan bases de datos locales o LDAP para rellenar el núcleo.

4 Recopile información de la transmisión para usarla como ayuda en la depuración.

a. Verifique la configuración de enrutamiento.

```
$ route get [ip] -secattr sl=label,doi=integer
```

Para obtener detalles, consulte la página del comando man `route`(1M).

b. Vea la información de la etiqueta en los paquetes.

```
$ snoop -v
```

La opción `-v` muestra los detalles de los encabezados de los paquetes, incluida la información de la etiqueta. Dado que este comando proporciona información muy detallada, quizás desee restringir los paquetes que el comando examina. Para obtener detalles, consulte la página del comando man `snoop`(1M).

c. Vea las entradas de la tabla de enrutamiento y los atributos de seguridad en sockets.

```
$ netstat -aR
```

La opción `-aR` muestra los atributos de seguridad ampliados para sockets.

```
$ netstat -rR
```

La opción `-rR` muestra las entradas de la tabla de enrutamiento. Para obtener detalles, consulte la página del comando man `netstat(1M)`.

▼ Cómo depurar la conexión de un cliente con el servidor LDAP

Un error en la configuración de una entrada del cliente en el servidor LDAP puede impedir la comunicación del cliente con el servidor. Un error en la configuración de los archivos del cliente también puede impedir la comunicación. Compruebe las entradas y los archivos siguientes cuando intente depurar un problema de comunicación entre el cliente y el servidor.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global del cliente LDAP.

1 Compruebe que la plantilla de host remoto para el servidor LDAP y para la puerta de enlace con el servidor LDAP sea correcta.

a. Utilice el comando `tncfg` o `tninfo` para ver información.

```
# tncfg get host=LDAP-server
# tncfg get host=gateway-to-LDAP-server

# tninfo -h LDAP-server
# tninfo -h gateway-to-LDAP-server
```

b. Determine la ruta del servidor.

```
# route get LDAP-server
```

Si existe una asignación de plantilla incorrecta, agregue el host a la plantilla correcta.

2 Revise y corrija el archivo `/etc/hosts` si es necesario.

El sistema, las interfaces para las zonas con etiquetas del sistema, la puerta de enlace con el servidor LDAP y el servidor LDAP deben figurar en el archivo. Puede que tenga más entradas.

Busque las entradas duplicadas. Elimine cualquier entrada que sea una zona con etiquetas en otros sistemas. Por ejemplo, si el nombre de su servidor LDAP es `Lserver`, y `LServer-zones` es la interfaz compartida para las zonas con etiquetas, elimine `LServer-zones` del archivo `/etc/hosts`.

3 Si utiliza DNS, compruebe la configuración del servicio `svc:/network/dns/client`.

```
# svccfg -s dns/client listprop config
config                      application
config/value_authorization  astring       solaris.smf.value.name-service.dns.switch
config/nameserver           astring       192.168.8.25 192.168.122.7
```

4 **Para cambiar los valores, utilice el comando `svccfg`.**

```
# svccfg -s dns/client setprop config/search = astring: example1.domain.com
# svccfg -s dns/client setprop config/nameserver = net_address: 192.168.8.35
# svccfg -s dns/client:default refresh
# svccfg -s dns/client:default validate
# svcadm enable dns/client
# svcadm refresh name-service/switch
# nslookup some-system
Server:         192.168.135.35
Address:        192.168.135.35#53

Name:   some-system.example1.domain.com
Address: 10.138.8.22
Name:   some-system.example1.domain.com
Address: 10.138.8.23
```

5 **Verifique que las entradas `tnrhdb` y `tnrhtp` del servicio `name-service/switch` son exactas.**

En la siguiente salida, no se muestran las entradas `tnrhdb` y `tnrhtp`. Por lo tanto, estas bases de datos utilizan los servicios de nombres predeterminados `files ldap`, en ese orden.

```
# svccfg -s name-service/switch listprop config
config                      application
config/value_authorization  astring      solaris.smf.value.name-service.switch
config/default              astring      "files ldap"
config/host                 astring      "files dns"
config/netgroup             astring      ldap
```

6 **Compruebe que el cliente esté configurado correctamente en el servidor.**

```
# ldaplist -l tnrhdb client-IP-address
```

7 **Compruebe que las interfaces para sus zonas con etiquetas estén configuradas correctamente en el servidor LDAP.**

```
# ldaplist -l tnrhdb client-zone-IP-address
```

8 **Verifique que puede establecer contacto con el servidor LDAP desde todas las zonas que se encuentran en ejecución.**

```
# ldapclient list
...
NS_LDAP_SERVERS= LDAP-server-address
# zlogin zone-name1 ping LDAP-server-address
LDAP-server-address is alive
# zlogin zone-name2 ping LDAP-server-address
LDAP-server-address is alive
...
```

9 **Configure LDAP y reinicie el sistema.**

a. **Para conocer el procedimiento, consulte "Conversión de la zona global en un cliente LDAP en Trusted Extensions" en la página 94.**

b. En cada zona con etiquetas, vuelva a establecer la zona como cliente del servidor LDAP.

```
# zlogin zone-name1
# ldapclient init \
-a profileName=profileName \
-a domainName=domain \
-a proxyDN=proxyDN \
-a proxyPassword=password  LDAP-Server-IP-Address
# exit
# zlogin zone-name2 ...
```

c. Detenga todas las zonas y reinicie el sistema.

```
# zoneadm list
zone1
zone2
,
,
,
# zoneadm -z zone1 halt
# zoneadm -z zone2 halt
.
.
.
# reboot
```

También puede usar la interfaz gráfica de usuario `txzonemgr` para detener las zonas con etiquetas.

◆ ◆ ◆ CAPÍTULO 17

Trusted Extensions y LDAP (descripción general)

En este capítulo se describe el uso de Oracle Directory Server Enterprise Edition (servidor de directorios) para sistemas que estén configurados con Trusted Extensions.

Uso del servicio de nombres en Trusted Extensions

Para alcanzar una uniformidad entre el usuario, el host y los atributos de red dentro de un dominio de seguridad con varios sistemas Trusted Extensions, se usa un servicio de nombres para distribuir la mayor parte de la información de configuración. El servicio `svc:/system/name-service/switch` determina qué servicio de nombres se utiliza. LDAP es el servicio de nombres recomendado para Trusted Extensions.

El servidor de directorios puede proporcionar el servicio de nombres LDAP para los clientes de Trusted Extensions y Oracle Solaris. El servidor debe incluir bases de datos de red de Trusted Extensions, y los clientes de Trusted Extensions deben conectarse al servidor mediante un puerto de varios niveles. El administrador de la seguridad especifica el puerto de varios niveles durante la configuración del sistema.

Trusted Extensions agrega dos bases de datos de red de confianza al servidor de directorios: `tnrhdb` y `tnrhtp`.

- Para obtener información sobre el uso del servicio de nombres LDAP en Oracle Solaris, consulte *Oracle Solaris Administration: Naming and Directory Services*.
- La configuración del servidor de directorios para Trusted Extensions se describe en el Capítulo 5, "Configuración de LDAP para Trusted Extensions (tareas)". Los sistemas Trusted Extensions pueden ser clientes de un servidor de directorios de Oracle Solaris si se utiliza un proxy de servidor de directorios configurado con Trusted Extensions.
- La configuración de clientes del servidor de directorios de Trusted Extensions se describe en "Creación de un cliente LDAP de Trusted Extensions" en la página 94.

Nota – Los sistemas configurados con Trusted Extensions no pueden ser clientes de servidores maestros NIS.

Sistemas Trusted Extensions gestionados de manera local

Si un servicio de nombres no se usa en un sitio, los administradores deben asegurarse de que la información de configuración para los usuarios, los sistemas y las redes sea idéntica en todos los sistemas. Si se realiza un cambio en un sistema, dicho cambio debe aplicarse en todos los sistemas.

En un sistema Trusted Extensions gestionado de manera local, la información de configuración se mantiene en archivos, en los directorios `/etc`, `/etc/security` y `/etc/security/tsol`.

Bases de datos LDAP de Trusted Extensions

Trusted Extensions amplía el esquema del servidor de directorios para acomodar las bases de datos `tnrhdb` y `tnrhtp`. Trusted Extensions define dos atributos nuevos, `ipTnetNumber` y `ipTnetTemplateName`, y dos clases de objeto nuevas, `ipTnetTemplate` y `ipTnetHost`.

Los atributos se definen de la siguiente manera:

```
ipTnetNumber
   ( 1.3.6.1.1.1.1.34 NAME 'ipTnetNumber'
     DESC 'Trusted network host or subnet address'
     EQUALITY caseExactIA5Match
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
     SINGLE-VALUE )

ipTnetTemplateName
   ( 1.3.6.1.1.1.1.35 NAME 'ipTnetTemplateName'
     DESC 'Trusted network template name'
     EQUALITY caseExactIA5Match
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
     SINGLE-VALUE )
```

Las clases de objeto se definen de la siguiente manera:

```
ipTnetTemplate
   ( 1.3.6.1.1.1.2.18 NAME 'ipTnetTemplate' SUP top STRUCTURAL
     DESC 'Object class for Trusted network host templates'
     MUST ( ipTnetTemplateName )
     MAY ( SolarisAttrKeyValue ) )

ipTnetHost
   ( 1.3.6.1.1.1.2.19 NAME 'ipTnetHost' SUP top AUXILIARY
```

```
    DESC 'Object class for Trusted network host/subnet address
          to template mapping'
    MUST ( ipTnetNumber $ ipTnetTemplateName ) )
```

La plantilla de definición `cipso` en LDAP es similar a la siguiente:

```
ou=ipTnet,dc=example,dc=example1,dc=exampleco,dc=com
 objectClass=top
 objectClass=organizationalUnit
 ou=ipTnet

 ipTnetTemplateName=cipso,ou=ipTnet,dc=example,dc=example1,dc=exampleco,dc=com
 objectClass=top
 objectClass=ipTnetTemplate
 ipTnetTemplateName=cipso
 SolarisAttrKeyValue=host_type=cipso;doi=1;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH;

 ipTnetNumber=0.0.0.0,ou=ipTnet,dc=example,dc=example1,dc=exampleco,dc=com
 objectClass=top
 objectClass=ipTnetTemplate
 objectClass=ipTnetHost
 ipTnetNumber=0.0.0.0
 ipTnetTemplateName=internal
```

Uso del servicio de nombres LDAP en Trusted Extensions

El servicio de nombres LDAP se gestiona en Trusted Extensions al igual que en Oracle Solaris. A continuación, se proporcionan algunos comandos útiles con referencias para obtener información más detallada:

- Para conocer las estrategias para resolver problemas de configuración de LDAP, consulte el Capítulo 13, "LDAP Troubleshooting (Reference)" de *Oracle Solaris Administration: Naming and Directory Services*.
- Para resolver problemas de conexión entre clientes y servidores LDAP que se ven afectados por las etiquetas, consulte "Cómo depurar la conexión de un cliente con el servidor LDAP" en la página 245.
- Para resolver otros problemas de conexión entre clientes y servidores LDAP, consulte el Capítulo 13, "LDAP Troubleshooting (Reference)" de *Oracle Solaris Administration: Naming and Directory Services*.
- Para visualizar las entradas LDAP desde un cliente LDAP, escriba:

  ```
  $ ldaplist -l
  $ ldap_cachemgr -g
  ```

- Para visualizar las entradas LDAP desde un servidor LDAP, escriba:

  ```
  $ ldap_cachemgr -g
  $ idsconfig -v
  ```

- Para visualizar los hosts que LDAP gestiona, escriba:

  ```
  $ ldaplist -l hosts      Long listing
  $ ldaplist hosts         One-line listing
  ```

- Para crear una lista con la información del árbol de información de directorios (DIT, Directory Information Tree) en LDAP, escriba:

```
$ ldaplist -l services | more
dn: cn=apocd+ipServiceProtocol=udp,ou=Services,dc=exampleco,dc=com
  objectClass: ipService
  objectClass: top
  cn: apocd
  ipServicePort: 38900
  ipServiceProtocol: udp

...
$ ldaplist services name
dn=cn=name+ipServiceProtocol=udp,ou=Services,dc=exampleco,dc=com
```

- Para visualizar el estado del servicio LDAP en el cliente, escriba:

```
# svcs -xv network/ldap/client
svc:/network/ldap/client:default (LDAP client)
 State: online since date
   See: man -M /usr/share/man -s 1M ldap_cachemgr
   See: /var/svc/log/network-ldap-client:default.log
Impact: None.
```

- Para iniciar y detener el cliente LDAP, escriba:

```
# svcadm enable network/ldap/client

# svcadm disable network/ldap/client
```

- Para iniciar y detener el servidor LDAP en la versión 6 ó 7 del software LDAP;, escriba:

```
# dsadm start /export/home/ds/instances/your-instance
# dsadm stop /export/home/ds/instances/your-instance
```

- Para iniciar y detener un servidor proxy LDAP en la versión 6 ó 7 del software LDAP;, escriba:

```
# dpadm start /export/home/ds/instances/your-instance
# dpadm stop /export/home/ds/instances/your-instance
```

◆ ◆ ◆ CAPÍTULO 18

Correo de varios niveles en Trusted Extensions (descripción general)

En este capítulo se tratan la seguridad y los servicios de envío de correo de varios niveles de los sistemas que se configuran con Trusted Extensions.

Servicio de correo de varios niveles

Trusted Extensions proporciona correo de varios niveles para cualquier aplicación de correo. Cuando los usuarios comunes inician su aplicación de correo, la aplicación se abre en la etiqueta actual del usuario. Si los usuarios operan en un sistema de varios niveles, quizás deseen enlazar o copiar sus archivos de inicialización de la aplicación de correo. Para obtener detalles, consulte "Cómo configurar los archivos de inicio para los usuarios en Trusted Extensions" en la página 146.

Funciones de correo de Trusted Extensions

En Trusted Extensions, el rol de administrador del sistema configura y administra los servidores de correo según las instrucciones detalladas en el Capítulo 13, "Servicios de correo (tareas)" de *Oracle Administración Solaris: Servicios de red*. Además, el administrador de la seguridad determina cómo se deben configurar las funciones de correo de Trusted Extensions.

Los siguientes aspectos de la gestión de correo son específicos de Trusted Extensions:

- El archivo `.mailrc` se encuentra en una etiqueta mínima del usuario.

  Por lo tanto, los usuarios que trabajan en varias etiquetas no tienen un archivo `.mailrc` en las etiquetas superiores, a menos que copien o enlacen el archivo `.mailrc` ubicado en el directorio de la etiqueta mínima a cada directorio superior.

El rol de administrador de la seguridad o el usuario individual pueden agregar el archivo `.mailrc` a `.copy_files` o a `.link_files`. Para obtener una descripción de estos archivos, consulte la página del comando man `updatehome(1)`. Para obtener sugerencias de configuración, consulte "Archivos `.copy_files` y `.link_files`" en la página 141.

- El lector de correo se puede ejecutar en cualquier etiqueta del sistema. Es necesario realizar algunas tareas de configuración para conectar un cliente de correo al servidor.

  Por ejemplo, para utilizar Thunderbird para el correo de varios niveles, es necesario que configure un cliente de correo de Thunderbird en cada etiqueta a fin de especificar el servidor de correo. El servidor de correo puede ser el mismo o uno diferente para cada una de las etiquetas, pero el servidor debe estar especificado.

- El software Trusted Extensions comprueba las etiquetas del host y del usuario antes de enviar o reenviar correo.
  - El software comprueba que el correo se encuentre dentro del rango de acreditación del host. Las comprobaciones se describen en esta lista y en "Comprobaciones de acreditaciones de Trusted Extensions" en la página 206.
  - El software comprueba que el correo se encuentre entre la autorización de la cuenta y la etiqueta mínima.
  - Los usuarios pueden leer el correo electrónico que se recibe dentro del rango de acreditación. Durante una sesión, los usuarios pueden leer el correo solamente en su etiqueta actual.

    Para ponerse en contacto con un usuario común mediante correo electrónico, un rol administrativo debe enviar un correo desde un espacio de trabajo que se encuentre en una etiqueta que el usuario pueda leer. Por lo general, la etiqueta predeterminada del usuario es una buena opción.

◆ ◆ ◆ CAPÍTULO 19

Gestión de impresión con etiquetas (tareas)

En este capítulo, se describe cómo imprimir etiquetas en Trusted Extensions.

Etiquetas, impresoras e impresión

El software Trusted Extensions usa etiquetas para controlar el acceso a las impresoras. Las etiquetas se usan para controlar el acceso a las impresoras y a la información sobre los trabajos de impresión en cola. El software también etiqueta el resultado de la impresión. Las páginas del cuerpo y las páginas de la carátula y el ubicador obligatorios tienen etiquetas.

El administrador del sistema se encarga de la administración básica de las impresoras. El rol de administrador de la seguridad se ocupa de la seguridad de las impresoras, que incluye las etiquetas y el tratamiento del la impresión con etiquetas. Los administradores siguen los procedimientos básicos de administración de impresoras de Oracle Solaris y, luego, asignan etiquetas a los servidores de impresión y a las impresoras.

El software Trusted Extensions admite la impresión de un solo nivel y también de varios niveles. La impresión de un solo nivel está configurada de manera predeterminada. La impresión de varios niveles se implementa únicamente en la zona global. Para utilizar el servidor de impresión de la zona global, se debe haber configurado una zona con etiquetas como instancia de IP o como VNIC. La dirección debe ser distinta de la dirección IP de la zona global.

Restricción del acceso a las impresoras y a la información de trabajos de impresión en Trusted Extensions

Los usuarios y los roles de los sistemas en los que está configurado el software Trusted Extensions crean trabajos de impresión en la etiqueta de su sesión. Los trabajos de impresión se pueden imprimir solamente en impresoras que reconozcan esa etiqueta. La etiqueta debe estar dentro del rango de etiquetas de la impresora.

Los usuarios y los roles pueden ver los trabajos de impresión que tengan la misma etiqueta que la sesión. En la zona global, un rol puede ver los trabajos cuyas etiquetas estén controladas por la etiqueta de la zona.

Las impresoras que se configuran con el software Trusted Extensions imprimen etiquetas en el resultado de la impresión. Las impresoras administradas con servidores de impresión sin etiquetas no imprimen etiquetas en el resultado de la impresión. Estas impresoras tienen la misma etiqueta que su servidor sin etiquetas. Por ejemplo, se puede asignar una etiqueta arbitraria a un servidor de impresión de Oracle Solaris. Así, los usuarios pueden imprimir los trabajos en esa etiqueta arbitraria con la impresora de Oracle Solaris. Como sucede con las impresoras de Trusted Extensions esas impresoras de Oracle Solaris solamente pueden aceptar trabajos de impresión de los usuarios que trabajan en la etiqueta asignada al servidor de impresión.

Resultado de impresión con etiquetas

Trusted Extensions imprime etiquetas en las páginas del cuerpo y en las páginas de la carátula y del ubicador. La información proviene del archivo `label_encodings`.

El administrador de la seguridad puede configurar cuentas de usuario para que utilicen impresoras que no imprimen etiquetas en el resultado.

Impresión PostScript de la información de seguridad

La impresión con etiquetas en Trusted Extensions se basa en las funciones de impresión de Oracle Solaris. En el SO Oracle Solaris, la opción `job-sheets` gestiona la creación de páginas de carátula. Para implementar las etiquetas, el trabajo de impresión se convierte en un archivo PostScript. A continuación, el archivo PostScript se manipula para que se inserten etiquetas en las páginas del cuerpo y se creen las páginas de la carátula y del ubicador.

Configuración de impresión con etiquetas (mapa de tareas)

El siguiente mapa de tareas describe los procedimientos de configuración comunes relativos a la impresión con etiquetas. Para obtener más información, consulte el Capítulo 15, "Configuración y administración de impresoras mediante CUPS (tareas)" de *Administración de Oracle Solaris: tareas comunes*.

Nota – Los clientes de la impresora pueden imprimir solamente los trabajos que se encuentren dentro del rango de etiquetas del servidor de impresión de Trusted Extensions.

Tarea	Descripción	Para obtener instrucciones
Configurar la impresión desde la zona global.	Se crea un servidor de impresión de varios niveles en la zona global.	"Cómo configurar un servidor de impresión de varios niveles y sus impresoras" en la página 258
Configurar la impresión desde una zona con etiquetas.	Se crea un servidor de impresión de una sola etiqueta para una zona con etiquetas.	"Cómo configurar una zona como un servidor de impresión de un solo nivel" en la página 257
Configurar un cliente de impresión de varios niveles.	Se conecta un host de Trusted Extensions con una impresora.	"Cómo habilitar un cliente de Trusted Extensions para que acceda a un impresora" en la página 260
Restringir el rango de etiquetas de una impresora.	Se restringe una impresora de Trusted Extensions a un rango de etiquetas menor.	"Cómo configurar un rango de etiquetas restringido para una impresora" en la página 262

▼ Cómo configurar una zona como un servidor de impresión de un solo nivel

Antes de empezar La zona no debe compartir una dirección IP con la zona global. Debe estar con el rol de administrador de la seguridad en la zona global.

1. **Agregue un espacio de trabajo.**

   Para obtener detalles, consulte "Cómo agregar un espacio de trabajo en una etiqueta mínima" de *Guía del usuario de Oracle Solaris Trusted Extensions*.

2. **Cambie la etiqueta del espacio de trabajo nuevo por la etiqueta de la zona que será servidor de impresión para esa etiqueta.**

   Para obtener detalles, consulte "Cómo cambiar la etiqueta de un espacio de trabajo" de *Guía del usuario de Oracle Solaris Trusted Extensions*.

3 **Defina las características de cada impresora conectada.**

   a. **En la etiqueta de la zona, edite el archivo de configuración del servidor de impresión CUPS, `/etc/cups/cupsd.conf`.**

4 **Asigne la hoja de trabajo adecuada a cada impresora conectada al servidor de impresión.**

   Por ejemplo, las siguientes especificaciones crean una hoja con etiquetas adecuada:

```
#CUPS-BANNER for INTERNAL print jobs
Show job-id job-name job-originating-user-name job-originating-host-name job-billing
Header CONFIDENTIAL : INTERNAL USE ONLY
Footer CONFIDENTIAL : INTERNAL USE ONLY
Image images/cups.png
```

   Utilice el comando siguiente:

```
$ lpadmin -p printer -o job-sheets-default=labeled,labeled
```

   Las impresoras conectadas pueden imprimir trabajos únicamente en la etiqueta de la zona.

5 **Pruebe la impresora.**

Nota – Por cuestiones de seguridad, los archivos que tienen una etiqueta administrativa, ya sea `ADMIN_HIGH` o `ADMIN_LOW`, imprimen `ADMIN_HIGH` en el cuerpo de la copia impresa. Las páginas de la carátula y del ubicador tienen la etiqueta máxima y los compartimientos del archivo `label_encodings`.

Como usuario `root` y como usuario común, realice los siguientes pasos:

   a. **Imprima los archivos sin formato desde la línea de comandos.**

   b. **Imprima los archivos desde las aplicaciones, como Oracle Beehive, el explorador y el editor.**

   c. **Verifique que las etiquetas se impriman correctamente.**

Véase también

- **Impedir el resultado con etiquetas**: "Reducción de las restricciones de impresión en Trusted Extensions (mapa de tareas)" en la página 263
- **Usar esta zona como servidor de impresión**: "Cómo habilitar un cliente de Trusted Extensions para que acceda a un impresora" en la página 260

▼ Cómo configurar un servidor de impresión de varios niveles y sus impresoras

Las impresoras gestionadas por un servidor de impresión de Trusted Extensions imprimen etiquetas en las páginas del cuerpo, de la carátula y del ubicador. Esta clase de impresoras

pueden imprimir los trabajos de impresión dentro del rango de etiquetas del servidor de impresión. Cualquier host de Trusted Extensions que pueda acceder al servidor de impresión puede utilizar las impresoras que están conectadas al servidor.

Antes de empezar Determine el servidor de impresión para su red de Trusted Extensions. Debe estar con el rol de administrador del sistema en la zona global de este servidor de impresión.

1 Habilite la impresión de varios niveles mediante la configuración de la zona global con el puerto del servidor de impresión, `515/tcp`.

```
# tncfg -z global add mlp_shared=515/tcp
# tncfg -z global add mlp_private=515/tcp
```

2 Defina las características de cada impresora conectada.

```
# lpadmin -p printer-name -v /dev/null \
-o protocol=tcp -o dest=printer-IP-address:9100 -T PS -I postscript
# accept printer-name
# enable printer-name
```

3 Configure cada impresora que está conectada al servidor de impresión con una hoja de trabajo con etiquetas.

```
$ lpadmin -p printer -o job-sheets-default=labeled,labeled
```

Si el rango de etiquetas predeterminado que va de `ADMIN_LOW` a `ADMIN_HIGH` es aceptable para todas las impresoras, significa que se completó la configuración de las etiquetas.

4 Configure la impresora en cada zona con etiquetas donde se permite la impresión.

Utilice la dirección IP `all-zones` como servidor de impresión para la zona global.

a. Inicie sesión como usuario root en la consola de la zona con etiquetas.

```
# zlogin -C labeled-zone
```

b. Cree un archivo `/etc/cups/client.conf` en cada zona con etiquetas.

Este archivo se conecta al daemon `cupsd` en la zona global para el servicio de impresión. Modifique este archivo para que incluya el nombre del servidor de impresión y su dirección IP. Para obtener información acerca del archivo de configuración, consulte la página del comando man `client.conf`(5).

c. (Opcional) Establezca la impresora como predeterminada.

```
# lpadmin -d printer-name
```

5 En cada zona con etiquetas, pruebe la impresora.

Como usuario `root` y como usuario común, realice los siguientes pasos:

a. Imprima los archivos sin formato desde la línea de comandos.

b. Imprima los archivos desde las aplicaciones, como Oracle Beehive, el explorador y el editor.

c. Verifique que las etiquetas se impriman correctamente.

Véase también

- **Limitar el rango de etiquetas de la impresora**: "Cómo configurar un rango de etiquetas restringido para una impresora" en la página 262
- **Impedir el resultado con etiquetas**: "Reducción de las restricciones de impresión en Trusted Extensions (mapa de tareas)" en la página 263
- **Usar esta zona como servidor de impresión**: "Cómo habilitar un cliente de Trusted Extensions para que acceda a un impresora" en la página 260

▼ Cómo habilitar un cliente de Trusted Extensions para que acceda a un impresora

Inicialmente, únicamente la zona en la que se configuró un servidor de impresión puede imprimir en las impresoras de ese servidor. El administrador del sistema debe agregar explícitamente el acceso a esas impresoras para otras zonas y sistemas. Las posibilidades son las siguientes:

- Para una zona global, agregue el acceso a las impresoras que estén conectadas a una zona global en un sistema diferente.
- Para una zona con etiquetas, agregue el acceso a las impresoras que estén conectadas a la zona global del sistema.
- Para una zona con etiquetas, agregue el acceso a una impresora para la que una zona remota de la misma etiqueta esté configurada.
- Para una zona con etiquetas, agregue el acceso a las impresoras que estén conectadas a una zona global en un sistema diferente.

Antes de empezar

Debe haber un servidor de impresión configurado con un rango de etiquetas o una sola etiqueta, y las impresoras conectadas a ese servidor deben estar configuradas. Para obtener detalles, consulte lo siguiente:

- "Cómo configurar una zona como un servidor de impresión de un solo nivel" en la página 257
- "Cómo configurar un servidor de impresión de varios niveles y sus impresoras" en la página 258
- "Cómo asignar una etiqueta a un servidor de impresión sin etiquetas" en la página 265

Debe estar con el rol de administrador del sistema en la zona global.

1. **Realice los procedimientos necesarios para habilitar el acceso las impresoras en los sistemas.**

   - **Configure la zona global en un sistema que no sea servidor de impresión y use la zona global de otro sistema para acceder a las impresoras.**

     a. **En el sistema que no tiene acceso a las impresoras, asuma el rol de administrador del sistema.**

     b. **Agregue el acceso a la impresora que está conectada al servidor de impresión de Trusted Extensions.**

        ```
        $ lpadmin -s printer
        ```

   - **Configure una zona con etiquetas a fin de usar su zona global para acceder a una impresora.**

     a. **Cambie la etiqueta del espacio de trabajo de rol por la etiqueta de la zona con etiquetas.**

        Para obtener detalles, consulte "Cómo cambiar la etiqueta de un espacio de trabajo" de *Guía del usuario de Oracle Solaris Trusted Extensions*.

     b. **Agregue el acceso a la impresora.**

        ```
        $ lpadmin -s printer
        ```

   - **Configure una zona con etiquetas a fin de usar la zona con etiquetas de otro sistema para acceder a una impresora.**

     Las etiquetas de las zonas deben ser idénticas.

     a. **En el sistema que no tiene acceso a las impresoras, asuma el rol de administrador del sistema.**

     b. **Cambie la etiqueta del espacio de trabajo de rol por la etiqueta de la zona con etiquetas.**

     c. **Agregue el acceso a la impresora que está conectada al servidor de impresión de la zona con etiquetas remota.**

        ```
        $ lpadmin -s printer
        ```

   - **Configure una zona con etiquetas a fin de usar un servidor de impresión sin etiquetas para acceder a una impresora.**

     La etiqueta de la zona debe ser idéntica a la etiqueta del servidor de impresión.

     a. **En el sistema que no tiene acceso a las impresoras, asuma el rol de administrador del sistema.**

b. Cambie la etiqueta del espacio de trabajo de rol por la etiqueta de la zona con etiquetas.

Para obtener detalles, consulte "Cómo cambiar la etiqueta de un espacio de trabajo" de *Guía del usuario de Oracle Solaris Trusted Extensions*.

c. Agregue el acceso a la impresora que está conectada al servidor de impresión con etiquetas asignadas de manera arbitraria.

```
$ lpadmin -s printer
```

2 Pruebe las impresoras.

Nota – Por cuestiones de seguridad, los archivos que tienen una etiqueta administrativa, ya sea `ADMIN_HIGH` o `ADMIN_LOW`, imprimen `ADMIN_HIGH` en el cuerpo de la copia impresa. Las páginas de la carátula y del ubicador tienen la etiqueta máxima y los compartimientos del archivo `label_encodings`.

En cada cliente, pruebe que la impresión funcione para los usuarios `root` y los roles en la zona global, y para los usuarios `root`, los roles y los usuarios comunes en las zonas con etiquetas.

a. Imprima los archivos sin formato desde la línea de comandos.

b. Imprima los archivos desde las aplicaciones, como Oracle Beehive, el explorador y el editor.

c. Verifique que las etiquetas se impriman correctamente.

▼ Cómo configurar un rango de etiquetas restringido para una impresora

El rango de etiquetas predeterminado de la impresora es de `ADMIN_LOW` a `ADMIN_HIGH`. Este procedimiento reduce el rango de etiquetas de las impresoras controladas mediante un servidor de impresión de Trusted Extensions.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1 Inicie Device Manager.

Seleccione la opción Allocate Device en el menú Trusted Path.

2 Haga clic en el botón Administration para ver el cuadro de diálogo Device Administration.

3 Escriba un nombre para la impresora nueva.

Si la impresora no está conectada al sistema, busque el nombre de la impresora.

4 Haga clic en el botón Configure para ver el cuadro de diálogo Device Configuration.

5 **Cambie el rango de etiquetas de la impresora.**

   a. **Haga clic en el botón Min Label para cambiar la etiqueta mínima.**

      Seleccione una etiqueta del generador de etiquetas. Para obtener información sobre el generador de etiquetas, consulte "Generador de etiquetas en Trusted Extensions" en la página 113.

   b. **Haga clic en el botón Max Label para cambiar la etiqueta máxima.**

6 **Guarde los cambios.**

   a. **Haga clic en OK en el cuadro de diálogo Configuration.**

   b. **Haga clic en OK en el cuadro de diálogo Administration.**

7 **Cierre Device Manager.**

Reducción de las restricciones de impresión en Trusted Extensions (mapa de tareas)

Las siguientes tareas son opcionales. Disminuyen la seguridad de la impresión que Trusted Extensions proporciona de manera predeterminada cuando se instala el software.

Tarea	Descripción	Para obtener instrucciones
Configurar una impresora para que no etiquete el resultado.	Impedir la impresión de información de seguridad en las páginas del cuerpo y eliminar las páginas de la carátula y del ubicador.	"Cómo eliminar las etiquetas del resultado de la impresión" en la página 264
Configurar las impresoras en una sola etiqueta sin resultado con etiquetas.	Habilitar a los usuarios para que impriman con una etiqueta específica en una impresora de Oracle Solaris. Los trabajos de impresión no se marcan con etiquetas.	"Cómo asignar una etiqueta a un servidor de impresión sin etiquetas" en la página 265
Eliminar las etiquetas visibles de las páginas del cuerpo.	Modificar el archivo `tsol_separator.ps` para impedir que las páginas del cuerpo de todos los trabajos de impresión que se envían desde un host de Trusted Extensions tengan etiquetas.	"Cómo eliminar las etiquetas de las páginas de todos los trabajos de impresión" en la página 266
Suprimir las páginas de la carátula y del ubicador.	Autorizar a usuarios específicos para que impriman trabajos sin las páginas de la carátula y del ubicador.	"Cómo suprimir las páginas de la carátula y del ubicador para usuarios específicos" en la página 267

Tarea	Descripción	Para obtener instrucciones
Habilitar usuarios de confianza para que impriman trabajos sin etiquetas.	Autorizar a usuarios específicos o a todos los usuarios de un sistema en particular para que impriman trabajos sin etiquetas.	"Cómo habilitar a usuarios específicos para que supriman las etiquetas de las páginas" en la página 266
Habilitar la impresión de archivos PostScript.	Autorizar a usuarios específicos o a todos los usuarios de un sistema en particular para que impriman archivos PostScript.	"Cómo habilitar a los usuarios para que impriman archivos PostScript en Trusted Extensions" en la página 267
Asignar autorizaciones de impresión.	Habilitar a los usuarios para que omitan las restricciones de impresión predeterminadas.	"Cómo crear perfiles de derechos para autorizaciones convenientes" en la página 151 "Cómo modificar los valores predeterminados de `policy.conf`" en la página 145

▼ Cómo eliminar las etiquetas del resultado de la impresión

Las impresoras que no tienen una secuencia de comandos del modelo de la impresora de Trusted Extensions no imprimen las páginas de la carátula y del ubicador con etiquetas. Tampoco se incluyen etiquetas en las páginas del cuerpo.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

- **En la etiqueta adecuada, realice una de las siguientes acciones:**

  - **Desde el servidor de impresión, detenga la impresión de la carátula por completo.**

    ```
    % lpadmin -p printer -o nobanner=never
    ```

    Las páginas del cuerpo se siguen etiquetando.

  - **Establezca la secuencia de comandos del modelo de la impresora en una secuencia de comandos de Oracle Solaris.**

    ```
    % lpadmin -p printer  \
    -m { standard | netstandard | standard_foomatic | netstandard_foomatic }
    ```

    No aparecen etiquetas en el resultado de la impresión.

▼ Cómo asignar una etiqueta a un servidor de impresión sin etiquetas

Un servidor de impresión de Oracle Solaris es un servidor de impresión sin etiquetas al cual se le puede asignar una etiqueta para que Trusted Extensions acceda a la impresora en esa etiqueta. Las impresoras conectadas a un servidor de impresión sin etiquetas pueden imprimir trabajos solamente en la etiqueta que esté asignada al servidor de impresión. Los trabajos se imprimen sin las etiquetas ni las páginas del ubicador, y puede que se impriman sin las páginas de la carátula. Si un trabajo se imprime con la página de la carátula, es porque la página no contiene ninguna información de seguridad.

El sistema Trusted Extensions puede configurarse para que envíen trabajos a una impresora gestionada con un servidor de impresión sin etiquetas. Los usuarios pueden imprimir los trabajos en la impresora sin etiquetas en la etiqueta que el administrador de la seguridad asigna al servidor de impresión.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

- **Asigne una plantilla sin etiquetas en el servidor de impresión.**

  Para obtener detalles, consulte "Cómo agregar un host a una plantilla de seguridad" en la página 223.

  Elija una etiqueta. Los usuarios que trabajen en ese etiqueta podrán enviar los trabajos de impresión a la impresora de Oracle Solaris en la etiqueta del servidor de impresión. Las páginas no se imprimen con etiquetas, y las páginas de la carátula y del ubicador tampoco forman parte del trabajo de impresión.

Ejemplo 19–1 Envío de trabajos de impresión públicos a una impresora sin etiquetas

Los archivos que se encuentran disponibles para el público en general se pueden imprimir en una impresora sin etiquetas. En este ejemplo, los responsables de marketing de una organización necesitan producir documentos que no tengan etiquetas impresas en la parte superior y en la parte inferior de las páginas.

El administrador de la seguridad asigna una plantilla con el tipo de host sin etiquetas al servidor de impresión Oracle Solaris. La plantilla se describe en el Ejemplo 16–5. La etiqueta arbitraria de la plantilla es `PUBLIC`. La impresora `pr-nolabel1` está conectada a este servidor de impresión. Los trabajos de impresión de los usuarios de la zona `PUBLIC` se imprimen en la impresora `pr-nolabel1` sin etiquetas. Según la configuración de la impresora, los trabajos pueden tener las páginas de la carátula o no tenerlas. Las páginas de la carátula no contienen información de seguridad.

▼ Cómo eliminar las etiquetas de las páginas de todos los trabajos de impresión

Este procedimiento impide que todos los trabajos de impresión de una impresora de Trusted Extensions incluyan etiquetas visibles en las páginas del cuerpo del trabajo de impresión.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1. **Edite el archivo `/usr/lib/lp/postscript/tsol_separator.ps`.**

2. **Encuentre la definición de `/PageLabel`.**

   Encuentre las siguientes líneas:

   ```
   %% To eliminate page labels completely, change this line to
   %% set the page label to an empty string: /PageLabel () def
   /PageLabel Job_PageLabel def
   ```

   Nota – El valor `Job_PageLabel` podría ser diferente en el sitio.

3. **Reemplace el valor de `/PageLabel` por un paréntesis vacío.**

   ```
   /PageLabel () def
   ```

▼ Cómo habilitar a usuarios específicos para que supriman las etiquetas de las páginas

Mediante este procedimiento se habilita a un rol o usuario autorizado a imprimir trabajos en una impresora Trusted Extensions sin etiquetas en la parte superior ni en la parte inferior de cada página del cuerpo. Las etiquetas de las páginas se suprimen para todas las etiquetas en las que el usuario puede trabajar.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1. **Determine quién tiene permiso para imprimir los trabajos sin las etiquetas de las páginas.**

2. **Autorice a esos roles y usuarios para imprimir los trabajos sin las etiquetas de las páginas.**

   Asigne un perfil de derechos que incluya la autorización Print without Label para esos roles y usuarios. Para obtener detalles, consulte "Cómo crear perfiles de derechos para autorizaciones convenientes" en la página 151.

3. **Indique al rol o al usuario que use el comando `lp` para ejecutar los trabajos de impresión:**

   ```
   % lp -o nolabels staff.mtg.notes
   ```

▼ Cómo suprimir las páginas de la carátula y del ubicador para usuarios específicos

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1. **Cree un perfil de derechos que incluya la autorización Print without Banner.**

   Asigne el perfil a cada rol o usuario que tenga permiso para imprimir sin las páginas de la carátula o del ubicador.

   Para obtener detalles, consulte "Cómo crear perfiles de derechos para autorizaciones convenientes" en la página 151.

2. **Indique al rol o al usuario que use el comando `lp` para ejecutar los trabajos de impresión:**

   ```
   % lp -o nobanner staff.mtg.notes
   ```

▼ Cómo habilitar a los usuarios para que impriman archivos PostScript en Trusted Extensions

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

- **Utilice uno de los tres métodos siguientes para habilitar a los usuarios para que impriman archivos PostScript:**

  - **Para habilitar la impresión PostScript en un sistema, modifique el archivo `/etc/default/print` .**

    a. **Cree o modifique el archivo `/etc/default/print`.**

    b. **Escriba la entrada siguiente:**

       ```
       PRINT_POSTSCRIPT=1
       ```

    c. **Guarde el archivo y cierre el editor.**

  - **Para autorizar a todos los usuarios a que impriman archivos de PostScript desde un sistema, modifique el archivo `/etc/security/policy.conf`.**

    a. **Modifique el archivo `policy.conf`.**

    b. **Agregue la autorización `solaris.print.ps`.**

       AUTHS_GRANTED=*other-authorizations*,solaris.print.ps

    c. **Guarde el archivo y cierre el editor.**

- **Para habilitar a un rol o un usuario para que impriman archivos PostScript desde cualquier sistema, proporcione la autorización adecuada solamente al rol o al usuario determinado.**

  Asigne un perfil que incluya la autorización `solaris.print.ps` para esos perfiles y roles. Para obtener detalles, consulte "Cómo crear perfiles de derechos para autorizaciones convenientes" en la página 151.

Ejemplo 19–2 Habilitación de la impresión PostScript desde un sistema público

En el siguiente ejemplo, el administrador de la seguridad restringió un quiosco público para operar en la etiqueta `PUBLIC`. El sistema también tiene algunos iconos que abren temas de interés. Estos temas se pueden imprimir.

El administrador de la seguridad crea un archivo `/etc/default/print` en el sistema. El archivo tiene una entrada para habilitar la impresión de archivos PostScript. Ningún usuario necesita una autorización `Print Postscript`.

```
# vi /etc/default/print

# PRINT_POSTSCRIPT=0
PRINT_POSTSCRIPT=1
```

◆ ◆ ◆ CAPÍTULO 20

Dispositivos en Trusted Extensions (descripción general)

En este capítulo, se describen las extensiones que Trusted Extensions proporciona para la protección de dispositivos.

Protección de los dispositivos con el software Trusted Extensions

En un sistema Oracle Solaris, los dispositivos se pueden proteger mediante la asignación y la autorización. De manera predeterminada, los dispositivos se encuentran disponibles para los usuarios comunes sin necesidad de autorización. Un sistema configurado con la función Trusted Extensions utiliza los mecanismos de protección de dispositivos del SO Oracle Solaris.

Sin embargo, de manera predeterminada, Trusted Extensions requiere que los dispositivos se asignen y que el usuario esté autorizado para usarlos. Además, los dispositivos se protegen mediante etiquetas. Trusted Extensions proporciona una interfaz gráfica de usuario (GUI, Graphical User Interface) para que los administradores puedan gestionar los dispositivos. Es la misma interfaz que utilizan los usuarios para asignar los dispositivos.

Nota – En Trusted Extensions, los usuarios no pueden utilizar los comandos `allocate` y `deallocate`. Los usuarios deben utilizar Device Manager.

Para obtener información sobre la protección de dispositivos en Oracle Solaris, consulte el Capítulo 5, "Control de acceso a dispositivos (tareas)" de *Administración de Oracle Solaris: servicios de seguridad*.

En el sistema configurado con Trusted Extensions, dos roles protegen los dispositivos.

- El rol de administrador del sistema controla el acceso a los dispositivos periféricos.

  El administrador del sistema permite que los dispositivos sean asignables. Nadie puede usar los dispositivos establecidos como no asignables por el administrador del sistema. Solamente los usuarios autorizados pueden asignar los dispositivos asignables.
- El rol de administrador de la seguridad restringe las etiquetas en las que se puede acceder a un dispositivo y establece la política de dispositivos. El administrador de la seguridad decide quién está autorizado a asignar un dispositivo.

Las siguientes son las principales funciones del control de los dispositivos con el software Trusted Extensions:

- De manera predeterminada, en el sistema Trusted Extensions, un usuario sin autorización no puede asignar dispositivos como unidades de cinta, unidades de CD-ROM o disquetes.

  Un usuario común que cuente con la autorización Allocate Device puede importar o exportar la información de la etiqueta en la que el usuario asigna el dispositivo.
- Los usuarios invocan Device Allocation Manager cuando inician sesión directamente. Para asignar un dispositivo de manera remota, los usuarios deben tener acceso a la zona global. En general, solamente los roles tienen acceso a la zona global.
- Puede que el rango de etiquetas de cada dispositivo esté restringido por el administrador de la seguridad. Los usuarios comunes están limitados a acceder a los dispositivos cuyo rango de etiquetas incluya las etiquetas en las que a los usuarios se les permite trabajar. El rango de etiquetas predeterminado de un dispositivo es de `ADMIN_LOW` a `ADMIN_HIGH`.
- Los rangos de etiquetas se pueden restringir tanto para los dispositivos que son asignables como para los que no son asignables. Entre los dispositivos que no son asignables se encuentran los búferes de trama y las impresoras.

Rangos de etiquetas de dispositivos

Para evitar que los usuarios copien información confidencial, cada dispositivo asignable tiene un rango de etiquetas. Para utilizar un dispositivo asignable, el usuario debe encontrarse operando en una etiqueta que esté dentro del rango de etiquetas del dispositivo. Si no fuera así, se deniega la asignación. La etiqueta actual del usuario se aplica a los datos que se importan o exportan mientras se asigna el dispositivo al usuario. La etiqueta de los datos exportados se muestra cuando el dispositivo se desasigna. El usuario debe colocar una etiqueta en el medio que contiene los datos exportados de manera física.

Efectos del rango de etiquetas en un dispositivo

Para restringir el acceso de inicio de sesión directo por medio de la consola, el administrador de la seguridad puede establecer un rango de etiquetas restringido en el búfer de trama.

Por ejemplo, se puede especificar un rango de etiquetas restringido a fin de limitar el acceso a un sistema de acceso público. El rango de etiquetas permite a los usuarios acceder al sistema solamente en una etiqueta que esté dentro del rango de etiquetas del búfer de trama.

Cuando un host tiene una impresora local, un rango de etiquetas restringido en la impresora limita los trabajos que se pueden imprimir con esa impresora.

Políticas de acceso a dispositivos

Trusted Extensions sigue las mismas políticas de dispositivos que Oracle Solaris. El administrador de la seguridad puede cambiar las políticas predeterminadas y definir políticas nuevas. El comando `getdevpolicy` recupera la información sobre la política de dispositivos y el comando `update_drv` cambia la política de dispositivos. Para obtener más información, consulte "Configuración de política de dispositivos (mapa de tareas)" de *Administración de Oracle Solaris: servicios de seguridad*. Consulte también las páginas del comando man `getdevpolicy`(1M) y `update_drv`(1M).

Secuencias de comandos device-clean

La secuencia de comandos device-clean se ejecuta cuando se asigna o desasigna un dispositivo. Oracle Solaris proporciona secuencias de comandos para unidades de cinta, de CD-ROM y de disquete. Si su sitio agrega tipos de dispositivos asignables al sistema, puede que los dispositivos agregados requieran secuencias de comandos. Para ver las secuencias de comandos existentes, vaya al directorio `/etc/security/lib`. Para obtener más información, consulte "Secuencias de comandos device-clean" de *Administración de Oracle Solaris: servicios de seguridad*.

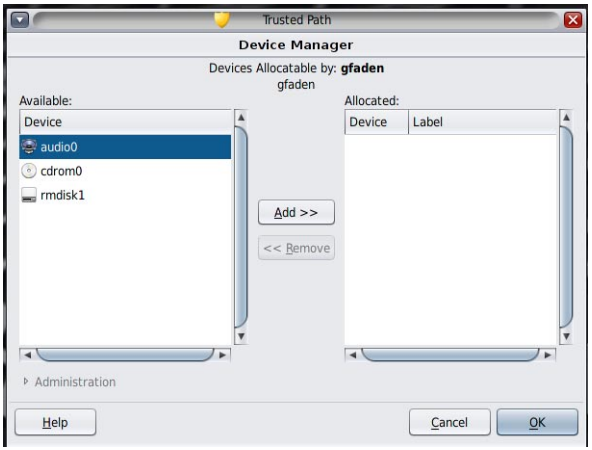
Para el software Trusted Extensions, las secuencias de comandos device-clean deben cumplir ciertos requisitos. Estos requisitos se describen en la página del comando man `device_clean`(5).

Interfaz gráfica de usuario Device Manager

Los administradores usan Device Manager para administrar dispositivos asignables y no asignables. Asimismo, los usuarios comunes utilizan Device Manager para asignar y desasignar dispositivos. Los usuarios deben tener la autorización Allocate Device.

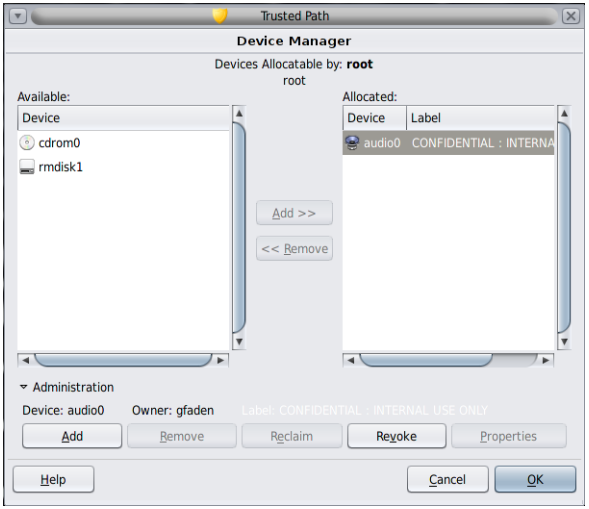
La interfaz gráfica de usuario se denomina Device Manager. Para iniciar esta interfaz gráfica de usuario, se debe seleccionar Allocate Device en el menú Trusted Path. La siguiente figura muestra un Device Manager abierto por un usuario que puede asignar el dispositivo `audio`.

FIGURA 20–1 Device Manager abierto por un usuario



Los usuarios ven una lista vacía si no están autorizados a asignar dispositivos. Igualmente, una lista vacía podría indicar que los dispositivos asignables se encuentran asignados por otro usuario o están en estado de error. Si un usuario no puede ver un dispositivo en la lista de dispositivos disponibles, debe ponerse en contacto con el administrador responsable.

La función Device Administration está disponible para los roles que tienen una o las dos autorizaciones necesarias para administrar dispositivos. Las autorizaciones de administración son Configure Device Attributes y Revoke or Reclaim Device. La siguiente figura muestra el cuadro de diálogo Device Allocation Administration.



Aplicación de la seguridad de los dispositivos en Trusted Extensions

El administrador de la seguridad decide quién puede asignar dispositivos y se asegura de que todos los usuarios autorizados para usar dispositivos reciban la formación necesaria. El usuario es de confianza para realizar lo siguiente:

- Etiquetar y manejar correctamente cualquier medio que contenga información confidencial exportada de modo que la información no esté disponible para ninguna persona que no deba verla.

  Por ejemplo, si la información que tiene la etiqueta `NEED TO KNOW ENGINEERING` se almacena en un disquete, la persona que exporta la información debe colocar en el disco una etiqueta `NEED TO KNOW ENGINEERING` de manera física. El disquete debe almacenarse en un lugar al que puedan acceder únicamente los miembros del grupo de ingeniería que deban saber acerca de la información.
- Asegurarse de que las etiquetas se mantengan de manera apropiada en cualquier información que se importe (lea) desde medios en estos dispositivos.

  Un usuario autorizado debe asignar el dispositivo en la etiqueta que coincida con la etiqueta de la información que se está importando. Por ejemplo, si un usuario asigna una unidad de disquete como `PUBLIC`, el usuario debe importar solamente la información que tenga la etiqueta `PUBLIC`.

El administrador de la seguridad también es responsable de hacer que estos requisitos de seguridad se cumplan como corresponda.

Dispositivos en Trusted Extensions (referencia)

La protección de dispositivos de Trusted Extensions utiliza las interfaces de Oracle Solaris y Trusted Extensions.

Para conocer las interfaces de la línea de comandos de Oracle Solaris, consulte "Protección de dispositivos (referencia)" de *Administración de Oracle Solaris: servicios de seguridad*.

Los administradores que no tienen acceso a Device Allocation Manager pueden administrar los dispositivos asignables mediante la línea de comandos. Los comandos `allocate` y `deallocate` tienen opciones administrativas. Para obtener ejemplos, consulte "Asignación forzada de un dispositivo" de *Administración de Oracle Solaris: servicios de seguridad* y "Desasignación forzada de un dispositivo" de *Administración de Oracle Solaris: servicios de seguridad*.

Para conocer las interfaces de la línea de comandos de Trusted Extensions, consulte las páginas del comando man `add_allocatable(1M)` y `remove_allocatable(1M)`.

◆ ◆ ◆ CAPÍTULO 21

Gestión de dispositivos para Trusted Extensions (tareas)

En este capítulo se describe cómo administrar y utilizar dispositivos en un sistema configurado con Trusted Extensions.

Control de dispositivos en Trusted Extensions (mapa de tareas)

El siguiente mapa de tareas incluye enlaces a mapas de tareas para administradores y usuarios para el control de dispositivos periféricos.

Tarea	Descripción	Para obtener instrucciones
Usar dispositivos.	Permite usar un dispositivo como rol o como usuario común.	"Uso de dispositivos en Trusted Extensions (mapa de tareas)" en la página 276
Administrar dispositivos.	Permite configurar dispositivos para los usuarios comunes.	"Gestión de dispositivos en Trusted Extensions (mapa de tareas)" en la página 276
Personalizar autorizaciones para dispositivos.	El rol de administrador de la seguridad crea autorizaciones nuevas, las agrega al dispositivo, las ubica en un perfil de derechos y, luego, asigna ese perfil al usuario.	"Personalización de autorizaciones para dispositivos en Trusted Extensions (mapa de tareas)" en la página 284

Uso de dispositivos en Trusted Extensions (mapa de tareas)

En Trusted Extensions, todos los roles están autorizados a asignar dispositivos. Al igual que los usuarios, los roles deben usar Device Manager. El comando `allocate` de Oracle Solaris no funciona en Trusted Extensions. El siguiente mapa de tareas contiene enlaces a procedimientos de usuario para el uso de dispositivos en Trusted Extensions.

Tarea	Para obtener instrucciones
Asignar y desasignar un dispositivo.	"Cómo asignar un dispositivo en Trusted Extensions" de *Guía del usuario de Oracle Solaris Trusted Extensions*
Utilizar medios portátiles para transferir archivos.	"Cómo copiar archivos desde medios portátiles en Trusted Extensions" en la página 79 "Cómo copiar archivos en medios portátiles en Trusted Extensions" en la página 78

Gestión de dispositivos en Trusted Extensions (mapa de tareas)

El siguiente mapa de tareas describe los procedimientos que se deben llevar a cabo para proteger los dispositivos en el sitio.

Tarea	Descripción	Para obtener instrucciones
Establecer o modificar la política de dispositivos.	Se modifican los privilegios necesarios para acceder a un dispositivo.	"Configuración de política de dispositivos (mapa de tareas)" de *Administración de Oracle Solaris: servicios de seguridad*
Autorizar a los usuarios a asignar un dispositivo.	El rol de administrador de la seguridad asigna un perfil de derechos al usuario con la autorización Allocate Device.	"Cómo autorizar a usuarios para que asignen un dispositivo" de *Administración de Oracle Solaris: servicios de seguridad*
	El rol de administrador de la seguridad asigna un perfil al usuario con las autorizaciones específicas del sitio.	"Personalización de autorizaciones para dispositivos en Trusted Extensions (mapa de tareas)" en la página 284
Configurar un dispositivo.	Se seleccionan funciones de seguridad para proteger el dispositivo.	"Cómo configurar un dispositivo en Trusted Extensions" en la página 277

Tarea	Descripción	Para obtener instrucciones
Revocar o reclamar un dispositivo.	Se utiliza Device Manager para hacer que un dispositivo esté disponible para su uso.	"Cómo revocar o reclamar un dispositivo en Trusted Extensions" en la página 281
	Se utilizan los comandos de Oracle Solaris para hacer que un dispositivo esté disponible o no para su uso.	"Asignación forzada de un dispositivo" de *Administración de Oracle Solaris: servicios de seguridad* "Desasignación forzada de un dispositivo" de *Administración de Oracle Solaris: servicios de seguridad*
Impedir el acceso a un dispositivo asignable.	Se proporciona control de acceso específico a un dispositivo.	Ejemplo 21–2
	Se rechaza el acceso de cualquier usuario a un dispositivo asignable.	Ejemplo 21–1
Proteger las impresoras y los búferes de trama.	Se garantiza que los dispositivos no asignables no se puedan asignar.	"Cómo proteger los dispositivos no asignables en Trusted Extensions" en la página 282
Utilizar una secuencia de comandos device-clean nueva.	Se agrega una secuencia de comandos nueva en los lugares adecuados.	"Cómo agregar una secuencia de comandos device_clean en Trusted Extensions" en la página 283

▼ Cómo configurar un dispositivo en Trusted Extensions

De manera predeterminada, los dispositivos asignables tienen un rango de etiquetas de `ADMIN_LOW` a `ADMIN_HIGH` y se deben asignar para su uso. Además, los usuarios deben estar autorizados para asignar dispositivos. Estos valores predeterminados se pueden cambiar.

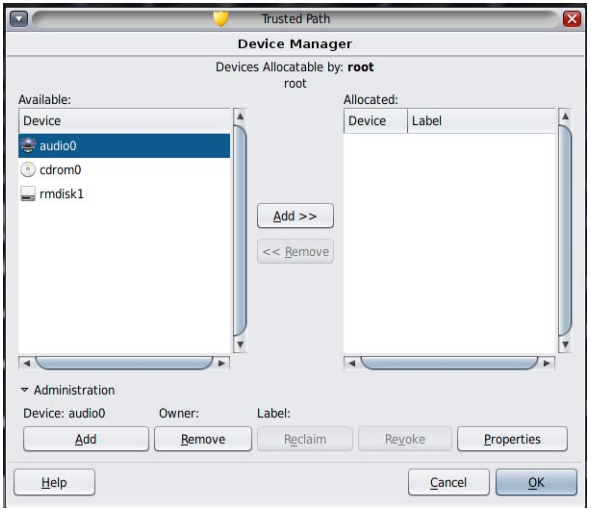
Los siguientes dispositivos se pueden asignar para su uso:

- `audio`*n*: indica un micrófono y un altavoz
- `cdrom`*n*: indica una unidad de CD-ROM
- `floppy`*n*: indica una unidad de disquete
- `mag_tape`*n*: indica una unidad de cinta (transmisión por secuencias)
- `rmdisk`*n*: indica un disco extraíble, como una unidad Jaz o Zip, o medios USB conectables

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

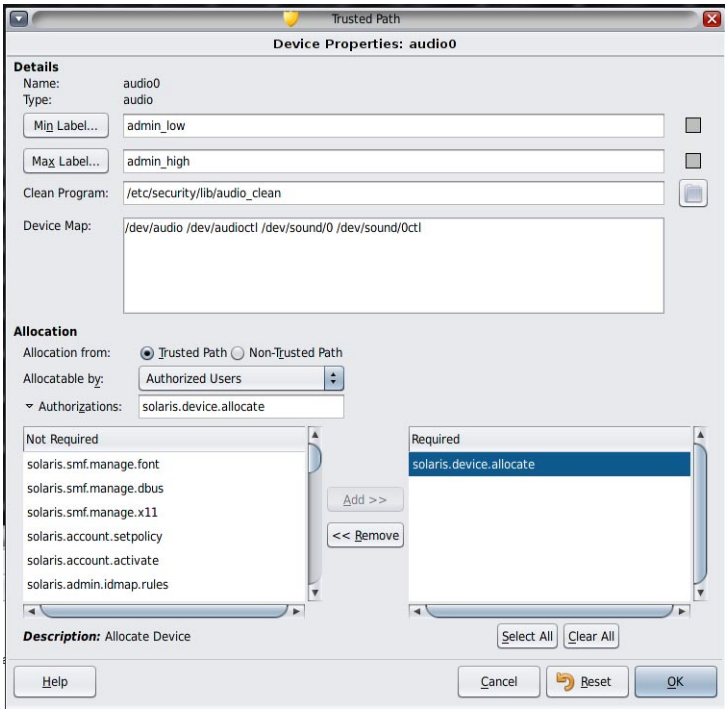
1 **En el menú Trusted Path, seleccione Allocate Device.**

Aparece Device Manager.



2 Vea las configuraciones de seguridad predeterminadas.

Haga clic en Administration y, a continuación, resalte el dispositivo. La siguiente figura muestra un dispositivo de audio que el rol de usuario `root` está visualizando.



3 (Opcional) Restrinja el rango de etiquetas en el dispositivo.

a. Establezca la etiqueta mínima.

Haga clic en el botón Min Label... y seleccione una etiqueta mínima del generador de etiquetas. Para obtener información sobre el generador de etiquetas, consulte "Generador de etiquetas en Trusted Extensions" en la página 113.

b. Establezca la etiqueta máxima.

Haga clic en el botón Max Label... y seleccione una etiqueta máxima del generador de etiquetas.

4 **Especifique si el dispositivo se puede asignar localmente.**

En el cuadro de diálogo Device Configuration, en For Allocations From Trusted Path, seleccione una opción de la lista Allocatable By. De manera predeterminada, la opción Authorized Users está activada. Por lo tanto, el dispositivo es asignable y los usuarios deben estar autorizados.

- **Para hacer que el dispositivo no sea asignable, haga clic en No Users.**

  Si configura una impresora, un búfer de trama u otro dispositivo que no deba ser asignable, seleccione No Users.

- **Para hacer que el dispositivo sea asignable, pero que no requiera autorización, haga clic en All Users.**

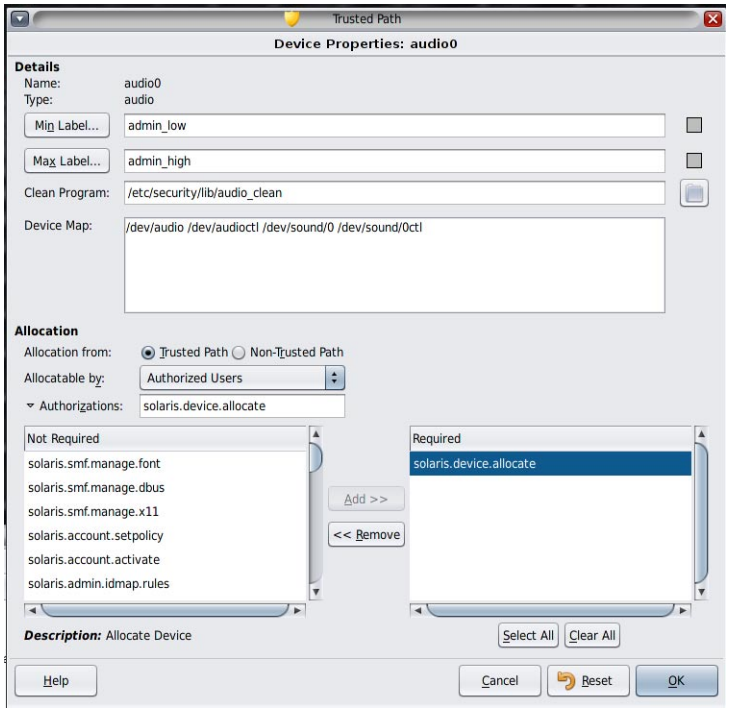
5 **Especifique si el dispositivo se puede asignar de manera remota.**

En la sección For Allocations From Non-Trusted Path, seleccione una opción de la lista Allocatable By. De manera predeterminada, la opción Same As Trusted Path está activada.

- **Para solicitar autorización del usuario, seleccione Allocatable by Authorized Users.**
- **Para hacer que los usuarios remotos no puedan asignar el dispositivo, seleccione No Users.**
- **Para hacer que cualquiera pueda asignar el dispositivo, seleccione All Users.**

6 **Si el dispositivo es asignable, *y* su sitio ha creado nuevas autorizaciones para dispositivos, seleccione la autorización adecuada.**

El cuadro de diálogo siguiente muestra que se requiere la autorización `solaris.device.allocate` para asignar el dispositivo `cdrom0`.



Para crear y utilizar autorizaciones para dispositivos específicas del sitio, consulte "Personalización de autorizaciones para dispositivos en Trusted Extensions (mapa de tareas)" en la página 284.

7 **Para guardar los cambios, haga clic en OK.**

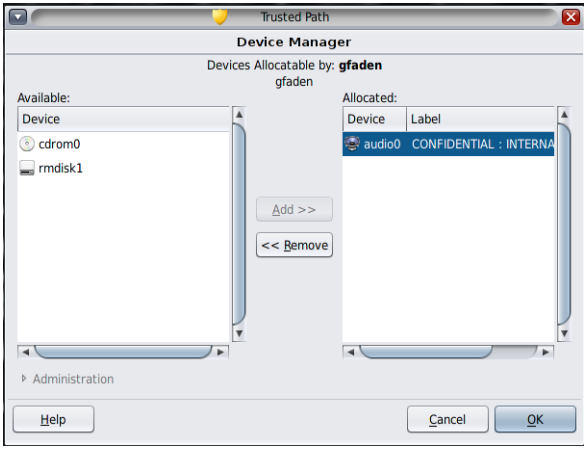
▼ Cómo revocar o reclamar un dispositivo en Trusted Extensions

Si un dispositivo no aparece en Device Manager, es posible ya esté asignado o que tenga un estado de error de asignación. El administrador del sistema puede recuperar el dispositivo para su uso.

Antes de empezar Debe estar con el rol de administrador del sistema en la zona global. Este rol cuenta con la autorización `solaris.device.revoke`.

1 **En el menú Trusted Path, seleccione Allocate Device.**

En la siguiente figura, el dispositivo de audio ya está asignado a un usuario.



2 **Haga clic en el botón Administration.**

3 **Compruebe el estado de un dispositivo.**

Seleccione el nombre del dispositivo y active el campo State.

- **Si el campo State dice Allocate Error State, haga clic en el botón Reclaim.**
- **Si el campo State dice Allocated, realice una de las siguientes acciones:**
  - **Solicite al usuario del campo Owner que desasigne el dispositivo.**
  - **Para llevar a cabo la desasignación forzosa del dispositivo, haga clic en el botón Revoke.**

4 **Cierre Device Manager.**

▼ Cómo proteger los dispositivos no asignables en Trusted Extensions

La opción No Users de la sección Allocatable By del cuadro de diálogo Device Configuration con frecuencia se utiliza para el búfer de trama y la impresora, que no requieren asignación para su uso.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1 **En el menú Trusted Path, seleccione Allocate Device.**

2. **En Device Manager, haga clic en el botón Administration.**
3. **Seleccione la impresora o el búfer de trama nuevos.**
   a. **Para hacer que el dispositivo no sea asignable, haga clic en No Users.**
   b. **(Opcional) Restrinja el rango de etiquetas en el dispositivo.**
      i. **Establezca la etiqueta mínima.**
         Haga clic en el botón Min Label... y seleccione una etiqueta mínima del generador de etiquetas. Para obtener información sobre el generador de etiquetas, consulte "Generador de etiquetas en Trusted Extensions" en la página 113.
      ii. **Establezca la etiqueta máxima.**
         Haga clic en el botón Max Label... y seleccione una etiqueta máxima del generador de etiquetas.

Ejemplo 21–1 Impedir la asignación remota del dispositivo de audio

La opción No Users de la sección Allocatable By impide que los usuarios remotos escuchen las conversaciones en un sistema remoto.

El administrador de la seguridad configura el dispositivo de audio en Device Manager de la siguiente manera:

```
Device Name: audio
For Allocations From: Trusted Path
Allocatable By: Authorized Users
Authorizations: solaris.device.allocate

Device Name: audio
For Allocations From: Non-Trusted Pathh
Allocatable By: No Users
```

▼ Cómo agregar una secuencia de comandos device_clean en Trusted Extensions

Si no se especifica ninguna secuencia de comandos `device_clean` cuando se crea un dispositivo, se usa la secuencia de comandos predeterminada `/bin/true`.

Antes de empezar Debe tener lista una secuencia de comandos que purgue todos los datos utilizables del dispositivo físico y que devuelva `0` para que el proceso se realice correctamente. Para los dispositivos con medios extraíbles, la secuencia de comandos intenta expulsar el medio si el

usuario no lo hace. La secuencia de comandos coloca el dispositivo en estado de error de asignación si el medio no se expulsa. Para obtener detalles sobre los requisitos, consulte la página del comando man `device_clean(5)`.

Debe estar con el rol de usuario `root` en la zona global.

1. **Copie la secuencia de comandos en el directorio `/etc/security/lib`.**
2. **En el cuadro de diálogo Device Properties, especifique la ruta completa de la secuencia de comandos.**
   a. **Abra Device Manager.**
   b. **Haga clic en el botón Administration.**
   c. **Seleccione el nombre del dispositivo y haga clic en el botón Configure.**
   d. **En el campo Clean Program, escriba la ruta completa para acceder a la secuencia de comandos.**
3. **Guarde los cambios.**

Personalización de autorizaciones para dispositivos en Trusted Extensions (mapa de tareas)

En el siguiente mapa de tareas, se describen los procedimientos para cambiar las autorizaciones para dispositivos en el sitio.

Tarea	Descripción	Para obtener instrucciones
Crear nuevas autorizaciones para dispositivos.	Se crean autorizaciones específicas del sitio.	"Cómo crear nuevas autorizaciones para dispositivos" en la página 285
Agregar autorizaciones a un dispositivo.	Se agregan autorizaciones específicas del sitio a dispositivos seleccionados.	"Cómo agregar autorizaciones específicas del sitio a un dispositivo en Trusted Extensions" en la página 288
Asignar autorizaciones para dispositivos a usuarios y roles.	Permite que los usuarios y los roles usen las autorizaciones nuevas.	"Cómo asignar autorizaciones para dispositivos" en la página 288

▼ Cómo crear nuevas autorizaciones para dispositivos

Si no se especifica ninguna autorización cuando se crea un dispositivo, de manera predeterminada, todos los usuarios pueden utilizar el dispositivo. Si se especifica una autorización, de manera predeterminada, solamente los usuarios autorizados pueden utilizar el dispositivo.

Para obtener información sobre cómo impedir cualquier acceso a un dispositivo asignable sin la debida autorización, consulte el Ejemplo 21–1.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1 Edite el archivo `auth_attr`.

2 Cree un encabezado para las autorizaciones nuevas.

Utilice el nombre de dominio de Internet de la organización en orden inverso seguido de componentes arbitrarios adicionales opcionales, como el nombre de la compañía. Separe los componentes con puntos. Finalice los encabezados con un punto.

domain-suffix`.`*domain-prefix*`.`*optional*`.:::`*Company* `Header::help=`*Company*`.html`

3 Agregue entradas de autorización nuevas.

Agregue las autorizaciones (una autorización por línea). Las líneas se dividen con fines de visualización. Se incluyen las autorizaciones `grant` que habilitan a los administradores para asignar las autorizaciones nuevas.

domain-suffix`.`*domain-prefix*`.grant:::Grant All` *Company* `Authorizations::help=`*Company*`Grant.html`
domain-suffix`.`*domain-prefix*`.grant.device:::Grant` *Company* `Device Authorizations::help=`*Company*`GrantDevice.html`
domain-suffix`.`*domain-prefix*`.device.allocate.tape:::Allocate Tape Device::help=`*Company*`TapeAllocate.html`
domain-suffix`.`*domain-prefix*`.device.allocate.floppy:::Allocate Floppy Device::help=`*Company*`FloppyAllocate.html`

4 Guarde el archivo y cierre el editor.

5 Si usa LDAP como servicio de nombres, actualice las entradas `auth_attr` en Oracle Directory Server Enterprise Edition (servidor de directorios).

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

6 Agregue las autorizaciones nuevas a los perfiles de derechos adecuados. Luego, asigne los perfiles a los usuarios y los roles.

7 **Utilice la autorización para restringir el acceso a unidades de cinta y de disquete.**

Agregue las autorizaciones nuevas a la lista de autorizaciones requeridas en Device Manager. Para conocer el procedimiento, consulte "Cómo agregar autorizaciones específicas del sitio a un dispositivo en Trusted Extensions" en la página 288.

Ejemplo 21–2 Creación de autorizaciones para dispositivos específicas

Un administrador de la seguridad de NewCo necesita establecer autorizaciones para dispositivos específicas para la compañía.

En primer lugar, el administrador escribe los siguientes archivos de ayuda y los coloca en el directorio `/usr/lib/help/auths/locale/C`:

```
Newco.html
NewcoGrant.html
NewcoGrantDevice.html
NewcoTapeAllocate.html
NewcoFloppyAllocate.html
```

Luego, el administrador agrega un encabezado a todas las autorizaciones para `newco.com` en el archivo `auth_attr`.

```
# auth_attr file
com.newco.:::NewCo Header::help=Newco.html
```

A continuación, el administrador agrega entradas de autorización al archivo:

```
com.newco.grant:::Grant All NewCo Authorizations::
help=NewcoGrant.html
com.newco.grant.device:::Grant NewCo Device Authorizations::
help=NewcoGrantDevice.html
com.newco.device.allocate.tape:::Allocate Tape Device::
help=NewcoTapeAllocate.html
com.newco.device.allocate.floppy:::Allocate Floppy Device::
help=NewcoFloppyAllocate.html
```

Las líneas se dividen con fines de visualización.

Las entradas `auth_attr` crean las siguientes autorizaciones:

- Una autorización para conceder todas las autorizaciones de NewCo
- Una autorización para conceder las autorizaciones para dispositivos de NewCo
- Una autorización para asignar una unidad de cinta
- Una autorización para asignar una unidad de disquete

Ejemplo 21–3 Creación de autorizaciones Trusted Path y Non-Trusted Path

De manera predeterminada, la autorización Allocate Devices habilita la asignación desde adentro y desde afuera de Trusted Path.

En el siguiente ejemplo, la política de seguridad del sitio requiere la restricción de la asignación de CD-ROM remota. El administrador de la seguridad crea la autorización `com.someco.device.cdrom.local`. Esta autorización corresponde a las unidades de CD-ROM que se asignan con Trusted Path. La autorización `com.someco.device.cdrom.remote` corresponde a los pocos usuarios que tienen permiso para asignar una unidad de CD-ROM fuera de Trusted Path.

El administrador de la seguridad crea los archivos de ayuda, agrega las autorizaciones a la base de datos `auth_attr`, agrega las autorizaciones para los dispositivos y, luego, aplica las autorizaciones en los perfiles de derechos. Los perfiles se asignan a los usuarios que tienen permiso para asignar dispositivos.

- A continuación, se muestran las entradas de base de datos `auth_attr`:

```
com.someco.:::SomeCo Header::help=Someco.html
com.someco.grant:::Grant All SomeCo Authorizations::
help=SomecoGrant.html
com.someco.grant.device:::Grant SomeCo Device Authorizations::
help=SomecoGrantDevice.html
com.someco.device.cdrom.local:::Allocate Local CD-ROM Device::
help=SomecoCDAllocateLocal.html
com.someco.device.cdrom.remote:::Allocate Remote CD-ROM Device::
help=SomecoCDAllocateRemote.html
```

- A continuación, se muestra la asignación de Device Manager:

  Trusted Path permite que los usuarios autorizados utilicen Device Manager al asignar la unidad de CD-ROM local.

```
Device Name: cdrom_0
For Allocations From: Trusted Path
Allocatable By: Authorized Users
Authorizations: com.someco.device.cdrom.local
```

  Non-Trusted Path permite que los usuarios asignen un dispositivo de manera remota mediante el comando `allocate`.

```
Device Name: cdrom_0
For Allocations From: Non-Trusted Path
Allocatable By: Authorized Users
Authorizations: com.someco.device.cdrom.remote
```

- A continuación, se muestran las entradas de derechos de perfiles:

```
# Local Allocator profile
com.someco.device.cdrom.local

# Remote Allocator profile
com.someco.device.cdrom.remote
```

- A continuación, se muestran los perfiles de derechos de los usuarios autorizados:

```
# List of profiles for regular authorized user
Local Allocator Profile
...

# List of profiles for role or authorized user
```

```
Remote Allocator Profile
...
```

▼ Cómo agregar autorizaciones específicas del sitio a un dispositivo en Trusted Extensions

Antes de empezar Debe estar con el rol de administrador de la seguridad o con un rol que incluya la autorización Configure Device Attributes. Ya debe haber creado las autorizaciones específicas del sitio, como se describe en "Cómo crear nuevas autorizaciones para dispositivos" en la página 285.

1. **Siga el procedimiento de "Cómo configurar un dispositivo en Trusted Extensions" en la página 277.**

   a. **Seleccione un dispositivo que deba protegerse con las autorizaciones nuevas.**

   b. **Haga clic en el botón Administration.**

   c. **Haga clic en el botón Authorizations.**

      Las autorizaciones nuevas se muestran en la lista Not Required.

   d. **Agregue las autorizaciones nuevas a la lista de autorizaciones Required.**

2. **Para guardar los cambios, haga clic en OK.**

▼ Cómo asignar autorizaciones para dispositivos

La autorización Allocate Device habilita a los usuarios para que asignen un dispositivo. Las autorizaciones Allocate Device y Revoke or Reclaim Device son adecuadas para los roles administrativos.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

Si los perfiles existentes no son adecuados, el administrador de la seguridad puede crear un perfil nuevo. Para ver un ejemplo, consulte "Cómo crear perfiles de derechos para autorizaciones convenientes" en la página 151.

- **Asigne al usuario un perfil de derechos que cuente con la autorización Allocate Device.**

  Para conocer el procedimiento paso a paso, consulte "Cómo cambiar las propiedades RBAC de un usuario" de *Administración de Oracle Solaris: servicios de seguridad*.

Los siguientes perfiles de derechos habilitan un rol para que asigne dispositivos:

- All Authorizations
- Device Management
- Media Backup
- Media Restore
- Object Label Management
- Software Installation

Los siguientes perfiles de derechos habilitan un rol para que revoque o reclame dispositivos:

- All Authorizations
- Device Management

Los siguientes perfiles de derechos habilitan un rol para que cree o configure dispositivos:

- All Authorizations
- Device Security

Ejemplo 21–4 Asignación de nuevas autorizaciones para dispositivos

En este ejemplo, el administrador de la seguridad configura las nuevas autorizaciones para dispositivos del sistema y asigna el perfil de derechos con las autorizaciones nuevas a usuarios de confianza. El administrador de la seguridad realiza lo siguiente:

1. Crea nuevas autorizaciones para dispositivos, como se indica en "Cómo crear nuevas autorizaciones para dispositivos" en la página 285.
2. En Device Manager, agrega las nuevas autorizaciones para dispositivos a las unidades de cinta y de disquete.
3. Coloca las autorizaciones nuevas en el perfil de derechos NewCo Allocation.
4. Agrega el perfil de derechos NewCo Allocation a los perfiles de usuarios y roles que están autorizados a asignar unidades de cinta y de disquete.

Así, los usuarios y los roles autorizados pueden usar las unidades de cinta y de disquete del sistema.

◆ ◆ ◆ CAPÍTULO 22

Auditoría de Trusted Extensions (descripción general)

En este capítulo, se describen las adiciones a la auditoría que Trusted Extensions proporciona.

Trusted Extensions y la auditoría

En un sistema configurado con el software Trusted Extensions, la configuración y la administración de la auditoría son similares a las de la auditoría en un sistema Oracle Solaris. Sin embargo, existen algunas diferencias:

- El software Trusted Extensions agrega al sistema clases, eventos y tokens de auditoría, y opciones de política de auditoría.
- No se recomienda usar la auditoría por zona, porque requiere una cuenta de usuario `root` en las zonas con etiquetas.
- Se utilizan dos roles, el administrador del sistema y el administrador de la seguridad, para configurar y administrar la auditoría en Trusted Extensions.

  El administrador de la seguridad planifica qué se debe auditar y establece asignaciones evento-clase específicas del sitio. El administrador del sistema planifica los requisitos de espacio en el disco para los archivos de auditoría, crea un servidor de administración de auditoría y revisa los registros de auditoría.

Gestión de auditoría por roles en Trusted Extensions

La auditoría en Trusted Extensions requiere la misma planificación que en el SO Oracle Solaris. Para obtener detalles sobre la planificación, consulte el Capítulo 27, "Planificación de la auditoría" de *Administración de Oracle Solaris: servicios de seguridad*.

Responsabilidades de los roles para la administración de auditoría

En Trusted Extensions, existen diferentes roles que son responsables de la auditoría.

- El rol de usuario `root` asigna indicadores de auditoría a los usuarios y perfiles de derechos, y edita los archivos del sistema, como la secuencia de comandos `audit_warn`.
- El rol de administrador del sistema configura los discos y la red de almacenamiento de auditoría. Este rol también puede revisar los registros de auditoría.
- El rol de administrador de la seguridad decide qué se auditará y configura la auditoría. El equipo de configuración inicial creó este rol siguiendo las instrucciones detalladas en "Cómo crear el rol de administrador de la seguridad en Trusted Extensions" en la página 68.

Nota – Un sistema sólo registra los eventos de las clases de auditoría que el administrador de la seguridad ha seleccionado previamente. Por lo tanto, en cualquier revisión de auditoría que se realice luego, solamente se pueden incluir los eventos que se hayan registrado. A causa de un error de configuración, puede que no se detecten los intentos de infracción de la seguridad del sistema o que el administrador no logre detectar al usuario que intentó infringir la seguridad. Los administradores deben analizar las pistas de auditoría con regularidad para verificar que no haya infracciones de la seguridad.

Tareas de auditoría en Trusted Extensions

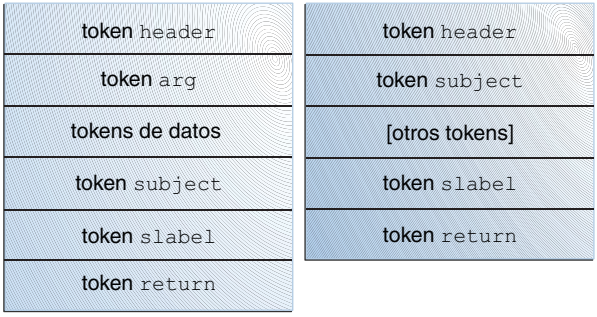
Los procedimientos para configurar y gestionar la auditoría en Trusted Extensions sólo difieren levemente de los procedimientos de Oracle Solaris. En Trusted Extensions, la configuración de la auditoría se realiza en la zona global. Dado que no se configura la auditoría por zona, las acciones del usuario se auditan de la misma manera en la zona global y en las zonas con etiquetas. La etiqueta de cada evento auditado se incluye en el registro de auditoría.

- El administrador de la seguridad puede seleccionar políticas de auditoría que son específicas de Trusted Extensions, `windata_down` y `windata_up`.
- Al revisar los registros de auditoría, el administrador del sistema puede seleccionar los registros de auditoría por etiqueta. Para obtener más información, consulte la página del comando man `auditreduce(1M)`.

Referencia de auditoría de Trusted Extensions

El software Trusted Extensions agrega a Oracle Solaris clases, eventos y tokens de auditoría, y opciones de política de auditoría. Varios comandos de auditoría se amplían para manejar etiquetas. La siguiente figura muestra un registro de auditoría de núcleo y un registro de auditoría de nivel de usuario típicos de Trusted Extensions.

FIGURA 22–1 Estructuras típicas de registros de auditoría en un sistema con etiquetas



Clases de auditoría de Trusted Extensions

Trusted Extensions agrega clases de auditoría de ventanas X a Oracle Solaris. Las clases se enumeran en el archivo `/etc/security/audit_class`. Para obtener más información sobre las clases de auditoría, consulte la página del comando man `audit_class(4)`.

Los eventos de auditoría del servidor X se asignan a estas clases según los criterios siguientes:

- **xa**: esta clase audita el acceso al servidor X, es decir, la conexión de clientes X y la desconexión de clientes X.
- **xc**: esta clase audita objetos de servidor de creación o destrucción. Por ejemplo, esta clase audita `CreateWindow()`.
- **xp**: esta clase audita el uso de privilegios. El uso de privilegios puede ser correcto o incorrecto. Por ejemplo, `ChangeWindowAttributes()` se audita cuando un cliente intenta cambiar los atributos de una ventana de otro cliente. Esta clase también incluye rutinas administrativas, como `SetAccessControl()`.
- **xs**: esta clase audita las rutinas que no devuelven mensajes de error X a los clientes en caso de errores causados por los atributos de seguridad. Por ejemplo, `GetImage()` no devuelve un error de `BadWindow` si no puede leer desde una ventana por falta de privilegios.

  Estos eventos se deben seleccionar para auditarlos únicamente cuando sean correctos. Si los eventos xs se seleccionan cuando son incorrectos, la pista de auditoría se llena de registros irrelevantes.
- **xx**: esta clase incluye todas las clases de auditoría X.

Eventos de auditoría de Trusted Extensions

El software Trusted Extensions agrega eventos de auditoría al sistema. Los eventos de auditoría nuevos y las clases de auditoría a las que los eventos pertenecen se enumeran en el archivo `/etc/security/audit_event`. Los números del evento de auditoría de Trusted Extensions se encuentran entre 9.000 y 10.000. Para obtener más información sobre los eventos de auditoría, consulte la página del comando man `audit_event(4)`.

Tokens de auditoría de Trusted Extensions

En la siguiente tabla, se enumeran en orden alfabético los tokens de auditoría que el software Trusted Extensions agrega a Oracle Solaris. Las definiciones de tokens se enumeran en la página del comando man `audit.log(4)`.

TABLA 22–1 Tokens de auditoría de Trusted Extensions

Nombre de token	Descripción
"Token `label`" en la página 294	Etiqueta de sensibilidad
"Token `xatom`" en la página 295	Identificación de los átomos de las ventanas X
"Token `xcolormap`" en la página 295	Información sobre el color de las ventanas X
"Token `xcursor`" en la página 295	Información sobre los cursores de las ventanas X
"Token `xfont`" en la página 295	Información sobre las fuentes de las ventanas X
"Token `xgc`" en la página 295	Información sobre el contexto gráfico de las ventanas X
"Token `xpixmap`" en la página 295	Información sobre los mapas de píxeles de las ventanas X
"Token `xproperty`" en la página 296	Información sobre las propiedades de las ventanas X
"Token `xselect`" en la página 296	Información sobre los datos de las ventanas X
"Token `xwindow`" en la página 296	Información sobre las ventanas X

Token label

El token `label` contiene una etiqueta de sensibilidad.

Con el comando `praudit -x`, el token `label` se muestra de la siguiente manera:

```
<sensitivity_label>ADMIN_LOW</sensitivity_label>
```

Token xatom

El token `xatom` identifica un átomo X.

Con `praudit`, el token `xatom` se muestra de la siguiente manera:

```
X atom,_DT_SAVE_MODE
```

Token xcolormap

El token `xcolormap` contiene información sobre el uso de mapas de colores, incluidos el identificador del servidor X y el ID de usuario del creador.

Con `praudit`, el token `xcolormap` se muestra de la siguiente manera:

```
<X_colormap xid="0x08c00005" xcreator-uid="srv"/>
```

Token xcursor

El token `xcursor` contiene información sobre el uso de cursores, incluidos el identificador del servidor X y el ID de usuario del creador.

Con `praudit`, el token `xcursor` se muestra de la siguiente manera:

```
X cursor,0x0f400006,srv
```

Token xfont

El token `xfont` contiene información sobre el uso de fuentes, incluidos el identificador del servidor X y el ID de usuario del creador.

Con `praudit`, el token `xfont` se muestra de la siguiente manera:

```
<X_font xid="0x08c00001" xcreator-uid="srv"/>
```

Token xgc

El token `xgc` contiene información sobre el contexto gráfico de una ventana X.

Con `praudit`, el token `xgc` se muestra de la siguiente manera:

```
Xgraphic context,0x002f2ca0,srv

<X_graphic_context xid="0x30002804" xcreator-uid="srv"/>
```

Token xpixmap

El token `xpixmap` contiene información sobre el uso de mapas de píxeles, incluidos el identificador del servidor X y el ID de usuario del creador.

Con `praudit -x`, el token `xpixmap` se muestra de la siguiente manera:

```
<X_pixmap xid="0x2f002004" xcreator-uid="srv"/>
```

Token xproperty

El token `xproperty` contiene información sobre varias propiedades de una ventana, como el identificador del servidor X, el ID de usuario del creador y un identificador de átomo.

Con `praudit`, el token `xproperty` se muestra de la siguiente manera:

```
X_property,0x000075d5,root,_MOTIF_DEFAULT_BINDINGS
```

Token xselect

El token `xselect` contiene los datos que se mueven entre las ventanas. Estos datos son una secuencia de bytes sin una estructura interna asumida ni una cadena de propiedades.

Con `praudit`, el token `xselect` se muestra de la siguiente manera:

```
X selection,entryfield,halogen
```

Token xwindow

El token `xwindow` identifica el servidor X y el ID de usuario del creador.

Con `praudit`, el token `xwindow` se muestra de la siguiente manera:

```
<X_window xid="0x07400001" xcreator-uid="srv"/>
```

Opciones de política de auditoría de Trusted Extensions

Trusted Extensions agrega dos opciones de políticas de auditoría de ventanas a las opciones de políticas de auditoría existentes.

```
$ auditconfig -lspolicy
...
windata_down Include downgraded window information in audit records
windata_up   Include upgraded window information in audit records
...
```

Extensiones realizadas en comandos de auditoría de Trusted Extensions

Los comandos `auditconfig`, `auditreduce` y `auditrecord` se extendieron a fin de manejar la información de Trusted Extensions:

- El comando `auditconfig` incluye las políticas de auditoría de Trusted Extensions. Para obtener detalles, consulte la página del comando man `auditconfig(1M)`.
- El comando `auditreduce` proporciona la opción `-l` para filtrar registros por etiqueta. Para obtener detalles, consulte la página del comando man `auditreduce(1M)`.
- El comando `auditrecord` incluye los eventos de auditoría de Trusted Extensions.

◆ ◆ ◆ CAPÍTULO 23

Gestión de software en Trusted Extensions (referencia)

Este capítulo contiene información sobre cómo garantizar que el software de terceros se ejecute de manera confiable en un sistema que está configurado con Trusted Extensions.

Adición de software a Trusted Extensions

Los programas de software que pueden agregarse a un sistema Oracle Solaris también pueden agregarse a un sistema que está configurado con Trusted Extensions. Además, es posible agregar los programas que utilizan las API de Trusted Extensions. La adición de software en un sistema Trusted Extensions es similar a la adición de software en un sistema Oracle Solaris que ejecuta zonas no globales.

En Trusted Extensions, los programas suelen instalarse en la zona global para que puedan utilizarlos los usuarios comunes en las zonas con etiquetas. Para obtener detalles sobre los paquetes y las zonas, consulte el Capítulo 24, "Acerca de la instalación automática y los paquetes de un sistema Oracle Solaris 11 con zonas instaladas" de *Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*.

En un sitio de Trusted Extensions, el administrador del sistema trabaja junto con el administrador de la seguridad para instalar el software. El administrador de la seguridad evalúa si las adiciones de software cumplen la política de seguridad. Cuando el software requiere que los privilegios o las autorizaciones se efectúen correctamente, el rol de administrador de la seguridad asigna un perfil de derechos adecuado a los usuarios del software.

La importación de software desde medios extraíbles requiere autorización. Una cuenta con la autorización Allocate Device puede importar o exportar datos desde medios extraíbles. Los datos pueden incluir código ejecutable. Un usuario común sólo puede importar datos en una etiqueta dentro de la acreditación del usuario.

El rol de administrador del sistema es responsable de agregar los programas que apruebe el administrador de la seguridad.

Mecanismos de seguridad para el software Oracle Solaris

Trusted Extensions utiliza los mismos mecanismos de seguridad que Oracle Solaris. Entre los mecanismos, se incluyen los siguientes:

- **Autorizaciones**: es posible que a los usuarios de un programa se les requiera una autorización específica. Para obtener información sobre las autorizaciones, consulte "Elementos y conceptos básicos de RBAC" de *Administración de Oracle Solaris: servicios de seguridad*. Asimismo, consulte la página del comando man `auth_attr(4)`.
- **Privilegios**: se pueden asignar privilegios a los programas y a los procesos. Para obtener información sobre los privilegios, consulte el Capítulo 8, "Uso de roles y privilegios (descripción general)" de *Administración de Oracle Solaris: servicios de seguridad*. También, consulte la página del comando man `privileges(5)`.

  El comando `ppriv` proporciona una utilidad de depuración. Para obtener detalles, consulte la página del comando man `ppriv(1)`. Para obtener instrucciones sobre el uso de esta utilidad con programas que funcionan en zonas no globales, consulte "Uso de la utilidad ppriv" de *Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*.
- **Perfiles de derechos**: los perfiles de derechos recopilan los atributos de seguridad en un solo lugar para asignarlos a los usuarios o a los roles. Para obtener información sobre los perfiles de derechos, consulte "Perfiles de derechos de RBAC" de *Administración de Oracle Solaris: servicios de seguridad*.
- **Bibliotecas de confianza**: las bibliotecas compartidas de manera dinámica que utilizan `setuid` y `setgid`, y los programas con privilegios pueden cargarse únicamente desde directorios de confianza. Como en Oracle Solaris, se utiliza el comando `crle` para agregar directorios de bibliotecas compartidas de un programa con privilegios a la lista de directorios de confianza. Para obtener detalles, consulte la página del comando man `crle(1)`.

Evaluación de software para la seguridad

Cuando se le asignan privilegios al software o cuando se lo ejecuta con un ID de grupo o de usuario alternativo, se convierte en un software *de confianza*. El software de confianza puede omitir aspectos de la política de seguridad de Trusted Extensions. Tenga en cuenta que puede convertir el software en confiable aunque podría no ser de confianza. El administrador de la seguridad debe esperar para otorgar privilegios al software hasta que se efectúe un examen minucioso que demuestre que el software utiliza los privilegios de manera confiable.

En un sistema de confianza, los programas se dividen en tres categorías:

- **Programas que no requieren atributos de seguridad**: algunos programas se ejecutan en un solo nivel y no requieren privilegios. Estos programas pueden instalarse en un directorio público, como `/usr/local`. Para obtener acceso, asigne el programa como comandos en los perfiles de derechos de los usuarios y de los roles.
- **Programas que se ejecutan como root**: algunos programas se ejecutan con `setuid 0`. Se puede asignar a estos programas un UID efectivo de `0` en un perfil de derechos. Luego, el administrador de la seguridad asigna el perfil a un rol administrativo.

  Consejo – Si la aplicación puede utilizar los privilegios de manera confiable, asigne los privilegios necesarios a la aplicación y no ejecute el programa como `root`.

- **Programas que requieren privilegios**: es posible que algunos programas requieran privilegios por motivos que no resultan evidentes. Incluso cuando un programa no ejerza ninguna función que pudiera infringir la política de seguridad del sistema, dicho programa podría realizar internamente una acción que infringe la seguridad. Por ejemplo, es posible que el programa utilice un archivo de registro compartido o que lea desde `/dev/kmem`. Para obtener información relativa a la seguridad, consulte la página del comando man `mem(7D)`.

  En algunas ocasiones, una invalidación de la política interna no es particularmente importante para el funcionamiento adecuado de la aplicación. En cambio, la invalidación proporciona una función conveniente para los usuarios.

  Si la organización tiene acceso al código de origen, compruebe si pueden eliminar las operaciones que requieran invalidaciones de la política, sin que se afecte el rendimiento de la aplicación.

Responsabilidades del desarrollador cuando se crean programas de confianza

Aunque el desarrollador de programas puede manipular los conjuntos de privilegios en el código de origen, si el administrador de la seguridad no asigna los privilegios necesarios al programa, el programa fallará. El desarrollador y el administrador de la seguridad deben cooperar cuando se crean programas de confianza.

El desarrollador que escribe un programa de confianza debe realizar lo siguiente:

1. Comprender cuándo el programa requiere privilegios para realizar su trabajo.
2. Conocer y aplicar las técnicas, como el escalonamiento de privilegios, para utilizar de un modo seguro los privilegios en los programas.
3. Tener en cuenta las consecuencias para la seguridad cuando asigna privilegios a un programa. El programa no debe infringir la política de seguridad.
4. Compilar el programa mediante las bibliotecas compartidas que están enlazadas al programa desde un directorio de confianza.

Para obtener información adicional, consulte la *Developer's Guide to Oracle Solaris 11 Security*. Para ver ejemplos de códigos para Trusted Extensions, consulte la *Trusted Extensions Developer's Guide* .

Responsabilidades del administrador de la seguridad para los programas de confianza

El administrador de la seguridad es el responsable de probar y evaluar el software nuevo. Después de establecer que el software es de confianza, el administrador de la seguridad configura los perfiles de derechos y otros atributos relevantes para la seguridad del programa.

Entre las responsabilidades del administrador de la seguridad, se incluyen las siguientes:

1. Asegurarse de que el programador y el proceso de distribución del programa sean de confianza.
2. A partir de una de las siguientes fuentes, determinar qué privilegios requiere el programa:
   - Preguntar al programador.
   - Buscar en el código de origen los privilegios que el programa prevé utilizar.
   - Buscar en el código de origen las autorizaciones que el programa requiere de los usuarios.
   - Usar las opciones de depuración para el comando `ppriv` a fin de buscar la utilización del privilegio. Para ver ejemplos, consulte la página del comando man `ppriv(1)`.
3. Examinar el código de origen para asegurarse de que se comporte de manera confiable con relación a los privilegios que el programa necesita para operar.

   Si el programa no puede utilizar los privilegios de manera confiable, y usted puede modificar el código de origen del programa, modifique el código. Un consultor de seguridad o un desarrollador que tenga conocimientos sobre la seguridad puede modificar el código. Las modificaciones pueden incluir la separación de privilegios o la comprobación de autorizaciones.

   La asignación de privilegios debe realizarse manualmente. Se pueden asignar privilegios a un programa que falla debido a la falta de privilegios. Como alternativa, el administrador de la seguridad puede decidir asignar un UID o un GID efectivo para que el privilegio resulte innecesario.

◆ ◆ ◆ APÉNDICE A

Política de seguridad del sitio

En este apéndice se explican los problemas de la política de seguridad del sitio, y se sugieren sitios web y manuales de referencia para obtener más información:

Creación y gestión de una política de seguridad

Cada sitio de Trusted Extensions es único y debe determinar su propia política de seguridad. Realice las siguientes tareas al crear y gestionar una política de seguridad.

- Establezca un equipo de seguridad. El equipo de seguridad debe tener representación de la gerencia superior, la gerencia de personal, los administradores y la gerencia de sistemas informáticos, y la gerencia de utilidades. El equipo debe revisar las políticas y los procedimientos de los administradores de Trusted Extensions y recomendar las políticas de seguridad generales que se aplican a todos los usuarios del sistema.
- Informe al personal de gestión y administración sobre la política de seguridad del sitio. Todo el personal que participa en la gestión y administración del sitio debe estar familiarizado con la política de seguridad. Las políticas de seguridad no se deben poner a disposición de los usuarios comunes porque esta información de la política está directamente relacionada con la seguridad de los sistemas informáticos.
- Informe a los usuarios sobre la política de seguridad y el software Trusted Extensions. Todos los usuarios deben estar familiarizados con la *Guía del usuario de Oracle Solaris Trusted Extensions*. Debido a que los usuarios, generalmente, son los primeros en saber cuándo un sistema no está funcionando normalmente, el usuario debe familiarizarse con el sistema e

informar sobre los problemas a un administrador del sistema. Un entorno seguro requiere que los usuarios notifiquen a los administradores del sistema inmediatamente si notan alguna de las siguientes irregularidades:

- Una discrepancia en la fecha y hora del último inicio de sesión que se informa al principio de cada sesión
- Un cambio poco común en los datos de un archivo
- Una copia impresa legible perdida o robada
- La incapacidad de utilizar una función de usuario

- Aplique la política de seguridad. Si la política de seguridad no se respeta y no se aplica, los datos incluidos en el sistema en el que está configurado Trusted Extensions no estarán protegidos. Es preciso establecer procedimientos para registrar cualquier problema y las medidas que se han tomado para resolver los incidentes.
- Revise periódicamente la política de seguridad. El equipo de seguridad debe llevar a cabo una revisión periódica de la política de seguridad y de todos los incidentes que se produjeron desde la última revisión. Los ajustes en esta política pueden ayudar a aumentar la seguridad.

Política de seguridad del sitio y Trusted Extensions

El administrador de la seguridad debe diseñar la red de Trusted Extensions en función de la política de seguridad del sitio. La política de seguridad dicta las decisiones relacionadas con la configuración, como las siguientes:

- Cuántas auditorías se realizan para todos los usuarios y para qué clases de eventos
- Cuántas auditorías se realizan para los usuarios con roles y para qué clases de eventos
- Cómo se gestionan, archivan y revisan los datos de la auditoría
- Qué etiquetas se utilizan en el sistema y si las etiquetas `ADMIN_LOW` y `ADMIN_HIGH` estarán visibles para los usuarios comunes
- Qué acreditaciones de usuario se asignan a las personas
- Qué dispositivos (si los hay) se pueden asignar por qué usuarios comunes
- Qué rangos de etiqueta se definen para los sistemas, las impresoras y otros dispositivos
- Si Trusted Extensions se utiliza en una configuración evaluada o no

Recomendaciones de seguridad informática

Considere la siguiente lista de directrices cuando desarrolle una política de seguridad para el sitio.

- Asigne la etiqueta máxima de un sistema con Trusted Extensions para que no sea mayor que el nivel de máxima seguridad del trabajo que se está realizando en el sitio.
- Registre de forma manual los cierres, los fallos de energía y los reinicios del sistema en un registro del sitio.
- Documente el daño en el sistema de archivos y analice todos los archivos afectados para verificar posibles infracciones de la política de seguridad.
- Restrinja los manuales de funcionamiento y la documentación del administrador a aquellas personas que realmente tengan la necesidad de acceder a dicha información.
- Informe y documente el comportamiento inusual o inesperado de cualquier software Trusted Extensions y determine la causa.
- Si es posible, asigne, al menos, dos personas para administrar los sistemas en los que esté configurado Trusted Extensions. Asigne a una persona la autorización de administrador de la seguridad para tomar las decisiones relacionadas con la seguridad. Asigne a la otra persona la autorización de administrador del sistema para realizar las tareas de gestión del sistema.
- Establezca una rutina de copia de seguridad regular.
- Asigne autorizaciones sólo a los usuarios que las necesiten y que sepa que las usarán adecuadamente.
- Asígneles privilegios sólo para los programas que necesitan para realizar su trabajo, y sólo una vez que se hayan examinado los programas y se haya comprobado que se les puede confiar el uso del privilegio. Revise los privilegios en los programas de Trusted Extensions existentes como guía para el establecimiento de privilegios en programas nuevos.
- Revise y analice la información de auditoría con regularidad. Investigue los eventos irregulares para determinar la causa del evento.
- Minimice el número de identificadores de administración.
- Minimice el número de programas de setuid y setgid. Utilice autorizaciones, privilegios y roles para ejecutar el programa y para evitar el uso indebido.
- Asegúrese de que un administrador verifique con regularidad que los usuarios comunes tengan un shell de inicio de sesión válido.
- Asegúrese de que un administrador verifique con regularidad que los usuarios comunes tengan valores de ID de usuario válidos en lugar de valores de ID de administración del sistema.

Recomendaciones de seguridad física

Considere la siguiente lista de directrices cuando desarrolle una política de seguridad para el sitio.

- Restrinja el acceso a los sistemas en los que está configurado Trusted Extensions. Las ubicaciones más seguras generalmente son cuartos interiores que no se encuentran en la planta baja.
- Supervise y documente el acceso a los sistemas en los que esté configurado Trusted Extensions.
- Sujete el equipo informático a objetos grandes como mesas y escritorios para impedir robos. Cuando fije un equipo a un objeto de madera, aumente la solidez del objeto agregando placas de metal.
- Evalúe la posibilidad de utilizar medios de almacenamiento extraíbles para la información confidencial. Bloquee todos los medios extraíbles cuando no se estén utilizando.
- Almacene los archivos y las copias de seguridad del sistema en una ubicación segura separada de la ubicación de los sistemas.
- Restrinja el acceso físico a los medios de archivo y las copias de seguridad en la misma forma en que restringe el acceso a los sistemas.
- Instale una alarma de alta temperatura en la instalación informática para indicar si la temperatura está fuera del rango de las especificaciones del fabricante. Un rango sugerido es de 10 °C a 32 °C (50 °F a 90 °F).
- Instale una alarma de agua en la instalación informática para que indique si hay agua en el piso, en la cavidad del subsuelo y en el techo.
- Instale una alarma de humo para indicar la presencia de fuego y un sistema de extinción de fuego.
- Instale una alarma de humedad para indicar si hay mucha o poca humedad.
- Si las máquinas no lo tienen, tenga en cuenta el aislamiento TEMPEST. El aislamiento TEMPEST puede ser adecuado para las paredes, el suelo y el techo de la instalación.
- Permita que sólo técnicos certificados abran y cierren el equipo TEMPEST para garantizar su capacidad para aislar la radiación electromagnética.
- Controle la existencia de huecos físicos que permitan la entrada a las instalaciones o a las salas que contienen equipo informático. Busque aberturas debajo de pisos elevados, en techos falsos, en el equipo de ventilación del techo y en paredes linderas entre las adiciones originales y secundarias.
- Prohíba comer, beber y fumar en las instalaciones informáticas o cerca del equipo informático. Establezca las áreas donde estas actividades se pueden realizar sin poner en peligro el equipo informático.
- Proteja los dibujos y diagramas arquitectónicos de la instalación informática.

- Restrinja el uso de diagramas del edificio, mapas de piso y fotografías de la instalación informática.

Recomendaciones de seguridad del personal

Considere la siguiente lista de directrices cuando desarrolle una política de seguridad para el sitio.

- Inspeccione los paquetes, los documentos y los medios de almacenamiento cuando lleguen al sitio protegido y antes de que lo abandonen.
- Exija que todo el personal y los visitantes utilicen credenciales de identificación en todo momento.
- Utilice credenciales de identificación que sean difíciles de copiar o falsificar.
- Establezca qué áreas están prohibidas para los visitantes y márquelas claramente.
- Acompañe a los visitantes en todo momento.

Infracciones de seguridad comunes

Dado que ningún equipo es completamente seguro, una instalación informática es tan segura como las personas que la utilizan. La mayoría de las acciones que infringen la seguridad se pueden resolver fácilmente con usuarios cuidadosos o equipos adicionales. Sin embargo, la siguiente lista proporciona ejemplos de los problemas que pueden producirse:

- Los usuarios proporcionan contraseñas a otras personas que no deberían tener acceso al sistema.
- Los usuarios anotan las contraseñas y, luego, las pierden o las dejan en ubicaciones inseguras.
- Los usuarios definen sus contraseñas con palabras o nombres que se pueden adivinar fácilmente.
- Los usuarios aprenden las contraseñas observando a otros usuarios escribir sus contraseñas.
- Los usuarios no autorizados extraen o sustituyen el hardware, o lo sabotean físicamente.
- Los usuarios se alejan de sus sistemas sin bloquear la pantalla.
- Los usuarios cambian los permisos en un archivo para permitir que otros usuarios lo lean.
- Los usuarios cambian las etiquetas de un archivo para permitir que otros usuarios lean el archivo.
- Los usuarios desechan documentos confidenciales impresos sin destruirlos, o los usuarios dejan documentos confidenciales impresos en ubicaciones inseguras.
- Los usuarios dejan las puertas de acceso sin traba.

- Los usuarios pierden sus llaves.
- Los usuarios no bloquean los medios de almacenamiento extraíbles.
- Las pantallas de los equipos se pueden ver a través de ventanas exteriores.
- Los cables de red tienen derivaciones.
- Una intercepción electrónica captura las señales emitidas por el equipo informático.
- Interrupciones, sobrevoltaje y picos de energía eléctrica destruyen los datos.
- Terremotos, inundaciones, tornados, huracanes y relámpagos destruyen los datos.
- La interferencia de la radiación electromagnética externa, como una mancha solar, desordena los archivos.

Referencias de seguridad adicionales

En las publicaciones del gobierno se describen detalladamente las normas, las políticas, los métodos y la terminología relacionados con la seguridad informática. Otras publicaciones que se muestran aquí son las guías para administradores de sistemas UNIX, y son muy útiles para entender cabalmente los problemas y las soluciones de seguridad de UNIX.

La Web también proporciona recursos. En particular, el sitio web de CERT (`http://www.cert.org`) alerta a las empresas y los usuarios sobre brechas de seguridad en el software. El sitio de SANS Institute (`http://www.sans.org/`) ofrece formación, un amplio glosario de términos y una lista actualizada de las principales amenazas de Internet.

Publicaciones del gobierno de los Estados Unidos

El gobierno estadounidense ofrece muchas de sus publicaciones en la Web. El Centro de Recursos de Seguridad Informática (CSRC) del Instituto Nacional de Estándares y Tecnología (NIST) publica artículos sobre seguridad informática. Los siguientes son algunos ejemplos de las publicaciones que se pueden descargar del sitio de NIST (`http://csrc.nist.gov/index.html`).

- *An Introduction to Computer Security: The NIST Handbook* (Introducción a la seguridad informática: El manual de NIST). SP 800-12, octubre de 1995.
- *Standard Security Label for Information Transfer* (Etiqueta de seguridad estándar para la transferencia de información). FIPS 188, septiembre de 1994.
- Swanson, Marianne y Barbara Guttman. *Generally Accepted Principles and Practices for Securing Information Technology Systems* (Principios y prácticas generalmente aceptados para proteger los sistemas de tecnología de la información). SP 800-14, septiembre de 1996.
- Tracy, Miles, Wayne Jensen y Scott Bisker. *Guidelines on Electronic Mail Security* (Directrices sobre la seguridad del correo electrónico). SP 800-45, septiembre de 2002. La sección E. 7 se refiere a la configuración segura de LDAP para el correo.

- Wilson, Mark y Joan Hash. *Building an Information Technology Security Awareness and Training Program* (Programa de formación y consciencia sobre la seguridad de la tecnología de la información). SP 800-61, enero de 2004. Incluye un glosario útil.
- Grace, Tim, Karen Kent y Brian Kim. *Computer Security Incident Handling Guidelines* (Directrices para el manejo de incidentes relacionados con la seguridad informática). SP 800-50, septiembre de 2002. La sección E. 7 se refiere a la configuración segura de LDAP para el correo.
- Scarfone, Karen, Wayne Jansen y Miles Tracy. *Guide to General Server Security* (Guía para la seguridad general del servidor). SP 800-123, julio de 2008.
- Souppaya, Murugiah, John Wack y Karen Kent. *Security Configuration Checklists Program for IT Products* (Programa de listas de comprobación de configuración de seguridad para productos de TI). SP 800-70, mayo de 2005.

Publicaciones de seguridad de UNIX

Ingenieros de seguridad de Sun Microsystems. *Solaris 10 Security Essentials*. Prentice Hall, 2009.

Chirillo, John y Edgar Danielyan. *Sun Certified Security Administration for Solaris 9 & 10 Study Guide* (Guía de estudio de administración de seguridad certificada por Sun para Solaris 9 y 10). McGraw-Hill/Osborne, 2005.

Garfinkel, Simson, Gene Spafford y Alan Schwartz. *Practical UNIX and Internet Security, 3rd Edition* (Seguridad práctica para Internet y UNIX, 3.ª edición). O'Reilly & Associates, Inc, Sebastopol, CA, 2006.

Publicaciones sobre seguridad informática general

Brunette, Glenn M. and Christoph L. *Toward Systemically Secure IT Architectures* (Hacia arquitecturas de TI seguras desde el punto de vista sistemático). Sun Microsystems, Inc, junio de 2005.

Kaufman, Charlie, Radia Perlman y Mike Speciner. *Network Security: Private Communication in a Public World, 2nd Edition* (Seguridad de la red: Comunicación privada en un mundo público, 2.ª edición). Prentice-Hall, 2002.

Pfleeger, Charles P. y Shari Lawrence Pfleeger. *Security in Computing* (Seguridad en el área informática). Prentice Hall PTR, 2006.

Privacy for Pragmatists: A Privacy Practitioner's Guide to Sustainable Compliance (Privacidad para pragmáticos: Una guía práctica sobre la privacidad para la conformidad sostenible). Sun Microsystems, Inc, agosto de 2005.

Rhodes-Ousley, Mark, Roberta Bragg y Keith Strassberg. *Network Security: The Complete Reference* (Seguridad de la red: La referencia completa). McGraw-Hill/Osborne, 2004.

Stoll, Cliff. *The Cuckoo's Egg* (El huevo del cuco). Doubleday, 1989.

Publicaciones generales de UNIX

Bach, Maurice J. *The Design of the UNIX Operating System* (El diseño del sistema operativo UNIX). Prentice Hall, Englewood Cliffs, NJ, 1986.

Nemeth, Evi, Garth Snyder y Scott Seebas. *UNIX System Administration Handbook* (Manual de administración del sistema UNIX). Prentice Hall, Englewood Cliffs, NJ, 1989.

◆ ◆ ◆ APÉNDICE B

Lista de comprobación de configuración de Trusted Extensions

Esta lista de comprobación ofrece una visión general de las principales tareas de configuración para Trusted Extensions. Las tareas más pequeñas se detallan dentro de las tareas principales. La lista de comprobación no sustituye los siguientes pasos en esta guía.

Lista de comprobación para la configuración de Trusted Extensions

En la siguiente lista se resume qué se requiere para habilitar y configurar Trusted Extensions en su sitio. Para las tareas que se tratan en otro lugar existen referencias cruzadas.

1. Lea.
   - Lea los primeros cinco capítulos de la Parte II.
   - Comprenda los requisitos de seguridad del sitio.
   - Lea "Política de seguridad del sitio y Trusted Extensions" en la página 304.
2. Prepare.
   - Elija la contraseña de usuario `root`.
   - Elija el nivel de seguridad de la PROM o el BIOS.
   - Elija la contraseña de la PROM o el BIOS.
   - Elija si se permite la conexión de periféricos.
   - Elija si se permite el acceso a impresoras remotas.
   - Elija si se permite el acceso a redes sin etiquetas.
3. Habilite Trusted Extensions. Consulte "Habilitación del servicio Trusted Extensions e inicio de sesión" en la página 48.
   a. Instale el SO Oracle Solaris.
   b. Cargue los paquetes de Trusted Extensions.
   c. Habilite `svc:/system/labeld`, el servicio de Trusted Extensions.
   d. Reinicie.

4. (Opcional) Personalice la zona global. Consulte "Configuración de la zona global en Trusted Extensions" en la página 51.
   a. Si utiliza IPv6, habilite IPv6 para Trusted Extensions.
   b. Si utiliza un dominio de interpretación distinto de `1`, defina el dominio de interpretación en el archivo `/etc/system` y en cada plantilla de seguridad.
   c. Verifique e instale el archivo `label_encodings` de su sitio.
   d. Reinicie.
5. Agregue zonas con etiquetas. Consulte "Creación de zonas con etiquetas" en la página 56.
   a. Configure dos zonas con etiquetas automáticamente.
   b. Configure sus zonas con etiquetas manualmente.
   c. Cree un espacio de trabajo con etiquetas.
6. Configure el servicio de nombres LDAP. Consulte el Capítulo 5, "Configuración de LDAP para Trusted Extensions (tareas)".

   Cree un servidor proxy para Trusted Extensions o un servidor LDAP para Trusted Extensions. El servicio de nombres de archivos no necesita ninguna configuración.
7. Configure las interfaces y las rutas para la zona global y las zonas con etiquetas. Consulte "Configuración de las interfaces de red en Trusted Extensions" en la página 61.
8. Configure la red. Consulte "Etiquetado de hosts y redes (mapa de tareas)" en la página 216.
   - Identifique los hosts de una sola etiqueta y los hosts de rango limitado.
   - Determine las etiquetas que se aplicarán a los datos entrantes de hosts sin etiquetas.
   - Personalice las plantillas de seguridad.
   - Asigne hosts individuales a las plantillas de seguridad.
   - Asigne subredes a las plantillas de seguridad.
9. Realice otras tareas de configuración.
   a. Configure las conexiones de red para LDAP.
      - Asigne el servidor LDAP o el servidor proxy al tipo de host `cipso` en todas plantillas de seguridad.
      - Asigne los clientes LDAP al tipo de host `cipso` en todas plantillas de seguridad.
      - Convierta el sistema local en un cliente del servidor LDAP.
   b. Configure los usuarios locales y los roles de administración locales. Consulte "Creación de roles y usuarios en Trusted Extensions" en la página 67.
      - Cree el rol de administrador de la seguridad.
      - Cree un usuario local que pueda asumir el rol de administrador de la seguridad.
      - Cree otros roles y posiblemente otros usuarios locales para que asuman estos roles.

c. Cree directorios principales en cada etiqueta a la que puede acceder el usuario. Consulte "Creación de directorios principales centralizados en Trusted Extensions" en la página 73.

- Cree directorios principales en un servidor NFS.
- Cree directorios principales ZFS locales que se puedan cifrar.
- (Opcional) Evite que los usuarios lean los directorios principales de nivel inferior.

d. Configure las opciones de impresión. Consulte "Configuración de impresión con etiquetas (mapa de tareas)" en la página 257.

e. Configure los dispositivos. Consulte "Control de dispositivos en Trusted Extensions (mapa de tareas)" en la página 275.

i. Asigne el perfil de gestión de dispositivos o el perfil de administrador del sistema a un rol.

ii. Para poder utilizar los dispositivos, realice una de las siguientes acciones:

- Por sistema, permita la asignación de los dispositivos.
- Asigne la autorización Allocate Device a los usuarios y roles seleccionados.

f. Configure las funciones de Oracle Solaris.

- Configure las opciones de auditoría.
- Configure los valores de seguridad del sistema.
- Permita que determinados clientes LDAP administren LDAP.
- Configure los usuarios en LDAP.
- Configure los roles de red en LDAP.

g. Monte y comparta sistemas de archivos. Consulte el Capítulo 14, "Gestión y montaje de archivos en Trusted Extensions (tareas)".

◆ ◆ ◆ APÉNDICE C

Referencia rápida a la administración de Trusted Extensions

Las interfaces de Trusted Extensions amplían el SO Oracle Solaris. En este apéndice, se proporciona una referencia rápida sobre las diferencias. Para obtener una lista detallada de las interfaces, incluidas las rutinas de biblioteca y las llamadas del sistema, consulte el Apéndice D, "Lista de las páginas del comando man de Trusted Extensions".

Interfaces administrativas en Trusted Extensions

Trusted Extensions proporciona interfaces para el software. Las siguientes interfaces están disponibles únicamente cuando se ejecuta el software Trusted Extensions:

Secuencia de comandos `txzonemgr`	Proporciona un asistente basado en menú para crear, instalar, inicializar e iniciar las zonas con etiquetas. El título del menú es Labeled Zone Manager. Esta secuencia de comandos también proporciona opciones de menú para las opciones de redes y de servicios de nombres, y para establecer la zona global como cliente de un servidor LDAP existente. En la versión Oracle Solaris 11, el comando `txzonemgr -c` omite los menús para crear las primeras dos zonas con etiquetas.
Device Manager	En Trusted Extensions, se utiliza esta interfaz gráfica de usuario para administrar dispositivos. Los administradores utilizan el cuadro de diálogo Device Administration para configurar dispositivos. Los roles y los usuarios comunes utilizan Device Allocation Manager para asignar dispositivos. La interfaz gráfica de usuario está disponible desde el menú Trusted Path.

Generador de etiquetas	Se invoca esta aplicación cuando el usuario puede elegir una etiqueta o una acreditación. Esta aplicación también aparece cuando un rol asigna etiquetas o rangos de etiquetas a los dispositivos, las zonas, los usuarios o los roles. La utilidad `tgnome-selectlabel` permite personalizar un generador de etiquetas. Consulte "tgnome-selectlabel Utility" de *Trusted Extensions Developer's Guide*,
Selection Manager	Se invoca esta aplicación cuando un usuario o un rol autorizados intentan aumentar o disminuir el nivel de la información.
Menú Trusted Path	Este menú gestiona las interacciones con la base de computación de confianza (TCB). Por ejemplo, este menú tiene una opción de menú Change (Login/Workspace) Password. En Trusted GNOME, para acceder al menú Trusted Path, debe hacer clic en el símbolo de confianza que se encuentra a la izquierda de la banda de confianza.
Comandos administrativos	Trusted Extensions proporciona comandos para obtener etiquetas y realizar otras tareas. Para ver una lista de los comandos, consulte "Herramientas de la línea de comandos en Trusted Extensions" en la página 114.

Interfaces de Oracle Solaris ampliadas por Trusted Extensions

Trusted Extensions amplía los archivos de configuración, los comandos y las interfaces gráficas de usuario existentes de Oracle Solaris.

Comandos administrativos	Trusted Extensions agrega opciones a comandos seleccionados de Oracle Solaris. Para obtener una lista de todas las interfaces de Trusted Extensions, consulte el Apéndice D, "Lista de las páginas del comando man de Trusted Extensions".
Archivos de configuración	Trusted Extensions agrega dos privilegios: `net_mac_aware` y `net_mlp`. Para obtener información sobre el uso de `net_mac_aware`,

consulte "Acceso a los sistemas de archivos montados en NFS en Trusted Extensions" en la página 183.

Trusted Extensions agrega autorizaciones a la base de datos `auth_attr`.

Trusted Extensions agrega archivos ejecutables a la base de datos `exec_attr`.

Trusted Extensions modifica los perfiles de derechos existentes en la base de datos `prof_attr`. También agrega perfiles a la base de datos.

Trusted Extensions agrega campos a la base de datos `policy.conf`. Para obtener información sobre los campos, consulte "Valores predeterminados del archivo `policy.conf` en Trusted Extensions" en la página 138.

Trusted Extensions agrega tokens de auditoría, eventos de auditoría, clases de auditoría y opciones de política de auditoría. Para ver una lista, consulte la "Referencia de auditoría de Trusted Extensions" en la página 293.

Directorios compartidos desde las zonas — Trusted Extensions le permite compartir directorios desde las zonas con etiquetas. Los directorios se comparten en la etiqueta de la zona mediante la creación de un archivo `/etc/dfs/dfstab` desde la zona global.

Valores predeterminados de seguridad que brindan mayor protección en Trusted Extensions

Trusted Extensions establece valores predeterminados de seguridad que brindan mayor protección que el SO Oracle Solaris:

Dispositivos — De manera predeterminada, la asignación de dispositivos está habilitada.

De manera predeterminada, la asignación de dispositivos requiere autorización. Por lo tanto, de manera predeterminada, los usuarios comunes no pueden utilizar los medios extraíbles.

	El administrador puede eliminar el requisito de autorización. Sin embargo, la asignación de dispositivos suele requerirse en sitios que instalan Trusted Extensions.
Impresión	Los usuarios comunes pueden imprimir únicamente en las impresoras que incluyen la etiqueta del usuario en el rango de etiquetas de la impresora. De manera predeterminada, el resultado de la impresión tiene las páginas de la carátula y del ubicador. Estas páginas, y las páginas del cuerpo, incluyen la etiqueta del trabajo de impresión.
Roles	Los roles están disponibles en el SO Oracle Solaris, pero su uso es opcional. En Trusted Extensions, los roles son necesarios para la correcta administración.

Opciones limitadas en Trusted Extensions

Trusted Extensions reduce el rango de opciones de configuración de Oracle Solaris:

Servicio de nombres	Se admite el servicio de nombres de LDAP. Todas las zonas deben administrarse desde un solo servicio de nombres.
Zonas	La zona global es una zona administrativa. Solamente el usuario `root` o un rol pueden entrar en la zona global. Por lo tanto, las interfaces administrativas que están disponibles para los usuarios comunes de Oracle Solaris no están disponibles para los usuarios comunes de Trusted Extensions. Las zonas no globales son las zonas con etiquetas. Los usuarios trabajan en las zonas con etiquetas.

◆ ◆ ◆ APÉNDICE D

Lista de las páginas del comando man de Trusted Extensions

Trusted Extensions es una configuración del SO Oracle Solaris. En este apéndice, se proporciona una descripción de las páginas del comando man que incluyen información sobre Trusted Extensions.

Páginas del comando man de Trusted Extensions en orden alfabético

Las siguientes páginas del comando man sólo son relevantes en un sistema que está configurado con Trusted Extensions. La descripción incluye enlaces a ejemplos o explicaciones de estas funciones en el conjunto de documentos de Trusted Extensions.

Página del comando man de Trusted Extensions	Finalidad y enlaces a información adicional
`add_allocatable(1M)`	Permite que los dispositivos se asignen mediante la adición del dispositivo a las bases de datos de asignación de dispositivos. De manera predeterminada, los dispositivos extraíbles se pueden asignar. Consulte "Cómo configurar un dispositivo en Trusted Extensions" en la página 277.
`atohexlabel(1M)`	Convierte una etiqueta en lenguaje natural a su equivalente de texto interno.

	Para ver un ejemplo, consulte "Cómo obtener el equivalente hexadecimal de una etiqueta" en la página 130.
`blcompare`(3TSOL)	Compara etiquetas binarias.
`blminmax`(3TSOL)	Determina el vínculo entre dos etiquetas.
`chk_encodings`(1M)	Comprueba la sintaxis del archivo de codificaciones de etiqueta.
	Para ver ejemplos, consulte "How to Debug a label_encodings File" de *Trusted Extensions Label Administration* y el Ejemplo 4–1.
`fgetlabel`(2)	Obtiene la etiqueta del archivo.
`getlabel`(1)	Muestra la etiqueta de los archivos o directorios seleccionados.
	Para ver un ejemplo, consulte "Cómo visualizar las etiquetas de los archivos montados" en la página 174.
`getlabel`(2)	Obtiene la etiqueta de un archivo.
`getpathbylabel`(3TSOL)	Obtiene el nombre de ruta de la zona.
`getplabel`(3TSOL)	Obtiene la etiqueta de un proceso.
`getuserrange`(3TSOL)	Obtiene el rango de etiquetas de un usuario.
`getzoneidbylabel`(3TSOL)	Obtiene el ID de zona de la etiqueta de la zona.
`getzonelabelbyid`(3TSOL)	Obtiene la etiqueta de la zona del ID de zona.
`getzonelabelbyname`(3TSOL)	Obtiene la etiqueta de la zona del nombre de la zona.
`getzonepath`(1)	Muestra la ruta root de la zona que corresponde a la etiqueta especificada.
	"Acquiring a Sensitivity Label" de *Trusted Extensions Developer's Guide*
`getzonerootbyid`(3TSOL)	Obtiene el nombre de ruta root de la zona del ID de root de la zona.
`getzonerootbylabel`(3TSOL)	Obtiene el nombre de ruta root de la zona a partir de la etiqueta de la zona.

getzonerootbyname(3TSOL)	Obtiene el nombre de ruta root de la zona del nombre de la zona.
hextoalabel(1M)	Convierte una etiqueta de texto interno a su equivalente en lenguaje natural. Para ver un ejemplo, consulte "Cómo obtener una etiqueta legible de su forma hexadecimal" en la página 131.
labelclipping(3TSOL)	Convierte una etiqueta binaria y la recorta al ancho especificado.
label_encodings(4)	Describe el archivo de codificaciones de etiqueta.
label_to_str(3TSOL)	Convierte las etiquetas a cadenas en lenguaje natural.
labels(5)	Describe los atributos de etiqueta de Trusted Extensions.
libtsnet(3LIB)	Es la biblioteca de red de Trusted Extensions.
libtsol(3LIB)	Es la biblioteca de Trusted Extensions.
m_label(3TSOL)	Asigna y libera recursos para una etiqueta nueva.
pam_tsol_account(5)	Comprueba las limitaciones de cuenta que originan las etiquetas. Para ver un ejemplo de su uso, consulte "Cómo realizar las tareas de inicio de sesión y administración en un sistema Trusted Extensions remoto" en la página 164.
plabel(1)	Obtiene la etiqueta de un proceso.
remove_allocatable(1M)	Impide la asignación de un dispositivo mediante la eliminación de su entrada de las bases de datos de asignación de dispositivos. Para ver un ejemplo, consulte "Cómo configurar un dispositivo en Trusted Extensions" en la página 277.
sel_config(4)	Establece las reglas de selección para las operaciones de copiar, cortar y pegar, y arrastrar y soltar.

	Consulte "Reglas para cambiar el nivel de seguridad de los datos" en la página 122.
`setflabel`(3TSOL)	Mueve un archivo a una zona con la etiqueta de sensibilidad correspondiente.
`setlabel`(1)	Vuelve a etiquetar el elemento seleccionado. Requiere las autorizaciones `solaris.label.file.downgrade` o `solaris.label.file.upgrade`. Estas autorizaciones están en el perfil de derechos de gestión de etiquetas de objetos.
`str_to_label`(3TSOL)	Analiza las cadenas en lenguaje natural para una etiqueta.
`tncfg`(1M)	Gestiona las bases de datos de la red de confianza. Una alternativa a la interfaz gráfica de usuario `txzonmgr` para gestionar la red de confianza. El subcomando `list` muestra las características de seguridad de las interfaces de red. `tncfg` proporciona información más completa que el comando `tninfo`. Para ver varios ejemplos, consulte el Capítulo 16, "Gestión de redes en Trusted Extensions (tareas)".
`tnctl`(1M)	Configura los parámetros de red de Trusted Extensions. También puede utilizar el comando `tncfg`. Para ver un ejemplo, consulte el Ejemplo 12–1.
`tnd`(1M)	Ejecuta el daemon de la red de confianza cuando está habilitado el servicio de nombres LDAP.
`tninfo`(1M)	Muestra la información y las estadísticas de red de Trusted Extensions en el nivel del núcleo. "Cómo depurar la red de Trusted Extensions" en la página 241. También puede utilizar el comando `tncfg` y la interfaz gráfica de usuario `txzonemgr`. Para ver una comparación con el comando `tncfg`, consulte "Cómo resolver problemas por fallos de montaje en Trusted Extensions" en la página 192.

`trusted_extensions`(5)	Presenta Trusted Extensions.
`txzonemgr`(1M)	Gestiona zonas con etiquetas e interfaces de red. Las opciones de la línea de comandos permiten la creación automática de dos zonas. Este comando acepta un archivo de configuración como entrada y permite la eliminación de zonas. `txzonemgr` es una secuencia de comandos `zenity` (1). Consulte "Creación de zonas con etiquetas" en la página 56 y "Resolución de problemas de la red de confianza (mapa de tareas)" en la página 240.
`TrustedExtensionsPolicy`(4)	Es el archivo de configuración de la extensión del servidor X de Trusted Extensions.
`tsol_getrhtype`(3TSOL)	Obtiene el tipo de host de la información de red de Trusted Extensions.
utilidad `tgnome-selectlabel`	Permite crear una interfaz gráfica de usuario del generador de etiquetas. Para obtener más información, consulte "tgnome-selectlabel Utility" de *Trusted Extensions Developer's Guide*.
`updatehome`(1)	Actualiza los archivos de enlace y la copia del directorio principal para la etiqueta actual. Consulte "Cómo configurar los archivos de inicio para los usuarios en Trusted Extensions" en la página 146.
`XTSOLgetClientAttributes`(3XTSOL)	Obtiene los atributos de etiqueta de un cliente X.
`XTSOLgetPropAttributes`(3XTSOL)	Obtiene los atributos de etiqueta de una propiedad de una ventana.
`XTSOLgetPropLabel`(3XTSOL)	Obtiene la etiqueta de una propiedad de una ventana.
`XTSOLgetPropUID`(3XTSOL)	Obtiene el UID de una propiedad de una ventana.
`XTSOLgetResAttributes`(3XTSOL)	Obtiene todos los atributos de etiqueta de una ventana o un mapa de píxeles.
`XTSOLgetResLabel`(3XTSOL)	Obtiene la etiqueta de una ventana, un mapa de píxeles o un mapa de colores.

XTSOLgetResUID(3XTSOL)	Obtiene el UID de una ventana o un mapa de píxeles.
XTSOLgetSSHeight(3XTSOL)	Obtiene la altura de la banda de la pantalla.
XTSOLgetWorkstationOwner(3XTSOL)	Obtiene la propiedad de la estación de trabajo.
XTSOLIsWindowTrusted(3XTSOL)	Determina si un cliente de confianza creó la ventana.
XTSOLMakeTPWindow(3XTSOL)	Convierte esta ventana en una ventana Trusted Path.
XTSOLsetPolyInstInfo(3XTSOL)	Establece la información para la creación de varias instancias.
XTSOLsetPropLabel(3XTSOL)	Establece la etiqueta de una propiedad de la ventana.
XTSOLsetPropUID(3XTSOL)	Establece el UID de una propiedad de una ventana.
XTSOLsetResLabel(3XTSOL)	Establece la etiqueta de una ventana o un mapa de píxeles.
XTSOLsetResUID(3XTSOL)	Establece el UID de una ventana, un mapa de píxeles o un mapa de colores.
XTSOLsetSessionHI(3XTSOL)	Establece la etiqueta de sensibilidad alta de sesión para el servidor de la ventana.
XTSOLsetSessionLO(3XTSOL)	Establece la etiqueta de sensibilidad baja de sesión para el servidor de la ventana.
XTSOLsetSSHeight(3XTSOL)	Establece la altura de la banda de la pantalla.
XTSOLsetWorkstationOwner(3XTSOL)	Establece la propiedad de la estación de trabajo.

Páginas del comando man de Oracle Solaris modificadas por Trusted Extensions

Trusted Extensions agrega información a las siguientes páginas del comando man de Oracle Solaris.

Página del comando man de Oracle Solaris	Modificación de Trusted Extensions y enlaces a información adicional
allocate(1)	Agrega opciones para admitir la asignación de un dispositivo en una zona y la limpieza del

	dispositivo en un entorno de ventanas. En Trusted Extensions, los usuarios comunes no utilizan este comando. Para conocer los procedimientos de usuario, consulte "Cómo asignar un dispositivo en Trusted Extensions" de *Guía del usuario de Oracle Solaris Trusted Extensions*.
`auditconfig`(1M)	Agrega la política de ventanas, las clases de auditoría, los eventos de auditoría y los tokens de auditoría para la información con etiquetas.
`auditreduce`(1M)	Agrega la opción `-l` para seleccionar los registros de auditoría por etiqueta. Para ver ejemplos, consulte "Cómo seleccionar eventos de auditoría de la pista de auditoría" de *Administración de Oracle Solaris: servicios de seguridad*.
`auth_attr`(4)	Agrega autorizaciones de etiqueta
`automount`(1M)	Agrega la capacidad para montar y, en consecuencia, ver los directorios principales de nivel inferior. Modificar los nombres y los contenidos de los mapas `auto_home` para justificar los nombres y la visibilidad de la zona de etiquetas superiores. Para obtener más información, consulte "Cambios en el montador automático en Trusted Extensions" en la página 184.
`deallocate`(1)	Agrega opciones para admitir la desasignación de un dispositivo en una zona, la limpieza del dispositivo en un entorno de ventanas y la especificación del tipo de dispositivo que debe desasignarse. En Trusted Extensions, los usuarios comunes no utilizan este comando. Para conocer los procedimientos de usuario, consulte "Cómo asignar un dispositivo en Trusted Extensions" de *Guía del usuario de Oracle Solaris Trusted Extensions*.

device_clean(5)	Se invoca en Trusted Extensions de manera predeterminada.
getpflags(2)	Reconoce los indicadores de proceso NET_MAC_AWARE y NET_MAC_AWARE_INHERIT.
getsockopt(3SOCKET)	Obtiene el estado del control de acceso obligatorio, SO_MAC_EXEMPT, del socket.
getsockopt(3XNET)	Obtiene el estado del control de acceso obligatorio, SO_MAC_EXEMPT, del socket.
ikeadm(1M)	Agrega un indicador de depuración, 0x0400, para los procesos IKE con etiquetas.
ike.config(4)	Agrega el parámetro global label_aware y tres palabras clave de transformación de fase 1, single_label, multi_label y wire_label.
in.iked(1M)	Admite la negociación de asociaciones de seguridad con etiquetas a través de los puertos UDP de varios niveles 500 y 4500 en la zona global. Asimismo, consulte la página del comando man ike.config(4).
ipadm(1M)	Agrega la interfaz all-zones como un valor de propiedad permanente. Para ver un ejemplo, consulte "Cómo verificar que las interfaces de un sistema estén activas" en la página 240.
ipseckey(1M)	Agrega las extensiones label, outer-label e implicit-label. Estas extensiones asocian las etiquetas de Trusted Extensions con el tráfico que se transporta dentro de una asociación de seguridad.
is_system_labeled(3C)	Determina si el sistema está configurado con Trusted Extensions.
ldaplist(1)	Agrega bases de datos de red de Trusted Extensions en LDAP.
list_devices(1)	Agrega atributos, como etiquetas, que estén asociados con un dispositivo. Agrega la opción -a para mostrar los atributos del dispositivo,

	como las autorizaciones y las etiquetas. Agrega la opción `-d` para mostrar los atributos predeterminados de un tipo de dispositivo asignado. Agrega la opción `-z` para mostrar los dispositivos disponibles que pueden asignarse a una zona con etiquetas.
`netstat`(1M)	Agrega la opción `-R` para mostrar los atributos de seguridad ampliados para los sockets y las entradas de la tabla de enrutamiento. Para ver un ejemplo, consulte "Cómo resolver problemas por fallos de montaje en Trusted Extensions" en la página 192.
`pf_key`(7P)	Agrega etiquetas a las asociaciones de seguridad (SA) IPsec.
`privileges`(5)	Agrega privilegios de Trusted Extensions como `PRIV_FILE_DOWNGRADE_SL`.
`prof_attr`(4)	Agrega perfiles de derechos, como el de gestión de etiquetas de objetos.
`route`(1M)	Agrega la opción `-secattr` para agregar atributos de seguridad ampliados a una ruta. Agrega la opción `-secattr` para mostrar los atributos de seguridad de la ruta: `cipso`, `doi`, `max_sl` y `min_sl`. Para ver un ejemplo, consulte "Cómo resolver problemas por fallos de montaje en Trusted Extensions" en la página 192.
`setpflags`(2)	Establece el indicador por proceso `NET_MAC_AWARE`.
`setsockopt`(3SOCKET)	Establece la opción `SO_MAC_EXEMPT`.
`setsockopt`(3XNET)	Establece el control de acceso obligatorio, `SO_MAC_EXEMPT`, en el socket.
`socket.h`(3HEAD)	Admite la opción `SO_MAC_EXEMPT` para iguales sin etiquetas.
`tar`(1)	Agrega la opción `-T` para archivar y extraer los archivos y directorios que tengan etiquetas.

	Consulte "Cómo realizar copias de seguridad de los archivos en Trusted Extensions" en la página 188 y "Cómo restaurar archivos en Trusted Extensions" en la página 188.
`tar.h`(3HEAD)	Agrega los tipos de atributos que se utilizan en los archivos tar con etiquetas.
`ucred_getlabel`(3C)	Agrega la obtención del valor de etiqueta en una credencial de usuario.
`user_attr`(4)	Agrega los atributos de seguridad de usuario `idletime`, `idlecmd`, `clearance` y `min_label` que son específicos de Trusted Extensions.
	Consulte "Planificación de la seguridad del usuario en Trusted Extensions" en la página 34.

Glosario

acreditación El límite superior del conjunto de etiquetas en el que puede trabajar el usuario. El límite inferior es la etiqueta mínima que es asignada por el administrador de la seguridad. Existen dos tipos de acreditación, acreditación de sesión o acreditación de usuario.

acreditación de usuario La acreditación asignada por el administrador de la seguridad, que establece el límite superior del conjunto de etiquetas en las que el usuario puede trabajar en cualquier momento. El usuario puede decidir aceptar la acreditación predeterminada, o bien, restringir más dicha acreditación durante cualquier sesión.

administrador de la seguridad En una organización donde se debe proteger la información confidencial, la persona o las personas que definen y aplican la política de seguridad del sitio. Estas personas tienen acreditación para acceder a toda la información que se esté procesando en el sitio. En el ámbito del software, el rol administrativo de administrador de la seguridad se asigna a una o varias personas que tengan la acreditación correspondiente. Estos administradores configuran los atributos de seguridad de todos los usuarios y hosts, para que el software aplique la política de seguridad del sitio. Para comparar, consulte administrador del sistema.

administrador del sistema En Trusted Extensions, el rol de confianza asignado al usuario o los usuarios responsables de realizar las tareas estándar de gestión del sistema, como la configuración de las partes de las cuentas de usuario no relacionadas con la seguridad. Para comparar, consulte administrador de la seguridad.

archivo .copy_files Un archivo de configuración opcional en un sistema de varias etiquetas. Este archivo contiene una lista de archivos de inicio, como `.cshrc` o `.mozilla`, que el entorno de usuario o las aplicaciones de usuario requieren para que el sistema o la aplicación funcionen bien. Los archivos que aparecen en `.copy_files` se *copian* en el directorio principal del usuario en etiquetas superiores cuando se crean dichos directorios. Consulte también archivo .link_files.

archivo .link_files Un archivo de configuración opcional en un sistema de varias etiquetas. Este archivo contiene una lista de archivos de inicio, como `.cshrc` o `.mozilla`, que el entorno de usuario o las aplicaciones de usuario requieren para que el sistema o la aplicación funcionen bien. Los archivos que aparecen en `.link_files` se *enlazan* al directorio principal del usuario en etiquetas superiores cuando se crean dichos directorios. Consulte también archivo .copy_files.

archivo label_encodings Archivo en el que se definen la etiqueta de sensibilidad completa, los rangos de acreditación, la vista de las etiquetas, la visibilidad predeterminada de las etiquetas, las acreditaciones de usuario predeterminadas y otros aspectos de las etiquetas.

asignación Un mecanismo mediante el que se controla el acceso a un dispositivo. Consulte asignación de dispositivos.

asignación de dispositivos Un mecanismo para impedir el acceso a la información almacenada en un dispositivo asignable a todos menos al usuario que asigna el dispositivo. Nadie, excepto el usuario que asignó el dispositivo, puede acceder a la información relacionada con el dispositivo hasta que se anula la asignación de éste. Para que un usuario pueda asignar un dispositivo el administrador de la seguridad le debe haber otorgado la autorización de asignación de dispositivos.

atributo de seguridad Un atributo que se utiliza para aplicar la política de seguridad de Trusted Extensions. Diversos conjuntos de atributos de seguridad se asignan a un proceso, usuario, zona, host, dispositivo asignable y otros objetos.

autorización Un derecho otorgado a un usuario o un rol para realizar una acción que, de lo contrario, no estaría permitida por la política de seguridad. Las autorizaciones se conceden en los perfiles de derechos. Determinados comandos requieren que el usuario cuente con ciertas autorizaciones para ejecutarse con éxito. Por ejemplo, para imprimir un archivo PostScript se requiere la autorización Print Postscript.

banda de confianza Una región que no se pude suplantar. En Trusted GNOME, la banda se ubica en la parte superior. La banda proporciona información visual sobre el estado del sistema de ventanas: un indicador de ruta de confianza y una etiqueta de sensibilidad de ventana. Cuando las etiquetas de sensibilidad se configuran para que un usuario no las pueda ver, la banda de confianza se reduce a un icono que muestra sólo el indicador de ruta de confianza.

base de datos tnrhdb La base de datos del host remoto de la red de confianza. Esta base de datos asigna un conjunto de características de etiquetas a un host remoto. La base de datos está disponible como un archivo en `/etc/security/tsol/tnrhdb`.

base de datos tnrhtp La plantilla de host remoto de la red de confianza. Esta base de datos define el conjunto de características de etiquetas que se pueden asignar a un host remoto. La base de datos está disponible como un archivo en `/etc/security/tsol/tnrhtp`.

bases de datos de la red de confianza `tnrhtp`, la plantilla de host remoto de la red de confianza, y `tnrhdb`, la base de datos del host remoto de la red de confianza, definen con qué host remoto se puede comunicar un sistema Trusted Extensions.

bits de permiso Un tipo de control de acceso discrecional en el que el propietario especifica un conjunto de bits para indicar quién puede leer, escribir o ejecutar un archivo o directorio. Se asignan tres conjuntos de permisos a cada archivo o directorio: uno para el propietario, uno para el grupo del propietario y uno para todos los demás.

clasificación El componente jerárquico de una acreditación o una etiqueta. Una clasificación indica un nivel jerárquico de seguridad, por ejemplo, `TOP SECRET` o `UNCLASSIFIED`.

cliente Un sistema conectado a una red.

compartimiento Un componente no jerárquico de una etiqueta que se utiliza con el componente de clasificación para formar una acreditación o una etiqueta. Un compartimiento representa una recopilación de información, como la que utilizaría un departamento de ingeniería o un equipo de proyecto multidisciplinario.

configuración de etiqueta Una opción de instalación de Trusted Extensions de etiquetas de sensibilidad de una sola etiqueta o de varias etiquetas. En la mayoría de los casos, la configuración de etiquetas es idéntica en todos los sistemas del sitio.

configuración evaluada

Uno o varios hosts de Trusted Extensions que se están ejecutando en una configuración cuyo cumplimiento con los criterios específicos haya sido certificado por una autoridad de certificación. En Estados Unidos, esos criterios conforman los Criterios de Evaluación de Sistemas Informáticos Fiables (TCSEC, Trusted Computer System Evaluation Criteria). El organismo de evaluación y certificación es la Agencia de Seguridad Nacional (NSA, National Security Agency).

- El software Trusted Extensions que se configura en la versión Solaris 10 11/06 está certificado según los criterios comunes v2.3 [agosto de 2005], una normativa ISO, con un nivel de seguridad (EAL) 4 y numerosos perfiles de protección.
- Mediante el proceso de continuidad de garantía, la NSA certificó el software Trusted Extensions que se configura en la versión Solaris 10 5/09.

Los criterios comunes v2 (CCv2) y los perfiles de protección convierten a la norma de TCSEC de Estados Unidos en obsoleta hasta el nivel B1+. Se ha firmado un acuerdo de reconocimiento mutuo para CCv2 entre Estados Unidos, el Reino Unido, Canadá, Dinamarca, Países bajos, Alemania y Francia.

La configuración de Trusted Extensions ofrece una funcionalidad similar a los niveles C2 y B1 de TCSEC, con algunas funciones adicionales.

conjunto de etiquetas

Consulte conjunto de etiquetas de seguridad.

conjunto de etiquetas de seguridad

Especifica un conjunto discreto de etiquetas de seguridad para una entrada de la base de datos tnrhtp. Los hosts que se asignan a una plantilla con un conjunto de etiquetas de seguridad pueden enviar y recibir paquetes que coincidan con cualquiera de las etiquetas del conjunto de etiquetas.

control de acceso discrecional

El tipo de acceso que es otorgado o denegado por el propietario de un archivo o un directorio según el criterio del propietario. Trusted Extensions proporciona dos tipos de control de acceso discrecional (DAC), listas de control de acceso (ACL) y bits de permiso de UNIX.

control de acceso obligatorio

Control de acceso que se basa en la comparación de la etiqueta de sensibilidad de un archivo, directorio o dispositivo con la etiqueta de sensibilidad del proceso que está intentando acceder a él. La regla de MAC, lectura en el mismo nivel y en sentido descendente, se aplica cuando un proceso de una etiqueta intenta leer un archivo de una etiqueta inferior. La regla MAC, escritura en el mismo nivel y lectura en sentido descendente, se aplica cuando un proceso de una etiqueta intenta escribir en un directorio de otra etiqueta.

DAC

Consulte control de acceso discrecional.

dirección IP

Dirección de protocolo de Internet. Un número único que identifica un sistema en red para que éste pueda comunicarse por medio de protocolos de Internet. En IPv4, la dirección está compuesta por cuatro números separados por puntos. La mayoría de las veces, cada parte de la dirección IP es un número entre 0 y 225. Sin embargo, el primer número debe ser menor que 224 y el último número no puede ser 0.

Las direcciones IP se dividen lógicamente en dos partes: la red, y el sistema de la red. El número de red es similar a un código de área de teléfono. En relación con la red, el número de sistema es similar a un número de teléfono.

dispositivo Entre los dispositivos se incluyen impresoras, equipos, unidades de cinta, unidades de disquete, unidades de CD-ROM, unidades de DVD, dispositivos de audio y dispositivos pseudoterminales internos. Los dispositivos están sujetos a la política MAC de lectura y escritura en el mismo nivel. El acceso a los dispositivos extraíbles, como las unidades de DVD, está controlado por la asignación de dispositivos.

dominio Parte de la jerarquía de nombres de Internet. Representa un grupo de sistemas de una red local que comparten los archivos administrativos.

dominio de interpretación (DOI) En un sistema Oracle Solaris en el que está configurado Trusted Extensions, el dominio de interpretación se utiliza para distinguir los distintos archivos `label_encodings` que pueden tener definidas etiquetas similares. El DOI es un conjunto de reglas que convierte los atributos de seguridad de los paquetes de red en la representación de esos atributos de seguridad según el archivo local `label_encodings`. Cuando los sistemas tienen el mismo DOI, comparten el mismo conjunto de reglas y pueden traducir los paquetes de red con etiquetas.

equipo de configuración inicial Un equipo de, al menos, dos personas que juntas supervisan la habilitación y configuración del software Trusted Extensions. Un miembro del equipo es el responsable de las decisiones relacionada con la seguridad y el otro es el responsable de las decisiones relacionadas con la administración del sistema.

escritorio de varios niveles En un sistema Oracle Solaris en el que está configurado Trusted Extensions, los usuarios pueden ejecutar un escritorio en una etiqueta determinada. Si el usuario está autorizado para trabajar en más de una etiqueta, el usuario puede crear un espacio de trabajo independiente para trabajar en cada etiqueta. En este escritorio de varios niveles, los usuarios autorizados pueden cortar y pegar entre las ventanas en diferentes etiquetas, recibir correo en diferentes etiquetas, y ver y utilizar ventanas con etiquetas en los espacios de trabajo de una etiqueta diferente.

etiqueta Un identificador de seguridad que se asigna a un objeto. La etiqueta se basa en el nivel en el que la información de ese objeto debe estar protegida. En función del modo en que el administrador de la seguridad ha configurado el usuario, el usuario puede ver la etiqueta de sensibilidad o ninguna etiqueta. Las etiquetas se definen en el archivo label_encodings.

etiqueta CIPSO Opción de seguridad de IP común (CIPSO, Common IP Security Option). CIPSO es la etiqueta estándar que implementa Trusted Extensions.

etiqueta de sensibilidad Una etiqueta de seguridad que se asigna a un objeto o un proceso. La etiqueta se usa para limitar el acceso según el nivel de seguridad de los datos incluidos.

etiqueta inicial La etiqueta mínima asignada a un usuario o un rol, y la etiqueta del espacio de trabajo inicial del usuario. La etiqueta inicial es la etiqueta de nivel más bajo en la que puede trabajar un usuario o un rol.

etiqueta mínima El límite inferior de etiqueta de sensibilidad de un usuario y el límite inferior de etiqueta de sensibilidad del sistema. La etiqueta mínima establecida por el administrador de la seguridad durante la especificación de atributo de seguridad de usuario es la etiqueta de sensibilidad del primer espacio de trabajo del usuario en el primer inicio de sesión. La etiqueta de sensibilidad especificada en el campo de etiqueta mínima por el administrador de la seguridad en el archivo `label_encodings` establece el límite inferior para el sistema.

fuera de la configuración evaluada Cuando un producto de software que ha demostrado que cumple con los criterios de una configuración evaluada se configura con valores que no cumplen con los criterios de seguridad, el software se describe como *fuera de la configuración evaluada*.

GFI Información proporcionada por el gobierno (GFI, Government Furnished Information). En este manual, se refiere a un archivo label_encodings proporcionado por el gobierno de Estados Unidos. Para utilizar la GFI con el software Trusted Extensions, debe agregar la sección `LOCAL DEFINITIONS` específica de Oracle al final de la GFI. Para obtener detalles, consulte el Capítulo 5, "Customizing the LOCAL DEFINITIONS Section (Tasks)" de *Trusted Extensions Label Administration*.

host con etiquetas Un sistema con etiquetas que forma parte de una red de confianza de sistemas con etiquetas.

host remoto Un sistema distinto del sistema local. Un host remoto puede ser un host sin etiquetas o un host con etiquetas.

host sin etiquetas Un sistema en red que envía paquetes de red sin etiquetas, como un sistema que ejecuta el SO Oracle Solaris.

MAC Consulte control de acceso obligatorio.

nombre de dominio Identificación de un grupo de sistemas. Un nombre de dominio está compuesto por una secuencia de nombres de componentes separados por puntos (por ejemplo: `example1.town.state.country.org`). Leídos de izquierda a derecha, los nombres de componentes hacen referencia a zonas cada vez más generales (y generalmente, más lejanas) de la autoridad de administración.

nombre de host El nombre con el que los otros sistemas de una red reconocen a un sistema. Este nombre debe ser único entre todos los sistemas de un dominio determinado. Generalmente, un dominio identifica una única organización. Un nombre de host puede estar formado por cualquier combinación de letras, números y signos de resta (-), pero no puede empezar ni terminar con este signo.

perfil de derechos Un mecanismo de agrupación para los comandos y para los atributos de seguridad que se asignan a estos ejecutables. Los perfiles de derechos permiten que los administradores de Oracle Solaris controlen quién puede ejecutar determinados comandos y los atributos que tienen estos comandos cuando se ejecutan. Cuando un usuario inicia sesión, se aplican todos los derechos que el usuario tiene asignados, y el usuario tiene acceso a todos los comandos y las autorizaciones asignados en todos los perfiles de derechos de ese usuario.

plantilla de seguridad Un registro en la base de datos `tnrhtp` que define los atributos de seguridad de una clase de hosts que puede acceder a la red de Trusted Extensions.

política de seguridad En un host de Trusted Extensions, el conjunto de reglas de DAC, MAC y etiquetado que definen cómo se puede acceder a la información. En un sitio de cliente, el conjunto de reglas que definen la sensibilidad de la información que se está procesando en ese sitio y las medidas que se utilizan para proteger la información del acceso no autorizado.

privilegio Facultades que se otorgan a un proceso que está ejecutando un comando. El conjunto completo de privilegios describe todas las capacidades del sistema, desde las básicas hasta las administrativas. Los privilegios que se omiten en la política de seguridad, como definir el reloj en un sistema, pueden ser concedidos por el administrador de la seguridad del sitio.

proceso Una acción que ejecuta un comando en nombre del usuario que invoca el comando. Un proceso recibe una cantidad de atributos de seguridad del usuario, incluidos el ID de usuario (UID), el ID de grupo (GID), la lista de grupo adicional y el ID de auditoría del usuario (AUID). Los atributos de seguridad recibidos por un proceso incluyen cualquier privilegio que esté disponible para el comando que se esté ejecutando y la etiqueta de sensibilidad del espacio de trabajo actual.

puerto de varios niveles (MLP) En un sistema Oracle Solaris en el que está configurado Trusted Extensions, un MLP se utiliza para proporcionar un servicio de varios niveles en una zona. De manera predeterminada el servidor X es un servicio de varios niveles que se define en la zona global. Un MLP se especifica mediante número de puerto y protocolo. Por ejemplo, el MLP del servidor X para el escritorio de varios niveles se especifica mediante 6000-6003 y TCP.

rango de acreditación Un conjunto de etiquetas de sensibilidad que están aprobadas para una clase de usuarios o recursos. Un conjunto de etiquetas válidas. Consulte también rango de acreditación del sistema y rango de acreditación de usuario.

rango de acreditación de usuario El conjunto de todas las etiquetas posibles en las que un usuario común puede trabajar en el sistema. El administrador de la seguridad del sitio especifica el rango en el archivo label_encodings. Las reglas para etiquetas con formato correcto que definen el rango de acreditación del sistema también están restringidas por los valores de la sección `ACCREDITATION RANGE` del archivo: el límite superior, el límite inferior, la combinación de restricciones y otras restricciones.

rango de acreditación del sistema El conjunto de etiquetas válidas creadas según las reglas que define el administrador de la seguridad en el archivo label_encodings más las dos etiquetas administrativas que se utilizan en todos los sistemas en los que esté configurado Trusted Extensions. Las etiquetas administrativos son `ADMIN_LOW` y `ADMIN_HIGH`.

rango de etiquetas Un conjunto de etiquetas de sensibilidad que se asignan a comandos, zonas y dispositivos asignables. El rango se especifica designando una etiqueta máxima y una etiqueta mínima. Para los comandos, las etiquetas mínima y máxima limitan las etiquetas en las que se puede ejecutar el comando. A los hosts remotos que no reconocen las etiquetas se les asigna una sola etiqueta de sensibilidad, al igual que a cualquier otro host que el administrador de la seguridad desee restringir a una sola etiqueta. Un rango de etiquetas limita las etiquetas en las que se pueden asignar dispositivos y restringe las etiquetas en las que se puede almacenar o procesar información al utilizar el dispositivo.

red abierta Una red de hosts de Trusted Extensions que se conecta físicamente a otras redes y que utiliza el software Trusted Extensions para comunicarse con hosts que no tienen Trusted Extensions . Compárese con red cerrada.

red cerrada Una red de sistemas en los que está configurado Trusted Extensions. La red está cortada para cualquier host que no pertenezca a Trusted Extensions. El corte puede ser físico, en cuyo caso no se extiende ningún cable fuera de la red de Trusted Extensions. El corte puede estar en el software, en cuyo caso los hosts de Trusted Extensions sólo reconocen los hosts de Trusted Extensions. La entrada de datos desde el exterior de la red está restringida a los periféricos conectados a los hosts de Trusted Extensions. Compárese con red abierta.

relaciones de etiquetas En un sistema Oracle Solaris en el que está configurado Trusted Extensions, una etiqueta puede dominar a otra etiqueta, ser igual a otra etiqueta o estar separada de otra etiqueta. Por ejemplo, la etiqueta `Top Secret` domina a la etiqueta `Secret`. Para dos sistemas con el mismo dominio de interpretación (DOI) la etiqueta `Top Secret` en un sistema es igual a la etiqueta `Top Secret` en el otro sistema.

rol Un rol es como un usuario, con la excepción de que un rol no puede iniciar sesión. Generalmente, un rol se utiliza para asignar capacidades administrativas. Los roles se limitan a un conjunto determinado de comandos y autorizaciones. Consulte rol administrativo.

rol administrativo Un rol que ofrece las autorizaciones, los comandos con privilegios y el atributo de seguridad Trusted Path necesarios para permitir que el rol lleve a cabo tareas administrativas. Los roles tienen un subconjunto de capacidades de superusuario de Oracle Solaris, por ejemplo, realizan tareas de copia de seguridad o auditoría.

rol de confianza Consulte rol administrativo.

ruta de confianza En un sistema Oracle Solaris en el que está configurado Trusted Extensions, la ruta de confianza es una manera confiable y segura de interactuar con el sistema. La ruta de confianza se utiliza para asegurarse de que las funciones administrativas no se puedan ver afectadas. Las funciones de usuario que se deben proteger, como cambiar una contraseña, también usan la ruta de confianza. Cuando la ruta de confianza está activa, en el escritorio aparece un indicador de seguridad.

secuencia de comandos txzonemgr La secuencia de comandos `/usr/sbin/txzonemgr` proporciona una interfaz gráfica de usuario sencilla para gestionar las zonas con etiquetas. La secuencia de comandos también proporciona opciones de menú para las opciones de redes. La secuencia de comandos `txzonemgr` es ejecutada por el usuario root en la zona global.

separación de tareas La política de seguridad que establece que dos administradores o roles deben crear y autenticar un usuario. Un administrador o rol es responsable de la creación del usuario y el directorio principal del usuario, y de otras tareas básicas de administración. El otro administrador o rol es responsable de los atributos de seguridad del usuario, como la contraseña y el rango de etiquetas.

servicio de nombres Una base de datos de red distribuida que contiene información clave sobre todos los sistemas de una red para que éstos se puedan comunicar entre sí. Sin este servicio, cada sistema debe mantener su propia copia de la información del sistema en los archivos `/etc` locales.

shell de perfil Un shell especial que reconoce atributos de seguridad, como privilegios, autorizaciones, y UID y GID especiales. Un shell de perfil generalmente limita a los usuarios a menos comandos, pero puede permitir que estos comandos se ejecuten con más derechos. El shell de perfil es el shell predeterminado de un rol de confianza.

sistema Nombre genérico de un equipo. Después de la instalación, a un sistema de una red generalmente se lo denomina host.

sistema con etiquetas Un sistema con etiquetas es un sistema que está ejecutando un sistema operativo de varios niveles, como Trusted Extensions o SELinux con MLS habilitado. El sistema puede enviar y recibir paquetes de red que están etiquetados con una opción de seguridad de IP común (CIPSO) en el encabezado del paquete.

sistema de archivos Una colección de archivos y directorios que, cuando se organiza en una jerarquía lógica, forma un conjunto de información organizado y estructurado. Los sistemas de archivos se pueden montar desde el sistema local o desde un sistema remoto.

sistema sin etiquetas Para un sistema Oracle Solaris en el que está configurado Trusted Extensions, un sistema sin etiquetas es un sistema que no ejecuta un sistema operativo de varios niveles, como Trusted Extensions o SELinux con MLS habilitado. Un sistema sin etiquetas no envía paquetes con etiquetas. Si el sistema Trusted Extensions que se está comunicando ha asignado una sola etiqueta al sistema sin etiquetas, la comunicación de red entre el sistema Trusted Extensions y el sistema sin etiquetas se produce en esa etiqueta. Al sistema sin etiquetas también se lo denomina "sistema de un solo nivel".

sistemas conectados en red Un grupo de sistemas que están conectados mediante hardware y software, al que a veces se denomina red de área local (LAN). Cuando los sistemas están conectados en red, se suelen necesitar uno o varios servidores.

sistemas no conectados en red Equipos que no están conectados a una red o que no dependen de otros hosts.

zona con etiquetas En un sistema Oracle Solaris en el que está configurado Trusted Extensions, se asigna una etiqueta única a cada zona. Aunque la zona global está etiquetada, *zona con etiquetas* generalmente se refiere a una zona no global a la que se le asigna una etiqueta. Las zonas con etiquetas tienen dos características diferentes de las zonas no globales en un sistema Oracle Solaris que no tiene etiquetas configuradas. En primer lugar, las zonas con etiquetas deben utilizar la misma agrupación de ID de usuario e ID de grupo. En segundo lugar, las zonas con etiquetas pueden compartir direcciones IP.

zona con marca En Trusted Extensions, una zona no global con etiquetas. Generalmente, una zona no global que contiene entornos operativos no nativos. Consulte la página del comando man `brands(5)`.

Índice

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

Z