Configuración y administración de Trusted Extensions

Referencia: E53980
Julio de 2014

Contenido

Uso de esta documentación 13

I Configuración inicial de Trusted Extensions 15

1 Planificación de la seguridad para Trusted Extensions 17
Novedades de Trusted Extensions en Oracle Solaris 11.2 17
Planificación de la seguridad en Trusted Extensions 18
Resultados de la activación de Trusted Extensions desde la perspectiva de un administrador 28

2 Guía básica de configuración de Trusted Extensions 29
Mapa de tareas: preparación y activación de Trusted Extensions 29
Mapa de tareas: selección de una configuración de Trusted Extensions 29
Mapa de tareas: configuración de Trusted Extensions con los valores predeterminados proporcionados 30
Mapa de tareas: configuración de Trusted Extensions para cumplir los requisitos del sitio 30

3 Agregación de la función Trusted Extensions a Oracle Solaris 33
Responsabilidades del equipo de configuración inicial 33
Resolución de problemas de seguridad antes de instalar Trusted Extensions 33
Instalación y activación de Trusted Extensions 35

4 Configuración de Trusted Extensions 39
Configuración de la zona global en Trusted Extensions 39
Creación de zonas con etiquetas 43
Configuración de las interfaces de red en Trusted Extensions 49
Creación de roles y usuarios en Trusted Extensions 56
Creación de directorios principales centralizados en Trusted Extensions 63
Resolución de los problemas de configuración de Trusted Extensions 66
Tareas adicionales de configuración de Trusted Extensions 67

5 Configuración de LDAP para Trusted Extensions 75
Configuración de LDAP en una red Trusted Extensions 75

Configuración de un servidor proxy LDAP en un sistema Trusted Extensions 76
Configuración de Oracle Directory Server Enterprise Edition en un sistema Trusted Extensions 76
Creación de un proxy de Trusted Extensions para un servidor Oracle Directory Server Enterprise Edition existente 84
Creación de un cliente LDAP de Trusted Extensions 86

II Administración de Trusted Extensions 89

6 Conceptos de la administración de Trusted Extensions 91
Trusted Extensions y el SO Oracle Solaris 91
Conceptos básicos de Trusted Extensions 93

7 Herramientas de administración de Trusted Extensions 101
Herramientas de administración para Trusted Extensions 101
Secuencia de comandos `txzonemgr` 102
Device Manager 103
Selection Manager en Trusted Extensions 103
Generador de etiquetas en Trusted Extensions 103
Herramientas de la línea de comandos en Trusted Extensions 104
Archivos de configuración en Trusted Extensions 105

8 Sobre los requisitos de seguridad en un sistema Trusted Extensions 107
Funciones de seguridad configurables 107
Aplicación de los requisitos de seguridad 109
Reglas para cambiar el nivel de seguridad de los datos 112

9 Tareas comunes en Trusted Extensions 117
Introducción para administradores de Trusted Extensions en un sistema de escritorio 117
Realización de tareas comunes en Trusted Extensions 119

10 Acerca de usuarios, derechos y roles en Trusted Extensions 127
Funciones de seguridad del usuario en Trusted Extensions 127
Responsabilidades del administrador para los usuarios 128
Decisiones que deben tomarse antes de crear usuarios en Trusted Extensions ... 129
Atributos de seguridad del usuario predeterminados en Trusted Extensions 130
Atributos de usuario que pueden configurarse en Trusted Extensions 131
Atributos de seguridad que deben asignarse a los usuarios 131

11 Gestión de usuarios, derechos y roles en Trusted Extensions 135

Personalización del entorno de usuario para la seguridad 135
Gestión de usuarios y derechos 141

12 Administración remota en Trusted Extensions 147
Administración remota en Trusted Extensions 147
Métodos para administrar sistemas remotos en Trusted Extensions 148
Configuración y administración de sistemas remotos en Trusted Extensions 149

13 Gestión de zonas en Trusted Extensions 157
Zonas en Trusted Extensions 157
Procesos de la zona global y de las zonas con etiquetas 160
Zonas etiquetadas primarias y secundarias 161
Utilidades de administración de zonas en Trusted Extensions 162
Gestión de zonas 162

14 Gestión y montaje de archivos en Trusted Extensions 173
Posibilidades de montaje en Trusted Extensions 173
Políticas de Trusted Extensions para sistemas de archivos montados 174
Resultados del uso compartido y el montaje de sistemas de archivos en Trusted Extensions 177
Conjuntos de datos de varios niveles para volver a etiquetar archivos 180
Servidor NFS y configuración de cliente en Trusted Extensions 182
Software Trusted Extensions y versiones del protocolo NFS 184
Copia de seguridad, uso compartido y montaje de archivos con etiquetas 185

15 Redes de confianza 193
Acerca de la red de confianza 193
Atributos de seguridad de red en Trusted Extensions 198
Mecanismo de reserva de la red de confianza 202
Acerca del enrutamiento en Trusted Extensions 203
Administración del enrutamiento en Trusted Extensions 207
Administración de IPsec con etiquetas 210

16 Gestión de redes en Trusted Extensions 215
Etiquetado de hosts y redes 215
Configuración de rutas y puertos de varios niveles 234
Configuración de IPsec con etiquetas 237
Resolución de problemas de la red de confianza 242

17 Sobre Trusted Extensions y LDAP 251
Uso del servicio de nombres LDAP en Trusted Extensions 251
Referencia rápida para el servicio de nombres LDAP en Trusted Extensions 253

18 Sobre correo de varios niveles en Trusted Extensions 257
Servicio de correo de varios niveles 257
Funciones de correo de Trusted Extensions 257

19 Gestión de impresión con etiquetas 259
Etiquetas, impresoras e impresión 259
Gestión de impresión en Trusted Extensions 269
Configuración de impresión con etiquetas 269
Reducción de las restricciones de impresión en Trusted Extensions 276

20 Acerca de los dispositivos en Trusted Extensions 281
Protección de los dispositivos con el software Trusted Extensions 281
Interfaz gráfica de usuario Device Manager 283
Aplicación de la seguridad de los dispositivos en Trusted Extensions 285
Dispositivos en Trusted Extensions (referencia) 286

21 Gestión de dispositivos para Trusted Extensions 287
Control de dispositivos en Trusted Extensions 287
Mapa de tareas de uso de dispositivos en Trusted Extensions 287
Gestión de dispositivos en Trusted Extensions 288
Personalización de autorizaciones para dispositivos en Trusted Extensions 296

22 Trusted Extensions y la auditoría 303
Auditoría en Trusted Extensions 303
Gestión de auditoría por roles en Trusted Extensions 303
Referencia de auditoría de Trusted Extensions 304

23 Gestión de software en Trusted Extensions 311
Agregación de software a Trusted Extensions 311

A Política de seguridad del sitio 315
Creación y gestión de una política de seguridad 315
Política de seguridad del sitio y Trusted Extensions 316
Recomendaciones de seguridad informática 316
Recomendaciones de seguridad física 317
Recomendaciones de seguridad del personal 318
Infracciones de seguridad comunes 319
Referencias de seguridad adicionales 319
Publicaciones del gobierno de los Estados Unidos 320
Publicaciones de UNIX 320
Publicaciones sobre seguridad informática general 321

B Lista de comprobación de configuración de Trusted Extensions 323
Lista de comprobación para la configuración de Trusted Extensions 323

C Referencia rápida a la administración de Trusted Extensions 327
Interfaces administrativas en Trusted Extensions 327
Interfaces de Oracle Solaris ampliadas por Trusted Extensions 328
Valores predeterminados de seguridad que brindan mayor protección en Trusted Extensions 329
Opciones limitadas en Trusted Extensions 329

D Lista de las páginas del comando man de Trusted Extensions 331
Páginas del comando man de Trusted Extensions en orden alfabético 331
Páginas del comando man de Oracle Solaris modificadas por Trusted Extensions 337

Glosario 341

Índice 349

Lista de figuras

FIGURA 1-1 Administración de un sistema Trusted Extensions: división de tareas por rol 27

FIGURA 6-1 Escritorio de varios niveles de Trusted Extensions 94

FIGURA 15-1 Rutas y entradas de la tabla de enrutamiento típicas de Trusted Extensions 209

FIGURA 19-1 Página de carátula típica de un trabajo de impresión con etiquetas 263

FIGURA 19-2 Diferencias en una página de ubicador 264

FIGURA 19-3 Etiqueta del trabajo impresa en la parte superior y en la parte inferior de una página del cuerpo 265

FIGURA 19-4 Etiqueta del trabajo impresa en modo vertical cuando la página del cuerpo se imprime en modo horizontal 266

FIGURA 20-1 Device Manager abierto por un usuario 284

FIGURA 22-1 Estructuras típicas de registros de auditoría en un sistema con etiquetas 305

Lista de tablas

TABLA 1-1 Plantillas de host predeterminadas en Trusted Extensions 21

TABLA 1-2 Valores predeterminados de seguridad de Trusted Extensions para las cuentas de usuario 25

TABLA 4-1 Configuración de la zona global en Trusted Extensions 39

TABLA 4-2 Creación de zonas con etiquetas 44

TABLA 4-3 Mapa de tareas de configuración de las interfaces de red en Trusted Extensions 50

TABLA 4-4 Mapa de tareas de creación de roles y usuarios en Trusted Extensions 56

TABLA 4-5 Mapa de tareas adicionales de configuración de Trusted Extensions 67

TABLA 5-1 Mapa de tareas de configuración de LDAP en una red de Trusted Extensions 75

TABLA 5-2 Mapa de tareas de configuración de un servidor proxy LDAP en un sistema Trusted Extensions 76

TABLA 6-1 Ejemplos de relaciones de etiquetas 96

TABLA 7-1 Herramientas administrativas de Trusted Extensions 101

TABLA 8-1 Condiciones para mover archivos a una etiqueta nueva 113

TABLA 8-2 Condiciones para mover selecciones a una etiqueta nueva 113

TABLA 9-1 Inicio de sesión y uso del escritorio de Trusted Extensions 117

TABLA 9-2 Realización de tareas administrativas comunes en Trusted Extensions (mapa de tareas) 119

TABLA 10-1 Valores predeterminados de seguridad de Trusted Extensions en el archivo `policy.conf` 131

TABLA 10-2 Atributos de seguridad que se asignan después la creación del usuario 131

TABLA 11-1 Mapa de tareas de personalización del entorno de usuario para la seguridad 135

TABLA 11-2 Mapa de tareas de gestión de usuarios y derechos 141

TABLA 12-1 Mapa de tareas de configuración y administración de sistemas remotos en Trusted Extensions 149

TABLA 13-1 Mapa de tareas de gestión de zonas 162

TABLA 14-1 Copia de seguridad, uso compartido y montaje de archivos con etiquetas (mapa de tareas) 185

TABLA 15-1 Entradas del mecanismo de reserva y la dirección de host de Trusted Extensions 202
TABLA 16-1 Mapa de tareas de configuración de IPsec con etiquetas 238
TABLA 16-2 Mapa de tareas de resolución de problemas de la red de confianza 242
TABLA 19-1 Diferencias entre CUPS y LP 260
TABLA 19-2 Valores configurables en el archivo `tsol_separator.ps` 267
TABLA 19-3 Mapa de tareas de configuración de impresión con etiquetas 269
TABLA 19-4 Mapa de tareas de reducción de las restricciones de impresión en Trusted Extensions 276
TABLA 21-1 Mapa de tareas de control de dispositivos en Trusted Extensions 287
TABLA 21-2 Mapa de tareas de uso de dispositivos en Trusted Extensions 288
TABLA 21-3 Mapa de tareas de gestión de dispositivos en Trusted Extensions 288
TABLA 21-4 Mapa de tareas de personalización de autorizaciones para dispositivos en Trusted Extensions 296
TABLA 22-1 Tokens de auditoría de Trusted Extensions 306

Uso de esta documentación

- **Descripción general**: describe cómo activar, configurar y mantener la función de Trusted Extensions de Oracle Solaris en uno o varios sistemas.
- **Destinatarios**: administradores del sistema de redes y sistemas con etiquetas.
- **Conocimiento requerido**: etiquetas de seguridad y requisitos de seguridad del sitio.

Biblioteca de documentación del producto

En la biblioteca de documentación, que se encuentra en http://www.oracle.com/pls/topic/lookup?ctx=E56339, se incluye información de última hora y problemas conocidos para este producto.

Acceso a My Oracle Support

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

Comentarios

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

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 instalación y activación 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 Trusted Extensions en uno o varios sistemas Oracle Solaris.

Capítulo 2, Guía básica de configuración de Trusted Extensions: proporciona mapas de tareas para diversas configuraciones de Trusted Extensions en los sistemas Oracle Solaris.

Capítulo 3, Agregación de la función Trusted Extensions a Oracle Solaris: proporciona instrucciones sobre la preparación de un sistema Oracle Solaris para Trusted Extensions. Describe cómo activar Trusted Extensions y cómo iniciar sesión.

Capítulo 4, Configuración de Trusted Extensions: proporciona instrucciones para la configuración de Trusted Extensions en un sistema con un monitor.

Capítulo 5, Configuración de LDAP para Trusted Extensions: proporciona instrucciones para configurar el 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.

- "Novedades de Trusted Extensions en Oracle Solaris 11.2" [17]
- "Planificación de la seguridad en Trusted Extensions" [18]
- "Resultados de la activación de Trusted Extensions desde la perspectiva de un administrador" [28]

Novedades de Trusted Extensions en Oracle Solaris 11.2

En esta sección, se resalta la información para clientes existentes sobre las nuevas funciones importantes de Trusted Extensions de esta versión.

- Trusted Extensions se puede instalar y configurar sin reiniciar. Para obtener más información, consulte la página del comando man `labeladm`(1M). Para conocer el procedimiento, consulte Activación de Trusted Extensions [36].
- Puede instalar un archivo de codificaciones de etiqueta personalizado antes de iniciar Trusted Extensions. Para obtener más información, consulte la página del comando man `labeladm`(1M). Para ver ejemplos y procedimientos, consulte Cómo comprobar e instalar el archivo de codificaciones de etiquetas [40].
- Trusted Extensions puede utilizar el juego de roles estandarizado de roles de autorización gestionados en RBAC (ARMOR) del paquete `armor`. Para obtener más información sobre ARMOR y otras funciones de seguridad nuevas de Oracle Solaris, consulte "Novedades de los derechos en Oracle Solaris 11.2" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".
- El comando `txzonemgr` se ejecuta de forma más rápida y fiable para asignaciones de interfaz de red.

Planificación de la seguridad en Trusted Extensions

En esta sección, se describe la planificación que se necesita antes de activar y configurar el software Trusted Extensions.

- "Comprensión de Trusted Extensions" [18]
- "Comprensión de la política de seguridad del sitio" [19]
- "Planificación de quién configurará Trusted Extensions" [19]
- "Diseño de una estrategia de etiqueta" [20]
- "Planificación del hardware y la capacidad del sistema para Trusted Extensions " [20]
- "Planificación de la red de confianza" [21]
- "Planificación de zonas etiquetadas en Trusted Extensions" [22]
- "Planificación de los servicios de varios niveles" [24]
- "Planificación del servicio de nombres LDAP en Trusted Extensions" [24]
- "Planificación de la auditoría en Trusted Extensions" [25]
- "Planificación de la seguridad del usuario en Trusted Extensions" [25]
- "Formación de un equipo de instalación para Trusted Extensions" [26]
- "Resolución de problemas adicionales antes de activar Trusted Extensions" [28]
- "Realización de copia de seguridad del sistema antes de activar Trusted Extensions" [28]

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" [20]. Si está interesado en la ejecución de una configuración evaluada, consulte "Comprensión de la política de seguridad del sitio" [19].

Comprensión de Trusted Extensions

La activación 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 `root` son gestionadas por varios roles administrativos.
- 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 cuenta con la certificación que acredita que cumple con el acuerdo de reconocimiento de criterios comunes (CCRA) con un nivel de seguridad EAL4+ en los siguientes perfiles de protección:

- Gestión avanzada
- Identificación y autenticación extendidas
- Seguridad con etiquetas
- Virtualización

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

Planificación de quién configurará Trusted Extensions

El rol `root` o el rol de administrador del sistema es el responsable de activar 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`.

La planificación de etiquetas también implica la planificación de la configuración de etiquetas. Después de activar 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 como un usuario 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 Oracle Solaris, como se describe en "Instalación de sistemas Oracle Solaris 11.2 " 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 para planificar el hardware de red, consulte "Planificación de la implementación de red en Oracle Solaris 11.2 ".

El software de Trusted Extensions reconoce cuatro tipos de host. Cada tipo de host tiene una plantilla de seguridad predeterminada, como se muestra en la Tabla 1-1, "Plantillas de host predeterminadas en Trusted Extensions".

TABLA 1-1 Plantillas de host predeterminadas en Trusted Extensions

Tipo de host	Nombre de la plantilla	Finalidad
`unlabeled`	`admin_low`	Identifica los host que no son de confianza que pueden comunicarse con la zona global. Estos hosts envían paquetes que no incluyen etiquetas. Para obtener más información, consulte sistema sin etiquetas.
`cipso`	`cipso`	Identifica los hosts o las redes que envían paquetes CIPSO. Los paquetes CIPSO tienen etiquetas.
`netif`	`netif`	Identifica los hosts que reciben paquetes en una interfaz de red específica de hosts `adaptive`.
`adaptive`	`adapt`	Identifica los hosts o las redes que no tienen etiquetas, pero envían paquetes sin etiquetas a una interfaz específica en un host `netif`.

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. La asignación de etiquetas a sistemas remotos se realiza después de la configuración inicial.

Planificación de zonas etiquetadas 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 o varias zonas etiquetadas para cada etiqueta única, aunque no es necesario crear una zona para cada 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 etiquetadas, los usuarios comunes pueden utilizar el sistema configurado, pero estos usuarios no pueden acceder a otros sistemas. Para aislar aún más los servicios que se ejecutan en la misma etiqueta, puede crear zonas secundarias. Para obtener más información, consulte “Zonas etiquetadas primarias y secundarias” [161].

- 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 zonas, 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 por el proceso. La secuencia de comandos tiene varias opciones de línea de comandos para automatizar la creación de zonas con etiquetas. Para obtener más información, consulte la página del comando man `txzonemgr`(1M).

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`.

Aplicaciones restringidas a una zona etiquetada

De manera predeterminada, las zonas etiquetadas comparten el servicio de nombres de la zona global y tienen copias de sólo lectura de los archivos de configuración de la zona global, incluidos los archivos `/etc/passwd` and `/etc/shadow`. Si planea instalar aplicaciones en una zona etiquetada desde la zona etiquetada y el paquete agrega usuarios a la zona, necesitará copias modificables de los archivos de la zona.

Los paquetes como `pkg:/service/network/ftp` crean cuentas de usuario. Para instalar este paquete ejecutando el comando `pkg` dentro de una zona etiquetada, debe haber un daemon `nscd` independiente ejecutándose en la zona y se debe asignar a la zona una dirección IP exclusiva. Para obtener más información, consulte Cómo configurar un servicio de nombres independiente para cada zona con etiquetas [54].

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.

Sugerencia - 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 Oracle Directory Server Enterprise Edition (servidor LDAP) 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.

Planificación de la auditoría en Trusted Extensions

De manera predeterminada, la auditoría está activada. 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” [56].

La planificación de la auditoría en Trusted Extensions es igual que en SO Oracle Solaris. Para obtener más información, consulte “Gestión de auditoría en Oracle Solaris 11.2 ”. 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 agregaciones de Trusted Extensions a la auditoría, consulte el Capítulo 22, Trusted Extensions y la auditoría.

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, “Valores predeterminados de seguridad de Trusted Extensions para las cuentas de usuario”. 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 de archivo	Palabra clave	Valor
`/etc/security/policy.conf`	`IDLECMD`	`lock` | `logout`
	`IDLETIME`	`15`
	`CRYPT_ALGORITHMS_ALLOW`	`1,2a,md5,5,6`
	`CRYPT_DEFAULT`	`5` (`sha256`)
	`LOCK_AFTER_RETRIES`	`no` | `yes`
	`PRIV_DEFAULT`	`basic`

Nombre de archivo	Palabra clave	Valor
	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	Acreditación de usuario predeterminada	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 vigentes 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.

Formación de un equipo de instalación 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 activa el software. En una fase temprana del proceso de configuración, este equipo crea roles administrativos y usuarios de confianza que pueden 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 administrativo. 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, “Administración de un sistema Trusted Extensions: división de tareas por rol”.
- Una persona activa 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.

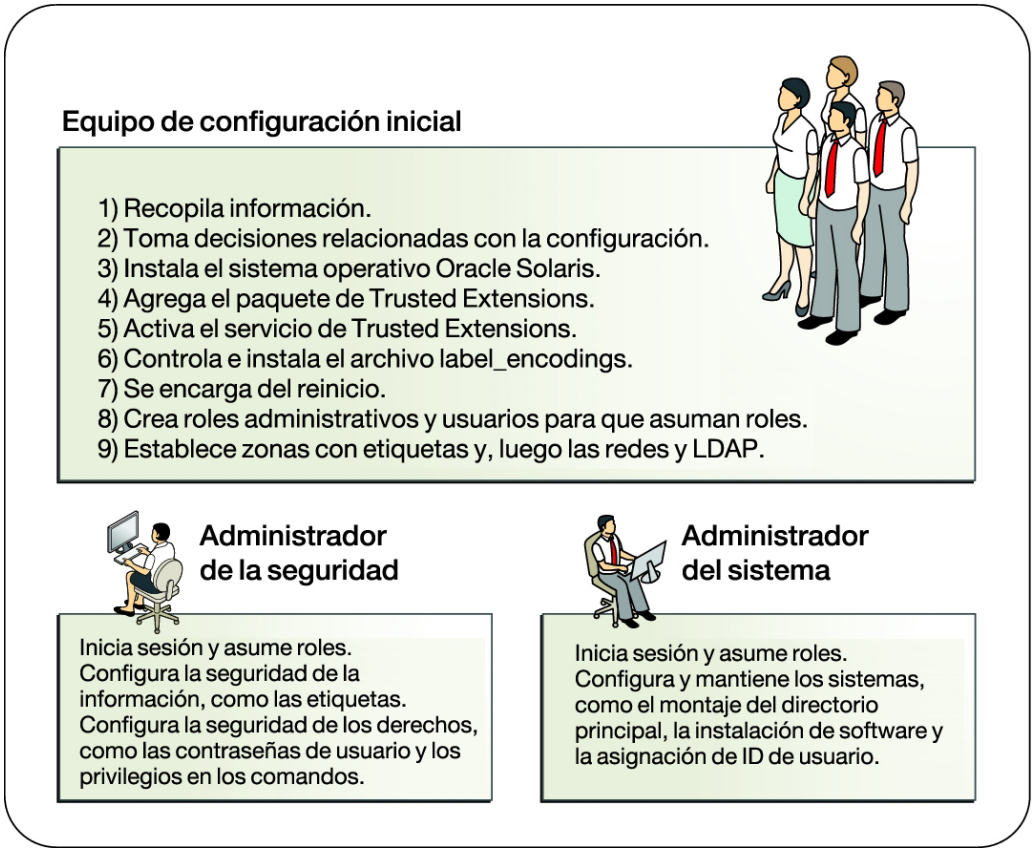
- Una persona asume el rol de usuario `root` para activar y configurar el software. El proceso de configuración no es auditado.

  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 activar 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 pasos, consulte “Resolución de problemas de seguridad antes de instalar Trusted Extensions” [33].

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

Si el sistema tiene archivos que se deben guardar, realice una copia de seguridad antes de activar 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 activación de Trusted Extensions desde la perspectiva de un administrador

Una vez que se haya activado el software Trusted Extensions y que se haya reiniciado el sistema de manera opcional, 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.
- 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.
- Los dispositivos se deben asignar para su uso.
- Si instala el sistema de ventanas, el software crea un escritorio de confianza, Solaris Trusted Extensions (GNOME). Este entorno de ventanas con etiquetas proporciona espacios de trabajo administrativos en la zona global. Estos espacios de trabajo están protegidos por Trusted Path, visible en la banda de confianza.

  Además, Trusted Extensions proporciona las interfaces gráficas de usuario para administrar el sistema. Para obtener una lista, consulte el Capítulo 7, Herramientas de administración de Trusted Extensions.

♦ ♦ ♦ CAPÍTULO 2

Guía básica de configuración de Trusted Extensions

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

Atención - Si desea activar y configurar Trusted Extensions de manera remota, lea atentamente el Capítulo 12, Administración remota en Trusted Extensions antes de iniciar el entorno Trusted Extensions.

Mapa de tareas: preparación y activación de Trusted Extensions

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

Tarea	Para obtener instrucciones
Reunir información y tomar decisiones relacionadas con el sistema y la red de Trusted Extensions.	"Resolución de problemas de seguridad antes de instalar Trusted Extensions" [33]
Activar Trusted Extensions.	Activación de Trusted Extensions [36]

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” [30]
Crear un sistema Trusted Extensions empresarial.	“Mapa de tareas: configuración de Trusted Extensions para cumplir los requisitos del sitio” [30]
Configurar Trusted Extensions en un sistema remoto.	Active Trusted Extensions sin reiniciar. Siga las instrucciones descritas en el Capítulo 12, Administración remota en Trusted Extensions. Luego, continúe con las instrucciones para sistemas con monitores.
Configurar Trusted Extensions en un servidor Sun Ray de Oracle.	Consulte el sitio web Sun Ray Products Documentation (http://www.oracle.com/technetwork/server-storage/sunrayproducts/docs/index.html). Para configurar comunicaciones iniciales de cliente-servidor, consulte “Etiquetado de hosts y redes” [215].

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.	Agregación de paquetes de Trusted Extensions a un sistema Oracle Solaris [36]
Activar Trusted Extensions y reiniciar.	Activación de Trusted Extensions [36]
Conectarse.	Inicio de sesión en Trusted Extensions [37]
Crear dos zonas con etiquetas.	Cómo crear un sistema Trusted Extensions predeterminado [44] O bien, Cómo crear zonas con etiquetas de forma interactiva [45]
Crear espacios de trabajo con etiquetas para las zonas.	Cómo asignar etiquetas a dos espacios de trabajo con zonas [48]

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

Sugerencia - 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” [43] 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” [39]
Configurar las zonas con etiquetas.	“Creación de zonas con etiquetas” [43]
Configurar redes para la comunicación con otros sistemas.	“Configuración de las interfaces de red en Trusted Extensions” [49]
Configurar el servicio de nombres LDAP. **Nota -** Omita esta tarea si no se utiliza LDAP.	Capítulo 5, Configuración de LDAP para Trusted Extensions
Completar la configuración del sistema.	Administración de Trusted Extensions [89]

♦ ♦ ♦ CAPÍTULO 3

Agregación de la función Trusted Extensions a Oracle Solaris

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

- "Responsabilidades del equipo de configuración inicial" [33]
- "Resolución de problemas de seguridad antes de instalar Trusted Extensions" [33]
- "Instalación y activación de Trusted Extensions" [35]

Responsabilidades del equipo de configuración inicial

La función Trusted Extensions está diseñada para ser configurada por dos personas con distintas responsabilidades. Esta división de tareas puede aplicarse mediante roles. Como los roles administrativos y los usuarios adicionales se crean después de la instalación, se recomienda contar con un equipo de configuración inicial de, al menos, dos personas presentes para activar y configurar Trusted Extensions.

Resolución de problemas de seguridad antes de instalar 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 activar Trusted Extensions

En cada sistema en el que se va a configura Trusted Extensions, tome estas decisiones de configuración antes de activar 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 y el menú de GRUB.
   - 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 ”. Para obtener instrucciones de edición, consulte Cómo comprobar e instalar el archivo de codificaciones de etiquetas [40]. Para instalar el archivo de codificaciones después de activar Trusted Extensions y antes de reiniciar, consulte Activación de Trusted Extensions [36].

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 automática crea las zonas `public` e `internal`.

4. **Decida cuándo crear roles.**

   Es posible que la política de seguridad de su sitio requiera que usted administre Trusted Extensions mediante la asunción de un rol. Si es así, debe crear estos roles en una fase temprana del proceso de configuración. Puede crear sus propios roles, puede instalar el paquete `armor` de siete roles o puede crear roles además de los roles de ARMOR. Para obtener una descripción de los roles de ARMOR, consulte la descripción de ARMOR standard.

   Si no es necesario que configure el sistema mediante el uso de roles, puede decidir 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.

Instalación y activación de Trusted Extensions

En el SO Oracle Solaris, el servicio Trusted Extensions, `svc:/system/labeld:default`, está desactivado de manera predeterminada.

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
- Todas las comunicaciones de red
- Todos los procesos, incluidos los procesos de ventana

Agregación de paquetes de Trusted Extensions a un sistema Oracle Solaris

Antes de empezar 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: xxxxxxxx
#
```

2. **Descargue e instale los paquetes de Trusted Extensions.**

   - **Para los sistemas que ejecutan un escritorio de varios niveles, instale el siguiente paquete:**

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

   - **Para un sistema sin periféricos o un servidor que no requiere un escritorio de varios niveles, instale los paquetes siguientes:**

```
# pkg install system/trusted
# pkg install system/trusted/trusted-global-zone
```

3. **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
```

Activación de Trusted Extensions

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

1. **En una ventana de terminal, active el servicio `labeld`.**

   Nota - Utilice el comando `labeladm` para controlar el servicio `labeld`. No manipule los servicios `labeld` directamente. Para obtener más información, consulte la página del comando man `labeladm`(1M).

```
# labeladm enable -r
```

   El comando `labeladm` proporciona varias opciones al activar el servicio.

`-i`	Impide que aparezca un mensaje de confirmación.
`-m`	Envía mensajes de error a syslog y la consola.
`-n`	Prueba el comando sin activar el servicio.
`-r`	Retrasa la activación del servicio hasta después de reiniciar el sistema. Éste es el mismo comportamiento que en versiones anteriores.

2. **Compruebe que el servicio esté activado.**

```
# labeladm info
     Labeling status: pending enable on boot
          Latest log: "/var/user/root/trusted-extensions-install-log"
Label encodings file: /etc/security/tsol/label_encodings
```

Atención - Si desea activar y configurar Trusted Extensions de manera remota, lea atentamente el Capítulo 12, Administración remota en Trusted Extensions. 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.

3. **Si tiene un archivo de codificaciones de etiquetas personalizado, instálelo ahora.**

```
# labeladm encodings path-to-encodings-file
```

4. **Reinicie el sistema.**

Debe ejecutar este comando si ha utilizado la opción `-r`.

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

Pasos siguientes Continúe con Inicio de sesión en Trusted Extensions [37].

▼ 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 Activación de Trusted Extensions [36].

- **Inicie sesión con la cuenta de usuario que creó durante la instalación de Oracle Solaris.**

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

  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. Trusted Extensions ofrece protección contra contraseñas inseguras, pero no puede evitar que un usuario divulgue su contraseña o la escriba.

  - **Si no instaló los paquetes de escritorio, abra un terminal y asuma el rol `root`.**
  - **Si ha instalado los paquetes de escritorio, realice los siguientes pasos.**

    a. **Utilice el mouse para cerrar la ventana Status y la ventana Clearance.**

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

       Cree la zona después de asumir el rol `root`.

    c. **Para asumir el rol `root` haga clic en el nombre de inicio de sesión en la banda de confianza.**

       Seleccione el rol `root` en el menú desplegable.

Consideraciones de seguridad

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 la zona global, vaya a “Configuración de la zona global en Trusted Extensions” [39].
- Para configurar un sistema predeterminado, vaya a “Creación de zonas con etiquetas” [43].
- Si el sistema no tiene una pantalla gráfica, vuelva al Capítulo 12, Administración remota en Trusted Extensions.

♦ ♦ ♦ CAPÍTULO 4

Configuración de Trusted Extensions

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.

- "Configuración de la zona global en Trusted Extensions" [39]
- "Creación de zonas con etiquetas" [43]
- "Creación de roles y usuarios en Trusted Extensions" [56]
- "Creación de directorios principales centralizados en Trusted Extensions" [63]
- "Resolución de los problemas de configuración de Trusted Extensions" [66]
- "Tareas adicionales de configuración de Trusted Extensions" [67]

Para otras tareas de configuración, consulte la Administración de Trusted Extensions [89].

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" [43].

TABLA 4-1 Configuración de la zona global en Trusted Extensions

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" de "Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 "
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 [40]
Configurar una red IPv6.	Permite la compatibilidad con una red CIPSO IPv6 de Trusted Extensions.	Cómo configurar una red CIPSO IPv6 en Trusted Extensions [42]
Cambiar el dominio de interpretación.	Se especifica un dominio de interpretación (DOI) diferente de `1`.	Cómo configurar un dominio de interpretación diferente [43]

Tarea	Descripción	Para obtener instrucciones
Configurar el servidor LDAP.	Se configura un servidor de directorios LDAP de Trusted Extensions.	Capítulo 5, Configuración de LDAP para Trusted Extensions
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 [86]

▼ 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.

Atención - 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 [73].

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” de “Trusted Extensions Label Administration ”.

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

  `# labeladm encodings` *full-pathname-of-label-encodings-file*

Atención - 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 /tmp/encodings/label_encodings1
No errors found in /tmp/encodings/label_encodings1
# /usr/sbin/chk_encodings /tmp/encodings/label_encodings2
No errors found in /tmp/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 /tmp/encodings/label_encodings2
No errors found in /tmp/encodings/label_encodings2

---> VERSION = MYCOMPANY LABEL ENCODINGS  3.0 10/10/2013

---> 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 el archivo y, a continuación, instala el archivo.

```
# labeladm encodings /tmp/encodings/label_encodings2
```

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

```
# labeladm
     Labeling status: disabled
          Latest log: ""
Label encodings file: /var/tsol/encodings/label-encodings-file
# /usr/sbin/chk_encodings -a /var/tsol/encodings/label-encodings-file | head -4
No errors found in /var/tsol/encodings/label-encodings-file

---> VERSION = MYCOMPANY LABEL ENCODINGS  3.0 10/10/2013
```

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

▼ Cómo configurar una red CIPSO IPv6 en Trusted Extensions

Para IPv6, Trusted Extensions utiliza la opción de seguridad de IPv6 de etiquetas de arquitectura común (CALIPSO) como el protocolo de etiquetado de seguridad. No es necesario realizar ninguna configuración. Si debe comunicarse con sistemas que ejecutan el protocolo CIPSO IPv6 obsoleto de Trusted Extensions, realice el siguiente procedimiento. Para comunicarse con otros sistemas CALIPSO, no realice este procedimiento.

Atención - Un sistema que utiliza CALIPSO para el protocolo IPv6 no se puede comunicar con ningún sistema que use el protocolo CIPSO IPv6 TX obsoleto porque estos protocolos son incompatibles.

Las opciones CIPSO IPv6 obsoletas de Trusted Extensions no tienen un número de la Autoridad de números asignados de Internet (IANA) para utilizar en el campo de tipo de opción IPv6 de un paquete. La entrada establecida en este procedimiento proporciona un número para utilizar en la red local.

Antes de empezar Realice este procedimiento si debe comunicarse con sistemas que utilizan la opción exclusiva, pero obsoleta, de etiqueta de seguridad de CIPSO IPv6 de Trusted Extensions.

Debe estar con 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 CIPSO IPv6 es incorrecta, corrija la entrada. Por ejemplo, una entrada escrita de manera incorrecta origina el

siguiente mensaje: `sorry, variable 'ip6opt_1d' is not defined in the 'ip' module. Verify that the entry is spelled correctly.`

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

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

▼ Cómo configurar un dominio de interpretación diferente

Si su sitio no utiliza un dominio de interpretación (DOI) de `1`, debe modificar el valor `doi` en cada plantilla de seguridad. Para obtener más información, consulte “Dominio de interpretación en plantillas de seguridad” [201].

Antes de empezar Debe estar con 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” [198]
- Cómo crear plantillas de seguridad [218]

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

De lo contrario, continúe con “Creación de zonas con etiquetas” [43].

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. Debe configurar LDAP antes de crear zonas con etiquetas.

TABLA 4-2 Creación de 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`. Este comando se puede ejecutar en un sistema que no tiene un escritorio.	Cómo crear un sistema Trusted Extensions predeterminado [44]
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 [45]
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 [45]
Crear una zona con etiquetas con los comandos de zonas.	Crea una zona con etiquetas. Este procedimiento se puede ejecutar en un sistema que no tiene un escritorio.	Cómo crear zonas con etiquetas mediante el comando `zonecfg` [49]
2. Crear un entorno con etiquetas activo.	En la configuración predeterminada, se etiquetan dos espacios de trabajo como `PUBLIC` y `INTERNAL USE ONLY`. Este procedimiento funciona sólo en un sistema de escritorio.	Cómo asignar etiquetas a dos espacios de trabajo con zonas [48]
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" [49]

▼ 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 Está en la zona global en un sistema que no tiene un escritorio o ha iniciado sesión en el escritorio al completar Inicio de sesión en Trusted Extensions [37]. Ha asumido el rol de usuario `root`.

1. **Abra una ventana de terminal.**
   En un escritorio, puede utilizar 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 acceder a una zona con etiquetas de Trusted Extensions desde un espacio de trabajo, vaya a Cómo asignar etiquetas a dos espacios de trabajo con zonas [48].

▼ Cómo crear zonas con etiquetas de forma interactiva

No es necesario que cree una zona para cada 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 [37]. 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.

Sugerencia - 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 [44] o en Cómo crear zonas con etiquetas de forma interactiva [45].

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.**
   Está 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.**
   Está en un espacio de trabajo `INTERNAL`.

6. **Abra una ventana de terminal.**
   La ventana tiene la etiqueta `CONFIDENTIAL : INTERNAL USE ONLY`.

El sistema está listo para usarse. 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" [49].

▼ Cómo crear zonas con etiquetas mediante el comando `zonecfg`

Si no está en un escritorio, debe crear zonas con etiquetas mediante comandos de zona comunes. Si está en un escritorio, también puede utilizar este método. La opción `-t` especifica la marca de la zona, y la etiqueta se debe definir de forma explícita. Para obtener más información, consulte la página del comando man `brands`(5).

1. **Ejecute el comando `zonecfg` para crear una zona con etiquetas.**

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

   En este ejemplo se crea una zona cuyo nombre es `public`.

   ```
   # zonecfg -t SYStsoldef -z public
   ```

2. **Establezca la etiqueta con el comando `tncfg`.**

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

   En este ejemplo se etiqueta la zona `public` con la etiqueta `public`.

   ```
   # tncfg -z public set label=PUBLIC
   ```

3. **Instale la zona con el comando `zoneadm`.**

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

   ```
   # zoneadm -z public install
   ```

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” [23]. En el siguiente mapa de tareas, se describen las tareas de configuración de red y se incluyen enlaces a ellas.

TABLA 4-3 Mapa de tareas de configuración de las interfaces de red en Trusted Extensions

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 [50]
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 [50]
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 [51]
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 [51]
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 [52]
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 [53]
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 [54]

▼ 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 [45].

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 [53].

▼ 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 [45]. 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 [53].

▼ 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 [45]. 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 *zonename_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 [53].

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

En este procedimiento, se define la red de Trusted Extensions mediante la agregación 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 [45]. 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
- "Etiquetado de hosts y redes" [215]

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

Este procedimiento permite configurar un daemon de servicio de nombres independiente (`nscd`) en cada zona con etiquetas. 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. En una zona etiquetada, si tiene la intención de instalar paquetes que requieren una cuenta de usuario en esa etiqueta, puede configurar un servicio de nombres independiente por zona. Para obtener información general, consulte "Aplicaciones restringidas a una zona etiquetada" [23] and "Decisiones que deben tomarse antes de crear usuarios en Trusted Extensions" [129].

Antes de empezar Aparece Labeled Zone Manager. Para abrir esta interfaz gráfica de usuario, consulte Cómo crear zonas con etiquetas de forma interactiva [45]. 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
   ```

   Tras el reinicio, la cuenta del usuario que asumió el rol `root` para ejecutar el gestor de zonas etiquetadas en el Paso 1 está configurada en cada zona. Otras cuentas que son específicas de una zona etiquetada se deben agregar manualmente a la zona.

   Nota - Las cuentas que están almacenadas en el repositorio LDAP siguen siendo gestionadas desde la zona global.

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, 2012  10:10:12 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 caché 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.

TABLA 4-4 Mapa de tareas de creación de roles y usuarios en Trusted Extensions

Tarea	Descripción	Para obtener instrucciones
Instalar los roles de ARMOR.	Crea siete roles definidos por el estándar ARMOR y los asigna.	Primer ejemplo en “Creación de roles” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”
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 [56]
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 [58]
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 [58]
Verificar que los roles puedan realizar sus tareas.	Se prueban los roles.	Cómo verificar que los roles de Trusted Extensions funcionan [61]
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 [62]

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

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

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

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

Nota - Para utilizar los roles de ARMOR, consulte el ejemplo de ARMOR en la sección "Creación de roles" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

Utilice la siguiente información como guía:

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

  No proporcione información de propiedad exclusiva.
- `-m` *home-directory*
- `-u` *role-UID*
- `-S` *repository*
- `-K` *key=value*

  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 de los comandos administrativos, 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 audit_flags=cusa:no secadmin
```

2. Proporcione una contraseña inicial para el rol.

```
# passwd -r files secadmin
New Password: xxxxxxxx
Re-enter new Password: xxxxxxxx
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 repositorio 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=cusa:no secadmin
```

El administrador proporciona una contraseña inicial para el rol.

```
# passwd -r ldap secadmin
New Password: xxxxxxxx
Re-enter new Password: xxxxxxxx
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 [58].

▼ Cómo crear un rol de administrador del sistema

Antes de empezar Debe estar con 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=cusa:no\
-K profiles="System Administrator" -K lock_after_retries=no sysadmin
```

2. **Proporcione una contraseña inicial para el rol.**

```
# passwd -r files sysadmin
New Password: xxxxxxxx
Re-enter new Password: xxxxxxxx
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`. Sólo el rol `root` puede definir indicadores de auditoría por usuario.

   ```
   # 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” [130].

3. **Asigne una contraseña de seis caracteres alfanuméricos como mínimo.**

   ```
   # passwd jdoe
   New Password: xxxxxxxx
   Re-enter new Password: xxxxxxxx
   ```

   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 sin etiquetas, iniciar sesión de manera remota y apagar el sistema. Para crear el perfil, consulte Cómo crear perfiles de derechos para autorizaciones convenientes [143].

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

      Consulte “Personalización del entorno de usuario para la seguridad” [135].

   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`” [133].

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, “Valores predeterminados de seguridad de Trusted Extensions para las cuentas de usuario” y crea el usuario. El administrador coloca el directorio de inicio del usuario en `/export/home1` en lugar del directorio predeterminado `/export/home`.

```
# useradd -c "Local user for Security Admin" -d /export/home1/jandoe -K
 audit_flags=lo,ex:no \
-K  idletime=8 -K idlecmd=lock -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: xxxxxxxx
Re-enter new Password: xxxxxxxx
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 [56].

```
# 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 un sistema que no está ejecutando un escritorio de varios niveles, abra una ventana de terminal.**

     a. **Cambie de rol.**

     ```
     % su - rolename
     ```

     b. **Verifique que el indicador `PRIV_PFEXEC` esté vigente.**

     ```
     # ppriv $$
     ...
     flags = PRIV_PFEXEC
     ...
     ```

   - **En un escritorio de varios niveles, 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 obtener información sobre las autorizaciones 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 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 activar el acceso a directorios principales en cada etiqueta para los usuarios.

▼ Cómo crear el servidor de directorio principal en Trusted Extensions

Antes de empezar Debe estar con 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 [189]. 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 [65].

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 tener el rol `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 - Si ha movido los paneles de escritorio a la parte superior de la pantalla, la banda de confianza de Trusted Extensions los cubre. Los paneles deben 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 solamente para el inicio de sesión, edite el archivo `top_panel_screen`*n* en el directorio de inicio.**

     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 siguientes tareas pueden ser útiles para configurar un sistema Trusted Extensions según sus necesidades. La tarea final permite eliminar la función Trusted Extensions de un sistema Oracle Solaris.

TABLA 4-5 Mapa de tareas adicionales de configuración de Trusted Extensions

Tarea	Descripción	Para obtener instrucciones
Informar a los usuarios sobre la seguridad del sitio.	Muestra un mensaje de seguridad durante el inicio de sesión.	"Cómo insertar un mensaje de seguridad en archivos de banner" de "Directrices de seguridad de Oracle Solaris 11 " "Cómo insertar un mensaje de seguridad en la pantalla de inicio de sesión del escritorio" de "Directrices de seguridad de Oracle Solaris 11 "
Crear una zona etiquetada que contiene un servicio	Crea una zona secundaria en la misma etiqueta que la zona primaria.	Cómo crear una segunda etiquetada secundaria [68]

Tarea	Descripción	Para obtener instrucciones
que funciona en la misma etiqueta como una zona existente.		
Crear un conjunto de datos para alojar directorios y archivos en todas las etiquetas.	Crea y monta un conjunto de datos donde los archivos se puedan volver a etiquetar con una carga mínima.	Cómo crear y compartir un conjunto de datos de varios niveles [69]
Crear un servidor de directorio raíz en cada etiqueta.	Crea varios servidores de directorios raíz, uno para cada etiqueta. O crea un servidor de directorio raíz de varios niveles.	Cómo crear el servidor de directorio principal en Trusted Extensions [63]
Crear usuarios iniciales que pueden asumir roles.	Crea usuarios de confianza para administrar el sistema cuando asuman un rol.	Cómo crear usuarios que puedan asumir roles en Trusted Extensions [58]
Eliminar Trusted Extensions.	Elimina Trusted Extensions y todos los datos de confianza del sistema. También prepara el sistema Oracle Solaris para ejecutar Trusted Extensions.	Cómo eliminar Trusted Extensions del sistema [74]

▼ Cómo crear una segunda etiquetada secundaria

Las zonas etiquetadas secundarias son útiles para aislar servicios en diferentes zonas y permiten que los servicios se ejecuten en la misma etiqueta. Para obtener más información, consulte “Zonas etiquetadas primarias y secundarias” [161].

Antes de empezar La zona primary debe existir. La zona secundaria debe tener una dirección IP exclusiva y no puede requerir un escritorio.

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

1. **Cree una zona secundaria.**

   Puede utilizar la línea de comandos o la interfaz gráfica de usuario de la zona etiquetada, `txzonemgr`.

   - **Use la línea de comandos.**

     ```
     # tncfg -z secondary-label-service primary=no
     # tncfg -z secondary-label-service label=public
     ```

   - **Use `txzonemgr`.**

     ```
     # txzonemgr &
     ```

     Navegue hasta la opción para crear una zona nueva y siga las indicaciones.

Nota - La máscara de red se debe introducir con un prefijo. Por ejemplo, el equivalente de prefijo de la máscara de red `255.255.254.0` es `/23`.

2. **Verifique que la zona sea una zona secundaria.**

```
# tncfg -z zone info primary
primary=no
```

ejemplo 4-6 Creación de una zona para secuencias de comandos públicos

En este ejemplo, el administrador aísla una zona pública que está diseñada para ejecutar secuencias de comandos y trabajos por lotes.

```
# tncfg -z public-scripts primary=no
# tncfg -z public-scripts label=public
```

▼ Cómo crear y compartir un conjunto de datos de varios niveles

Los conjuntos de datos de varios niveles son contenedores útiles al degradar o actualizar información. Para obtener más información, consulte “Conjuntos de datos de varios niveles para volver a etiquetar archivos” [180]. Los conjuntos de datos de varios niveles también son útiles para servidores de archivos NFS de varios niveles a fin de proporcionar archivos en muchas etiquetas para varios clientes NFS.

Antes de empezar Para crear un conjunto de datos de varios niveles, debe tener el rol `root` en la zona global.

1. **Cree un conjunto de datos de varios niveles.**

```
# zfs create -o mountpoint=/multi -o multilevel=on rpool/multi
```

`rpool/multi` es un conjunto de datos de varios niveles montado en la zona global en `/multi`.

Para limitar el rango de etiquetas superior del conjunto de datos, consulte el Ejemplo 4-7, “Creación de un conjunto de datos de varios niveles con una etiqueta superior por debajo de `ADMIN_HIGH`”.

2. **Verifique que el conjunto de datos de varios niveles esté montado y que el punto de montaje tenga la etiqueta `ADMIN_LOW`.**

```
# getlabel /multi
/multi: ADMIN_LOW
```

3. **Proteja el sistema de archivos principal.**

Defina las siguientes propiedades ZFS en `off` para todos los sistemas de archivos de la agrupación:

```
# zfs set devices=off rpool/multi
```

```
# zfs set exec=off rpool/multi
# zfs set setuid=off rpool/multi
```

4. **(Opcional) Defina la propiedad de compresión de la agrupación.**

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

   ```
   # zfs set compression=on rpool/multi
   ```

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

5. **Cree directorios de nivel superior para cada etiqueta que desea en el conjunto de datos de varios niveles.**

   ```
   # cd /multi
   # mkdir public internal
   # chmod 777 public internal
   # setlabel PUBLIC public
   # setlabel "CNF : INTERNAL" internal
   ```

6. **Utilice LOFS para montar el conjunto de datos de varios niveles en cada zona etiquetada aprobada para tener acceso.**

   Por ejemplo, la siguiente serie de comandos `zonecfg` monta el conjunto de datos en la zona `public`.

   ```
   # zonecfg -z public
   zonecfg:public> add fs
   zonecfg:public:fs> set dir=/multi
   zonecfg:public:fs> set special=/multi
   zonecfg:public:fs> set type=lofs
   zonecfg:public:fs> end
   zonecfg:public> exit
   ```

   Los conjuntos de datos de varios niveles permiten la escritura de archivos en la misma etiqueta que la zona de montaje y la lectura de archivos de nivel inferior. La etiqueta de los archivos montados se puede ver y definir.

7. **Para utilizar NFS para compartir el conjunto de datos de varios niveles con otros sistemas, haga lo siguiente:**

   a. **Convierta el servicio NFS en la zona global en un servicio de varios niveles.**

      ```
      # tncfg -z global add mlp_private=2049/tcp
      # tncfg -z global add mlp_private=111/udp
      # tncfg -z global add mlp_private=111/tcp
      ```

   b. **Reinicie el servicio NFS.**

```
# svcadm restart nfs/server
```

c. Comparta el conjunto de datos de varios niveles.

```
# share /multi
```

Los conjuntos de datos de varios niveles montados mediante NFS permiten la escritura de archivos en la misma etiqueta que la zona de montaje y la lectura de archivos de nivel inferior. La etiqueta de los archivos montados no se puede ver de forma confiable ni definir. Para obtener más información, consulte “Montaje de conjuntos de datos de varios niveles desde otro sistema” [181].

ejemplo 4-7 Creación de un conjunto de datos de varios niveles con una etiqueta superior por debajo de `ADMIN_HIGH`

En este ejemplo, el administrador crea un conjunto de datos de varios niveles con un límite superior, o etiqueta superior, que es inferior al valor predeterminado `ADMIN_HIGH`. En la creación de conjuntos de datos, el administrador especifica el límite de la etiqueta superior en la propiedad `mslabel`. Este límite superior impide que los procesos de la zona global creen archivos o directorios en el conjunto de datos de varios niveles. Sólo los procesos de zonas etiquetadas pueden crear directorios y archivos en el conjunto de datos. Dado que la propiedad `multilevel` es `on`, la propiedad `mlslabel` define el límite superior, no la etiqueta para un conjunto de datos de una sola etiqueta.

```
# zfs create -o mountpoint=/multiIUO -o multilevel=on \
   -o mlslabel="CNF : INTERNAL" rpool/multiIUO
```

A continuación, el administrador inicia sesión en cada zona etiquetada para crear un directorio en esa etiqueta en el conjunto de datos montado.

```
# zlogin public
# mkdir /multiIUO
# chmod 777 /multiIUO
# zlogin internal
# mkdir /multiIUO
# chmod 777 /multiIUO
```

Los conjuntos de datos de varios niveles son visibles en la etiqueta de la zona de montaje para los usuarios autorizados después de que se reinicia la zona.

Pasos siguientes Para permitir que los usuarios vuelvan a etiquetar los archivos, consulte Cómo permitir que los archivos se vuelvan a etiquetar desde una zona con etiquetas [170].

Para obtener instrucciones sobre el reetiquetado de archivos, consulte “Cómo actualizar los datos de un conjunto de datos con varios niveles” de “Guía del usuario de Trusted Extensions ” and “Cómo disminuir de nivel los datos de un conjunto de datos con varios niveles” de “Guía del usuario de Trusted Extensions ”.

▼ 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.**

   Por ejemplo, el siguiente comando asigna un disco extraíble, como una unidad JAZ o ZIP, o medios USB de conexión en marcha.

   ```
   # allocate rmdisk0
   ```

   En un sistema de ventanas, puede utilizar Device Manager. Abra dos exploradores de archivos y arrastre el archivo del dispositivo al disco. Para obtener detalles, consulte “Cómo asignar un dispositivo en Trusted Extensions” de “Guía del usuario de Trusted Extensions ”.

2. **Desasigne el dispositivo.**

   ```
   # deallocate rmdisk0
   ```

   Para desasignar el dispositivo mediante Device manager, consulte “Cómo desasignar un dispositivo en Trusted Extensions” de “Guía del usuario de Trusted Extensions ”.

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

---

ejemplo 4-8 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 \
/export/commonfiles
```

El administrador inserta un CD en una unidad de CD-ROM y la asigna.

```
# allocate cdrom0
```

Después de transferir los archivos al CD, el administrador coloca una etiqueta `Trusted Path`.

▼ Cómo copiar archivos desde medios portátiles en Trusted Extensions

Es una práctica segura cambiar el nombre del archivo de Trusted Extensions original antes de reemplazar el archivo. 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.**

   ```
   # allocate cdrom0
   ```

   En un sistema de ventanas, puede utilizar Device Manager. Para obtener detalles, consulte "Cómo asignar un dispositivo en Trusted Extensions" de "Guía del usuario de Trusted Extensions ".

2. **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/policy.conf /etc/security/policy.conf.orig
   ```

3. **Copie los archivos de los medios asignados a una ubicación en el disco y, a continuación, transfiéralos.**

   Por ejemplo, transfiera el archivo `policy.conf`.

   ```
   # cp /dev/rdsk/cdrom0/trusted/* /tmp
   # cp /tmp/policy.conf /etc/security/policy.conf
   ```

4. **Desasigne el dispositivo.**

   ```
   # deallocate cdrom0
   ```

   Para desasignar desde Device Manager, consulte "Cómo desasignar un dispositivo en Trusted Extensions" de "Guía del usuario de Trusted Extensions ".

5. **Expulse y retire el medio.**

```
# eject cdrom0
```

▼ Cómo eliminar Trusted Extensions del sistema

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

Antes de empezar Debe estar con 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 más información, consulte “Cómo eliminar una zona no global” de “Creación y uso de zonas de Oracle Solaris ”.

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

```
# labeladm disable -r
```

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

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

5. **Configure el sistema.**

   Es posible que deba configurar varios servicios para su sistema Oracle Solaris, como las funciones básicas de redes, los servicios de nombres y los montajes de sistemas de archivos.

♦ ♦ ♦ CAPÍTULO 5

Configuración de LDAP para Trusted Extensions

En este capítulo, se describe cómo configurar Oracle Directory Server Enterprise Edition (servidor LDAP) para su uso con Trusted Extensions. El servidor LDAP proporciona servicios LDAP. LDAP es el servicio de nombres admitido para Trusted Extensions. En la sección final, “Creación de un cliente LDAP de Trusted Extensions” [86], se explica cómo configurar un cliente LDAP.

Al configurar el servidor LDAP, 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 Trusted Extensions” [75]
- “Configuración de un servidor proxy LDAP en un sistema Trusted Extensions” [76]

Configuración de LDAP en una red Trusted Extensions

TABLA 5-1 Mapa de tareas de configuración de LDAP en una red de Trusted Extensions

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 LDAP. Este sistema no tiene zonas con etiquetas. Los demás sistemas Trusted Extensions son clientes de este servidor.	Recopilación de información para el servidor LDAP [77] Instalación de Oracle Directory Server Enterprise Edition [77] Configuración de los logs para Oracle Directory Server Enterprise Edition [81]
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 [83]
Configurar todos los demás sistemas Trusted	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 [86]

Tarea	Descripción	Para obtener instrucciones
Extensions como clientes de este servidor.		

Configuración de un servidor proxy LDAP en un sistema Trusted Extensions

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

TABLA 5-2 Mapa de tareas de configuración de un servidor proxy LDAP en un sistema Trusted Extensions

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 [83]
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 [85]
Configurar el servidor proxy para que tenga un puerto de varios niveles para LDAP.	Active 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 [82]
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 [86]

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 LDAP, 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 un servidor NFS o como un servidor para clientes Sun Ray, no es necesario que instale zonas con etiquetas en este servidor.

▼ Recopilación de información para el servidor LDAP

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

  Los elementos se muestran en el orden en que aparecen en el asistente de instalación del sistema.

Petición de datos del asistente de instalación	Acción o información
Oracle Directory Server Enterprise Edition *version*	
Administrator User ID	El valor predeterminado es `admin`.
Administrator Password	Cree una contraseña, como `admin123`.
Directory Manager DN	El valor predeterminado es `cn=Directory Manager`.
Directory Manager Password	Cree una contraseña, como `dirmgr89`.
Directory Server Root	El valor predeterminado es `/var/Sun/mps`. Esta ruta también se utiliza posteriormente si se instala el software de proxy.
Server Identifier	El valor predeterminado es el sistema local.
Server Port	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`.
Suffix	Incluya el componente de dominio, como en `dc=example-domain,dc=com`.
Administration Domain	Cree un dominio que corresponda al sufijo, como en `example-domain.com`.
System User	El valor predeterminado es `root`.
System Group	El valor predeterminado es `root`.
Data Storage Location	El valor predeterminado es `Store configuration data on this server`.
Data Storage Location	El valor predeterminado es `Store user data and group data on this server`.
Administration Port	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 Oracle web site (http://www.oracle.com/technetwork/middleware/id-mgmt/overview/index-085178.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 determinan las operaciones de contraseña y la política de contraseñas. 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 "Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 ". También puede consultar 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:

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

2. **Descargue los paquetes del servidor Oracle Directory Server Enterprise Edition desde Oracle web site (http://www.oracle.com/technetwork/middleware/id-mgmt/overview/index-085178.html).**

   Seleccione el software más reciente adecuado para su plataforma.

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

   Responda las preguntas utilizando la información de Recopilación de información para el servidor LDAP [77]. Para obtener una lista completa de las preguntas, los valores predeterminados y las respuestas sugeridas, consulte el Capítulo 4, "Configuración de Oracle Directory Server Enterprise Edition con clientes LDAP" de "Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: LDAP " y el Capítulo 5, "Configuración de clientes LDAP" de "Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: LDAP ".

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. **Active el programa `cacaoadm` y verifique que el programa esté activado.**

```
# /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, active 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, active 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 Capítulo 6, “Resolución de problemas de LDAP” de “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: LDAP ”.

Creación de un cliente LDAP para el servidor LDAP

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

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

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

   Puede utilizar el servidor LDAP de Trusted Extensions o agregar Trusted Extensions en un sistema diferente. Para obtener instrucciones, consulte Capítulo 3, Agregación de la función Trusted Extensions a Oracle Solaris.

2. **En el cliente, configure 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 "Conmutador enableShadowUpdate" de "Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: LDAP " y la página del comando man `ldapclient`(1M).

▼ Configuración de los logs para Oracle Directory Server Enterprise Edition

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

- Todos los logs se activan y almacenan en el buffer.
- Los logs se colocan en el directorio `/export/home/ds/instances/`*your-instance*`/logs/`*LOG_TYPE* adecuado.
- Los eventos se registran en el nivel de log 256.
- Los logs están protegidos por `600` permisos de archivo.
- Los logs de acceso rotan diariamente.
- Los logs de errores rotan semanalmente.

La configuración de este procedimiento cumple con los siguientes requisitos:

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

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

1. Configure los logs de acceso.

El *LOG_TYPE* para el acceso es `ACCESS`. La sintaxis para la configuración de logs 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 logs 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 logs de auditoría es de una semana.

3. **Configure los logs de errores.**

   En esta configuración, puede especificar los datos adicionales que se van a recopilar en el log 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 logs.**

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

```
# 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 LDAP 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. **En una ventana de terminal, 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 LDAP 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 activada la actualización de shadow. Para conocer los requisitos previos, consulte Creación de un cliente LDAP para el servidor LDAP [80].

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
```

Atención - 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 repositorio 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 LDAP 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, desactive 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” [215].

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 LDAP existente en un sistema Oracle Solaris. En segundo lugar, debe activar los sistemas Trusted

Extensions para el acceso al servidor LDAP 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 LDAP [80].

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 [83].

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` activa 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 5, “Configuración de clientes LDAP” de “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: LDAP ”.

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 Capítulo 6, “Resolución de problemas de LDAP” de “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: LDAP ”.

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 LDAP, 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 LDAP 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 activación 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 del 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, Sobre los requisitos de seguridad en un sistema Trusted Extensions: describe los requisitos de seguridad fijos y configurables en Trusted Extensions.

Capítulo 9, Tareas comunes en Trusted Extensions: presenta la administración de Trusted Extensions.

Capítulo 10, Acerca de usuarios, derechos y roles en Trusted Extensions: presenta el control de acceso basado en roles (RBAC) en Trusted Extensions.

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

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

Capítulo 13, Gestión de zonas en Trusted Extensions: proporciona instrucciones sobre la gestión de zonas etiquetadas.

Capítulo 14, Gestión y montaje de archivos en Trusted Extensions: 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: proporciona una descripción general del enrutamiento y las bases de datos de red en Trusted Extensions.

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

Capítulo 17, Sobre Trusted Extensions y LDAP: describe cuestiones específicas del correo en Trusted Extensions.

Capítulo 18, Sobre correo de varios niveles en Trusted Extensions: describe cuestiones específicas del correo en Trusted Extensions.

Capítulo 19, Gestión de impresión con etiquetas: proporciona instrucciones sobre la gestión de la impresión en Trusted Extensions.

Capítulo 20, Acerca de los dispositivos en Trusted Extensions: describe las extensiones que Trusted Extensions proporciona para la protección de dispositivos en Oracle Solaris.

Capítulo 21, Gestión de dispositivos para Trusted Extensions: proporciona instrucciones sobre la gestión de dispositivos mediante Device Manager.

Capítulo 22, Trusted Extensions y la auditoría: proporciona información específica de Trusted Extensions sobre la auditoría.

Capítulo 23, Gestión de software en Trusted Extensions: 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" [91]
- "Conceptos básicos de Trusted Extensions" [93]

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 shell seguro, 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, el cifrado y el almacenamiento.

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 activadas 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 de Oracle Solaris, Solaris Trusted Extensions (GNOME). El nombre puede abreviarse 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, la interfaz

de línea de comandos `updatehome` se utiliza para colocar los archivos de inicio en los directorios de inicio de los usuarios en cada etiqueta.

- En un entorno de ventanas, Trusted Extensions proporciona interfaces gráficas de usuario para la administración. Por ejemplo, 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 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.

Sin embargo, cuando se visualizan diferentes espacios de trabajo en los monitores de un sistema de varios encabezados, 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 Trusted Extensions ”, se presentan estos conceptos para los usuarios.

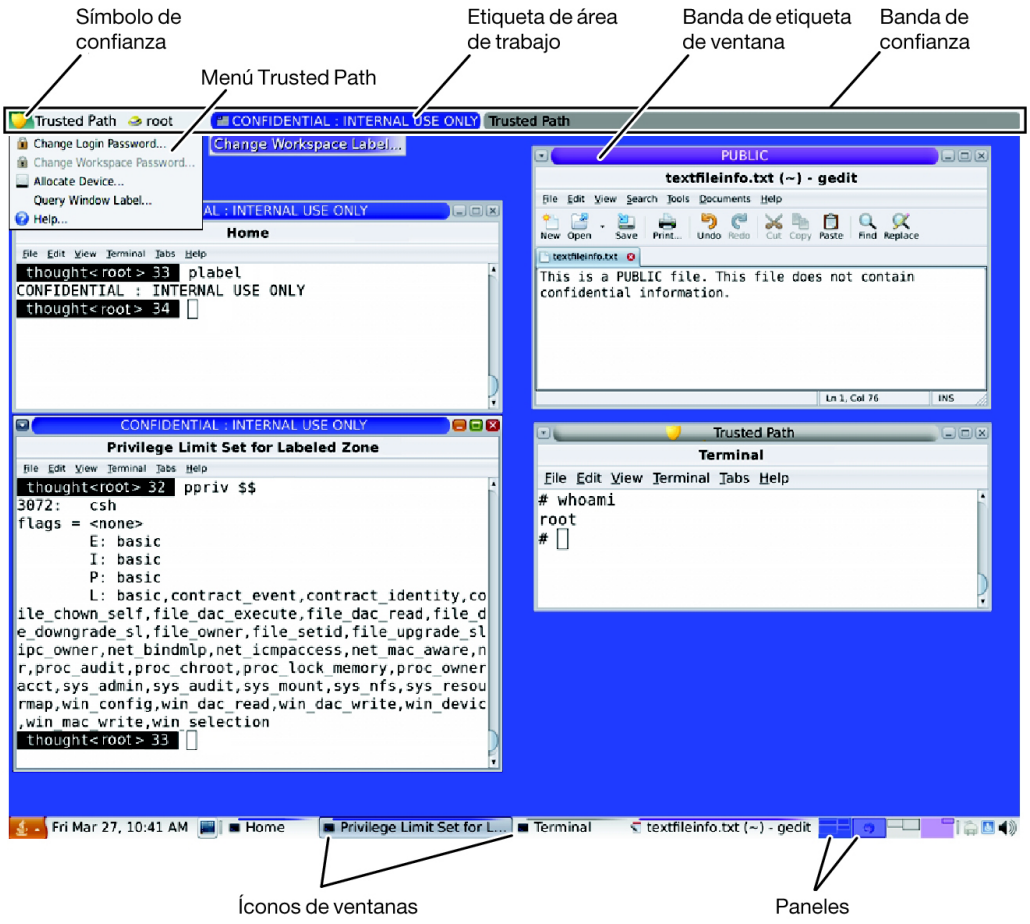
Protecciones de Trusted Extensions

El software Trusted Extensions mejora la protección del SO Oracle Solaris. Trusted Extensions restringe 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.

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, “Escritorio de varios niveles de Trusted Extensions”.

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 están sujetos al 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` y `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, *privilegios* y *autorizaciones*. Los privilegios son permisos especiales que se pueden otorgar 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. El archivo original se encuentra en el directorio /etc/security/tsol. Una vez que se activa Trusted Extensions, la ubicación del archivo se almacena como una propiedad del servicio labeld. 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**: información de identificación y tratamiento de carátulas, ubicadores, encabezados, pies de página y otras funciones de seguridad en las copias impresas
- **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”:

minimum-label ≤ *permitted-label* ≤ *clearance*

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 puede asignar una acreditación y una etiqueta mínima a los usuarios para permitirles 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 la salida que se ejecuta en el escritorio, como las copias impresas.

- **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 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, “Escritorio de varios niveles de Trusted Extensions”.

  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 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 configurado con Trusted Extensions, varios roles aparte de `root` administran el sistema. Normalmente, el rol de administrador del sistema y el rol de administrador de la seguridad realizan la mayoría de las funciones administrativas. En algunos casos, el rol `root` puede administrar después de la configuración inicial. En un sistema de escritorio, el espacio de trabajo cambia para un espacio de trabajo de rol cuando un usuario asume un rol.

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 sobre roles y perfiles de derechos, consulte el Capítulo 1, “Sobre el uso de los derechos para controlar los usuarios y los procesos” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

♦ ♦ ♦ 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" [101]
- "Secuencia de comandos `txzonemgr`" [102]
- "Device Manager" [103]
- "Selection Manager en Trusted Extensions" [103]
- "Generador de etiquetas en Trusted Extensions" [103]
- "Herramientas de la línea de comandos en Trusted Extensions" [104]
- "Archivos de configuración en Trusted Extensions" [105]

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. Las herramientas de administración sólo están disponibles para los roles.

En un sistema de escritorio, 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. Las herramientas de la línea de comandos están disponibles en los sistemas que no están ejecutando un escritorio.

TABLA 7-1 Herramientas administrativas de Trusted Extensions

Herramienta	Descripción	Para obtener más información
`/usr/sbin/labeladm`	Activa y desactiva Trusted Extensions. También se utiliza para instalar un archivo de codificaciones de etiqueta.	Consulte "Instalación y activación de Trusted Extensions" [35], Cómo comprobar e instalar el archivo de

Herramienta	Descripción	Para obtener más información
		codificaciones de etiquetas [40] y la página del comando man labeladm(1M).
/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" [43] 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" [103] and "Control de dispositivos en Trusted Extensions" [287].
Label Builder	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 [142].
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 activar a un usuario para que cambie el nivel de seguridad de los datos [145]. Para ver una ilustración, consulte "Cómo mover datos entre ventanas de etiquetas diferentes" de "Guía del usuario de 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 es una herramienta de configuración de red y zona que ofrece dos modos.

- Como una interfaz de la línea de comandos, el comando crea zonas con etiquetas. 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 le preguntará si desea suprimir todas las zonas una por una.
- 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. La secuencia de comandos gestiona las direcciones IPv4 e IPv6.

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 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.

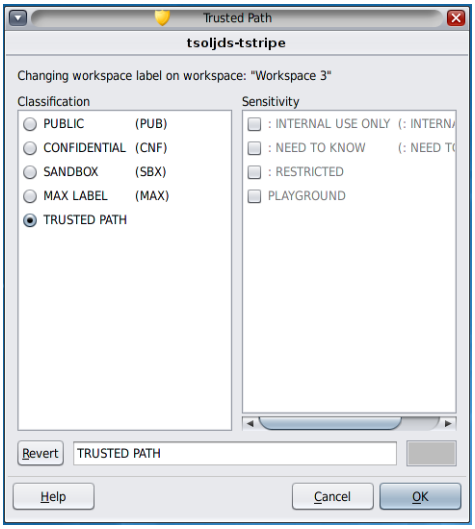
Selection Manager en Trusted Extensions

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” [112].

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 de escritorio (consulte el Capítulo 2, “Inicio de sesión en Trusted Extensions” de “Guía del usuario de 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

Sobre los requisitos de seguridad en un sistema Trusted Extensions

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

- "Funciones de seguridad configurables" [107]
- "Aplicación de los requisitos de seguridad" [109]
- "Reglas para cambiar el nivel de seguridad de los datos" [112]

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, por lo general, usted asume un rol limitado para administrar los sistemas.

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 "Asignación de derechos a usuarios" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".
- Para crear roles, consulte "Creación de roles y usuarios en Trusted Extensions" [56].

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 agregación de clases de auditoría se describe en el Capítulo 3, "Gestión del servicio de auditoría" de "Gestión de auditoría en Oracle Solaris 11.2 ".

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 agregación de roles y perfiles de derechos se describe en el Capítulo 3, “Asignación de derechos en Oracle Solaris” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.
- **Autorizaciones**: para ver un ejemplo de cómo agregar una nueva autorización, consulte “Personalización de autorizaciones para dispositivos en Trusted Extensions” [296].

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 le permite cambiar la contraseña de rol o usuario.
- **Menú Change Workspace Label**: los usuarios de sesiones de varios niveles pueden cambiar la etiqueta de 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.
- **Cuadro de diálogo Selection Manager**: los usuarios autorizados en sesiones de varios niveles pueden subir o bajar de nivel la información a una etiqueta diferente.
- **Archivo TrustedExtensionsPolicy**: los administradores pueden cambiar la política en extensiones de servidor X que son exclusivas de Trusted Extensions. Para obtener más información, consulte la página de comando man `TrustedExtensionsPolicy`(4).

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. Debe formar a los usuarios para que hagan su parte. 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.

Directrices de uso de 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 mediante 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 conservan en el archivo `/etc/shadow`, que solamente puede leer el usuario `root`. Para obtener más información, consulte la página del comando man `shadow`(4).

Prácticas de administración de grupo

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 suprimido como grupo principal se les asigne otro grupo principal.

Prácticas de supresión 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. Para obtener más información, consulte “Archivo `sel_config`” [114] y la página del comando man `sel_config`(4).
- 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
	Bajar de nivel la información	Mismo UID	`solaris.label.file.downgrade`
	Subir de nivel la información	Mismo UID	`solaris.label.file.upgrade`
	Bajar de nivel la información	Diferentes UID	`solaris.label.file.downgrade`
	Subir de nivel la información	Diferentes UID	`solaris.label.file.upgrade`

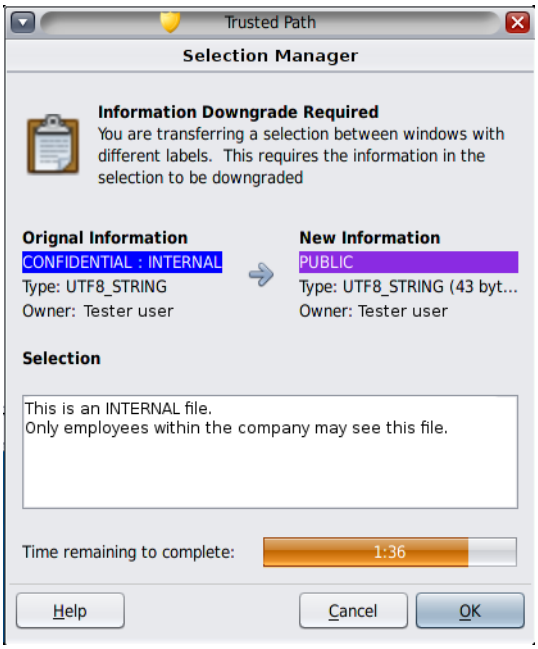
Se aplican reglas diferentes a las selecciones en una ventana que en un archivo. La acción de arrastrar y soltar *selecciones* siempre requiere que exista igualdad de etiquetas y propiedad. La acción de arrastrar y soltar entre ventanas es mediada por la aplicación Selection Manager, no por el archivo `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
	Bajar de nivel la información	Mismo UID	`solaris.label.win.downgrade`
	Subir de nivel la información	Mismo UID	`solaris.label.win.upgrade`
	Bajar de nivel la información	Diferentes UID	`solaris.label.win.downgrade`
	Subir de nivel la información	Diferentes UID	`solaris.label.win.upgrade`
Arrastrar y soltar las selecciones entre las ventanas	Misma etiqueta	Mismo UID	Ninguna

En un sistema de ventanas, Trusted Extensions proporciona un gestor de selecciones para que medie en los cambios de etiquetas. Este cuadro de diálogo 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 gestor de selecciones 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 comprueba para determinar el comportamiento del gestor de selecciones cuando una operación sube o baja de nivel una etiqueta.

El archivo `sel_config` define lo siguiente:

- Qué tipos de selecciones obtienen respuestas automáticas
- Qué tipos de operaciones pueden confirmarse automáticamente

- Si se muestra un cuadro de diálogo Selection Manager

♦ ♦ ♦ CAPÍTULO 9

Tareas comunes en Trusted Extensions

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 en un sistema de escritorio" [117]
- "Realización de tareas comunes en Trusted Extensions" [119]

Introducción para administradores de Trusted Extensions en un sistema de escritorio

Familiarícese con los siguientes procedimientos antes de administrar Trusted Extensions.

TABLA 9-1 Inicio de sesión y uso del escritorio de 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 Trusted Extensions "
Realizar tareas de usuario comunes en un escritorio.	Estas 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 Trusted Extensions "
Realizar tareas que requieren la ruta de confianza.	Estas tareas incluyen: ■ Asignar un dispositivo ■ Cambiar la contraseña ■ Cambiar la etiqueta de un espacio de trabajo	"Realización de acciones de confianza" de "Guía del usuario de Trusted Extensions "
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 [118]
Seleccionar un espacio de trabajo de usuario.	Permite salir de la zona global.	Cómo salir de la zona global en Trusted Extensions [118]

▼ 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 [141].

Antes de empezar Se le asigna un rol administrativo. Para obtener referencias, consulte “Creación de roles en Trusted Extensions” [108].

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, “Escritorio de varios niveles de Trusted Extensions”. Para obtener una explicación de estas funciones, consulte el Capítulo 4, “Elementos de Trusted Extensions” de “Guía del usuario de 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 Trusted Extensions ”.

Realización de tareas comunes en Trusted Extensions

En el siguiente mapa de tareas, se describen los procedimientos administrativos comunes en Trusted Extensions.

TABLA 9-2 Realización de tareas administrativas comunes en Trusted Extensions (mapa de tareas)

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 un sistema de escritorio [119]
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 [120]
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 [121]
Determinar el número hexadecimal de una etiqueta.	Muestra la representación interna de una etiqueta de texto.	Cómo obtener el equivalente hexadecimal de una etiqueta [122]
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 [123]
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 “Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 ” “Cómo asignar un dispositivo en Trusted Extensions” de “Guía del usuario de Trusted Extensions ”
Cambiar un archivo de configuración del sistema.	Cambia los valores de seguridad predeterminados de Trusted Extensions y Oracle Solaris.	Cómo cambiar los valores predeterminados de seguridad en los archivos del sistema [124]
Administrar un sistema de manera remota.	Permite administrar los sistemas Trusted Extensions desde un sistema remoto.	Capítulo 12, Administración remota en Trusted Extensions

▼ Cómo cambiar la contraseña de `root` en un sistema de escritorio

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 [118].
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 caché 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.
- 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 [54].

▼ 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 [118].

- **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

Los archivos de los directorios `/etc/security` y `/etc/default` contienen valores de seguridad. Para obtener más información, consulte Capítulo 3, “Control de acceso a sistemas” de “Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 ”.

Atención - Reduzca los valores predeterminados de seguridad del sistema únicamente si la política de seguridad del sitio lo permite.

Antes de empezar Debe estar en la zona global y tener asignada la autorización `solaris.admin.edit/` *filename*. De manera predeterminada, el rol `root` tiene esta autorización.

- **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. Los dos primeros archivos son exclusivos de Trusted Extensions.

Archivo	Tarea	Para obtener más información
`sel_config` en `/usr/share/gnome/`	Especificar cómo se comporta el sistema cuando la información se mueve a una etiqueta diferente.	Página del comando man `sel_config`(4)
`TrustedExtensionsPolicy` en `/usr/lib/xorg/`	Modificar la aplicación de la política de seguridad `SUN_TSOL` de la separación de etiquetas en el servidor X.	Página del comando man `TrustedExtensionsPolicy`(4)
`/etc/default/login`	Reducir el número permitido de intentos de introducción de contraseña.	Página del comando man `passwd`(1)
`/etc/default/kbd`	Desactivar la interrupción del teclado.	“Cómo desactivar una secuencia de interrupción del sistema” de “Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 ”

Archivo	Tarea	Para obtener más información
		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

Acerca de usuarios, derechos y roles en Trusted Extensions

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” [56].

- “Funciones de seguridad del usuario en Trusted Extensions” [127]
- “Responsabilidades del administrador para los usuarios” [128]
- “Decisiones que deben tomarse antes de crear usuarios en Trusted Extensions” [129]
- “Atributos de seguridad del usuario predeterminados en Trusted Extensions” [130]
- “Atributos de usuario que pueden configurarse en Trusted Extensions” [131]
- “Atributos de seguridad que deben asignarse a los usuarios” [131]

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:

- "Mapa de tareas para la configuración y gestión de cuentas de usuario mediante el uso de la interfaz de línea de comandos" de "Gestión de las cuentas de usuario y los entornos de usuario en Oracle Solaris 11.2 "
- "Protección de los usuarios y los procesos en Oracle Solaris 11.2 "

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” [130].
- 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 [138].
- 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 [300]. Para crear un conjunto de autorizaciones para dispositivos más específico, consulte “Personalización de autorizaciones para dispositivos en Trusted Extensions” [296].
- Decida si las cuentas de usuario se deben crear por separado en las zonas etiquetadas.

  De manera predeterminada, las zonas etiquetadas comparten la configuración del servicio de nombres de la zona global. Por lo tanto, las cuentas de usuario se crean en la zona global para todas las zonas. Los archivos `/etc/passwd` y `/etc/shadow` de las zonas con etiquetas son vistas de sólo lectura de los archivos de la zona global. Del mismo modo, las bases de datos LDAP son de sólo lectura en las zonas etiquetadas.

  Las aplicaciones que instala en una zona desde dentro de una zona posiblemente requieran la creación de cuentas de usuario, por ejemplo, `pkg:/service/network/ftp`. Para activar una aplicación específica de zona para crear una cuenta de usuario, debe configurar el daemon de servicio de nombres por zona, como se describe en Cómo configurar un servicio de nombres independiente para cada zona con etiquetas [54]. Las cuentas de usuario que

esas aplicaciones agregan a una zona etiquetada deben estar gestionadas manualmente por el administrador de zona.

Nota - Las cuentas que almacena en LDAP siguen siendo gestionadas desde la zona global.

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” [131].

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” [20] 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 *keyword=value* 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`	`15`	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” [25], 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`” [133].

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” [130]. 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	Ninguna	Requerida	El usuario tiene contraseña
Roles	Ninguna	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

Atributo de usuario	Ubicación de valor predeterminado	Condición de la acción	Efecto de la asignación
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 más información, 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. Para obtener escalabilidad, agregue las autorizaciones a un perfil de derechos y, luego, asigne 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 derechos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

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 [144].

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 sobre la auditoría, consulte "Gestión de auditoría en Oracle Solaris 11.2 " and Capítulo 22, Trusted Extensions y la auditoría.

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 [138].

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

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" [135]
- "Gestión de usuarios y derechos" [141]

Personalización del entorno de usuario para la seguridad

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.

TABLA 11-1 Mapa de tareas de personalización del entorno de usuario para la seguridad

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 [136]
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` [137]
	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, "Cambio de la configuración del tiempo de inactividad del sistema"
	Se eliminan los privilegios innecesarios de todos los usuarios comunes de un sistema.	Ejemplo 11-2, "Modificación del conjunto de privilegios básico de cada usuario"
	Impide que las etiquetas aparezcan en la salida impresa en un quiosco público.	Ejemplo 11-3, "Asignación de las autorizaciones relacionadas con la impresión a todos los usuarios de un sistema"
Configurar los archivos de inicialización para los usuarios.	Configura 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 [138]

Tarea	Descripción	Para obtener instrucciones
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 [141]

Cómo modificar atributos de etiquetas de usuarios predeterminados

Puede modificar los atributos de etiquetas de usuarios predeterminados durante la configuración del primer sistema. Utilice el archivo de codificaciones modificado al instalar sistemas Trusted Extensions adicionales.

Atención - 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 [118].

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, “Valores predeterminados de seguridad de Trusted Extensions para las cuentas de usuario” en “Planificación de la seguridad del usuario en Trusted Extensions” [25].

2. **Edite una copia del archivo de codificaciones activo.**

   a. **Ubique el archivo activo.**

   ```
   # labeladm encodings
   Label encodings file: /var/tsol/encodings/label_encodings.fSaG.L
   ```

   b. **Edite una copia del archivo activo.**

   ```
   # cp /var/tsol/encodings/label_encodings.fSaG.L /tmp/tmp-encodings
   # pfedit /tmp/tmp-encodings
   ```

3. **Reemplace el archivo de codificaciones de etiqueta del sistema y reinicie el sistema.**

   ```
   # labeladm encodings /tmp/tmp-encodings
   # /usr/sbin/reboot
   ```

4. **Repita el procedimiento en cada sistema Trusted Extensions.**

Atención - El contenido del archivo de codificaciones de etiqueta activo debe ser el mismo en todos los sistemas.

▼ 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 [118].

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, “Valores predeterminados de seguridad de Trusted Extensions en el archivo policy.conf”.

2. **Modifique la configuración.**

   ```
   # pfedit /etc/security/policy.conf
   ```

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 *keyword=value* 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 *keyword=value* 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 seguridad de una gran instalación de Sun Ray no quiere que los usuarios comunes vean los procesos de otros usuarios de Sun Ray. 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 [118].

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`.**

   ```
   # pfedit /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`” [133] para obtener ideas. Para ver archivos de muestra, consulte el Ejemplo 11-4, “Personalización de los archivos de inicio para los usuarios”.

3. **Personalice el archivo `.link_files`.**

   a. **En un editor, escriba el nombre completo de la ruta de `.link_files`.**

   ```
   # pfedit /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 incluirán en los archivos de inicio, consulte “Acerca del entorno de trabajo del usuario” de “Gestión de las cuentas de usuario y los entornos de usuario en Oracle Solaris 11.2 ”.
   - Para obtener detalles, consulte “Cómo personalizar los archivos de inicialización de usuario” de “Gestión de las cuentas de usuario y los entornos de usuario en Oracle Solaris 11.2 ”.

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 agrega personalizaciones.

```
## .cshrc file
setenv EDITOR emacs
setenv ETOOLS /net/tools/etools
```

```
## .ksh file
export EDITOR emacs
export ETOOLS /net/tools/etools
```

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 de inicio, 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

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.

TABLA 11-2 Mapa de tareas de gestión de usuarios y derechos

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 [142]

Tarea	Descripción	Para obtener instrucciones
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 [143]
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 [144]
Impedir el bloqueo de cuentas para usuarios concretos.	Los usuarios que pueden asumir un rol deben tener el bloqueo de cuenta desactivado.	Cómo impedir el bloqueo de cuentas de los usuarios [144]
Permitir que un usuario vuelva a etiquetar datos.	Se autoriza a un usuario a reducir o aumentar el nivel de la información.	Cómo activar a un usuario para que cambie el nivel de seguridad de los datos [145]
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 [146]

▼ 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 activar a todos los usuarios de un sistema en particular que se van a autorizar, consulte Cómo modificar los valores predeterminados de `policy.conf` [137].

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 ver el procedimiento paso a paso, consulte "Cómo crear un perfil de derechos" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

   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.nobanner`: autoriza a un usuario a que haga copias impresas sin la página de 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 ver el procedimiento paso a paso, consulte “Asignación de derechos a usuarios” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

▼ 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. Por ejemplo, en un sitio que utiliza Trusted Extensions en los sistemas Sun Ray, puede que desee impedir que los usuarios vean los procesos de los demás usuarios en el servidor Sun Ray.

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`.**

Atención - 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 recopilación de restricciones de privilegios en un perfil de derechos, consulte los ejemplos que siguen a “Cómo crear un perfil de derechos” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

Para restringir los privilegios de todos los usuarios en un sistema, consulte el Ejemplo 11-2, “Modificación del conjunto de privilegios básico de cada usuario”.

▼ 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 repositorio LDAP.

```
# usermod -S ldap -K lock_after_retries=no jdoe
```

▼ Cómo activar 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 [170].

Atención - 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.

- **Asigne el perfil de derechos de gestión de etiquetas de objetos para los usuarios y roles adecuados.**

  Para ver el procedimiento paso a paso, consulte "Asignación de derechos a usuarios" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

ejemplo 11-5 Cómo permitir que un usuario actualice, pero no degrade, la etiqueta de un archivo

El perfil de derechos de gestión de etiquetas de objetos permite que los usuarios actualicen y degraden etiquetas. En este ejemplo, el administrador permite que un usuario de confianza actualice los datos, pero no los degrade.

El administrador crea un perfil de derechos basado en el perfil de gestión de etiquetas de objetos y elimina las autorizaciones Downgrade File Label y Downgrade DragNDrop or CutPaste Info en el nuevo perfil.

```
# profiles -p "Object Label Management"
profiles:Object Label Management> set name="Object Upgrade"
profiles:Object Upgrade> info auths
...
profiles:Object Upgrade> remove auths="solaris.label.file.downgrade,
solaris.label.win.downgrade"
```

```
profiles:Object Upgrade> commit
profiles:Object Upgrade> end
```

Luego, el administrador asigna el perfil a un usuario de confianza.

```
# usermod -P +"Object Upgrade" jdoe
```

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 supresión 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 supresión de usuarios” [112].

♦ ♦ ♦ CAPÍTULO 12

Administración remota en Trusted Extensions

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.

- "Administración remota en Trusted Extensions" [147]
- "Métodos para administrar sistemas remotos en Trusted Extensions" [148]
- "Configuración y administración de sistemas remotos en Trusted Extensions" [149]

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" [19].

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 usar el protocolo shell seguro con la 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 shell seguro 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 iniciar 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, “Asignación del tipo de host CIPSO para la administración remota”.
- **Administración desde un sistema sin etiquetas**: si la administración mediante un sistema Trusted Extensions no es práctica, la política de protocolo de red se puede flexibilizar especificando la opción `allow_unlabeled` para el módulo `pam_tsol_account` en la pila PAM.

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 [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 [152].

Configuración y administración de sistemas remotos en Trusted Extensions

Después de activar la administración remota y antes de reiniciar el sistema remoto en Trusted Extensions, puede configurar el sistema mediante la informática en red virtual (VNC) o el protocolo `ssh`.

TABLA 12-1 Mapa de tareas de configuración y administración de sistemas remotos en Trusted Extensions

Tarea	Descripción	Para obtener instrucciones
Activar la administración remota de un sistema Trusted Extensions.	Permite la administración de sistemas Trusted Extensions desde clientes `ssh` especificados.	Cómo activar la administración remota de un sistema Trusted Extensions remoto [150]
Activar 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 [152]
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 [155]

Nota - Consulte su política de seguridad para determinar qué métodos de administración remota están permitidos en su sitio.

▼ Cómo activar la administración remota de un sistema Trusted Extensions remoto

En este procedimiento, se activa la autenticación basada en host en un sistema remoto Oracle Solaris antes de agregar la función Trusted Extensions. El sistema remoto es el servidor shell seguro.

Antes de empezar El sistema remoto se instala con Oracle Solaris, y es posible acceder a ese sistema. Debe tener el rol `root`.

1. **En ambos sistemas, active la autenticación basada en host.**

   Para conocer el procedimiento, consulte “Cómo configurar la autenticación basada en host para el shell seguro” de “Gestión de acceso mediante shell seguro en Oracle Solaris 11.2 ”.

   Nota - No utilice el comando `cat`. Copie y pegue la clave pública mediante una conexión shell seguro. Si el cliente shell seguro no es un sistema Oracle Solaris, siga las instrucciones de la plataforma para configurar un cliente shell seguro con la 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 shell seguro, flexibilice la política `ssh` para permitir que `root` inicie sesión de manera remota.**

   ```
   # pfedit /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 shell seguro, reinicie el servicio `ssh`.**

   ```
   # svcadm restart ssh
   ```

4. **En el servidor shell seguro, en el directorio raíz `root`, especifique el host y el usuario para la autenticación basada en host.**

   ```
   # cd
   # pfedit .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 shell seguro, flexibilice las dos políticas PAM.**

   a. **Copie `/etc/pam.d/other` en `/etc/pam.d/other.orig`.**

      ```
      # cp /etc/pam.d/other /etc/pam.d/other.orig
      ```

   b. **Modifique la entrada `pam_roles` para permitir el acceso remoto mediante roles.**

      ```
      # pfedit /etc/pam.d/other
      ...
      # Default definition for Account management
      # Used when service name is not explicitly mentioned for account management
      # ...
      #account requisite    pam_roles.so.1
      # Enable remote role assumption
      account requisite    pam_roles.so.1   allow_remote
      ...
      ```

      Esta política permite que *username* en el sistema *client-host* asuma un rol en el servidor.

   c. **Modifique la entrada `pam_tsol_account` para permitir que los hosts sin etiquetar se pongan en contacto con el sistema remoto de Trusted Extensions.**

      ```
      # pfedit /etc/pam.d/other
      # Default definition for Account management
      # Used when service name is not explicitly mentioned for account management
      # ...
      #account requisite    pam_roles.so.1
      # Enable remote role assumption
      account requisite    pam_roles.so.1   allow_remote
      #
      account required     pam_unix_account.so.1
      #account required     pam_tsol_account.so.1
      # Enable unlabeled access to TX system
      account required     pam_tsol_account.so.1  allow_unlabeled
      ```

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, active 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*

Para permitir que un administrador configure el host Trusted Extensions remoto desde un sistema sin etiquetas, el administrador deja la opción `allow_unlabeled` en el archivo `pam.d/other` del host remoto.

▼ 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 [229].

Si actualmente ejecuta una sesión GNOME en la consola del futuro servidor Xvnc de Trusted Extensions, no tiene activado 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.**

```
# pkg search vnc
... set    VNC client based on the TigerVNC open source release that
           displays a session over RFB protocol from a VNC server
           pkg:/desktop/remote-desktop/tigervnc@version
... set    X Window System server based on X.Org Foundation open source
           release and TigerVNC open source release that displays over
           RFB protocol to a VNC client
           pkg:/x11/server/xvnc@version
...
```

Una opción es el software de servidor TigerVNC X11/VNC.

```
# pkg install server/xvnc
# pkg install remote-desktop/tigervnc
```

Nota - Si no puede abrir la interfaz gráfica de usuario, agregue la cuenta `root` local a la lista de control de acceso del servidor X. Ejecute este comando como el usuario que inició sesión en el servidor X.

```
% xhost +si:localuser:root
```

Para obtener más información, consulte las páginas del comando man `xhost`(1) y `Xsecurity`(5).

---

2. **Active 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.**

Sugerencia - Guarde una copia del archivo `Xsession` original antes de realizar el cambio.

```
DISPLAY=unix:$(echo $DISPLAY|sed -e s/::ffff://|cut -d: -f2)
```

Los archivos del Paso 2 y el Paso 3 están marcados con el atributo de paquetes `preserve=true`. Para obtener información sobre el efecto que tiene este atributo en los archivos modificados durante las actualizaciones y correcciones de paquetes, consulte la página de comando man `pkg`(5).

4. **Active 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 activado.**

   ```
   % 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 repositorio de Oracle Solaris.

8. **(Opcional) Audite las conexiones VNC.**

   Para obtener información sobre la preselección de eventos de auditoría por sistema y por usuario, consulte "Configuración del servicio de auditoría" de "Gestión de auditoría en Oracle Solaris 11.2 ".

9. **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 Trusted Extensions ".

ejemplo 12-2 Uso de Vino para compartir un escritorio en un entorno de prueba

En este ejemplo, dos programadores usan el servicio Vino de GNOME para compartir la visualización desde el menú Launch (Lanzar) -> System (Sistema) -> Preferences (Preferencias) -> Desktop Sharing (Compartición de escritorio). Además de los pasos anteriores, flexibilizan la política de Trusted Extensions al permitir la extensión `XTEST`.

```
# pfedit /usr/X11/lib/X11/xserver/TrustedExtensionsPolicy
```

```
## /usr/X11/lib/X11/xserver/TrustedExtensionsPolicy file
...
#extension XTEST
extension XTEST
...
```

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 activar la administración remota de un sistema Trusted Extensions remoto [150].

1. **En el sistema de escritorio, active 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: xxxxxxxx
   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: xxxxxxxx
   ```

   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. Si desea ver un ejemplo, consulte el Ejemplo 12-3, “Configuración de zonas con etiquetas en un sistema remoto”.

ejemplo 12-3 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 activa el acceso del sistema de escritorio al servidor X utilizando 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: xxxxxxxx
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: xxxxxxxx
```

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 12-4 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 el espacio de trabajo de la zona global y, a continuación, cambiar el espacio de trabajo 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* utiliza el servicio de nombres de archivos, la contraseña de la zona `PUBLIC` 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 desactiva 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

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" [157]
- "Procesos de la zona global y de las zonas con etiquetas" [160]
- "Zonas etiquetadas primarias y secundarias" [161]
- "Utilidades de administración de zonas en Trusted Extensions" [162]
- "Gestión de zonas" [162]

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 etiqueta a cada zona, lo que crea zonas etiquetadas. Las etiquetas proceden del archivo `label_encodings`. Puede crear una o varias zonas para cada etiqueta, pero esto no es obligatorio. Es posible tener más etiquetas que zonas con etiquetas en un sistema.

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, todas las zonas tienen una marca *etiquetado*, y todos los directorios y archivos modificables en una zona con etiquetas están 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 independiente. 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 etiquetada y cómo montar directorios desde zonas etiquetadas de manera remota, consulte el Capítulo 14, Gestión y montaje de archivos en Trusted Extensions y “Propiedad `mlslabel` y montaje de sistemas de archivos de un solo nivel” [179].

Las zonas en Trusted Extensions están incorporadas en el producto Oracle Solaris Zones. Para obtener referencia, consulte “Introducción a Zonas de Oracle Solaris ”.

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” [23] 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 “Introducción a Zonas de Oracle Solaris ”.

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 activan 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 [235].

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.

Un proceso de zona global puede montar un sistema de archivos remoto con permisos de lectura y escritura en las siguientes condiciones:

- 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 raíz 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 están 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 [187].

Zonas etiquetadas primarias y secundarias

La primera zona que crea en una etiqueta específica es una zona etiquetada primaria. Su etiqueta es única. No puede crear ninguna otra zona primaria en esa etiqueta.

Una zona secundaria es una zona en la etiqueta de una zona primaria. Con una zona secundaria, puede aislar servicios en diferentes zonas en la misma etiqueta. Esos servicios pueden compartir recursos de red, como servidores de nombres, impresoras y bases de datos sin el uso de un privilegio. Puede tener varias zonas secundarias en la misma etiqueta.

Específicamente, las zonas secundarias difieren de las zonas primarias en los siguientes aspectos:

- No es necesario que las asignaciones de etiquetas de las zonas secundarias sean únicas.
- Las zonas secundarias deben utilizar funciones de red IP exclusivas.

  Esta restricción garantiza que un paquete etiquetado llegue a la zona correcta.
- Las zonas secundarias no tienen paquetes GNOME instalados.

  Las zonas secundarias no son visibles en el escritorio de confianza GNOME.
- Las zonas secundarias no pueden ser la zona de destino para el comando `setlabel`.

  Si hay varias zonas en la misma etiqueta, la zona de destino no se puede resolver mediante el comando.

Para cualquier etiqueta, puede haber como máximo una zona etiquetada primaria y un número arbitrario de zonas etiquetadas secundarias. La zona global sigue siendo una excepción. Es la única zona que puede tener asignada la etiqueta `ADMIN_LOW` y, por tanto, no puede tener una zona secundaria. Para crear una zona secundaria, consulte Cómo crear una segunda etiquetada secundaria [68] y la página del comando man `zenity`(1).

Utilidades de administración de zonas en Trusted Extensions

Algunas tareas de administración de la zona pueden realizarse 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 menú para crear, instalar, inicializar e iniciar las zonas. Para obtener detalles, consulte las páginas del comando man `txzonemgr`(1M) y `zenity`(1).

Gestión de zonas

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.

TABLA 13-1 Mapa de tareas de gestión de zonas

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 [163]

Tarea	Descripción	Para obtener instrucciones
Ver directorios montados.	En cualquier etiqueta, se visualizan los directorios dominados por la etiqueta actual.	Cómo visualizar las etiquetas de los archivos montados [164]
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 [165]
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 desactiva el montaje de una zona de nivel inferior, puede desactivar todos los montajes de las zonas de nivel inferior.	Cómo desactivar el montaje de archivos de nivel inferior [166]
Crear un conjunto de datos de varios niveles para cambiar las etiquetas de los archivos.	Permite el reetiquetado de archivos en un conjunto de datos ZFS; no se necesitan privilegios.	Cómo crear y compartir un conjunto de datos de varios niveles [69]
Configurar una zona para permitir el cambio de las etiquetas en los archivos.	De manera predeterminada, las zonas con etiquetas no tienen el privilegio que permite que un usuario autorizado vuelva 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 [170]
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 [168].
Configurar una nueva zona primaria.	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 [45].
Configurar una zona secundaria.	Crea una zona para aislar los servicios que no requieren un escritorio.	Cómo crear una segunda etiquetada secundaria [68].
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 [235] Ejemplo 16-22, “Configuración de un puerto de varios niveles privado para NFSv3 mediante `udp`”
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 [190]
Eliminar una zona con etiquetas.	Se elimina por completo una zona con etiquetas del sistema.	“Cómo eliminar una zona no global” de “Creación y uso de zonas de Oracle Solaris ”

▼ 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. **En un sistema de ventanas, ejecute el comando `txzonemgr &`.**

Los nombres de las zonas, su estado y sus etiquetas se muestran en una interfaz gráfica de usuario.

2. **También puede utilizar 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 activa 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, permita que los usuarios comunes 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 permite a los evaluadores y programadores verificar si sus contraseñas locales están establecidas. Después de que se detiene la zona `sandbox`, esta se configura para montar en bucle de retorno el archivo `passwd`. Una vez que se reinicia la zona, los usuarios comunes pueden ver las entradas en el archivo `passwd`.

```
# 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 desactivar el montaje de archivos de nivel inferior

De manera predeterminada, los usuarios pueden ver los archivos de nivel inferior. Para impedir la visualización de todos los archivos de nivel inferior de una zona determinada,

elimine el privilegio `net_mac_aware` de esa zona. 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 impide que los usuarios de 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 agregación 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. **Active 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 de 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 activar 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 activar a un usuario para que cambie el nivel de seguridad de los datos [145].

ejemplo 13-5 Cómo permitir degradaciones únicamente de la zona `internal`

En este ejemplo, el administrador de seguridad utiliza el comando `zonecfg` para permitir la degradación de información (no la actualización) de la zona `CNF: INTERNAL USE ONLY` zone.

```
# zonecfg -z internal set limitpriv=default,file_downgrade_sl
```

ejemplo 13-6 Cómo evitar las disminuciones de nivel desde la zona `internal`

En este ejemplo, el administrador de la seguridad impide 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

En este capítulo, se explica la política de Trusted Extensions al compartir y montar archivos, y el efecto de esta política en los montajes ZFS de conjuntos de datos de varios niveles, y los montajes LOFS y NFS de conjuntos de datos ZFS de un solo nivel. Además, se explica cómo realizar copias de seguridad de los archivos y cómo restaurarlos.

- "Posibilidades de montaje en Trusted Extensions" [173]
- "Políticas de Trusted Extensions para sistemas de archivos montados" [174]
- "Resultados del uso compartido y el montaje de sistemas de archivos en Trusted Extensions" [177]
- "Conjuntos de datos de varios niveles para volver a etiquetar archivos" [180]
- "Servidor NFS y configuración de cliente en Trusted Extensions" [182]
- "Software Trusted Extensions y versiones del protocolo NFS" [184]
- "Copia de seguridad, uso compartido y montaje de archivos con etiquetas" [185]

Posibilidades de montaje en Trusted Extensions

Trusted Extensions puede montar dos tipos de conjuntos de datos de ZFS.

- Un *conjunto de datos etiquetado de un solo nivel* tiene la misma etiqueta que la zona en la cual residen o se montan los datos. Todos los archivos y directorios en un conjunto de datos de un solo nivel estén en la misma etiqueta. Estos conjuntos de datos son los típicos de Trusted Extensions.
- Un *conjunto de datos de varios niveles* puede contener archivos y directorios en distintas etiquetas. Un conjunto de datos de este tipo es eficaz para prestar servicio a los clientes NFS en muchas etiquetas distintas y puede optimizar el proceso de reetiquetado de archivos.

Los siguientes montajes posibles en Trusted Extensions:

- **Montajes ZFS**: los conjuntos de datos de varios niveles creados por el administrador se pueden montar mediante ZFS en la zona global. Un conjunto de datos montado mediante ZFS se puede montar mediante LOFS en zonas etiquetadas del mismo sistema.

Los conjuntos de datos de un solo nivel también pueden ser creados y montados mediante ZFS por administradores en zonas etiquetadas.

- **Montajes LOFS**: como se mencionó en el párrafo anterior, la zona global puede montar mediante LOFS un conjunto de datos de un solo nivel en una zona etiquetada. La etiqueta del montaje es `ADMIN_LOW`; por lo tanto, todos los archivos montados son de sólo lectura en la zona etiquetada.

  La zona global también puede montar mediante LOFS un conjunto de datos de varios niveles en una zona etiquetada. Los archivos montados que tienen la misma etiqueta que la zona se pueden modificar. Con los permisos adecuados, los archivos se pueden volver a etiquetar. Los archivos montados que se encuentran en un nivel inferior al de la etiqueta de la zona se pueden ver.
- **Montajes NFS**: las zonas etiquetadas pueden montar conjuntos de datos de un solo nivel en la etiqueta de la zona. Estos archivos pueden proceder de otra zona etiquetada o de un sistema que no es de confianza y que tenga asignada la misma etiqueta que la zona etiquetada.

  Una zona global puede montar mediante NFS un conjunto de datos de varios niveles desde otro sistema Trusted Extensions. Los archivos montados se pueden ver y modificar, pero no se pueden volver a etiquetar. Además, sólo los archivos y directorios en la etiqueta de la zona de montaje devuelven la etiqueta correcta.

  Una zona etiquetada puede montar mediante NFS un conjunto de datos de varios niveles desde otro sistema Trusted Extensions. Los archivos montados mediante NFS no se pueden volver a etiquetar y la etiqueta de los archivos no se puede determinar con el comando `getlabel`. Sin embargo, la política MAC funciona correctamente. Los archivos montados que están en la misma etiqueta que la zona se pueden ver y modificar. Los archivos de nivel inferior se pueden ver.

Políticas de Trusted Extensions para sistemas de archivos montados

Aunque Trusted Extensions admite los mismos sistemas de archivos y comandos de gestión de sistemas de archivos que Oracle Solaris, los sistemas de archivos montados en Trusted Extensions están sujetos a las políticas de control de acceso obligatorio (MAC) para ver y modificar los datos etiquetados. Las políticas de montaje y las políticas de lectura y escritura aplican las políticas MAC para el etiquetado.

Política de Trusted Extensions para conjuntos de datos de un solo nivel

Para conjuntos de datos de un solo nivel, la política de montaje impide los montajes NFS o LOFS que posiblemente violen MAC. 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. Cualquier sistema de archivos compartidos que pertenezca a otras zonas o a servidores NFS se monta en la etiqueta del propietario.

A continuación, se resume el comportamiento de los conjuntos de datos de un solo nivel montados mediante NFS:

- En la zona global, se pueden ver todos los archivos montados, pero únicamente se pueden montar los archivos con la etiqueta `ADMIN_HIGH`.
- En una zona etiquetada, se pueden ver todos los archivos montados que son iguales o inferiores a la etiqueta de la zona, pero únicamente se pueden modificar los archivos en la etiqueta de la zona.
- En un sistema que no es de confianza, únicamente pueden verse y modificarse los sistemas de archivos de una zona etiquetada cuya etiqueta es la misma que la etiqueta asignada del sistema que no es de confianza.

Para los conjuntos de datos de un solo nivel montados mediante LOFS, se pueden ver los archivos montados. Están en la etiqueta `ADMIN_LOW`, de modo que no pueden modificarse.

Política de Trusted Extensions para conjuntos de datos de varios niveles

Para conjuntos de datos de varios niveles, las políticas de lectura y escritura de MAC se aplican en el nivel de granularidad de archivos y directorios, y no de granularidad del sistema de archivos.

Los conjuntos de datos de varios niveles únicamente se pueden montar en la zona global. Las zonas etiquetadas solamente pueden acceder a los conjuntos de datos de varios niveles mediante puntos de montaje LOFS especificados con el comando `zonecfg`. Para conocer el procedimiento, consulte Cómo crear y compartir un conjunto de datos de varios niveles [69]. Mediante los procesos con privilegios adecuados en la zona global o las zonas etiquetadas, se pueden volver a etiquetar archivos y directorios. Para ver ejemplos de reetiquetado, consulte “Guía del usuario de Trusted Extensions ”.

- En la zona global, se pueden ver todos los archivos del conjunto de datos de varios niveles. Se pueden modificar los archivos montados que tienen la etiqueta `ADMIN_HIGH`.

- En una zona etiquetada, el conjunto de datos de varios niveles está montado mediante LOFS. Se pueden ver los archivos montados en la misma etiqueta o en un nivel inferior que la zona. Se pueden modificar los archivos montados en la misma etiqueta que la zona.
- Los conjuntos de datos de varios niveles también se pueden compartir desde la zona global mediante NFS. Los clientes remotos pueden ver los archivos que están dominados por la etiqueta de red y modificar los archivos con las mismas etiquetas. Sin embargo, el reetiquetado no es posible en un conjunto de datos de varios niveles montado mediante NFS. Para obtener información sobre los montajes NFS, consulte “Montaje de conjuntos de datos de varios niveles desde otro sistema” [181].

Para obtener más información, consulte “Conjuntos de datos de varios niveles para volver a etiquetar archivos” [180].

Ninguna sustitución de privilegios para la política de lectura y escritura de MAC

La política MAC para la lectura y escritura de archivos no tiene sustituciones de privilegios. Los conjuntos de datos de un solo nivel únicamente se pueden montar como lectura y escritura si la etiqueta de la zona es igual a la etiqueta del conjunto de datos. Para montajes de sólo lectura, la etiqueta de la zona debe dominar la etiqueta del conjunto de datos. Para conjuntos de datos de varios niveles, todos los archivos y directorios deben estar dominados por la propiedad `mlslabel`, que se establece de forma predeterminada en `ADMIN_HIGH`. Para conjuntos de datos de varios niveles, la política MAC se aplica en el nivel de archivo y directorio. La aplicación de la política MAC es invisible para todos los usuarios. Los usuarios no pueden ver un objeto a menos que tengan acceso MAC al objeto.

A continuación, se resumen las políticas de uso compartido y montaje de Trusted Extensions para conjuntos de datos de un solo nivel:

- 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 sistema Trusted Extensions monte un sistema de archivos desde un sistema que no es de confianza, la etiqueta única asignada al sistema que no es de confianza por el sistema Trusted Extensions debe coincidir con la etiqueta de la zona global.

  De forma similar, para que una zona etiquetada monte un sistema de archivos desde un sistema que no es de confianza, la etiqueta única asignada al sistema que no es de confianza por el sistema Trusted Extensions debe coincidir con la etiqueta de la zona de montaje.
- Se pueden ver los archivos cuyas etiquetas difieren de la zona de montaje y están montados con LOFS, pero no se pueden modificar. Para obtener detalles sobre los montajes NFS, consulte “Servidor NFS y configuración de cliente en Trusted Extensions” [182].

A continuación, se resumen las políticas de uso compartido y montaje de Trusted Extensions para conjuntos de datos de varios niveles:

- Para que un sistema Trusted Extensions comparta un conjunto de datos de varios niveles con otro sistema, el servidor NFS debe estar configurado como un servicio de varios niveles.
- Para que un sistema Trusted Extensions comparta un conjunto de datos de varios niveles con zonas con etiquetas en su propio sistema, la zona global debe montar mediante LOFS el conjunto de datos en las zonas.

  La zona etiquetada tiene acceso de escritura a los archivos y directorios montados mediante LOFS cuya etiqueta coincide con la etiqueta de la zona y tiene acceso de lectura a los archivos y los directorios que domina. La política MAC se aplica en el nivel de archivos y directorios individuales.

Resultados del uso compartido y el montaje de sistemas de archivos en Trusted Extensions

En Trusted Extensions, los archivos compartidos pueden facilitar la administración y ofrecen eficacia y velocidad. MAC siempre está en vigor.

- Compartir conjuntos de datos de un solo nivel desde una zona etiquetada, mediante NFS: Al igual que en Oracle Solaris, los directorios compartidos facilitan la administración. Por ejemplo, puede instalar las páginas del comando man para Oracle Solaris en un sistema y compartir el directorio de la página del comando man con otros sistemas.
- Compartir conjuntos de datos de varios niveles desde la zona global, mediante LOFS: los conjuntos de datos montados mediante LOFS ofrecen eficacia y velocidad al mover archivos de una etiqueta a otra. Los archivos se mueven dentro del conjunto de datos, de modo que no se utilizan operaciones de E/S.
- Compartir conjuntos de datos de varios niveles desde la zona global, mediante NFS: un servidor NFS puede compartir con muchos clientes un conjunto de datos que contiene archivos en muchas etiquetas. Esta configuración facilita la administración y proporciona una sola ubicación para la distribución de archivos. No es necesario tener un servidor en una etiqueta determinada para ofrecer servicio a los clientes en esa etiqueta.

Uso compartido y montaje de archivos en la zona global

El montaje de archivos en la zona global es idéntico al montaje de archivos en Oracle Solaris, sujeto a la política MAC. Los archivos que se comparten desde la zona global se comparten en la etiqueta del archivo. Por lo tanto, los sistemas de archivos de una zona global no se comparten de manera útil con las zonas globales de otros sistemas Trusted Extensions, ya que todos los archivos se comparten en la etiqueta `ADMIN_LOW`. Los archivos que la zona global comparte de manera útil con otros sistemas son conjuntos de datos de varios niveles.

Los archivos y directorios en un conjunto de datos de un solo nivel que se comparten mediante LOFS desde la zona global se comparten en `ADMIN_LOW`. Por ejemplo, los archivos `/etc/passwd` y `/etc/shadow` de la zona global se pueden montar mediante LOFS en las zonas con etiquetas del sistema. Dado que los archivos son `ADMIN_LOW`, son visibles y de sólo lectura en las zonas etiquetadas. Los archivos y directorios en conjuntos de datos de varios niveles se comparten en la etiqueta del objeto.

La zona global también puede compartir conjuntos de datos de varios niveles mediante NFS. Un cliente puede solicitar montar el conjunto de datos cuando el servicio NFS está configurado para utilizar puertos de varios niveles. La solicitud funcionará correctamente cuando la etiqueta del cliente se encuentre dentro del rango de etiquetas especificado en la plantilla `cipso` para la interfaz de red que gestiona la solicitud de montaje NFS del cliente.

Específicamente, el comportamiento de las zonas globales y los archivos montados es el siguiente:

- En la zona global en clientes de Trusted Extensions, todo lo que hay en el recurso compartido se puede leer, y los clientes pueden escribir en `ADMIN_HIGH`, al igual que los procesos de la zona global y local.
- Cuando el cliente es una zona etiquetada, los archivos montados son de lectura y escritura cuando la etiqueta de la zona coincide con la etiqueta del archivo compartido.
- Cuando el cliente es un sistema sin etiquetar, los archivos montados son de lectura y escritura cuando la etiqueta asignada del cliente coincide con la etiqueta del archivo compartido.
- Los clientes en la etiqueta `ADMIN_LOW` no pueden montar el conjunto de datos.
- Para compartir conjuntos de datos de varios niveles con zonas etiquetadas en el mismo sistema, la zona global puede utilizar LOFS.

Para obtener más información sobre la visualización y el reetiquetado de archivos en un montaje NFS, consulte “Montaje de conjuntos de datos de varios niveles desde otro sistema” [181].

Uso compartido y montaje de archivos en una zona etiquetada

Una zona etiquetada puede compartir sus archivos con otros sistemas en la etiqueta de la zona. Por lo tanto, los sistemas de archivos de una zona etiquetada se pueden compartir con zonas en la misma etiqueta en otros sistemas Trusted Extensions y con sistemas que no sean de confianza que tengan asignada la misma etiqueta que la zona. Para obtener información acerca de la propiedad ZFS que media estos montajes, consulte “Propiedad `mlslabel` y montaje de sistemas de archivos de un solo nivel” [179].

Los montajes LOFS de la zona global en una zona etiquetada son de sólo lectura para los conjuntos de datos de un solo nivel. Para los conjuntos de datos de varios niveles, la política

MAC se aplica por etiqueta de archivo y directorio, como se describe en “Ninguna sustitución de privilegios para la política de lectura y escritura de MAC” [176].

Propiedad `mlslabel` y montaje de sistemas de archivos de un solo nivel

ZFS proporciona una propiedad 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 define 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, utilice una sintaxis similar a la 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.

Conjuntos de datos de varios niveles para volver a etiquetar archivos

Un conjunto de datos ZFS de varios niveles contiene archivos y directorios en diferentes etiquetas. Cada archivo y directorio se etiqueta individualmente, y las etiquetas pueden cambiarse sin necesidad de mover o copiar los archivos. Los archivos pueden volver a etiquetarse dentro del rango de etiquetas del conjunto de datos. Para crear y compartir conjuntos de datos de varios niveles, consulte Cómo crear y compartir un conjunto de datos de varios niveles [69].

Generalmente, todos los archivos y directorios en un conjunto de datos tienen la misma etiqueta que la zona en la que se monta el conjunto de datos. Esta etiqueta se registra automáticamente en una propiedad ZFS denominada `mlslabel` cuando el conjunto de datos se monta por primera vez en la zona. Estos conjuntos de datos son *conjuntos de datos etiquetados de un solo nivel*. La propiedad `mlslabel` no se puede cambiar mientras el conjunto de datos está montado, es decir, la zona de montaje no puede cambiar la propiedad `mlslabel`.

Una vez que se define la propiedad `mlslabel`, el conjunto de datos no se puede montar en modo de lectura y escritura en una zona a menos que la etiqueta de la zona coincida con la propiedad `mlslabel` del conjunto de datos. Además, un conjunto de datos no se puede montar en ZFS en una zona si actualmente está montado en ZFS en otra zona, incluida la zona global. Dado que las etiquetas de los archivos en un conjunto de datos con etiquetas de un solo nivel son fijas, al volver a etiquetar un archivo con el comando `setlabel`, el archivo se mueve al nombre de ruta equivalente en la zona principal que corresponde a la etiqueta de destino. Este movimiento en las zonas puede ser ineficaz y confuso. Los conjuntos de datos de varios niveles ofrecen un contenedor eficaz para volver a etiquetar los datos.

Para conjuntos de datos de varios niveles montados en la zona global, el valor predeterminado de la propiedad `mlslabel` es `ADMIN_HIGH`. Este valor especifica el límite superior del rango de etiquetas del conjunto de datos. Si especifica una etiqueta inferior, solamente podrá escribir en el conjunto de datos de zonas cuyas etiquetas están dominadas por la propiedad `mlslabel`.

Los usuarios o roles con el perfil de derechos de gestión de etiquetas de objetos tienen los privilegios adecuados para actualizar o degradar archivos o directorios a los que tienen acceso DAC. Para conocer el procedimiento, consulte Cómo activar a un usuario para que cambie el nivel de seguridad de los datos [145].

Para el proceso de usuario, se aplican restricciones de políticas adicionales.

- De manera predeterminada, ningún proceso en una zona con etiquetas puede volver a etiquetar archivos o directorios. Para permitir el reetiquetado, consulte Cómo permitir que los archivos se vuelvan a etiquetar desde una zona con etiquetas [170]. Para especificar controles más detallados, por ejemplo, que permitan degradar pero no actualizar archivos, consulte el Ejemplo 13-5, “Cómo permitir degradaciones únicamente de la zona `internal`”.

- Los directorios no se pueden volver a etiquetar a menos que estén vacíos.
- Los archivos y directorios no se pueden degradar por debajo de la etiqueta de su directorio que los contiene.

  Para cambiar la etiqueta, primero debe mover el archivo al directorio de nivel inferior y, a continuación, volver a etiquetarlo.
- Las zonas que montan el conjunto de datos no pueden actualizar un archivo o un directorio por encima de la etiqueta de zona.
- Los archivos no se pueden volver a etiquetar si están abiertos mediante un proceso en cualquier zona.
- Los archivos y directorios no se pueden actualizar por encima del valor `mlslabel` del conjunto de datos.

Montaje de conjuntos de datos de varios niveles desde otro sistema

La zona global pueden compartir conjuntos de datos de varios niveles mediante NFS con sistemas Trusted Extensions y sistemas sin etiquetar. Los conjuntos de datos se pueden montar en la zona global y en zonas etiquetadas, y en sistemas sin etiquetar en su etiqueta asignada. La excepción es un sistema sin etiquetar `ADMIN_LOW`. No puede montar un conjunto de datos de varios niveles.

Cuando un conjunto de datos de varios niveles se crea con una etiqueta que es inferior a `ADMIN_HIGH`, el conjunto de datos se puede montar en la zona global de otro sistema Trusted Extensions. Sin embargo, los archivos sólo se pueden ver en la zona global, no se pueden modificar. Cuando un NFS de zona con etiquetas monta un conjunto de datos de varios niveles desde una zona global de un sistema diferente, se aplican algunas restricciones.

- Se aplican algunas restricciones a los conjuntos de datos de varios niveles montados mediante NFS.
- Un cliente NFS de Trusted Extensions puede ver las etiquetas correctas solamente para los archivos modificables. El comando `getlabel` informa incorrectamente la etiqueta de los archivos de nivel inferior y la confunde con la etiqueta del cliente. La política MAC está en vigor, de modo que los archivos siguen siendo de sólo lectura y los archivos de nivel superior no son visibles.
- El servidor NFS ignora los posibles privilegios del cliente.

Debido a estas restricciones, se prefiere utilizar LOFS para clientes de zonas con etiquetas que reciben servicios desde su propia zona global. NFS funciona para estos clientes, pero éstos están sujetos a las restricciones. Para conocer el procedimiento de montaje LOFS, consulte Cómo crear y compartir un conjunto de datos de varios niveles [69].

Servidor NFS y configuración de cliente en Trusted Extensions

Los directorios de nivel inferior pueden ser visibles para los usuarios en una zona de nivel superior. El servidor NFS para los directorios de nivel inferior puede ser un sistema Trusted Extensions o un sistema que no es de confianza.

El sistema de confianza requiere la configuración del servidor. El sistema que no es de confianza requiere la configuración del cliente.

- **Configuración del servidor NFS en un sistema de confianza**: para que los directorios de nivel inferior de un sistema de confianza sean visibles en una zona con etiquetas, es necesario configurar el servidor.
  - En la zona global del servidor NFS, debe configurar el servicio NFS como un servicio de varios niveles.
  - Desde la zona global, debe agregar el privilegio `net_bindmlp` al conjungo de privilegios `limitpriv` de la zona con etiquetas.
  - En la zona etiquetada, exporte el sistema de archivos ZFS definiendo las propiedades del recurso compartido. Cuando el estado de la zona etiquetada es `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 [187].
- **Configuración de cliente NFS para un servidor NFS que no es de confianza**: dado que el servidor no es de confianza, el cliente NFS debe ser de confianza. El privilegio `net_mac_aware` debe estar especificado en el archivo de configuración de zona que se utiliza durante la configuración inicial de 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 [189].

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`.

Nota - La secuencia de comandos `txzonemgr` asume que los directorios principales se monten como `/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" [183].

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 [146].

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 [64].

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 de inicio de las zonas de nivel inferior se montan como de sólo lectura en `/zone/`*zone-name*`/export/home`. El mapa `auto_home_`*zone-name* especifica la ruta `/zone` como el directorio de origen para un nuevo montaje `lofs` en `/zone/`*zone-name*`/home/`*username*.

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.

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 NFSv3 para que usen 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 16-22, “Configuración de un puerto de varios niveles privado para NFSv3 mediante `udp`”.

Un sistema Trusted Extensions también puede compartir sus conjuntos de datos de un solo nivel con hosts sin etiquetar. Un sistema de archivos que se exporta a un host sin etiquetar es *modificable* si su etiqueta es igual a la etiqueta asignada al host remoto por el sistema de exportación. Un sistema de archivos que se exporta a un host sin etiquetar *se puede leer* únicamente si su etiqueta está dominada por la etiqueta asignada al host remoto.

Para conjuntos de datos de varios niveles que la zona global comparte con clientes que ejecutan el servicio NFSv4, la política MAC está en el nivel de granularidad de archivos y directorios individuales, no en la etiqueta de todo el conjunto de datos.

La comunicación con los sistemas que ejecutan una versión del software Trusted Solaris es posible sólo en una sola etiqueta. La etiqueta asignada del sistema Trusted Solaris determina el acceso a conjuntos de datos de un solo nivel y de varios niveles.

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.

Copia de seguridad, uso compartido y montaje de archivos con etiquetas

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.

TABLA 14-1 Copia de seguridad, uso compartido y montaje de archivos con etiquetas (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Realizar copias de seguridad de archivos.	Archiva los datos a la vez que conserva las etiquetas.	Cómo realizar copias de seguridad de los archivos en Trusted Extensions [186]
Restaurar datos.	Restaura los datos etiquetados de una copia de seguridad.	Cómo restaurar archivos en Trusted Extensions [186]
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 [187]
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 [189]
Crear puntos de montaje del directorio principal.	Se crean puntos de montaje para cada usuario en cada etiqueta. Esta tarea permite a los	Cómo permitir que los usuarios accedan a sus directorios principales remotos en cada etiqueta

Tarea	Descripción	Para obtener instrucciones
	usuarios acceder a su directorio principal en cada etiqueta, en un sistema que no es el servidor de directorio principal NFS.	mediante el inicio de sesión en cada servidor NFS [64]
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 desactivar el montaje de archivos de nivel inferior [166]
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 [190]

▼ 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.

- **Realice una copia de seguridad que conserve las etiquetas utilizando uno de los siguientes comandos:**
  - `zfs send -r | -R` *filesystem*`@snap` para copias de seguridad principales

    Para conocer los métodos disponibles, incluido el envío de copias de seguridad a un servidor remoto, consulte "Envío y recepción de datos ZFS" de "Gestión de sistemas de archivos ZFS en Oracle Solaris 11.2 ".
  - `/usr/sbin/tar cT` para las copias pequeñas

    Para obtener detalles sobre la opción `T` para el comando `tar`, consulte la página del comando man `tar`(1).
  - Una secuencia de comandos que llama a los comandos de copia de seguridad `zfs` o `tar`

▼ Cómo restaurar archivos en Trusted Extensions

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

- **Restaure una copia de seguridad con etiquetas mediante uno de los siguientes comandos:**
  - `zfs receive -vF` *filesystem*`@snap` para restauraciones principales

    Para conocer los métodos disponibles, incluida la restauración de copias de seguridad de un servidor remoto, consulte "Envío y recepción de datos ZFS" de "Gestión de sistemas de archivos ZFS en Oracle Solaris 11.2 ".
  - `/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).

- Una secuencia de comandos que llama a los comandos de restauración `zfs` o `tar`

▼ 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 uso compartido de ZFS adecuadas en el sistema de archivos. A continuación, reinicie la zona para compartir los directorios con etiquetas.

Atención - 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 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 "Gestión de sistemas de archivos ZFS en Oracle Solaris 11.2 ".

6. **Para permitir que el cliente monte el sistema de archivos compartido, consulte Cómo montar archivos en NFS en una zona con etiquetas [189].**

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/reference` 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 al host remoto que no es de confianza la misma etiqueta que la zona de montaje.
  - El host remoto de confianza 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, un sistema con una zona global y una zona public tiene 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 `auto_home_`*nombre-de-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 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-de-zona-con-etiqueta-inferior*.**

    b. **Edite el archivo `/etc/auto_home`_*nombre-de-zona-con-etiqueta-inferior* a fin de que señale al archivo que recién se rellenó.**

    c. **Modifique el archivo `/etc/auto_home`_*nombre-de-zona-con-etiqueta-inferior* en cada zona de nivel superior a fin de que apunte al archivo que creó en el Paso 1.3.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 de 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, utilice las opciones `vers=3` y `proto=udp` del 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

En este capítulo, se describen los conceptos y los mecanismos de las redes de confianza de Trusted Extensions.

- “Acerca de la red de confianza” [193]
- “Atributos de seguridad de red en Trusted Extensions” [198]
- “Mecanismo de reserva de la red de confianza” [202]
- “Acerca del enrutamiento en Trusted Extensions” [203]
- “Administración del enrutamiento en Trusted Extensions” [207]
- “Administración de IPsec con etiquetas” [210]

Acerca de 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. La etiqueta 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.

Trusted Extensions admite etiquetas en paquetes IPv4 e IPv6.

- Para los paquetes IPv4, Trusted Extensions las etiquetas de opción de seguridad de IP comercial (CIPSO).
- Para los paquetes IPv6, Trusted Extensions admite la opción de seguridad de IPv6 de etiquetas de arquitectura común (CALIPSO).

  Si debe interactuar con sistemas en una red CIPSO IPv6, consulte Cómo configurar una red CIPSO IPv6 en Trusted Extensions [42].

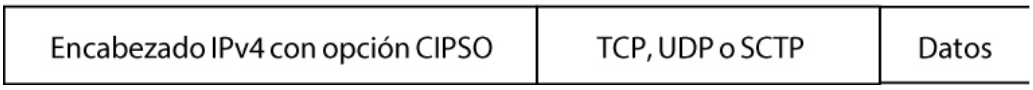
Por lo general, en una red de confianza, el host de envío genera la etiqueta y el host de recepción la procesa. Sin embargo, un enrutador de confianza también puede agregar o filtrar etiquetas cuando reenvía paquetes en una red de confianza. Antes de la transmisión, se asigna una etiqueta de sensibilidad a una etiqueta CALIPSO o CIPSO. Esta etiqueta se incrusta en el paquete IP que, luego, es un paquete *etiquetado* paquete. 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. Los paquetes de datos CIPSO se envían mediante redes IPv4. Los paquetes CALIPSO se envían mediante redes 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 opciones es seguido de un encabezado TCP, UDP o SCTP, y, a continuación, de los datos reales. La versión de Trusted Extensions de un paquete IPv6 utiliza la opción CALIPSO del encabezado IP para los atributos de seguridad.

Paquetes de multidifusión Trusted Extensions

Trusted Extensions puede agregar etiquetas a paquetes de multidifusión dentro de una LAN. Esta función le permite enviar paquetes de multidifusión etiquetados a sistemas CIPSO o CALIPSO que operan en la misma etiqueta o dentro del rango de etiquetas de paquetes de multidifusión. En una LAN heterogénea, es decir, una LAN con hosts etiquetados y sin etiquetar, la multidifusión no puede verificar la pertenencia de un grupo de multidifusión.

Atención - No envíe paquetes de multidifusión etiquetados mediante una LAN heterogénea. Es posible que se filtre información de etiquetas.

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 y que reconocen etiquetas CIPSO para paquetes IPv4 y etiquetas CALIPSO para paquetes IPv6.

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” [196].

  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” [197].
- 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 Configuración inicial de Trusted Extensions [15], 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.

- Trusted Extensions amplía el archivo de configuración de IKE, `/etc/inet/ike/config`. Para obtener más información, consulte “Administración de IPsec con etiquetas” [210] 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 `txzonemgr` o `tncfg`. 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 caché 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 caché 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` *label*, `outer-label` *label* e `implicit-label` *label*. Para obtener detalles, 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” [159].
- `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. Sin embargo, cuando un host *adaptativo* es el remitente, la interfaz de red receptora asigna la etiqueta predeterminada a los paquetes entrantes. Para obtener detalles sobre los atributos de seguridad, consulte “Atributos de seguridad de red en Trusted Extensions” [198].

- `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:

- Uno de cuatro tipos de host: `unlabeled`, `cipso`, `adaptive` o `netif`. El tipo de host de la plantilla determina el protocolo que se utiliza para las comunicaciones de red. Consulte “Tipo de host y nombre de plantilla en plantillas de seguridad” [199].
- 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” [198].

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” [202].

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 CALIPSO o CIPSO, o no tienen ningún tipo de etiqueta.
- **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” [200].
- **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 cuatro tipos de hosts en las bases de datos de red de confianza y proporciona cuatro plantillas predeterminadas:

- **Tipo de host** `cipso`: destinado a los hosts que ejecutan sistemas operativos de confianza. Este tipo de host admite etiquetas CALIPSO y CIPSO.

  Para IPv6, el protocolo CALIPSO se utiliza para especificar las etiquetas de seguridad que se transfieren en el campo de opciones IP. Para IPv4, se utiliza el protocolo CIPSO. Las etiquetas en encabezados CALIPSO y CISCO se derivan automáticamente de la etiqueta de los datos. La etiqueta derivada se utiliza para realizar comprobaciones de seguridad en el nivel IP y para etiquetar los paquetes de red.

- **Tipo de host** `unlabeled`: destinado a los hosts que usan protocolos de red estándar, pero que no admiten opciones etiquetadas. Trusted Extensions proporciona 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 host tipo proporciona una etiqueta predeterminada para aplicarla a las comunicaciones con el host sin etiquetar. 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.
- **Tipo de host** `adaptive`: destinado a subredes de hosts sin etiquetar, pero que envían paquetes a una interfaz de red específica en un sistema etiquetado. El sistema etiquetado aplica su etiqueta predeterminada de interfaz de red a los paquetes entrantes.

  Este tipo de host se asigna a los hosts que ejecutan SO Oracle Solaris u otros sistemas operativos sin etiquetar, que se espera que envíen datos a un sistema etiquetado. Este tipo de host no proporciona una etiqueta predeterminada. La etiqueta de comunicación se deriva de la interfaz de red etiquetada del sistema receptor. Este tipo de host se asigna a sistemas de nodo final, no puertas de enlace.

  El tipo de host `adaptive` proporciona flexibilidad para planificar y escalar una red de confianza. Los administradores pueden ampliar la red con nuevos sistemas sin etiquetar, sin necesidad de conocer de forma anticipada la etiqueta predeterminada de los nuevos sistemas. Cuando un host `adaptive` está configurado para enviar paquetes a una interfaz de red etiquetada en un host `netif`, la etiqueta predeterminada de la interfaz en ese host `netif` asigna la etiqueta adecuada para los paquetes entrantes.
- **Tipo de host** `netif`: destinado para los nombres de host de las interfaces que reciben paquetes en una interfaz de red específica de hosts `adaptive`. Este tipo de host se asigna a las interfaces en sistemas Trusted Extensions. La etiqueta predeterminada de la interfaz `netif` se aplica a los paquetes entrantes.

Atención - 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 los tipos de host `unlabeled` y `netif` 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 un dominio de interpretación diferente [43].

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:

- Para establecer el rango de etiquetas que puede utilizarse cuando un host se comunica con un host etiquetado 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.
- Para establecer un rango de etiquetas para los paquetes que se reenvían mediante una puerta de enlace etiquetada o una sin etiquetar

  Puede especificarse el rango de etiquetas en la plantilla para un tipo de host sin etiquetas. El rango de etiquetas activa 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, “Entradas del mecanismo de reserva y la dirección de host de Trusted Extensions”.

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`
	
	`192.168.118.57/32`
		`192.168.118.57`
		
		`/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`
	
	`192.168.118.0/24`
		Todas las direcciones de la subred `192.168.118.`

	`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.`

Versión de IP	Entrada de host para `host_type=cipso`	Direcciones IP cubiertas
	`192.168.0.0/16`	
	`192.0.0.0` `192.0.0.0/8`	Todas las direcciones de la subred `192.`
	`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` en un servidor Sun Ray que presta servicios a clientes DHCP, consulte el Ejemplo 16-19, “Configuración de una dirección inicial válida para un servidor Sun Ray etiquetado”. Para crear una entrada `tnrhdb` para una aplicación que presta servicios a clientes DHCP, consulte el Ejemplo 16-18, “Cómo hacer que la dirección de host `0.0.0.0/32` sea una dirección inicial válida”. 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 [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 “Planificación de la implementación de red en Oracle Solaris 11.2 ”.

Acerca 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.

Nota - La puerta de enlace etiquetada que se espera que reenvíe paquetes de hosts `adaptive` debe configurar su interfaz entrante con una plantilla de tipo de host `netif`. Para obtener definiciones de los tipos de host `adaptive` y `netif`, consulte “Tipo de host y nombre de plantilla en plantillas de seguridad” [199].

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 verifica el rango de etiquetas y la información de etiquetas CALIPSO o 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.

En las comunicaciones entrantes, el software de Trusted Extensions obtiene etiquetas de los mismos 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 que se indica en la opción CALIPSO o CIPSO.
- Las comprobaciones para el reenvío 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 etiquetado debe estar dentro del rango de etiquetas del host de destino.
  - La puerta de enlace etiquetada que se espera que reenvíe paquetes de hosts `adaptive` debe configurar su interfaz entrante con una plantilla de tipo de host `netif`. Para obtener definiciones de los tipos de host `adaptive` y `netif`, consulte “Tipo de host y nombre de plantilla en plantillas de seguridad” [199].

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 que se indica en la opción etiquetada.
- 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:

- “Dónde encontrar más información acerca de la administración de redes en Oracle Solaris” de “Configuración y administración de componentes de red en Oracle Solaris 11.2 ”
- Página del comando man `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 etiquetados descartan los paquetes cuando no encuentran el tipo correcto de información en la sección de opciones IP del paquete. Por ejemplo, un enrutador etiquetado descarta un paquete si no encuentra una opción etiquetada en las opciones IP cuando la

opción es necesaria o cuando el DOI de las opciones IP no es coherente 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 los paquetes que incluyen una opción etiquetada. Solamente las puertas de enlace que reconocen las etiquetas, como Trusted Extensions, pueden utilizar el contenido de la opción IP de CALIPSO o CIPSO para aplicar la 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” [205], 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).

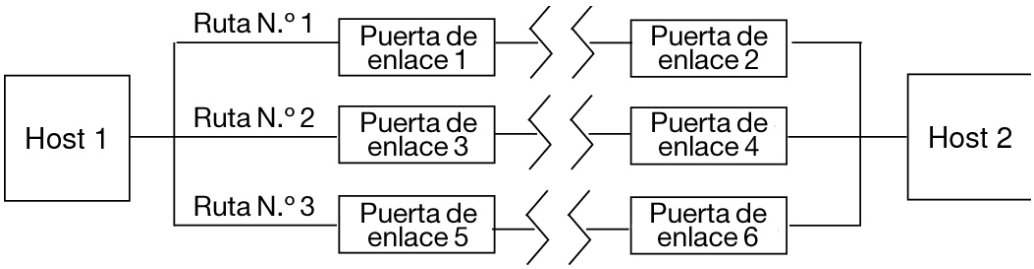
El software de enrutamiento intenta buscar una ruta para el host de destino en las tablas de enrutamiento. Cuando el host no está nombrado de manera explícita, el software de enrutamiento busca una entrada para la subred donde reside el host. Cuando no están definidos ni el host ni la subred, el host 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
#1	Puerta de enlace 1	`CONFIDENTIAL`	`SECRET`	1
#2	Puerta de enlace 3	`ADMIN_LOW`	`ADMIN_HIGH`	1
#3	Puerta de enlace 5			

- La ruta n.° 1 puede transmitir paquetes dentro del rango de etiquetas de `CONFIDENTIAL` a `SECRET`.
- La ruta n.° 2 puede transmitir paquetes de `ADMIN_LOW` a `ADMIN_HIGH`.
- La ruta n.° 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 [234].

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 explícitamente utilizando las opciones IP de CALIPSO o CIPSO. Las etiquetas se envían implícitamente utilizando las asociaciones de seguridad (SA) IPsec etiquetadas. 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 IPsec generales, consulte “Protección de la red en Oracle Solaris 11.2 ”. Para conocer las modificaciones de Trusted Extensions en los procedimientos de IPsec, consulte “Configuración de IPsec con etiquetas” [237].

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” [205].

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.
- Suprima el uso de las opciones IP de CALIPSO o CIPSO en los paquetes IP. Esta configuración permite que el tráfico etiquetado atraviese las redes que reconocen las etiquetas o que son hostiles respecto de las etiquetas.

Puede especificar si desea usar extensiones de etiquetas automáticamente mediante IKE, como se describe en “Extensiones de etiquetas para IKE” [212], 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

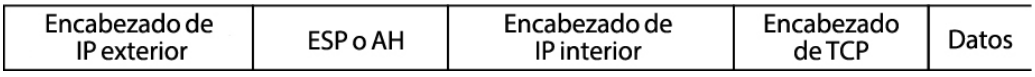
IKE en los sistemas Trusted Extensions admite la negociación de etiquetas para las asociaciones de seguridad con iguales que reconocen etiquetas. Para controlar este mecanismo, puede usar las siguientes palabras clave en el archivo `/etc/inet/ike/config`:

- **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 las opciones IP etiquetadas 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 etiquetadas en los paquetes transmitidos.
- *label* **wire_label none**: genera un comportamiento similar a *label* `wire_label`, excepto que las opciones IP etiquetadas se suprimen en los paquetes IKE transmitidos y los paquetes de datos en la asociación de seguridad.

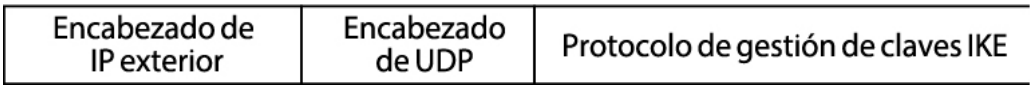
Para obtener más información, consulte la página del comando man `ike.config`(4).

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.



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” [205].

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	La etiqueta es visible en la opción IP etiquetada.	La etiqueta de mensaje en la opción IP etiquetada es cubierta por AH, no por ESP. Consulte la nota.
Con extensiones de etiquetas	Una opción IP etiquetada es 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. La opción IP etiquetada en la transferencia es cubierta por AH. Consulte la nota.
Con extensiones de etiquetas y opción IP etiquetada 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 etiquetada si los enrutadores que reconocen etiquetas pueden filtrar o agregar la opción IP etiquetada a medida que el mensaje viaja a través de la red. Cualquier modificación realizada a la IP etiquetada invalidará el mensaje y hará que se descarte un paquete protegido por AH en el destino.

♦ ♦ ♦ CAPÍTULO 16

Gestión de redes en Trusted Extensions

En este capítulo se proporcionan detalles y procedimientos de implementación para proteger las redes de Trusted Extensions.

- "Etiquetado de hosts y redes" [215]
- "Configuración de rutas y puertos de varios niveles" [234]
- "Configuración de IPsec con etiquetas" [237]
- "Resolución de problemas de la red de confianza" [242]

Etiquetado de hosts y redes

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.

Cómo determinar si necesita plantillas de seguridad específicas del sitio

Puede crear plantillas de seguridad específicas del sitio si desea realizar alguna de las siguientes acciones para los hosts con los que se comunica:

- 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 hosts sin etiquetas que no sea `AD MIN_LOW`.
- Cree un host que reconozca un conjunto limitado de etiquetas.
- Utilice un dominio de interpretación distinto de `1`.
- Envíe información desde hosts sin etiquetar especificados hasta una interfaz de red de confianza configurada para asignar la etiqueta correcta a los paquetes desde los hosts sin etiquetas.

Visualización de plantillas de seguridad existentes

Antes de etiquetar redes y hosts remotos, revise la plantillas de seguridad proporcionadas y asegúrese de que puede acceder a las redes y los hosts remotos. Para obtener instrucciones, consulte lo siguiente:

- Ver las plantillas de seguridad. Consultar Cómo ver plantillas de seguridad [216].
- Determinar si el sitio requiere plantillas de seguridad personalizadas. Consultar “Cómo determinar si necesita plantillas de seguridad específicas del sitio” [215].
- Agregar sistemas y redes a la red de confianza. Consultar Cómo agregar hosts a la red conocida del sistema [217].

▼ 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 usan las plantillas de seguridad predeterminadas.

1. **Consulte las plantillas de seguridad disponibles.**

```
# tncfg list
cipso
admin_low
adapt
netif
```

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 no 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 la entrada `0.0.0.0/0` 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 la entrada `0.0.0.0/0` 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 [229].

```
# tncfg -t adapt info
name=adapt
host_type=adapt
doi=1
min_label=ADMIN_LOW
max_label=ADMIN_HIGH
host=0.0.0.0/0
```

Una plantilla `adapt` identifica un host `adaptive`, es decir, un sistema que no es de confianza que no puede tener una etiqueta predeterminada. En cambio, su etiqueta es asignada por el sistema de confianza receptor. La etiqueta se deriva de la etiqueta predeterminada de la interfaz IP que recibe el paquete, como se especifica en la plantilla `netif` del sistema etiquetado.

```
# tncfg -t netif info
name=netif
host_type=netif
doi=1
def_label=ADMIN_LOW
min_label=ADMIN_LOW
max_label=ADMIN_HIGH
host=127.0.0.1/32
```

Una plantilla `netif` especifica una interfaz de red local de confianza, *no* un host remoto. La etiqueta predeterminada de una plantilla `netif` debe ser igual a la etiqueta de cada zona con una interfaz de red dedicada cuya dirección IP coincide con una dirección de host en esa plantilla. Además, el enlace inferior correspondiente a la interfaz de zona coincidente solamente se puede asignar a otras zonas que comparten la misma etiqueta.

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

1. **Agregue hosts individuales al archivo `/etc/hosts`.**

```
# pfedit /etc/hosts

...
192.168.111.121   ahost
```

2. **Agregue un grupo de hosts al archivo `/etc/hosts`.**

```
# pfedit /etc/hosts

...
192.168.111.0   111-network
```

Creación de plantillas de seguridad

Esta sección contiene referencias o ejemplos sobre la creación de plantillas de seguridad para las siguientes configuraciones de red:

- El dominio de interpretación es un valor distinto de `1`. Consulte Cómo configurar un dominio de interpretación diferente [43].
- A los hosts remotos de confianza se les asigna una etiqueta específica. Consulte el Ejemplo 16-1, “Creación de una plantilla de seguridad para una puerta de enlace que gestiona paquetes en una sola etiqueta”.
- A los hosts remotos no de confianza se les asigna una etiqueta específica. Consulte el Ejemplo 16-2, “Creación de una plantilla de seguridad sin etiquetas en la etiqueta `PUBLIC`”.

Para ver más ejemplos de plantillas de seguridad que satisfacen requisitos específicos, consulte “Agregación de hosts a plantillas de seguridad” [221].

▼ 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.

Nota - Por razones de compatibilidad, no modifique ni 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 [229].

---

1. **(Opcional) Determine la versión hexadecimal de cualquier etiqueta que no sea `ADMIN_HIGH` ni `ADMIN_LOW`.**

   Para las etiquetas como `CONFIDENTIAL`, puede utilizar la cadena de etiqueta o el valor hexadecimal como valor 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 [122].

2. **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. Presione la tecla de tabulación para completar los valores y las propiedades parciales. Escriba `exit` para completar la plantilla.

     ```
     # tncfg -t newunlabeled
     tncfg:newunlabeled> info
     name=newunlabeled
     host_type=unlabeled
     doi=1
     def_label=ADMIN_LOW
     min_label=ADMIN_LOW
     max_label=ADMIN_HIGH
     tncfg:newunlabeled> set mTab
     set max_label=" set min_label="      Auto-complete shows two possible completions
     tncfg:newunlabeled> set maTab        User types the letter a
     tncfg:newunlabeled> set max_label=ADMIN_LOW
     ...
     tncfg:newunlabeled> commit
     tncfg:newunlabeled> exit
     ```

     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`. Un atributo omitido recibe el valor predeterminado. Para obtener información sobre los atributos de seguridad de la red, consulte “Atributos de seguridad de red en Trusted Extensions” [198].

     ```
     # 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: unlab_1> set host_type=unlabeled
...
# tncfg -f template-file
```

Para ver un ejemplo de creación de 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 información sobre la agregación, consulte el Ejemplo 16-4, “Creación de una puerta de enlace que gestiona paquetes en una sola etiqueta”.

ejemplo 16-2 Creación de una plantilla de seguridad sin etiquetas en la etiqueta `PUBLIC`

En este ejemplo, el administrador de seguridad crea una plantilla sin etiquetar para hosts que no son de confianza 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 información sobre la agregación, consulte el Ejemplo 16-15, “Creación de una subred sin etiquetas en la etiqueta `PUBLIC`”.

Agregación de hosts a plantillas de seguridad

Esta sección contiene referencias o ejemplos sobre la agregación de hosts a plantillas de seguridad. Para direcciones IP discontinuas, consulte Cómo agregar un host a una plantilla de seguridad [221]. Para un rango de hosts, consulte Cómo agregar un rango de hosts a una plantilla de seguridad [227].

Los ejemplos de esta sección muestran las siguientes asignaciones de etiqueta de host remoto:

- Una puerta de enlace remota de confianza gestiona el tráfico `PUBLIC`. Consulte el Ejemplo 16-4, “Creación de una puerta de enlace que gestiona paquetes en una sola etiqueta”.
- Los hosts remotos que no son de confianza actúan como enrutadores de una sola etiqueta: Ejemplo 16-5, “Creación de un enrutador sin etiquetas para redirigir paquetes con etiquetas”
- Los hosts remotos de confianza restringen el tráfico a un rango de etiquetas estrecho. Consulte el Ejemplo 16-6, “Creación de una puerta de enlace con un rango de etiquetas limitado”.
- A los hosts remotos de confianza se les asigna un conjunto limitado de etiquetas. Consulte el Ejemplo 16-7, “Creación de hosts en etiquetas discretas”.
- A los hosts remotos de confianza se les asignan etiquetas que están separadas del resto de la red. Consulte el Ejemplo 16-8, “Creación de un host con etiquetas para desarrolladores”.
- Un host `netif` de confianza etiqueta paquetes de sistemas `adaptive`. Consulte el Ejemplo 16-9, “Creación de una plantilla de seguridad para un host `netif`”.
- Un host `adaptive` no de confianza envía paquetes a un host `netif`. Consulte el Ejemplo 16-10, “Creación de plantillas de seguridad para hosts adaptables”.
- Una red homogénea de confianza agrega una dirección de multidifusión en una etiqueta específica. Consulte el Ejemplo 16-11, “Envío de mensajes de multidifusión etiquetados”.
- Un host se elimina de una plantilla de seguridad. Consulte el Ejemplo 16-12, “Eliminación de varios hosts de una plantilla de seguridad”.
- Se asignan etiquetas a redes y hosts remotos que no son de confianza. Consulte el Ejemplo 16-15, “Creación de una subred sin etiquetas en la etiqueta `PUBLIC`”.

▼ Cómo agregar un host a una plantilla de seguridad

Antes de empezar Se deben cumplir los siguientes requisitos:

- 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 [217].

Para el DNS, consulte el Capítulo 3, “Gestión de sistema de nombres de dominio” de “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: DNS y NIS ”.

- Los puntos finales de la etiqueta deben coincidir. Para las reglas, consulte “Acerca del enrutamiento en Trusted Extensions” [203].
- Debe estar con el rol de administrador de la seguridad en la zona global.

1. **(Opcional) Verifique que pueda acceder al nombre de host o la dirección IP que va a agregar.**

   En este ejemplo, verifique que puede acceder a `192.168.1.2`.

   ```
   # arp 192.168.1.2
   gateway-2.example.com (192.168.1.2) at 0:0:0:1:ad:cd
   ```

   El comando `arp` verifica que el host está definido en el archivo `/etc/hosts` del sistema o que DNS puede resolverlo.

2. **Agregue un nombre de host o una dirección IP a una plantilla de seguridad.**

   En este ejemplo, agrega 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. Para el mensaje informativo, consulte el Ejemplo 16-3, “Reemplazo de la asignación de plantilla de seguridad de un host”.

3. **Vea la plantilla de seguridad modificada.**

   En el siguiente ejemplo 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.

4. **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 16-12, “Eliminación de varios hosts de una plantilla de seguridad”.

ejemplo 16-3 Reemplazo de la asignación de plantilla de seguridad de un host

En este ejemplo se muestra el mensaje informativo que aparece cuando se asigna una plantilla de seguridad a un host que ya tiene una asignación de plantilla.

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.1.2
192.168.1.2 previously matched the admin_low template
tncfg:cipso> info
...
host=192.168.1.2/32
tncfg:cipso> exit
```

ejemplo 16-4 Creación de una puerta de enlace que gestiona paquetes en una sola etiqueta

En el Ejemplo 16-1, “Creación de una plantilla de seguridad para una puerta de enlace que gestiona paquetes en una sola etiqueta”, el administrador de la seguridad 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 16-5 Creación de un enrutador sin etiquetas para redirigir paquetes con etiquetas

Cualquier enrutador IP puede reenviar mensajes con etiquetas CALIPSO o 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`.

En primer lugar, el administrador de la seguridad crea la plantilla desde el principio.

```
# tncfg -t unl_public_router
tncfg:unl_public_router> set host_type=unlabeled
tncfg:unl_public_router> set doi=1
tncfg:unl_public_router> set def_label="PUBLIC"
tncfg:unl_public_router> set min_label=ADMIN_LOW
tncfg:unl_public_router> set max_label=ADMIN_HIGH
tncfg:unl_public_router> exit
```

A continuación, el administrador agrega el enrutador a la plantilla de seguridad.

```
# tncfg -t unl_public_router
tncfg:unl_public_router> add host=192.168.131.82
tncfg:unl_public_router> exit
```

El sistema puede enviar y recibir de inmediato paquetes en todas las etiquetas por medio de `router-1`, el nombre de host de la dirección `192.168.131.82`.

ejemplo 16-6 Creación de una puerta de enlace con un rango de etiquetas limitado

En este ejemplo, el administrador de la seguridad crea una plantilla que limita los paquetes a un rango de etiquetas estrecho y agrega la puerta de enlace a la plantilla.

```
# arp 192.168.131.78
gateway-ir.example.com (192.168.131.78) at 0:0:0:3:ab:cd

# 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 sistema puede enviar y recibir de inmediato paquetes con las etiquetas `internal` y `restricted` por medio de `gateway-ir`.

ejemplo 16-7 Creación de hosts en 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.

Primero, el administrador de seguridad garantiza que se puedan 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
```

A continuación, 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 `cnf :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
```

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 16-8 Creación de un host con etiquetas para desarrolladores

En este ejemplo, el administrador de la seguridad crea una plantilla de seguridad `cipso_sandbox`. Esta plantilla 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> 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 16-9 Creación de una plantilla de seguridad para un host `netif`

En este ejemplo, el administrador de seguridad crea una plantilla de seguridad `netif`. Esta plantilla se asigna a la interfaz de red etiquetada que contiene la dirección IP `10.121.10.3`. Con esta asignación, el módulo IP de Trusted Extensions agrega la etiqueta predeterminada, `PUBLIC`, a todos los paquetes entrantes que provienen de un host `adaptive`.

```
# tncfg -t netif_public
tncfg:netif_public> set host_type=netif
tncfg:netif_public> set doi=1
tncfg:netif_public> set def_label="PUBLIC"
tncfg:netif_public> add host=10.121.10.3
tncfg:netif_public> commit
tncfg:netif_public> exit
```

ejemplo 16-10 Creación de plantillas de seguridad para hosts adaptables

En este ejemplo, el administrador de seguridad planifica con anticipación. El administrador crea diferentes subredes para una red que contiene información pública y una red que contiene información interna. Luego, el administrador define dos hosts `adaptive`. A los sistemas de la subred pública se les asigna la etiqueta `PUBLIC`. A los sistemas de la red interna se les asigna la etiqueta `IUO`. Dado que esta red se planifica con anticipación, cada red contiene y transmite información en una determinada etiqueta. Otra ventaja es que la red es fácil de depurar cuando los paquetes no se entregan en la interfaz esperada.

```
# tncfg -t adpub_192_168_10
tncfg:adapt_public> set host_type=adapt
tncfg:adapt_public> set doi=1
tncfg:adapt_public> set min_label="public"
tncfg:adapt_public> set max_label="public"
tncfg:adapt_public> add host=192.168.10.0
tncfg:adapt_public> commit
tncfg:adapt_public> exit

# tncfg -t adiuo_192_168_20
tncfg:adapt_public> set host_type=adapt
tncfg:adapt_public> set doi=1
tncfg:adapt_public> set min_label="iuo"
tncfg:adapt_public> set max_label="iuo"
tncfg:adapt_public> add host=192.168.20.0
tncfg:adapt_public> commit
tncfg:adapt_public> exit
```

ejemplo 16-11 Envío de mensajes de multidifusión etiquetados

En este ejemplo, en una LAN homogénea con etiquetas, el administrador de la seguridad elige una dirección de multidifusión disponible por medio de la cual enviar paquetes en la etiqueta `PUBLIC`.

```
# tncfg -t cipso_public
tncfg:cipso_public> add host=224.4.4.4
tncfg:cipso_public> exit
```

ejemplo 16-12 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 [221].

1. **Para asignar una plantilla de seguridad a una subred, agregue la dirección de subred a la plantilla.**

   En este ejemplo, agrega dos subredes IPv4 a la plantilla `cipso` y, a continuación, visualiza 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.

   ```
   # 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 rango de direcciones, especifique la dirección IP y la longitud del prefijo.**

   En el siguiente ejemplo, la longitud del prefijo `/25` abarca direcciones IPv4 contiguas de `192.168.113.0` a `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 `/56` abarca direcciones IPv6 contiguas de `2001:a08:3903:200::0` a `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 agrega un host que se agregó anteriormente a otra plantilla, se le notificará que está sustituyendo la asignación de plantilla de seguridad. Para el mensaje informativo, consulte el Ejemplo 16-13, “Reemplazo de la plantilla de seguridad para un rango de hosts”.

   Una entrada mal escrita también genera un mensaje informativo, como se muestra en el Ejemplo 16-14, “Manejo de una dirección IP mal escrita en una plantilla de seguridad”.

ejemplo 16-13 Reemplazo de la plantilla de seguridad para un rango de hosts

En este ejemplo, se muestra el mensaje informativo que aparece cuando se asigna una plantilla de seguridad a un rango de hosts que ya tiene una asignación de plantilla.

```
# 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 explicó en “Mecanismo de reserva de la red de confianza” [202].

ejemplo 16-14 Manejo de una dirección IP mal escrita en una plantilla de seguridad

Una entrada mal escrita genera un mensaje informativo. En la siguiente agregación de host se omite `:200` de la dirección:

```
# tncfg -t cipso
```

```
tncfg:cipso> add host=2001:a08:3903::0/56
Invalid host: 2001:a08:3903::0/56
```

ejemplo 16-15 Creación de una subred sin etiquetas en la etiqueta `PUBLIC`

En el Ejemplo 16-2, “Creación de una plantilla de seguridad sin etiquetas en la etiqueta `PUBLIC`”, el administrador de la seguridad crea una plantilla de seguridad que asigna la etiqueta `PUBLIC` a un host que no es de confianza. En este ejemplo, el administrador de la seguridad asigna una subred a la etiqueta `PUBLIC`. Los usuarios del sistema de asignación pueden montar sistemas de archivos desde hosts de esta subred en una zona `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`.

Limitación de los hosts que pueden acceder a la red de confianza

En esta sección, puede proteger la red limitando los hosts que pueden acceder a la red.

- Cómo limitar los hosts que se pueden contactar en la red de confianza [229].
- Aumente la seguridad mediante la especificación de sistemas para contactar durante el inicio. Consulte el Ejemplo 16-16, “Cambio de la etiqueta de la dirección IP `0.0.0.0/0`”.
- Configure un servidor de aplicaciones para aceptar el contacto inicial desde un cliente remoto. Consulte el Ejemplo 16-18, “Cómo hacer que la dirección de host `0.0.0.0/32` sea una dirección inicial válida”.
- Configure un servidor Sun Ray con etiquetas para aceptar el contacto inicial desde un cliente remoto. Consulte el Ejemplo 16-19, “Configuración de una dirección inicial válida para un servidor Sun Ray etiquetado”.

▼ 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`.

Atención - La plantilla `admin_low` predeterminada puede ser 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 inicialmente reconoce 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`. Por ejemplo, para recibir las solicitudes de conexión inicial de los posibles clientes Sun Ray, los servidores Sun Ray deben incluir esta entrada. A continuación, cuando el servidor reconoce los clientes, se proporciona una dirección IP a los clientes y se los conecta como clientes etiquetados.

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 16-17, “Enumeración de sistemas que un sistema Trusted Extensions puede contactar durante el inicio” para ver una base de datos de ejemplo.

3. **Compruebe que las asignaciones de hosts permitan que el sistema se inicie.**

ejemplo 16-16 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 16-17 Enumeración de sistemas que un sistema Trusted Extensions puede 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 16-18 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.

ejemplo 16-19 Configuración de una dirección inicial válida para un servidor Sun Ray etiquetado

En este ejemplo, el administrador de la seguridad configura un servidor Sun Ray para aceptar las solicitudes de conexión inicial de clientes potenciales. El servidor utiliza una topología privada y los valores predeterminados del servidor Sun Ray.

```
# utadm -a net0
```

Luego, 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       Sun Ray server address
host=192.168.128.0/24       Sun Ray 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       Sun Ray 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       Sun Ray 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` permite que solamente los clientes Sun Ray accedan al servidor.

Configuración de rutas y puertos de varios niveles

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

Este procedimiento agrega una ruta predeterminada mediante la interfaz gráfica de usuario. El ejemplo muestra cómo agregar una ruta predeterminada mediante la línea de comandos.

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 [221] y Cómo agregar un rango de hosts a una plantilla de seguridad [227].

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 16-20 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 que explícitamente tienen la etiqueta `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` por medio 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 [234].

ejemplo 16-21 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 16-22 Configuración de un puerto de varios niveles privado para NFSv3 mediante `udp`

En este ejemplo, el administrador activa 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 16-23 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

El siguiente mapa de tareas describe las tareas que se utilizan para agregar etiquetas a las protecciones IPsec.

TABLA 16-1 Mapa de tareas de configuración de IPsec con etiquetas

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 [238]
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 [240]

▼ 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 CALIPSO o 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 Debe estar con 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 descriptos en "Etiquetado de hosts y redes" [215]. 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 de red seguro entre dos servidores con IPsec" de "Protección de la red en Oracle Solaris 11.2 ". Utilice IKE para la gestión de claves, como se describe en el siguiente paso.

3. **Agregue etiquetas a las negociaciones IKE.**

   Siga el procedimiento descripto en "Cómo configurar IKEv2 con claves compartidas previamente" de "Protección de la red en Oracle Solaris 11.2 " 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, en la red, no se puede utilizar la protección AH de las opciones IP de CALIPSO o CIPSO, 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 los archivos `ike/config` de manera similar cuando complete los procedimientos descriptos en “Configuración de IKEv2 con certificados de claves públicas” de “Protección de la red en Oracle Solaris 11.2 ”.

▼ 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 “Protección de la red en Oracle Solaris 11.2 ”.

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 CALIPSO o CIPSO se visualizan en estas 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 CALIPSO o CIPSO.
- El tráfico con etiquetas entre `euro-vpn` y `calif-vpn` está protegido contra cambios no autorizados.

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

1. **Siga los procedimientos descriptos en “Etiquetado de hosts y redes” [215] 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 `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 descripto en "Cómo proteger la conexión entre dos LAN con IPsec en modo de túnel" de "Protección de la red en Oracle Solaris 11.2 ". Utilice IKE para la gestión de claves, como se describe en el siguiente paso.

3. **Agregue etiquetas a las negociaciones IKE.**

Siga el procedimiento descripto en "Cómo configurar IKEv2 con claves compartidas previamente" de "Protección de la red en Oracle Solaris 11.2 " 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 los archivos `ike/config` de manera similar cuando complete los procedimientos descriptos en “Configuración de IKEv2 con certificados de claves públicas” de “Protección de la red en Oracle Solaris 11.2 ”.

Resolución de problemas de la red de confianza

El siguiente mapa de tareas describe las tareas que ayudan a depurar la red de Trusted Extensions.

TABLA 16-2 Mapa de tareas de resolución de problemas de la red de confianza

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 [243]
	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 [244]
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 [247]

▼ 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) and `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” [162].
- Para obtener información sobre la depuración de los montajes de NFS, consulte Cómo resolver problemas por fallos de montaje en Trusted Extensions [190].

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 `tninfoo` 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 caché del núcleo, reinicie el sistema.

Durante el inicio, la caché 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 del 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 [86].**

   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

Sobre Trusted Extensions y LDAP

En este capítulo, se describe el uso de Oracle Directory Server Enterprise Edition (servidor LDAP) para un sistema configurado con Trusted Extensions.

- "Uso del servicio de nombres LDAP en Trusted Extensions" [251]
- "Referencia rápida para el servicio de nombres LDAP en Trusted Extensions" [253]

Uso del servicio de nombres LDAP 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 LDAP 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.

Por lo general, este puerto de varios niveles está configurado en la zona global para la zona global. Por lo tanto, una zona etiquetada no tiene acceso de escritura al directorio LDAP. En cambio, las zonas etiquetadas envían solicitudes de lectura mediante el servicio de proxy de varios niveles que se está ejecutando en el sistema o en otro sistema de confianza en la red. Trusted Extensions también admite una configuración LDAP de un servidor de directorio por etiqueta. Este tipo de configuración es necesaria cuando los usuarios tienen credenciales diferentes por etiqueta.

Trusted Extensions agrega dos bases de datos de red de confianza al servidor LDAP: `tnrhdb` y `tnrhtp`.

- Para obtener información sobre el uso del servicio de nombres LDAP en Oracle Solaris, consulte "Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: LDAP ".

- La configuración del servidor LDAP para Trusted Extensions se describe en el Capítulo 5, Configuración de LDAP para Trusted Extensions. Los sistemas Trusted Extensions pueden ser clientes de un servidor LDAP de Oracle Solaris mediante un proxy configurado con Trusted Extensions.
- La configuración de clientes del servidor LDAP de Trusted Extensions se describe en "Creación de un cliente LDAP de Trusted Extensions" [86].

Sistemas Trusted Extensions gestionados de manera local

Si un servicio de nombres distribuido no se usa en un sitio, los administradores deben garantizar 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 localmente, la información de configuración se conserva en los archivos en lo directorios `/etc`, `/etc/security` y `/etc/security/tsol`, y mediante las propiedades de configuración en el servicio SMF `name-service/switch`.

Bases de datos LDAP de Trusted Extensions

Trusted Extensions amplía el esquema del servidor LDAP 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
```

Referencia rápida para el 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 Capítulo 6, “Resolución de problemas de LDAP” de “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: LDAP ”.
- 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 [247].
- Para resolver otros problemas de conexión entre clientes y servidores LDAP, consulte Capítulo 6, “Resolución de problemas de LDAP” de “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: LDAP ”.
- 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 Oracle Directory Server Enterprise Edition, 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 Oracle Directory Server Enterprise Edition, escriba:

```
# dpadm start /export/home/ds/instances/your-instance
```

```
# dpadm stop /export/home/ds/instances/your-instance
```

♦ ♦ ♦ CAPÍTULO 18

Sobre correo de varios niveles en Trusted Extensions

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" [257]
- "Funciones de correo de Trusted Extensions" [257]

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 [138].

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 Capítulo 2, "Administración de servicios de correo" de "Gestión de servicios de sendmail en Oracle Solaris 11.2 ". 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 de configuración local del usuario, como `.mailrc`, está en la 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`" [133].

- 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" [205].
  - 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

En este capítulo, se describe cómo utilizar Trusted Extensions para configurar la impresión con etiquetas. Además, se explica cómo configurar los trabajos de impresión de Trusted Extensions sin opciones de etiquetas.

- "Etiquetas, impresoras e impresión" [259]
- "Configuración de impresión con etiquetas" [269]
- "Reducción de las restricciones de impresión en Trusted Extensions" [276]

Etiquetas, impresoras e impresión

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 las copias impresas. Las páginas del cuerpo y las páginas de la carátula y el ubicador obligatorios tienen etiquetas. Además, las páginas de carátula y ubicador pueden incluir instrucciones de tratamiento.

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 de administración de impresoras básicos de Oracle Solaris. La configuración es necesaria para aplicar etiquetas, limitar el rango de etiquetas de los trabajos de impresión, configurar las zonas con etiquetas para imprimir y flexibilizar restricciones de impresión.

Trusted Extensions admite la impresión de un solo nivel y de varios niveles. De manera predeterminada, un servidor de impresión configurado en la zona global de un sistema Trusted Extensions puede imprimir toda la gama de las etiquetas, es decir, el servidor de impresión tiene varios niveles. Cualquier sistema o zona etiquetados que puedan acceder a ese servidor de impresión tienen la capacidad de imprimir en la impresora conectada. Una zona etiquetada admite la impresión de un solo nivel. La zona puede conectarse a la impresora a través de la zona global o se puede configurar como servidor de impresión. Cualquier zona en esa etiqueta que pueda acceder a la zona etiquetada y, por lo tanto, al servidor de impresión, tiene la capacidad de imprimir en la impresora conectada. La impresión de un solo nivel también es

posible mediante el servidor de impresión en un sistema sin etiquetar que tiene asignada una etiqueta arbitraria. Estos trabajos de impresión se imprimen sin una etiqueta.

Diferencias entre la impresión de Trusted Extensions en Oracle Solaris 10 y Oracle Solaris 11

El protocolo de impresión predeterminado para Oracle Solaris 10 es el servicio de impresión LP. El valor predeterminado para Oracle Solaris 11 es el sistema común de impresión de Unix (CUPS). Para ver una guía completa de CUPS en Oracle Solaris, consulte "Configuración y gestión de la impresión en Oracle Solaris 11.2 ". En la siguiente tabla, se muestran las diferencias principales entre los protocolos de impresión CUPS y LP.

TABLA 19-1 Diferencias entre CUPS y LP

Área de diferencia	CUPS	LP
Número de puerto IANA	`631`	`515`
Caras de impresión	Una cara	Dos caras
Impresión en cascada	Debe compartir la impresora en el servidor de impresión	Debe configurar la ruta a la impresora
Acceso a impresoras de red	Debe poder hacer `ping` correctamente a la dirección IP del servidor de impresión y de la impresora	Debe configurar la ruta a la impresora
Trabajos de impresión remotos	No puede imprimir sin etiquetas	Puede imprimir sin etiquetas
Agregar una impresora remota a un cliente	`lpadmin -p` *printer-name* `-E \ -v ipp://`*print-server-IP-address*`/printers/`*printer-name-on-server*	`lpadmin -p` *printer-name* `\ -s` *server-name*
Activar y aceptar el servidor de impresión	Opción `lpadmin -E`	Comandos `accept` y `enable`
Protección PostScript	Se proporciona de manera predeterminada	Requiere una autorización
Activación de páginas de carátula	Opción `-o job-sheets=labeled`	Se proporciona de manera predeterminada
Desactivar las páginas de carátula y de ubicador	Opción `-o job-sheets=none`	Opción `-o nobanner`
`lp -d` *printer* `file1 file2`	Una página de carátula y una página de ubicador por trabajo de impresión	Una página de carátula y una página de ubicador por cada trabajo de impresión
Orientación de la etiqueta en las páginas de trabajos	Siempre vertical	Siempre la orientación del trabajo
Servicios de impresión	`svc:/application/cups/scheduler` `.../in-lpd:default`	`svc:/application/print/service-selector` `.../server` `.../rfc1179`

Área de diferencia	CUPS	LP
		`.../ipp-listener svc:/network/device-discovery/printers:snmp`

Restricción del acceso a las impresoras y a la información de trabajos de impresión en Trusted Extensions

Los usuarios y los roles de un sistema configurado con Trusted Extensions crean trabajos de impresión en la etiqueta de su sesión. Los trabajos de impresión son aceptados solamente por servidores de impresión que reconocen esa etiqueta. La etiqueta debe estar en el rango de etiquetas del servidor de impresión.

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.

Salida de impresión con etiquetas

Trusted Extensions imprime la información de seguridad en las páginas del cuerpo y en las páginas de carátula y de ubicador. La información proviene del archivo `/etc/security/tsol/label_encodings` y del archivo `/usr/lib/cups/filter/tsol_separator.ps`. Las etiquetas que tienen más de 80 caracteres se imprimen truncadas en la parte superior e inferior de todas las páginas. El truncamiento se indica mediante una flecha (`->`). Las etiquetas del encabezado y el pie de página se imprimen en forma vertical, aun cuando las páginas del cuerpo se imprimen en forma horizontal. Para ver un ejemplo, consulte la Figura 19-4, “Etiqueta del trabajo impresa en modo vertical cuando la página del cuerpo se imprime en modo horizontal”.

El texto, las etiquetas y las advertencias que aparecen en los trabajos de impresión se pueden configurar. El texto también se puede reemplazar con texto en otro idioma para su localización. El administrador de seguridad puede configurar lo siguiente:

- Localizar o personalizar el texto de las páginas de carátula y de ubicador
- Especificar etiquetas alternativas que se vayan a imprimir en las páginas del cuerpo o en los diversos campos de las páginas de carátula y de ubicador
- Cambiar u omitir cualquiera de los textos o las etiquetas

Los usuarios que son dirigidos a una impresora sin etiquetas pueden imprimir la salida sin etiquetas. Los usuarios en una zona etiquetada con su propio servidor de impresión pueden

imprimir la salida sin etiquetas si se les asigna la autorización `solaris.print.unlabeled`. Los roles se pueden configurar para imprimir la salida sin etiquetas en una impresora local controlada por un servidor de impresión de Trusted Extensions. Para obtener ayuda, consulte “Reducción de las restricciones de impresión en Trusted Extensions” [276].

Páginas de carátula y de ubicador con etiquetas

Las siguientes figuras muestran la página de carátula predeterminada y las variaciones de la página de ubicador predeterminada. Las llamadas identifican las distintas secciones. Para obtener una explicación del origen del texto en estas secciones, consulte el Capítulo 4, “Labeling Printer Output” de “Trusted Extensions Label Administration ”. Tenga en cuenta que la página de ubicador utiliza una línea exterior diferente.

FIGURA 19-1 Página de carátula típica de un trabajo de impresión con etiquetas

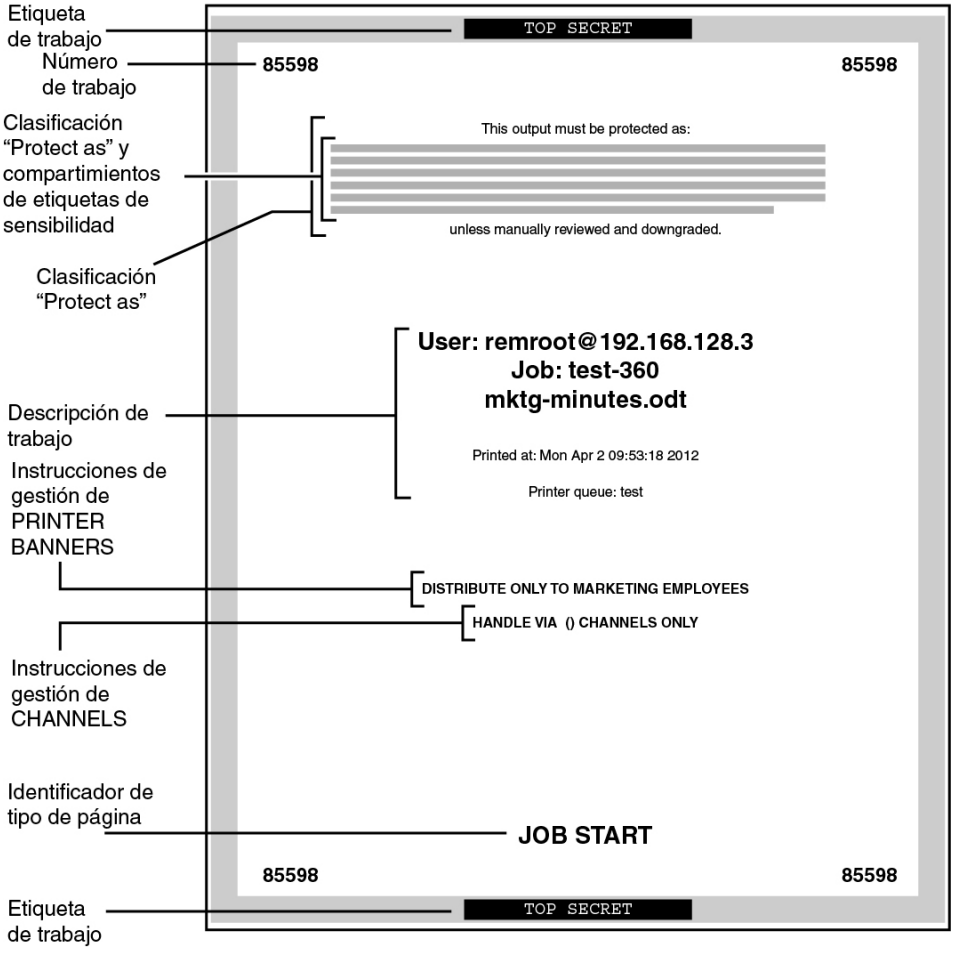
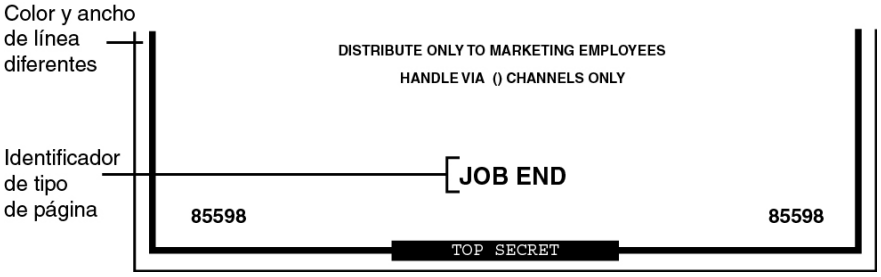


FIGURA 19-2 Diferencias en una página de ubicador

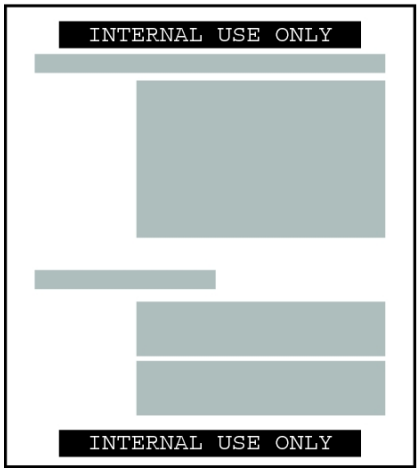


Páginas del cuerpo con etiquetas

De manera predeterminada, la clasificación “Protect as” se imprime en la parte superior y en la parte inferior de cada página del cuerpo. La clasificación “Protect as” es la clasificación dominante cuando la clasificación de la etiqueta del trabajo se compara con la clasificación `minimum protect as`. La clasificación `minimum protect as` se define en el archivo `label_encodings`.

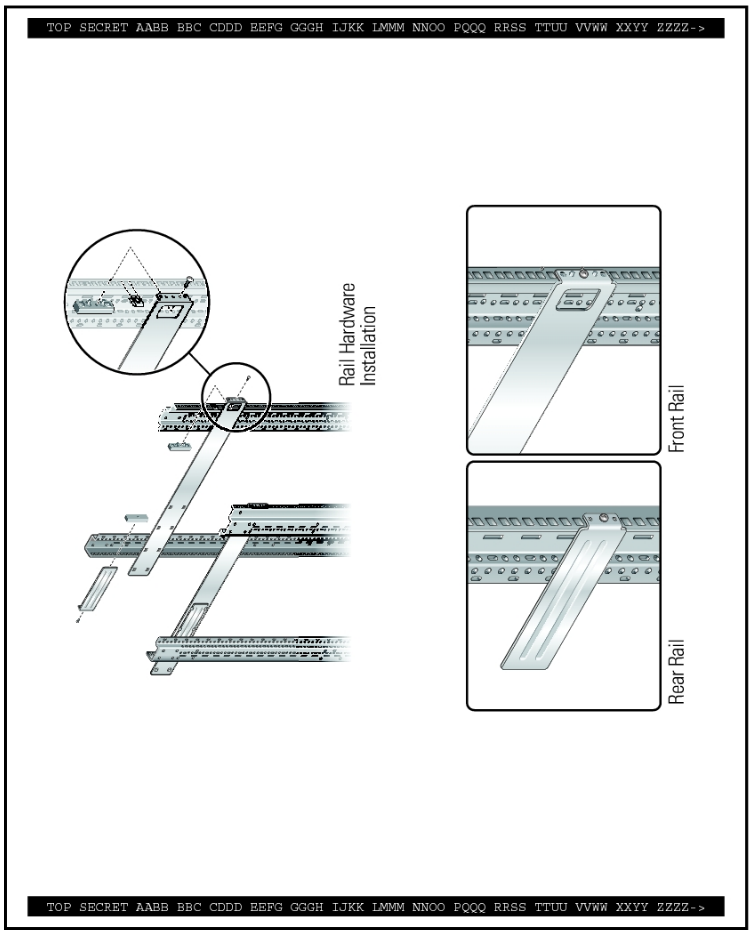
Por ejemplo, si el usuario se encuentra en una sesión `Internal Use Only`, los trabajos de impresión del usuario están en esa etiqueta. Si la clasificación `minimum protect as` en el archivo `label_encodings` es `Public`, la etiqueta `Internal Use Only` se imprime en las páginas del cuerpo.

FIGURA 19-3 Etiqueta del trabajo impresa en la parte superior y en la parte inferior de una página del cuerpo



Cuando las páginas del cuerpo se imprimen en modo horizontal, la etiqueta se imprime en modo vertical. En la figura siguiente, se ilustra una página del cuerpo, impresa en modo horizontal, cuya etiqueta Protect As se extiende más allá de los límites de la página. La etiqueta se trunca a 80 caracteres.

FIGURA 19-4 Etiqueta del trabajo impresa en modo vertical cuando la página del cuerpo se imprime en modo horizontal



Archivo de configuración `tsol_separator.ps`

En la siguiente tabla, se muestran los aspectos de la impresión de confianza que el administrador de la seguridad puede cambiar mediante la modificación del archivo `/usr/lib/cups/filter/tsol_separator.ps`.

TABLA 19-2 Valores configurables en el archivo `tsol_separator.ps`

Salida	Valor predeterminado	Definición	Para efectuar cambios
`PRINTER BANNERS`	`/Caveats Job_Caveats`	`/Caveats Job_Caveats`	Consulte "Specifying Printer Banners" de "Trusted Extensions Label Administration ".
`CHANNELS`	`/Channels Job_Channels`	`/Channels Job_Channels`	Consulte "Specifying Channels" de "Trusted Extensions Label Administration ".
Etiqueta en la parte superior de las páginas de carátula y de ubicador	`/HeadLabel Job_Protect def`	Consulte la descripción `/Page Label`.	Igual que para cambiar `/PageLabel`. Consulte también "Specifying the "Protect As" Classification" de "Trusted Extensions Label Administration ".
Etiqueta en la parte superior de las páginas del cuerpo	`/PageLabel Job_Protect def`	Compara la etiqueta del trabajo con la clasificación `minimum protect as classification` en el archivo `label_encodings`. Imprime la clasificación más dominante. Contiene compartimientos si la etiqueta del trabajo de impresión tiene compartimientos.	Cambie la definición `/PageLabel` para especificar otro valor. O bien, escriba una cadena que elija. O bien, no imprima nada.

Texto y etiqueta de la instrucción de clasificación "Protect as"	`/Protect Job_Protect def`
	`/Protect_Text1 () def`
	`/Protect_Text2 () def`
		Consulte la descripción `/Page Label`.
		Texto que aparecerá encima de la etiqueta.
		Texto que aparecerá debajo de la etiqueta.
			Igual que para cambiar `/PageLabel`.
			Reemplace `()` en `Protect_Text1` y `Protect_Text2` con cadenas de texto.

Impresión PostScript de la información de seguridad

La impresión con etiquetas en Trusted Extensions se basa en las funciones de impresión de Oracle Solaris. Al igual que en el SO Oracle Solaris, la `job-sheets` gestiona la creación de páginas de carátula. Para implementar el etiquetado, un filtro convierte el trabajo de impresión 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.

Nota - CUPS evita la modificación de los archivos PostScript. Por lo tanto, un programador capacitado de PostScript no puede crear un archivo PostScript que modifica las etiquetas en la copia impresa.

Interfaces de impresión de Trusted Extensions (referencia)

Trusted Extensions agrega las siguientes autorizaciones de impresión para implementar la política de seguridad de Trusted Extensions. Estas autorizaciones se comprueban en el servidor de impresión. Por lo tanto, los usuarios remotos, como los usuarios de zonas etiquetadas, no pueden aprobar la comprobación de autorización.

- `solaris.print.admin`: activa un rol para administrar la impresión
- `solaris.print.list`: activa un rol para ver trabajos de impresión que no pertenecen al rol
- `solaris.print.nobanner`: activa un rol para imprimir trabajos sin páginas de carátula ni de ubicador de la zona global
- `solaris.print.unlabeled`: activa un rol para imprimir trabajos de impresión sin etiquetas de páginas de la zona global

Los siguientes comandos de usuario se amplían a fin de cumplir con la política de seguridad de Trusted Extensions:

- `cancel`: el emisor de llamada debe ser igual a la etiqueta del trabajo de impresión para cancelar un trabajo. Los usuarios normales solamente pueden cancelar sus propios trabajos.
- `lp`: la opción `-o nolabel`, que imprime páginas del cuerpo sin etiquetas, requiere la autorización `solaris.print.unlabeled`. La opción `-o job-sheets=none`, que imprime el trabajo sin una página de carátula ni de ubicador, requiere la autorización `solaris.print.nobanner`.
- `lpstat`: el emisor de llamada debe ser igual a la etiqueta del trabajo de impresión para obtener el estado de un trabajo. Los usuarios normales solamente pueden ver sus propios trabajos de impresión.

Los siguientes comandos administrativos se amplían a fin de cumplir con la política de seguridad de Trusted Extensions. Al igual que en el SO Oracle Solaris, solamente los roles que incluyen el perfil de derechos de gestión de impresoras pueden ejecutar estos comandos.

- `lpmove`: el emisor de llamada debe ser igual a la etiqueta del trabajo de impresión para mover un trabajo. De manera predeterminada, los usuarios comunes pueden mover solamente sus propios trabajos de impresión.
- `lpadmin`: en la zona global, este comando funciona para todos los trabajos. En una zona etiquetada, el emisor de llamada debe dominar la etiqueta del trabajo de impresión para ver un trabajo y debe ser igual para cambiar un trabajo.
- `lpsched`: en la zona global, este comando siempre se ejecuta correctamente. Al igual que en el SO Oracle Solaris, use el comando `svcadm` para activar, desactivar, iniciar o reiniciar el servicio de impresión. En una zona etiquetada, el emisor de llamada debe ser igual a la etiqueta del servicio de impresión para cambiar el servicio de impresión. Para obtener

detalles sobre la utilidad de gestión de servicios, consulte las páginas del comando man `smf`(5), `svcadm`(1M) y `svcs`(1).

Gestión de impresión en Trusted Extensions

Realice procedimientos de Trusted Extensions para configurar la impresión después de terminar la configuración de la impresora en Oracle Solaris. En estos procedimientos, se incluye parte de la configuración básica. Para obtener más información, consulte el Capítulo 2, “Configuración de impresoras mediante CUPS (tareas)” de “Configuración y gestión de la impresión en Oracle Solaris 11.2 ”. Los siguientes enlaces hacen referencia a las tareas principales que gestionan la impresión con etiquetas:

- “Configuración de impresión con etiquetas” [269]
- “Reducción de las restricciones de impresión en Trusted Extensions” [276]

Configuración de impresión con etiquetas

El siguiente mapa de tareas describe los procedimientos de configuración comunes relativos a la impresión con etiquetas.

TABLA 19-3 Mapa de tareas de configuración de impresión con etiquetas

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 [269]
Configurar una impresora de red.	Comparte una impresora.	Cómo configurar una impresora de red [271]
Configurar la impresión desde una zona con etiquetas.	Crea un servidor de impresión de una sola etiqueta para una zona etiquetada.	Cómo configurar una zona como un servidor de impresión de un solo nivel [272]
Configurar un cliente de impresión de varios niveles.	Se conecta un host de Trusted Extensions con una impresora.	Cómo activar un cliente de Trusted Extensions para que acceda a un impresora [273]

▼ Cómo configurar un servidor de impresión de varios niveles y sus impresoras

Las impresoras conectadas a un servidor de impresión de Trusted Extensions imprimen etiquetas en páginas del cuerpo, de carátula y de ubicador. Esta clase de impresoras pueden

imprimir los trabajos de impresión dentro del rango de etiquetas del servidor de impresión. Si la impresora está compartida, cualquier host de Trusted Extensions que pueda acceder al servidor de impresión puede utilizar la impresora compartida.

Antes de empezar Debe estar con el rol de administrador del sistema en la zona global de este servidor de impresión.

1. **Determine la marca y el modelo de impresora.**

   ```
   # lpinfo -m | grep printer-manufacturer
   ```

   Por ejemplo, la siguiente sintaxis busca todas las impresoras Xerox:

   ```
   # lpinfo -m | grep Xerox
   gutenprint.5.2://xerox-able_1406/expert Xerox Able 1406 - CUPS+Gutenprint v5.2.4
   gutenprint.5.2://xerox-able_1406/simple Xerox Able 1406 - CUPS+Gutenprint v5.2.4 ...
   gutenprint.5.2://xerox-dc_400/expert Xerox Document Centre 400 - ...
   gutenprint.5.2://xerox-dc_400/simple Xerox Document Centre 400 - ...
   gutenprint.5.2://xerox-dp_4508/expert Xerox DocuPrint 4508 - ...
   gutenprint.5.2://xerox-dp_4508/simple Xerox DocuPrint 4508 - ...
   ...
   ```

2. **Defina las características de cada impresora conectada.**

   ```
   # lpadmin -p printer-name -E -v socket://printer-IP-address -m printer-make-and-model
   -
   ```

   La opción `-E` permite que las impresoras designadas acepten una cola de solicitudes de impresión. También activa las impresoras.

3. **Para crear una impresora de red, comparta la impresora.**

   ```
   # lpadmin -p printer-name -o printer-is-shared=true
   ```

   Para evitar que la impresora sea utilizada por otros sistemas, omita este paso.

4. **Visualice los valores predeterminados de la impresora.**

   ```
   # lpoptions -p printer-name
   ```

5. **Ajuste los valores predeterminados.**

   Por ejemplo, puede imprimir a dos caras y dos hojas por página.

   Sugerencia - Puede utilizar la interfaz web de CUPS, `http://localhost:631`, para configurar la impresora.

   ---

6. **Configure cada impresora conectada al servidor de impresión con una página de carátula y ubicador etiquetada.**

   ```
   # lpadmin -p printer-name -o job-sheets=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.

7. **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 `root` en la consola de la zona etiquetada.**

      ```
      # zlogin -C labeled-zone
      ```

   b. **Agregue la impresora.**

      ```
      # lpadmin -p zone-printer-name -E \
      -v ipp://global-zone-IP-address/printers/printer-name-in-global-zone
      ```

   c. **(Opcional) Establezca la impresora como predeterminada.**

      ```
      # lpadmin -d zone-printer-name
      ```

8. **En cada zona con etiquetas, pruebe la impresora.**

   Como usuario `root` y como usuario común, realice los siguientes pasos:

   a. **Imprima archivos de texto y PostScript desde la línea de comandos.**

      ```
      # lp /etc/motd ~/PostScriptTest.ps
      % lp $HOME/file1.txt $HOME/PublicTest.ps
      ```

   b. **Imprima archivos desde las aplicaciones, como el correo, Oracle OpenOffice, Adobe Reader y su explorador.**

   c. **Verifique que las etiquetas de las páginas de carátula, las páginas de ubicador y las páginas del cuerpo se impriman correctamente.**

Véase también

- **Impedir la salida con etiquetas**: “Reducción de las restricciones de impresión en Trusted Extensions” [276]
- **Usar esta zona como servidor de impresión**: Cómo activar un cliente de Trusted Extensions para que acceda a un impresora [273]

▼ Cómo configurar una impresora de red

Cuando una impresora se comparte, cualquier host de Trusted Extensions que pueda acceder al servidor de impresión puede utilizar la impresora compartida.

Antes de empezar Debe estar con el rol de administrador del sistema en la zona global de este servidor de impresión.

1. **Defina las características de la impresora de red.**

   Siga el Paso 1 al Paso 6 de Cómo configurar un servidor de impresión de varios niveles y sus impresoras [269] para configurar la impresora de red.

   Una vez que la impresora se comparte en el Paso 3, todos los sistemas de la red que pueden acceder a este servidor de impresión pueden imprimir en esta impresora.

2. **Pruebe la impresora de red.**

   Como `root` y usuario normal, lleve a cabo los siguientes pasos desde los sistemas que usan este servidor de impresión:

   a. **Imprima archivos de texto y PostScript desde la línea de comandos.**

   ```
   # lp /etc/motd ~/PostScriptTest.ps
   % lp $HOME/file1.txt $HOME/PublicTest.ps
   ```

   b. **Imprima archivos desde las aplicaciones, como el correo, Oracle OpenOffice, Adobe Reader y su explorador.**

   c. **Verifique que las etiquetas de las páginas de carátula, las páginas de ubicador y las páginas del cuerpo se impriman correctamente.**

Véase también Para evitar la salida con etiquetas, consulte "Reducción de las restricciones de impresión en Trusted Extensions" [276].

▼ 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 del sistema 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 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 Trusted Extensions ".

3. **Defina las características de cada impresora conectada.**

   Siga el Paso 1 al Paso 6 de Cómo configurar un servidor de impresión de varios niveles y sus impresoras [269] para configurar la impresora de zona.

   Las impresoras conectadas pueden imprimir trabajos únicamente en la etiqueta de la zona.

4. **Pruebe la impresora.**

   Nota - Por motivos de seguridad, los archivos con una etiqueta administrativa, `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 archivos de texto y PostScript desde la línea de comandos.**

      ```
      # lp /etc/motd ~/PostScriptTest.ps
      % lp $HOME/file1.txt $HOME/PublicTest.ps
      ```

   b. **Imprima archivos desde las aplicaciones, como el correo, Oracle OpenOffice, Adobe Reader y su explorador.**

   c. **Verifique que las etiquetas de las páginas de carátula, las páginas de ubicador y las páginas del cuerpo se impriman correctamente.**

Véase también

- **Impedir la salida con etiquetas**: “Reducción de las restricciones de impresión en Trusted Extensions” [276]
- **Usar esta zona como servidor de impresión**: Cómo activar un cliente de Trusted Extensions para que acceda a un impresora [273]

▼ Cómo activar 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 compartidas que están conectadas a una zona global en un sistema diferente.
- Para una zona etiquetada, agregue el acceso a las impresoras compartidas que estén conectadas a la zona global del sistema.

- Para una zona etiquetada, agregue el acceso a una impresora compartida para la cual está configurada una zona remota en la misma etiqueta.
- Para una zona etiquetada, agregue el acceso a las impresoras compartidas que están 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. Además, las impresoras que están conectadas al servidor de impresión deben haber sido configuradas y compartidas. Para obtener detalles, consulte lo siguiente:

- Cómo configurar un servidor de impresión de varios niveles y sus impresoras [269]
- Cómo configurar una zona como un servidor de impresión de un solo nivel [272]
- Cómo asignar una etiqueta a un servidor de impresión sin etiquetas [277]

Debe estar con el rol de administrador del sistema en la zona global.

1. **Verifique que puede hacer ping a la impresora.**

   ```
   # ping printer-IP-address
   ```

   Si este comando falla, hay un problema de conexión de red. Corrija el problema de conexión y, luego, regrese a este procedimiento. Para obtener ayuda, consulte “Resolución de problemas de la red de confianza” [242].

2. **Complete uno o más procedimientos que permiten que los sistemas accedan a la impresora.**

   - **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 remoto de Trusted Extensions.**

        ```
        # lpadmin -p printer-name -E \
        -v ipp://print-server-IP-address/printers/printer-name-on-server
        ```

   - **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 Trusted Extensions ”.

b. Agregue el acceso a la impresora.

```
# lpadmin -p printer-name -E \
-v ipp://print-server-IP-address/printers/printer-name-on-print-server
```

- **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 -p printer-name -E \
  -v ipp://zone-print-server-IP-address/printers/printer-name-on-zone-print-server
  ```

- **Configure una zona etiquetada para utilizar un servidor de impresión sin etiquetar para imprimir la salida sin ninguna información de seguridad.**

  Para obtener instrucciones, consulte Cómo asignar una etiqueta a un servidor de impresión sin etiquetas [277].

3. Pruebe las impresoras.

Nota - Por motivos de seguridad, los archivos con una etiqueta administrativa, `ADMIN_HIGH` o `ADMIN_LOW`, imprimen `ADMIN_HIGH` en las páginas del 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 todas las cuentas que pueden acceder a la zona global y para todas las cuentas que pueden acceder a las zonas etiquetadas.

a. Imprima archivos de texto y PostScript desde la línea de comandos.

```
# lp /etc/motd ~/PostScriptTest.ps
% lp $HOME/file1.txt $HOME/PublicTest.ps
```

b. Imprima archivos desde las aplicaciones, como el correo, Oracle OpenOffice, Adobe Reader y su explorador.

c. Verifique que las etiquetas de las páginas de carátula, las páginas de ubicador y las páginas del cuerpo se impriman correctamente.

Reducción de las restricciones de impresión en Trusted Extensions

Las siguientes tareas son opcionales. Reducen la seguridad de la impresión que proporciona Trusted Extensions.

TABLA 19-4 Mapa de tareas de reducción de las restricciones de impresión en Trusted Extensions

Tarea	Descripción	Para obtener instrucciones
Configurar una impresora para que no etiquete el resultado.	Impide que la información de seguridad se imprima en copias impresas desde la zona global.	Cómo eliminar páginas de carátula y de ubicador [276]
Configurar las impresoras en una sola etiqueta sin resultado con etiquetas.	Permite que los usuarios impriman una etiqueta específica. Los trabajos de impresión no se marcan con etiquetas.	Cómo asignar una etiqueta a un servidor de impresión sin etiquetas [277]
Eliminar las etiquetas visibles de las páginas del cuerpo.	Imprime en un servidor de impresión sin etiquetar. Asigna autorizaciones de impresión que suprimen el etiquetado.	Cómo asignar una etiqueta a un servidor de impresión sin etiquetas [277] Cómo permitir que usuarios y roles específicos omitan el etiquetado de la salida impresa [278]
Suprimir las páginas de la carátula y del ubicador.	Elimina las páginas de carátula y de ubicador, lo cual elimina la información de seguridad adicional en esas páginas.	Cómo eliminar páginas de carátula y de ubicador [276]
Asignar autorizaciones de impresión.	Autoriza que usuarios y roles específicos impriman los trabajos de impresión sin etiquetas.	Cómo permitir que usuarios y roles específicos omitan el etiquetado de la salida impresa [278]

▼ Cómo eliminar páginas de carátula y de ubicador

La impresoras que tienen la opción `job-sheets` definida en `none` *no* imprimen páginas de carátula o ubicador.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

- **En la etiqueta adecuada, configure la impresora sin páginas de carátula o ubicador.**

  ```
  # lpadmin -p print-server-IP-address -o job-sheets=none,none
  ```

  También puede especificar `none` una vez.

```
# lpadmin -p print-server-IP-address -o job-sheets=none
```

Las páginas del cuerpo siguen estando etiquetadas. Para eliminar etiquetas de páginas del cuerpo, consulte Cómo permitir que usuarios y roles específicos omitan el etiquetado de la salida impresa [278].

▼ Cómo asignar una etiqueta a un servidor de impresión sin etiquetas

Un sistema Trusted Extensions puede asignarle una etiqueta a un servidor de impresión de Oracle Solaris para tener acceso a una impresora en esa etiqueta. Los trabajos se imprimen en la etiqueta asignada sin etiquetas. 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 trabajos en la impresora sin etiquetar en la etiqueta asignada.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1. **Asigne una plantilla sin etiquetas en el servidor de impresión.**
   Para obtener detalles, consulte Cómo agregar un host a una plantilla de seguridad [221].
   Los usuarios que trabajan en la etiqueta asignada al servidor de impresión en la plantilla sin etiquetar pueden enviar trabajos de impresión a la impresora de Oracle Solaris en esa etiqueta.
2. **En el sistema que no tiene acceso a las impresoras, asuma el rol de administrador del sistema.**
3. **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 Trusted Extensions ”.
4. **Agregue el acceso a la impresora que está conectada al servidor de impresión con etiquetas asignadas de manera arbitraria.**

   ```
   # lpadmin -p printer-name -E \
   -v ipp://print-server-IP-address/printers/printer-name-on-print-server
   ```

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 Cómo configurar un túnel en una red que no es de confianza [240]. 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 permitir que usuarios y roles específicos omitan el etiquetado de la salida impresa

Para permitir que usuarios y roles impriman trabajos sin etiquetas, se necesita la autorización del administrador de seguridad y una acción por parte del usuario o rol autorizado al enviar un trabajo de impresión.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1. **Asignar autorizaciones de impresión a un usuario o rol.**

   - **Para permitir que el usuario o el rol elimine etiquetas de las páginas de carátula o ubicador, asigne la autorización `solaris.print.nobanner`.**

     ```
     # usermod -A +solaris.print.nobanner username
     ```

     ```
     # rolemod -A +solaris.print.nobanner rolename
     ```

   - **Para permitir que el usuario o el rol elimine etiquetas de las páginas del cuerpo, asigne la autorización `solaris.print.unlabeled`.**

     ```
     # usermod -A +solaris.print.unlabeled username
     ```

     ```
     # rolemod -A +solaris.print.unlabeled rolename
     ```

   - **Para permitir que el usuario o el rol elimine todas las etiquetas de las copias de impresión, asigne ambas autorizaciones.**

     ```
     # usermod -A +solaris.print.unlabeled,+solaris.print.nobanner username
     ```

     ```
     # rolemod -A +solaris.print.unlabeled,+solaris.print.nobanner rolename
     ```

2. **Prepare la impresión de la salida sin etiquetar.**

   Asegúrese de que la impresora sea local.

Para el usuario, eso significa que el usuario debe imprimir desde una zona etiquetada con un servidor de impresión para esa zona. Un rol puede imprimir desde la zona global o una zona etiquetada.

3. **Para imprimir una salida sin etiquetar, especifique las opciones que eliminan las etiquetas en la línea de comandos.**

   Debe estar autorizado para imprimir una salida sin etiquetar.

   - **Para imprimir sin carátulas, utilice la opción `job-sheets=none`.**

     ```
     # lp -o job-sheets=none file
     ```

   - **Para imprimir sin etiquetas en las páginas del cuerpo, utilice la opción `nolabel`.**

     ```
     # lp -o nolabels file
     ```

   - **Para imprimir sin etiquetas en la salida, use ambas opciones.**

     ```
     # lp -o job-sheets=none -o nolabels file
     ```

♦ ♦ ♦ CAPÍTULO 20

Acerca de los dispositivos en Trusted Extensions

En este capítulo, se describen las protecciones para los dispositivos periféricos en un sistema Trusted Extensions.

- "Protección de los dispositivos con el software Trusted Extensions" [281]
- "Interfaz gráfica de usuario Device Manager" [283]
- "Aplicación de la seguridad de los dispositivos en Trusted Extensions" [285]
- "Dispositivos en Trusted Extensions (referencia)" [286]

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 Capítulo 4, "Control de acceso a dispositivos" de "Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 ".

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, un usuario no autorizado en un sistema Trusted Extensions no puede asignar dispositivos, como unidades de cinta o unidades de CD-ROM.

  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.
- El administrador de seguridad puede restringir el rango de etiquetas de cada dispositivo. 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" de "Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 ". 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 y unidades de CD-ROM. 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 "Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 ".

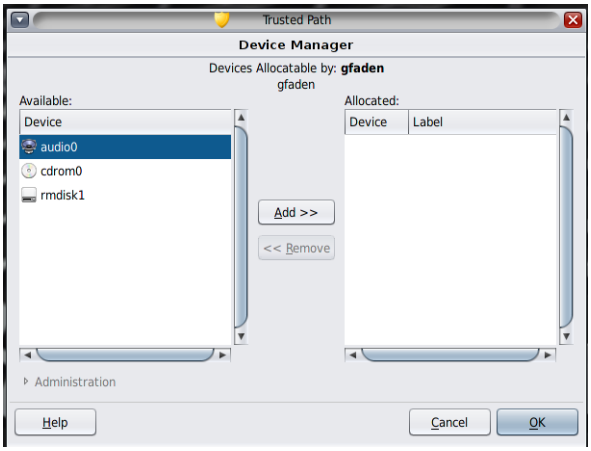
Para el software Trusted Extensions, las secuencias de comandos device-clean deben cumplir ciertos requisitos. Estos requisitos se describen en la página del comando man `device_clean`(5).

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.

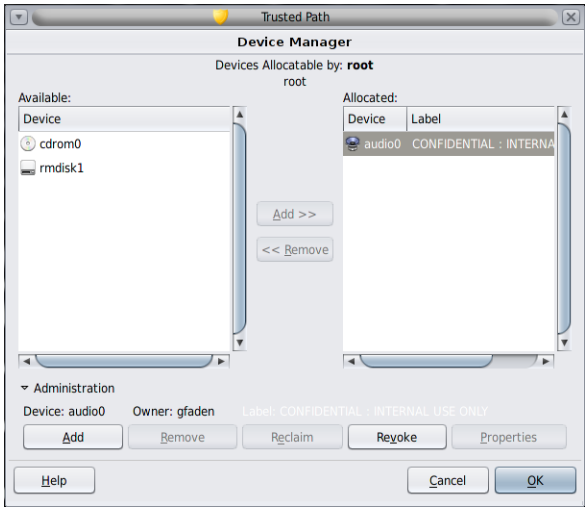
La interfaz gráfica de usuario se denomina Device Manager. Para iniciar esta interfaz gráfica de usuario, se debe seleccionar Allocate Device en el menú Trusted Path. La siguiente figura muestra un Device Manager abierto por un usuario que puede asignar el dispositivo `audio`.

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 CD, la persona que exporta la información debe colocar en el disco una etiqueta `NEED TO KNOW ENGINEERING` de manera física. El CD debe almacenarse en un lugar al que puedan acceder únicamente los miembros del grupo de ingeniería que deban tener conocimiento 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 CD-ROM 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 obtener información sobre las interfaces de la línea de comandos de Oracle Solaris, consulte "Protección de dispositivos (referencia)" de "Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 ".

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 ver ejemplos, consulte "Cómo asignar de manera forzada un dispositivo" de "Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 " y "Cómo desasignar de manera forzada un dispositivo" de "Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 ".

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

En este capítulo se describe cómo administrar y utilizar dispositivos en un sistema configurado con Trusted Extensions.

- "Control de dispositivos en Trusted Extensions" [287]
- "Mapa de tareas de uso de dispositivos en Trusted Extensions" [287]
- "Gestión de dispositivos en Trusted Extensions" [288]
- "Personalización de autorizaciones para dispositivos en Trusted Extensions" [296]

Control de dispositivos en Trusted Extensions

El siguiente mapa de tareas incluye enlaces a mapas de tareas para administradores y usuarios para el control de dispositivos periféricos.

TABLA 21-1 Mapa de tareas de control de dispositivos en Trusted Extensions

Tarea	Descripción	Para obtener instrucciones
Usar dispositivos.	Permite usar un dispositivo como rol o como usuario común.	"Mapa de tareas de uso de dispositivos en Trusted Extensions" [287]
Administrar dispositivos.	Permite configurar dispositivos para los usuarios comunes.	"Gestión de dispositivos en Trusted Extensions" [288]
Personalizar autorizaciones para dispositivos.	El rol de administrador de seguridad crea nuevas autorizaciones de dispositivos, las agrega al dispositivo, las ubica en un perfil de derechos y asigna ese perfil al usuario.	"Personalización de autorizaciones para dispositivos en Trusted Extensions" [296]

Mapa de tareas de uso de dispositivos en Trusted Extensions

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.

TABLA 21-2 Mapa de tareas de 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 Trusted Extensions "
Utilizar medios portátiles para transferir archivos.	Cómo copiar archivos desde medios portátiles en Trusted Extensions [73] Cómo copiar archivos en medios portátiles en Trusted Extensions [72]

Gestión de dispositivos en Trusted Extensions

El siguiente mapa de tareas describe los procedimientos que se deben llevar a cabo para proteger los dispositivos en el sitio.

TABLA 21-3 Mapa de tareas de gestión de dispositivos en Trusted Extensions

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" de "Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 "
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 "Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 "
	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" [296]
Configurar un dispositivo.	Se seleccionan funciones de seguridad para proteger el dispositivo.	Cómo configurar un dispositivo mediante Device Manager en Trusted Extensions [289]
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 [293]
	Se utilizan los comandos de Oracle Solaris para hacer que un dispositivo esté disponible o no para su uso.	"Cómo asignar de manera forzada un dispositivo" de "Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 " "Cómo desasignar de manera forzada un dispositivo" de "Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 "
Impedir el acceso a un dispositivo asignable.	Se proporciona control de acceso específico a un dispositivo.	Ejemplo 21-2, "Creación de autorizaciones para dispositivos específicas"

Tarea	Descripción	Para obtener instrucciones
	Se rechaza el acceso de cualquier usuario a un dispositivo asignable.	Ejemplo 21-1, “Impedir la asignación remota del dispositivo de audio”
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 [294]
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 [295]

▼ Cómo configurar un dispositivo mediante Device Manager 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 en un sistema de ventanas. En un sistema sin un escritorio, sólo los roles de la zona global pueden configurar y utilizar dispositivos asignables.

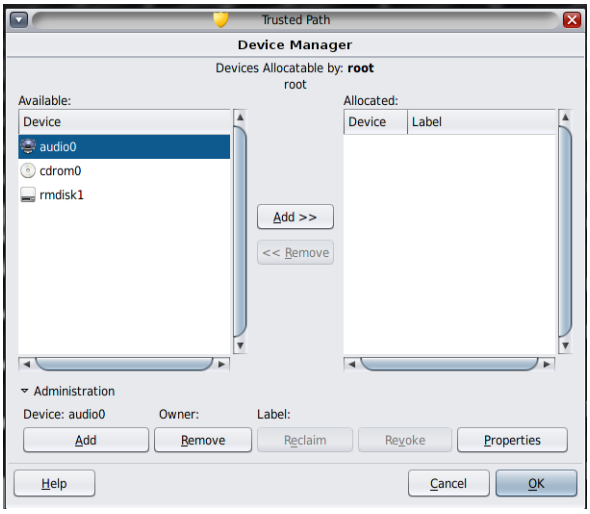
En un sistema de ventanas, los siguientes dispositivos se pueden asignar para su uso:

- `audio`*n*: indica un micrófono y un altavoz
- `cdrom`*n*: indica una unidad de CD-ROM
- `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.

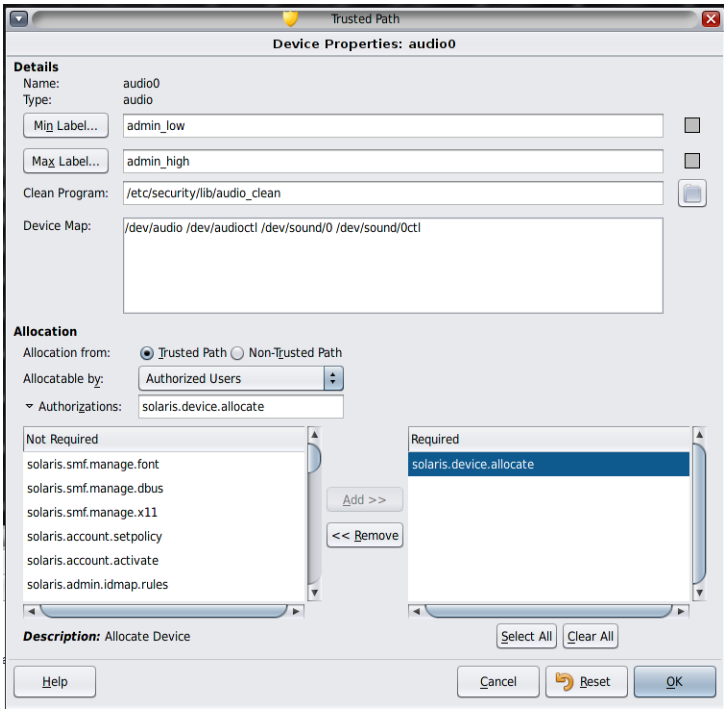
1. **En el menú Trusted Path, seleccione Allocate Device.**

   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” [103].

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 un búfer de trama u otro dispositivo que no deba ser asignable, seleccione No Users.

Nota - No puede configurar una impresora para la asignación.

- **Para hacer que el dispositivo sea asignable, pero que no requiera autorización, haga clic en All Users.**

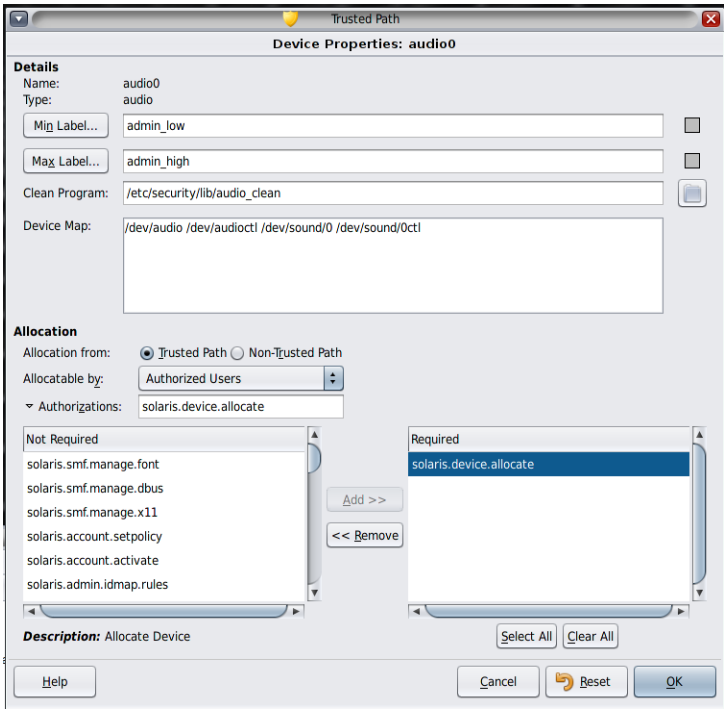
5. **Especifique si el dispositivo se puede asignar de manera remota.**

   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” [296].

7. **Para guardar los cambios, haga clic en OK.**

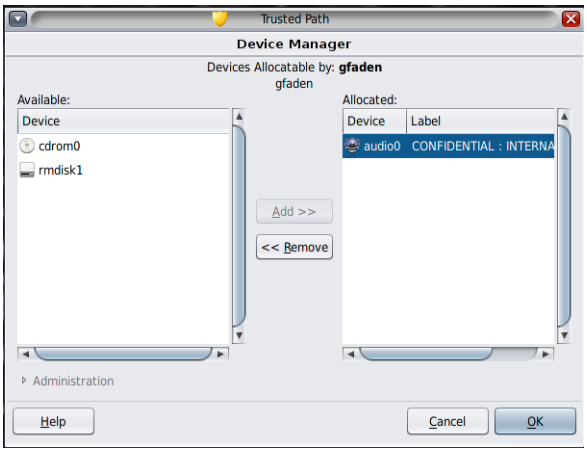
Cómo revocar o reclamar un dispositivo en Trusted Extensions

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” [103].
      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 realizados.**

Personalización de autorizaciones para dispositivos en Trusted Extensions

En el siguiente mapa de tareas, se describen los procedimientos para cambiar las autorizaciones para dispositivos en el sitio.

TABLA 21-4 Mapa de tareas de personalización de autorizaciones para dispositivos en Trusted Extensions

Tarea	Descripción	Para obtener instrucciones
Crear nuevas autorizaciones para dispositivos.	Se crean autorizaciones específicas del sitio.	Cómo crear nuevas autorizaciones para dispositivos [297]
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 [300]
Asignar autorizaciones para dispositivos a usuarios y roles.	Permite que los usuarios y los roles usen las autorizaciones nuevas.	Cómo asignar autorizaciones para dispositivos [300]

Cómo crear nuevas autorizaciones para dispositivos

Si un dispositivo no requiere una autorización, de manera predeterminada, todos los usuarios pueden utilizar el dispositivo. Si se requiere una autorización, solamente los usuarios autorizados pueden utilizar el dispositivo.

Para denegar el acceso total a un dispositivo asignable, consulte el Ejemplo 21-1, “Impedir la asignación remota del dispositivo de audio”. Para crear y utilizar una nueva autorización, consulte el Ejemplo 21-3, “Creación y asignación de autorizaciones de dispositivos Trusted Path y Non-Trusted Path”.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1. **(Opcional) Cree un archivo de ayuda para cada nueva autorización de dispositivo.**

   Los archivos de ayuda están en formato HTML. La convención de denominación es *AuthName*`.html`, como en `DeviceAllocateCD.html`.

2. **Cree las autorizaciones de dispositivos.**

   ```
   # auths add -t "Authorization description" -h /full/path/to/helpfile.html authorization-name
   ```

3. **Agregue las autorizaciones nuevas a los perfiles de derechos adecuados.**

   ```
   # profiles rights-profile
   profiles:rights-profile > add auths="authorization-name"...
   ```

4. **Asigne los perfiles a usuarios y roles.**

   ```
   # usermod -P "rights-profile" username
   # rolemod -P "rights-profile" rolename
   ```

5. **Utilice las autorizaciones para restringir el acceso a dispositivos seleccionados.**

   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 [300].

ejemplo 21-2 Creación de autorizaciones para dispositivos específicas

En este ejemplo, un administrador de seguridad de NewCo necesita establecer autorizaciones específicas de dispositivos para la compañía.

En primer lugar, el administrador crea los siguientes archivos de ayuda:

```
Newco.html
```

```
NewcoDevAllocateCDVD.html
NewcoDevAllocateUSB.html
```

A continuación, el administrador crea un archivo de ayuda de plantilla a partir del cual se copian y modifican los demás archivos de ayuda.

```
<HTML>
-- Copyright 2012 Newco.  All rights reserved.
-- NewcoDevAllocateCDVD.html
-->
<HEAD>
<TITLE>Newco Allocate CD or DVD Authorization</TITLE>
</HEAD>
<BODY>
The com.newco.dev.allocate.cdvd authorization enables you to allocate the
CD drive on your system for your exclusive use.
<p>
The use of this authorization by a user other than the authorized account
is a security violation.
<p>
</BODY>
</HTML>
```

Después de crear los archivos de ayuda, el administrador utiliza el comando `auths` para crear cada autorización de dispositivo. Dedo que las autorizaciones se utilizan en toda la compañía, el administrador coloca las autorizaciones en el repositorio LDAP. El comando incluye el nombre de la ruta a los archivos de ayuda.

El administrador crea dos autorizaciones de dispositivos y un encabezado de autorización Newco.

- Una autorización autoriza al usuario para asignar una unidad de CD-ROM o DVD.

  ```
  # auths add -S ldap -t "Allocate CD or DVD" \
    -h /docs/helps/NewcoDevAllocateCDVD.html com.newco.dev.allocate.cdvd
  ```

- Una autorización autoriza al usuario para asignar un dispositivo USB.

  ```
  # auths add -S ldap -t "Allocate USB" \
    -h /docs/helps/NewcoDevAllocateUSB.html com.newco.dev.allocate.usb
  ```

- El encabezado de autorización Newco identifica todas las autorizaciones Newco.

  ```
  # auths add -S ldap -t "Newco Auth Header" \
    -h /docs/helps/Newco.html com.newco
  ```

ejemplo 21-3 Creación y asignación de autorizaciones de dispositivos Trusted Path y Non-Trusted Path

De manera predeterminada, la autorización Allocate Devices permite la asignación desde adentro de Trusted Path y desde afuera de Trusted Path.

En el siguiente ejemplo, la política de seguridad del sitio requiere la restricción de la asignación remota de CD-ROM y DVD. El administrador de seguridad crea la

autorización `com.newco.dev.allocate.cdvd.local`. Esta autorización corresponde a las unidades de CD-ROM y DVD que se asignan con Trusted Path. La autorización `com.newco.dev.allocate.cdvd.remote` corresponde a los pocos usuarios que tienen permiso para asignar una unidad de CD-ROM o DVD fuera de Trusted Path.

El administrador de seguridad crea los archivos de ayuda, agrega las autorizaciones de dispositivos a la base de datos `auth_attr`, agrega las autorizaciones a los dispositivos y, luego, aplica las autorizaciones en los perfiles de derechos. El rol `root` asigna los perfiles a los usuarios que tienen permiso para asignar dispositivos.

- Los siguientes comandos agregan las autorizaciones de dispositivos a la base de datos `auth_attr`:

```
# auths add -S ldap -t "Allocate Local DVD or CD" \
  -h /docs/helps/NewcoDevAllocateCDVDLocal.html \
  com.newco.dev.allocate.cdvd.local
# auths add -S ldap -t "Allocate Remote DVD or CD" \
  -h /docs/helps/NewcoDevAllocateCDVDRemote.html \
  com.newco.dev.allocate.cdvd.remote
```

- A continuación, se muestra la asignación de Device Manager:

  La asignación local de la unidad de CD-ROM está protegida por Trusted Path.

```
Device Name: cdrom_0
For Allocations From: Trusted Path
Allocatable By: Authorized Users
Authorizations: com.newco.dev.allocate.cdvd.local
```

  La asignación remota no está protegida por Trusted Path; por lo tanto, los usuarios remotos deben ser confiables. En el paso final, el administrador autorizará la asignación remota para dos roles únicamente.

```
Device Name: cdrom_0
For Allocations From: Non-Trusted Path
Allocatable By: Authorized Users
Authorizations: com.newco.dev.allocate.cdvd.remote
```

- Los siguientes comandos crean los perfiles de derechos Newco para estas autorizaciones y agregan las autorizaciones a los perfiles:

```
# profiles -S ldap "Remote Allocator"
profiles:Remote Allocator > set desc="Allocate Remote CDs and DVDs"
profiles:Remote Allocator > set help="/docs/helps/NewcoDevRemoteCDVD.html"
profiles:Remote Allocator > add auths="com.newco.dev.allocate.cdvd.remote"
profiles:Remote Allocator > end
profiles:Remote Allocator > exit

# profiles -S ldap "Local Only Allocator"
profiles:Local Only Allocator > set desc="Allocate Local CDs and DVDs"
```

```
profiles:Local Only Allocator > set help="/docs/helps/NewcoDevLocalCDVD.html"
profiles:Local Only Allocator > add auths="com.newco.dev.allocate.cdvd.local"
profiles:Local Only Allocator > end
profiles:Local Only Allocator > exit
```

- Los siguientes comandos asignan los perfiles de derechos a los usuarios autorizados. El rol `root` asigna los perfiles. En este sitio, únicamente los roles están autorizados para asignar remotamente dispositivos periféricos.

```
# usermod -P "Local Only Allocator" jdoe
# usermod -P "Local Only Allocator" kdoe

# rolemod -P "Remote Allocator" secadmin
# rolemod -P "Remote Allocator" sysadmin
```

▼ 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 [297].

1. **Siga el procedimiento descripto en Cómo configurar un dispositivo mediante Device Manager en Trusted Extensions [289].**

   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 activa 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 [143].

- **Asigne al usuario un perfil de derechos que cuente con la autorización Allocate Device.**

  Para ver el procedimiento paso a paso, consulte “Asignación de derechos a usuarios” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

  Los siguientes perfiles de derechos activan un rol para que asigne dispositivos:

  - Todas las autorizaciones
  - Gestión de dispositivos
  - Copia de seguridad de medios
  - Gestión de etiquetas de objetos
  - Instalación de software

  Los siguientes perfiles de derechos activan un rol para que revoque o reclame dispositivos:

  - Todas las autorizaciones
  - Gestión de dispositivos

  Los siguientes perfiles de derechos activan un rol para que cree o configure dispositivos:

  - Todas las autorizaciones
  - Seguridad de dispositivos

  El Ejemplo 21-2, “Creación de autorizaciones para dispositivos específicas” muestra cómo asignar las autorizaciones.

♦ ♦ ♦ CAPÍTULO 22

Trusted Extensions y la auditoría

En este capítulo, se describen las adiciones a la auditoría que Trusted Extensions proporciona.

- "Auditoría en Trusted Extensions" [303]
- "Gestión de auditoría por roles en Trusted Extensions" [303]
- "Referencia de auditoría de Trusted Extensions" [304]

Auditoría en Trusted Extensions

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 logs 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 2, "Planificación de la auditoría" de "Gestión de auditoría en Oracle Solaris 11.2 ".

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 [56].

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.

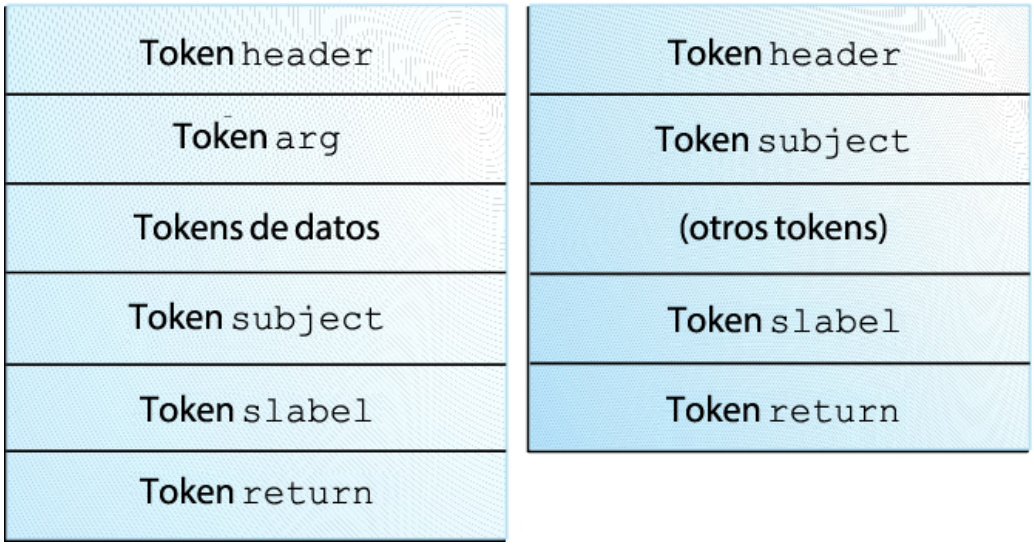
- El administrador de la seguridad puede seleccionar políticas de auditoría que son específicas de Trusted Extensions, `windata_down` y `windata_up`.
- Al revisar los registros de auditoría, el administrador del sistema puede seleccionar los registros de auditoría por etiqueta. Para obtener más información, 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 muestran en la página del comando man `audit.log`(4).

TABLA 22-1 Tokens de auditoría de Trusted Extensions

Nombre de token	Descripción
"Token `label`" [307]	Etiqueta de sensibilidad
"Token `xatom`" [307]	Identificación de los átomos de las ventanas X
"Token `xcolormap`" [307]	Información sobre el color de las ventanas X
"Token `xcursor`" [307]	Información sobre los cursores de las ventanas X
"Token `xfont`" [307]	Información sobre las fuentes de las ventanas X
"Token `xgc`" [308]	Información sobre el contexto gráfico de las ventanas X
"Token `xpixmap`" [308]	Información sobre los mapas de píxeles de las ventanas X
"Token `xproperty`" [308]	Información sobre las propiedades de las ventanas X
"Token `xselect`" [308]	Información sobre los datos de las ventanas X
"Token `xwindow`" [309]	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

Este capítulo contiene información sobre cómo garantizar que el software de terceros se ejecute de manera confiable en un sistema Trusted Extensions.

Agregación 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 agregación de software en un sistema Trusted Extensions es similar a la agregación 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. Sin embargo, puede instalar paquetes en una zona etiquetada ejecutando el comando `pkg` en la zona. Si lo hace, debe asegurarse de que la zona puede gestionar cuentas administrativas e indicadores de contraseña. Para ver una explicación, consulte “Aplicaciones restringidas a una zona etiquetada” [23]. Para obtener detalles sobre los paquetes y las zonas, consulte el Capítulo 9, “Acerca de la instalación automática y los paquetes de un sistema Oracle Solaris 11.2 con zonas instaladas” de “Creación y uso de zonas de Oracle Solaris ”.

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 "Aspectos básicos del usuario y derechos de procesos" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ". Además, 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 privilegios, consulte el Capítulo 1, "Sobre el uso de los derechos para controlar los usuarios y los procesos" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ". 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 "Creación y uso de zonas de Oracle Solaris ".
- **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 perfiles de derechos, consulte "Más información sobre los perfiles de derechos" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".
- **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.

Sugerencia - 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 log 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). También puede utilizar `dtrace` para evaluar el uso de privilegios y autorizaciones.
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.
4. Crear y asignar perfiles de derechos para el nuevo programa.

♦ ♦ ♦ 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:

- "Política de seguridad del sitio y Trusted Extensions" [316]
- "Recomendaciones de seguridad informática" [316]
- "Recomendaciones de seguridad física" [317]
- "Recomendaciones de seguridad del personal" [318]
- "Infracciones de seguridad comunes" [319]
- "Referencias de seguridad adicionales" [319]

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 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 log 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 de seguridad son 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 Departamento de Seguridad Nacional de EE. UU. (http://www.us-cert.gov/security-publications) publica información de seguridad. Además, 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 UNIX

Ingenieros de seguridad de Sun Microsystems. *Fundamentos de seguridad de Solaris 10*. Prentice Hall, 2009.

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.

Nemeth, Evi, Garth Snyder, Trent R. Hein y Ben Whaley. *Manual de administración del sistema UNIX y Linux (cuarta edición)* Pearson Education, Inc. 2010.

Publicaciones sobre seguridad informática general

Brunette, Glenn M. *Toward Systemically Secure IT Architectures* (Hacia arquitecturas de TI seguras desde el punto de vista sistemático). Especificaciones técnicas de Oracle archivadas, junio de 2006.

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. *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.

McClure, Stuart, Joel Scambray, George Kurtz. *Hackers expuestos 7: Secretos y soluciones de la seguridad de redes, séptima edición*. McGraw-Hill, 2012.

Stoll, Cliff. *El huevo del cuco*. Doubleday, 1989.

♦ ♦ ♦ APÉNDICE B

Lista de comprobación de configuración de Trusted Extensions

Esta lista de comprobación ofrece una descripción 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 activar 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 Administración de Trusted Extensions [89].
   - Comprenda los requisitos de seguridad del sitio.
   - Lea "Política de seguridad del sitio y Trusted Extensions" [316].
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.
   - Instale el SO Oracle Solaris.
3. Active Trusted Extensions. Consulte "Instalación y activación de Trusted Extensions" [35].
   a. Cargue el conjunto de paquetes de Trusted Extensions adecuado, para un sistema que ejecuta un escritorio de varios niveles o para un sistema que no lo hace.
   b. Ejecute el comando `labeladm enable` *options* para activar el servicio Trusted Extensions.

c. (Opcional) Ejecute el comando `labeladm encodings` *encodings-file* para instalar el archivo de codificaciones.

d. Reinicie el equipo.

4. (Opcional) Personalice la zona global. Consulte “Configuración de la zona global en Trusted Extensions” [39].

   a. 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.

   b. Verifique e instale el archivo `label_encodings` de su sitio.

   c. Reinicie el equipo.

5. Agregue zonas con etiquetas. Consulte “Creación de zonas con etiquetas” [43].

   a. Configure dos zonas con etiquetas automáticamente.

   b. Configure sus zonas con etiquetas manualmente.

   c. Cree un espacio de trabajo con etiquetas.

6. Configurar el servicio de nombres LDAP. Consulte el Capítulo 5, Configuración de LDAP para Trusted Extensions.

   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” [49].

8. Configure la red. Consulte “Etiquetado de hosts y redes” [215].

   - 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” [56].

      - 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” [63].

- 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” [269].

e. Configure los dispositivos. Consulte “Control de dispositivos en Trusted Extensions” [287].

   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.

♦ ♦ ♦ 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. El comando `labeladm` activa y desactiva el servicio `labeld`, y establece el archivo `label_encodings` para un sistema Trusted Extensions. 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.
Label Builder	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" [104].

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 "Servidor NFS y configuración de cliente en Trusted Extensions" [182]. 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" [130].

	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” [304].
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 activada. 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" [331]
- "Páginas del comando man de Oracle Solaris modificadas por Trusted Extensions" [337]

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 agregación 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 mediante Device Manager en Trusted Extensions [289].
`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 [122].

`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 Ejemplo 4-1, "Comprobación de la sintaxis de `label_encodings` en la línea de comandos".
`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 [164].
`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 [123].
labeladm(1M)	Activa y desactiva el servicio de etiquetas de Trusted Extensions y puede establecer el archivo `label_encodings`.
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 [155].
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 obtener un ejemplo, consulte Cómo configurar un dispositivo mediante Device Manager en Trusted Extensions [289].

`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” [112].
`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 para la interfaz gráfica de usuario de `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.
`tnctl`(1M)	Configura los parámetros de red de Trusted Extensions. También puede utilizar el comando `tncfg`. Si desea ver un ejemplo, consulte el Ejemplo 12-1, “Asignación del tipo de host CIPSO para la administración remota”.
`tnd`(1M)	Ejecuta el daemon de la red de confianza cuando está activado 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 [244]. 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 [190].
`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 supresión de zonas. `txzonemgr` es una secuencia de comandos `zenity` (1). Consulte "Creación de zonas con etiquetas" [43] and "Resolución de problemas de la red de confianza" [242].
`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 [138].
`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 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 "Selección de eventos de auditoría que se mostrarán" de "Gestión de auditoría en Oracle Solaris 11.2 ".
`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" [183].
`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 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. Además, 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 [243].
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 [190].
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. Agregar 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 [190].
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 [186] y Cómo restaurar archivos en Trusted Extensions [186].
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 clearance y min_label que son específicos de Trusted Extensions. Consulte "Planificación de la seguridad del usuario en Trusted Extensions" [25].

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 `.firefox`, 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 de inicio 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 `.firefox`, 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 de inicio 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 una ejecución correcta.

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.

El software Trusted Extensions está en proceso de evaluación para obtener la certificación según los criterios comunes v2.3 [agosto de 2005], una normativa ISO, con el nivel de seguridad (EAL) 4 respecto de numerosos perfiles de protección.

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 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 activación 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 de Trusted Extensions, debe agregar la sección `LOCAL DEFINITIONS` específica de Oracle al final de la GFI. Para obtener detalles, consulte Capítulo 5, “Customizing the LOCAL DEFINITIONS Section” 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 administrativas 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 `root` 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 activado. 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 activado. 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 configurado con Trusted Extensions, se asigna una etiqueta 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

A

acceso *Ver* acceso a equipos
  conjunto de datos ZFS montado en una zona de nivel inferior desde una zona de nivel superior, 169
  directorios de inicio, 157
  dispositivos, 281
  escritorio de varios niveles remoto, 152
  herramientas administrativas, 117
  impresoras, 259
  registros de auditoría por etiqueta, 304
  sistemas remotos, 147
  usuarios a zonas con etiquetas, 62
  zona global, 118
acceso a equipos
  responsabilidades del administrador, 111
  restricción, 282
acreditaciones
  descripción general de las etiquetas, 95
activación
  dominio de interpretación diferente de `1`, 43
  función de Trusted Extensions, 35
  interrupción del teclado, 124
  red CIPSO IPv6, 42
  servicio `dpadm` , 79
  servicio `dsadm`, 79
  servicio `labeld`, 35
activación de Trusted Extensions
  `/usr/sbin/labeladm`, 101
etiqueta `ADMIN_LOW`
  etiqueta mínima, 97
  protección de archivos administrativos, 111
administración
  archivos
    copia de seguridad con etiquetas, 186
    restauración con etiquetas, 186
  archivos de inicio para los usuarios, 138
  archivos de sistema, 124
  asignación de autorizaciones para dispositivos, 300
  asignación de dispositivos, 300
  auditoría en Trusted Extensions, 303
  autorizaciones convenientes para usuarios, 143
  autorizaciones para dispositivos, 297
  bloqueo de cuentas, 144
  cambio de etiquetas de información, 145
  conjuntos de datos de varios niveles, 177
  correo, 257
  de la zona global, 118
  dispositivos, 287, 288
  impresión, 269
  impresión con etiquetas, 259
  impresión sin etiquetas, 276
  IPsec con etiquetas, 237
  LDAP, 251
  plantillas de host remoto, 218
  plantillas de seguridad, 221, 227
  privilegios de usuario, 144
  puertos de varios niveles, 237
  red de confianza, 215
  referencia rápida para administradores, 327
  remota, 147
  rutas con atributos de seguridad, 234
  sistemas de archivos
    descripción general, 174
    montaje, 189
    resolución de problemas, 190
  software de terceros, 311
  uso compartido de sistemas de archivos, 187
  usuarios, 129, 135, 141
  zonas, 162
  zonas por uso `txzonemgr`, 162
administración remota
  métodos, 148

valores predeterminados, 147
administradores de la seguridad *Ver* rol de administrador de la seguridad
agregación
bases de datos de red al servidor LDAP, 83
conjuntos de datos de varios niveles, 69
daemon `nscd` a cada zona con etiquetas, 54
daemon `nscd` específico de zona, 54
hosts remotos, 53
interfaces de red compartidas, 50
interfaces lógicas, 51
interfaces VNIC, 52
paquetes Trusted Extensions, 36
plantillas de host remoto, 218
protecciones IPsec, 238
rol LDAP con `roleadd`, 58
rol local con `roleadd`, 56
roles, 56
usuario local con `useradd`, 60
usuarios que puedan asumir roles, 58
zonas secundarias, 68
aplicación `/usr/bin/tsoljdsselmgr`, 112
aplicación `tsoljdsselmgr`, 112
aplicaciones
activación del contacto de red inicial entre el cliente y el servidor, 232
de confianza y confiables, 312
evaluación para la seguridad, 314
aplicaciones comerciales
evaluación, 314
aplicaciones de confianza
en un espacio de trabajo de rol, 101
archivo `.copy_files`
configuración para usuarios, 138, 139
descripción, 133
archivo `.link_files`
configuración para usuarios, 138
descripción, 133
archivo `/etc/default/kbd`
cómo editar, 124
archivo `/etc/default/login`
cómo editar, 124
archivo `/etc/default/passwd`
cómo editar, 124
archivo `/etc/hosts`, 217
archivo `/etc/security/policy.conf`
cómo editar, 124
modificación, 137
valores predeterminados, 130
archivo `/etc/security/tsol/label_encodings`, 97
archivo `/etc/system`
modificación para red CIPSO IPv6, 42
archivo `/usr/lib/cups/filter/tsol_separator.ps`, 261
archivo `/usr/share/gnome/sel_config`, 114
archivo de codificaciones *Ver* archivo `label_encodings`
archivo de imagen del núcleo `/dev/kmem`
infracción de seguridad, 313
archivo de imagen del núcleo `kmem`, 313
archivo `label_encodings`
comprobación, 40
contenido, 97
fuente de rangos de acreditación, 97
instalación, 37, 40
localización, 20
modificación, 37, 40
referencia para la impresión con etiquetas, 261
archivo `policy.conf`
cambio de valores predeterminados, 124
cómo editar, 137
palabras clave de cambio de Trusted Extensions, 137
valores predeterminados, 130
archivo `sel_config`, 114, 114
archivo TrustedExtensionsPolicy
descripción, 109
archivo `tsol_separator.ps`
personalización de la impresión con etiquetas, 261
valores configurables, 266
archivos
`.copy_files`, 133, 138
`.link_files`, 133, 138
`/etc/default/kbd`, 124
`/etc/default/login`, 124
`/etc/default/passwd`, 124
`/etc/security/policy.conf`, 130, 137
`/usr/bin/tsoljdsselmgr`, 112
`/usr/lib/cups/filter/tsol_separator.ps`, 261

/usr/sbin/txzonemgr, 102, 162
/usr/share/gnome/sel_config, 114
acceso desde las etiquetas dominantes, 164
archivo /etc/security/tsol/label_encodings, 97
autorizar a un usuario o rol a cambiar etiquetas, 145
copia de seguridad con etiquetas, 186
copia desde medios extraíbles, 73
getmounts, 164
impedir el acceso de etiquetas dominantes, 166
inicio, 138
montaje en bucle de retorno, 165
policy.conf, 124
restauración con etiquetas, 186
volver a etiquetar privilegios, 170
archivos de configuración
carga, 73
copia, 72
archivos de inicio
procedimientos de personalización, 138
archivos de sistema
edición, 124
sel_config, 114
archivos del sistema
label_encodings, 40
tsol_separator.ps, 278
archivos log
protección de logs del servidor LDAP, 81
archivos y sistemas de archivos
montaje, 187
nombres, 187
uso compartido, 187
asignación
perfiles de derechos, 133
privilegios a usuarios, 133
uso de Device Manager, 283
asignación de dispositivos
autorización, 300
descripción general, 281
para la copia de datos, 72
perfiles que incluyen autorizaciones de asignación, 301
asignación de nombres
zonas, 45
asunción
roles, 118
atributo de ruta de confianza
si está disponible, 100
atributos de seguridad, 205
configuración de hosts remotos, 218
modificación de valores predeterminados de usuarios, 136
modificación de valores predeterminados para todos los usuarios, 137
uso en enrutamiento, 234
auditoría en Trusted Extensions
adiciones a los comandos de auditoría existentes, 309
clases de auditoría X, 305
diferencias con la auditoría de Oracle Solaris, 303
eventos de auditoría adicionales, 306
planificación, 25
políticas de auditoría adicionales, 309
referencia, 303
roles de administración, 303
tareas, 304
tokens de auditoría adicionales, 306
autorización
asignación de dispositivos, 300
impresión sin etiquetas, 276
autorización Allocate Device, 143, 282, 300
autorización Configure Device Attributes, 301
autorización Downgrade DragNDrop or CutPaste Info, 143
autorización Downgrade File Label, 143
autorización DragNDrop or CutPaste without viewing contents, 143
autorización Print without Banner, 143
autorización Print without Label, 143
autorización Remote Login, 143
autorización Revoke or Reclaim Device, 300, 301
autorización Shutdown, 143
autorización solaris.print.nobanner, 138
autorización solaris.print.unlabeled, 138
autorización Upgrade DragNDrop or CutPaste Info, 143
autorización Upgrade File Label, 143
autorizaciones
agregar nuevas autorizaciones para dispositivos, 297
Allocate Device, 282, 300
asignación, 132

asignación de autorizaciones para dispositivos, 300
autorizar a un usuario o rol a cambiar etiquetas, 145
Configure Device Attributes, 301
convenientes para usuarios, 143
creación de autorizaciones para dispositivos locales y remotos, 298
creación de autorizaciones para dispositivos personalizadas, 297
otorgadas, 95
perfiles que incluyen autorizaciones de asignación de dispositivos, 301
personalización para dispositivos, 300
Revoke or Reclaim Device, 300, 301
aviso de seguridad
combinación de teclas, 121

B

bajada de nivel de etiquetas
configuración de reglas para el confirmador de selección, 114
banda de confianza
dirigir el puntero hacia, 122
en el sistema de varios periféricos, 93
movimiento de paneles a la parte inferior de la pantalla, 66
bases de datos
en LDAP, 251
red de confianza, 197
bases de datos de red
descripción, 197
en LDAP, 251
bloqueo de cuentas
impedir para usuarios que pueden asumir roles, 144
búsqueda
equivalente de la etiqueta en formato de texto, 123
equivalente de la etiqueta en hexadecimal, 122

C

cambio
etiquetas de usuarios autorizados, 145
nivel de seguridad de datos, 145
palabra clave `IDLETIME`, 137
privilegios de usuario, 144
reglas para cambios de etiqueta, 114
valores predeterminados de seguridad del sistema, 124
captura de confianza
combinación de teclas, 121
cierre de sesión
requisito, 137
clases de auditoría X, 305
colores
que señalan la etiqueta del espacio de trabajo, 99
comando `atohexlabel`, 122
comando `chk_encodings`, 41
comando `dtsession`
ejecución de `updatehome`, 133
comando `hextoalabel`, 123
comando `ipadm`, 196
comando `ipseckey`, 197
comando `labeladm`, 35
activación de Trusted Extensions, 35
eliminación de Trusted Extensions, 74
instalación del archivo de codificaciones, 37, 37
comando `netstat`, 197, 244
comando `roleadd`, 56
comando `route`, 197
comando `snoop`, 197, 244
comando `tncfg`
creación de un puerto de varios niveles, 235
descripción, 196
modificación del valor del dominio de interpretación, 43
comando `tnchkdb`
descripción, 196
comando `tnctl`
descripción, 196
comando `tnd`
descripción, 196
comando `tninfo`
descripción, 196
uso, 247
comando `updatehome`, 133
comando `useradd`, 60
comando `utadm`
configuración del servidor Sun Ray predeterminado, 233
comandos

ejecución con privilegio, 118
resolución de problemas de red, 244
combinaciones de teclas
comprobación de confianza de la captura, 121
componente de etiqueta de clasificación, 96
componente de etiqueta de compartimiento, 96
comprobación
archivo `label_encodings`, 40
funcionamiento de roles, 61
comprobaciones de acreditaciones, 205
conceptos de redes, 195
configuración
acceso a Trusted Extensions remoto, 147
archivos de inicio para los usuarios, 138
autorizaciones para dispositivos, 297
dispositivos, 289
impresión con etiquetas, 269
interfaces de red, 50, 53
interfaces lógicas, 51
LDAP para Trusted Extensions, 76
mediante la asunción de un rol limitado o como `root`, 35
red de confianza, 215
rutas con atributos de seguridad, 234
servidor proxy LDAP para clientes de Trusted Extensions, 84
Trusted Extensions, 39
VNIC, 52
zonas con etiquetas de Trusted Extensions, 43
configuración de impresión con etiquetas (mapa de tareas), 269
configuración de IPsec con etiquetas (mapa de tareas), 237
configuración de la administración remota en Trusted Extensions (mapa de tareas), 149
configuración de LDAP
creación de cliente, 86
para Trusted Extensions, 76
servidores NFS, y, 76
servidores Sun Ray, y, 76
configuración de LDAP en una red Trusted Extensions Network (mapa de tareas), 75
configuración de Trusted Extensions
acceso remoto, 147
agregación de bases de datos de red al servidor LDAP, 83
bases de datos para LDAP, 76
cambio del valor predeterminado del dominio de interpretación, 43
configuración evaluada, 19
división de tareas, 33
LDAP, 76
lista de comprobación para el equipo de configuración inicial, 323
mapas de tareas, 29, 29
procedimientos iniciales, 39
reinicio para activar etiquetas, 37
resolución de problemas, 66
responsabilidades del equipo de configuración inicial, 33
sistemas remotos, 147
zonas con etiquetas, 43, 43
configuración de un servidor proxy LDAP en un sistema Trusted Extensions (mapa de tareas), 76
conjunto de etiquetas de seguridad
plantillas de host remoto, 199
conjuntos de datos *Ver* ZFS
conjuntos de datos de varios niveles
creación, 69
descripción general, 180
contraseñas
almacenamiento, 111
asignación, 132
cambio de contraseña de usuario `root`, 119
cambio de contraseñas de usuario, 109
cambio en zona con etiquetas, 120
comprobar si la petición de contraseña es de confianza, 121
especificación al cambiar etiquetas, 109, 109, 109
opción de menú Change Password, 109, 119
control *Ver* restricción
control de acceso discrecional (DAC), 95
control de acceso obligatorio (MAC)
aplicación en la red, 193
en Trusted Extensions, 95
control de dispositivos en Trusted Extensions (mapa de tareas), 287
copia de seguridad de
sistema anterior previo a la instalación, 28
correo
administración, 257
implementación en Trusted Extensions, 257

varios niveles, 257
cortar y pegar
configuración de reglas para cambios de etiquetas, 114
y etiquetas, 112
creación
autorizaciones para dispositivos, 297
cliente LDAP, 86
cuentas, 56
cuentas durante la configuración o después, 35
directorios de inicio, 63, 182
rol LDAP con `roleadd`, 58
rol local con `roleadd`, 56
roles, 56
servidor de directorios de inicio, 63
servidor proxy LDAP para clientes de Trusted Extensions, 85
usuario local con `useradd`, 60
usuarios que puedan asumir roles, 58
zonas, 43
zonas con etiquetas, 43
creación de zonas con etiquetas, 43
cuadro de diálogo Selection Manager
descripción, 109
cuentas, 91, 91
Ver también roles
Ver también usuarios
creación, 56
planificación, 25

D

DAC *Ver* control de acceso discrecional (DAC)
daemon de caché de servicio de nombres *Ver* daemon `nscd`
daemon `nscd`
agregación a cada zona con etiquetas, 54
datos
reetiquetado eficaz, 69
decisión
de configurar mediante la asunción de un rol limitado o como `root`, 35
de usar un archivo de codificaciones suministrado por Oracle, 34
decisiones que se deben tomar
antes de activar Trusted Extensions, 34
en función de la política de seguridad del sitio, 316
definiciones de componente
archivo `label_encodings`, 97
depuración *Ver* resolución de problemas
derechos *Ver* perfiles de derechos
desactivación
Trusted Extensions, 74
desasignación
forzar, 293
desasignación de dispositivos, 73
Device Manager
descripción, 283
herramienta administrativa, 102
uso de los administradores, 289
diferencias
ampliación de interfaces de Oracle Solaris, 328
entre la auditoría de Trusted Extensions y Oracle Solaris, 303
entre Trusted Extensions y SO Oracle Solaris, 92
interfaces administrativas en Trusted Extensions, 327
opciones limitadas en Trusted Extensions, 329
valores predeterminados en Trusted Extensions, 329
dirección comodín *Ver* mecanismo de reserva
direcciones IP
dirección de host `0.0.0.0`, 203
mecanismo de reserva en redes de confianza, 202
directorios
acceso a nivel inferior, 157
autorizar a un usuario o rol a cambiar etiquetas, 145
montaje, 187
para configuración de servicio de nombres, 83
uso compartido, 187
directorios de inicio
acceso, 157
creación, 63, 182
creación de servidor para, 63
inicio de sesión y obtención, 64, 65
dispositivos
acceso, 283
administración, 287
administración con Device Manager, 289
agregación de secuencia de comandos `device_clean`, 295
agregar autorizaciones personalizadas, 300

asignación, 281
configuración de dispositivos, 289
configuración rango de etiquetas para dispositivos no asignables, 282
crear autorizaciones nuevas, 297
en Trusted Extensions, 281
impedimento de asignación remota de audio, 295
política de acceso, 283
política de configuración, 283
protección, 103
protección de no asignables, 294
reclamación, 293
resolución de problemas, 293
uso, 287
valores predeterminados de políticas, 283
dispositivos de audio
impedimento de asignación remota, 295
dispositivos no asignables
configuración del rango de etiquetas, 282
protección, 294
DOI
plantillas de hosts remotos, 199
dominio de etiquetas, 96
dominio de interpretación (DOI)
modificación, 43

E

edición de archivos de sistema, 124
elección *Ver* selección
eliminación
daemos `nscd` específico de zona, 55
etiquetas en las copias impresas, 276
eliminación de Trusted Extensions *Ver* desactivación
enrutamiento, 203
comandos en Trusted Extensions, 209
comprobaciones de acreditaciones, 205
conceptos, 207
ejemplo de, 208
tablas, 205, 207
uso del comando `route`, 234
equipo de configuración inicial
lista de comprobación para la configuración de Trusted Extensions, 323
equipos portátiles
planificación, 24
equivalentes de etiquetas de texto
determinación, 123
escritorio de varios niveles remoto
acceso, 152
escritorios
acceso de varios niveles remoto, 152
cambios de color de espacios de trabajo, 118
inicio de sesión en modo a prueba de fallos, 141
movimiento de paneles a la parte inferior de la pantalla, 66
uso de Vino para compartir, 154
espacio de trabajo de rol
zona global, 107
espacios de trabajo
cambios de color, 118
colores que señalan la etiqueta de, 99
zona global, 107
estado de error de asignación
corrección, 293
estructura de gestión de servicios (SMF)
`dpadm`, 79
`dsadm`, 79
etiqueta `ADMIN_HIGH`
acreditación de rol, 58
archivos montados mediante NFS en la zona global, 175
conjuntos de datos de varios niveles y, 176
dispositivos y, 282
etiqueta administrativa superior, 96
etiquetas de páginas del cuerpo y, 273
`mlslabel` y, 179
procesos de zona global y zonas, 160
roles y, 108
sin localización, 20
etiqueta `ADMIN_LOW`
limitaciones de los montajes de sistemas sin etiquetar, 178
montaje de archivos y, 177
etiqueta de seguridad de la aplicación, 210
etiqueta de transferencia, 211
etiqueta interna, 210
etiquetado
activación de etiquetas, 37
zonas, 45
etiquetado de hosts y redes (tareas), 215
etiquetas, 91

Ver también rangos de etiquetas
acreditación en modo túnel, 212
archivo TrustedExtensionsPolicy, 109
autorizar a un usuario o rol a cambiar etiquetas de datos, 145
bajada y subida de nivel, 114
bien formadas, 97
componente de clasificación, 96
componente de compartimiento, 96
configuración de reglas para cambios de etiqueta, 114
cuadro de diálogo Selection Manager, 109
de procesos, 99
de procesos de usuario, 98
descripción, 95
descripción general, 95
determinación de equivalentes de texto, 123
dominio, 96
en copias impresas, 261
en intercambios IPsec, 210
especificación para zonas, 45
extensiones para asociaciones de seguridad IKE, 212
extensiones para asociaciones de seguridad IPsec, 211
impresión sin etiquetas de páginas, 278
opción de menú Change Workspace Label, 109
planificación, 20
predeterminadas en plantillas de host remoto, 199
relaciones, 96
reparación en bases de datos internas, 123
resolución de problemas, 123
visualización de etiquetas de sistemas de archivos en zona con etiquetas, 165
visualización en hexadecimal, 122
etiquetas administrativas, 96
etiquetas bien formadas, 97
etiquetas máximas
plantillas de host remoto, 199
etiquetas mínimas
plantillas de host remoto, 199
evaluación de programas para la seguridad, 312
exportación *Ver* uso compartido
extensiones de etiquetas
asociaciones de seguridad IPsec, 211
negociaciones IKE, 212

G

gestión *Ver* administración
gestión de dispositivos en Trusted Extensions (mapa de tareas), 288
gestión de impresión en Trusted Extensions (mapa de tareas), 269
gestión de usuarios y derechos (mapa de tareas), 141
gestión de zonas (mapa de tareas), 162
gestor de selecciones
configuración de reglas para el confirmador de selección, 114
configuración predeterminada, 112
grupos
precauciones para suprimir, 112
requisitos de seguridad, 112
guías básicas
mapa de tareas: configuración de Trusted Extensions con los valores predeterminados proporcionados, 30
mapa de tareas: configuración de Trusted Extensions según los requisitos del sitio, 30
mapa de tareas: preparación y activación de Trusted Extensions, 29
mapa de tareas: selección de una configuración de Trusted Extensions, 29

H

herramientas *Ver* herramientas administrativas
herramientas administrativas
acceso, 117
archivos de configuración, 105
comandos, 104
descripción, 101
Device Manager, 103
generador de etiquetas, 103
Labeled Zone Manager, 102
secuencia de comandos `txzonemgr`, 102
Selection Manager, 103
hosts
agregación a plantilla de seguridad, 221, 227
agregación de archivo `/etc/hosts`, 217
asignación de una plantilla, 221
conceptos de redes, 195
hosts remotos
uso de mecanismo de reserva en `tnrhdb`, 202

I

IKE
  etiquetas en modo túnel, 212
importación
  software, 311
impresión
  autorizaciones, 268
  autorizaciones para un resultado sin etiquetas de un sistema público, 138
  configuración de etiquetas y texto, 266
  configuración de trabajos de impresión públicos, 277
  configuración de zona con etiquetas, 272
  configuración para cliente de impresión, 273
  configuración para salida etiquetada de varios niveles, 269, 271
  en idioma local, 266
  etiquetado de un servidor de impresión de Oracle Solaris, 277
  gestión, 259
  internacionalización de salida con etiquetas, 266
  localización de salida con etiquetas, 266
  PostScript, 267
  prevención de etiquetas en la salida, 276
  sin carátulas ni ubicadores, 143
  sin etiquetas de páginas, 143, 278
  trabajos públicos de un servidor de impresión de Oracle Solaris, 277
  uso de un servidor de impresión de Oracle Solaris, 277
  y archivo `label_encodings`, 97
impresión con etiquetas
  eliminación de etiqueta, 143
  páginas de la carátula, 262
  páginas del cuerpo, 264
  sin página de carátula, 143
impresión de varios niveles
  acceso mediante cliente de impresión, 273
  configuración, 269, 271
impresión sin etiquetas
  configuración, 276
impresiones *Ver* impresión
impresoras
  configuración de rango de etiquetas, 282
información de seguridad
  en copias impresas, 261
  planificación para Trusted Extensions, 28
informática en red virtual (VNC) *Ver* sistemas Xvnc que ejecutan Trusted Extensions
inicio de sesión
  en un servidor de directorio de inicio, 64, 65
  mediante el comando `ssh`, 155
  por roles, 107
  remoto, 150
instalación
  archivo `label_encodings`, 37, 40
  Oracle Directory Server Enterprise Edition, 76
  SO Oracle Solaris para Trusted Extensions, 33
interfaces
  agregación a plantilla de seguridad, 221, 227
  verificar que estén activas, 243
internacionalización *Ver* localización
interrupción del teclado
  activación, 124
introducción para administradores de Trusted Extensions (mapa de tareas), 117
IPsec
  con etiquetas de Trusted Extensions, 210
  etiquetas en intercambios de confianza, 210
  etiquetas en modo túnel, 212
  extensiones de etiquetas, 211
  protecciones con extensiones de etiquetas, 213
IPsec con etiquetas *Ver* IPsec
IPv6
  entrada en archivo `/etc/system` , 42
  resolución de problemas, 42

L

Labeled Zone Manager *Ver* secuencia de comandos `txzonemgr`
LDAP
  bases de datos de Trusted Extensions, 251
  detención de servidor, 254
  detención de servidor proxy, 254
  gestión del servicio de nombres, 253
  inicio de servidor, 254
  inicio de servidor proxy, 254
  planificación, 24
  resolución de problemas, 247
  servicio de nombres para Trusted Extensions, 251
  visualización de entradas, 253

limitación
hosts definidos en la red, 229
listas de comprobación para el equipo de configuración inicial, 323
localización
configuración de copias impresas con etiquetas, 266
LOFS
montaje de conjuntos de datos en Trusted Extensions, 173

M

MAC *Ver* control de acceso obligatorio (MAC)
mecanismo de reserva
en plantillas de seguridad, 202
mecanismos de seguridad
ampliación, 108
Oracle Solaris, 312
medios
copia de archivos desde extraíbles, 73
menú Trusted Extensions
Assume Role, 118
MLP *Ver* puertos de varios niveles (MLP)
modificación
archivo `label_encodings`, 40
montaje
archivos en bucle de retorno, 165
conjunto de datos ZFS en zona con etiquetas, 168
descripción general, 177
resolución de problemas, 190
sistemas de archivos, 187
montaje de conjuntos de datos en Trusted Extensions, 173
montajes de varios niveles
versiones del protocolo NFS, 184
montajes NFS
acceso a directorios de nivel inferior, 182
en zonas globales y con etiquetas, 177

N

NFS
montaje de conjuntos de datos en Trusted Extensions, 173
nombres
especificación para zonas, 45
nombres de sistemas de archivos, 187

O

opción `-c`
secuencia de comandos `txzonemgr`, 44
opción de menú Assume Role, 118
opción de menú Change Password
descripción, 109
uso para cambio de contraseña de usuario `root`, 119
opción de menú Change Workspace Label
descripción, 109
Oracle Directory Server Enterprise Edition *Ver* servidor LDAP

P

páginas de carátula
diferencia respecto de una página de ubicador, 264
eliminación de etiquetas, 278
típicas, 263
páginas de la carátula
descripción de «con etiquetas», 262
páginas de ubicador *Ver* páginas de la carátula
páginas del comando man
referencia rápida para administradores de Trusted Extensions, 331
páginas del cuerpo
descripción de «con etiquetas», 264
etiqueta `ADMIN_HIGH`en, 273
sin etiquetas, 278
palabra clave `IDLECMD`
cambio de valor predeterminado, 137
palabra clave `IDLETIME`
cambio de valor predeterminado, 137
paneles
movimiento a la parte inferior de la pantalla, 66
paquetes
función Trusted Extensions, 36
paquetes de multidifusión, 195
paquetes de multidifusión etiquetados, 195
paquetes de red, 194
perfil de revisión de auditoría
revisión de registros de auditoría, 304
perfiles *Ver* perfiles de derechos

perfiles de derechos
asignación, 133
autorizaciones convenientes , 143
con autorizaciones de asignación de dispositivos, 301
con la autorización Allocate Device, 301
con nuevas autorizaciones para dispositivos, 298
permitir
inicio de sesión en zona con etiquetas, 62
personalización
archivo `label_encodings`, 97
autorizaciones para dispositivos, 300
cuentas de usuario, 135
impresión sin etiquetas, 276
personalización de autorizaciones para dispositivos en Trusted Extensions (mapa de tareas), 296
Personalización del entorno de usuario para la seguridad (mapa de tareas), 135
planificación, 17
Ver también uso de Trusted Extensions
auditoría, 25
configuración de equipo portátil, 24
creación de cuenta, 25
estrategia de administración, 19
estrategia de configuración de Trusted Extensions, 26
etiquetas, 20
hardware, 20
red, 21
servicio de nombres LDAP, 24
Trusted Extensions, 18
zonas, 22
planificación del hardware, 20
plantillas *Ver* plantillas de host remoto
plantillas de host remoto
agregación de sistemas a, 221, 227
asignación, 221
asignación de comodín `0.0.0.0/0`, 230
creación, 218
entrada para servidores Sun Ray, 230
plantillas de seguridad *Ver* plantillas de host remoto
política de acceso
control de acceso discrecional (DAC), 91, 92
control de acceso obligatorio (MAC), 92
dispositivos, 283
política de seguridad
auditoría, 309
formación de los usuarios, 109
usuarios y dispositivos, 285
política de seguridad del sitio
comprensión, 19
decisiones de la configuración de Trusted Extensions, 316
infracciones comunes, 319
recomendaciones, 316
recomendaciones de acceso físico, 317
recomendaciones para el personal, 318
tareas implicadas, 315
prevención *Ver* protección
privilegio `net_mac_aware`, 166
privilegio `proc_info`
eliminación del conjunto básico, 138
privilegios
al ejecutar comandos, 118
cambio de valores predeterminados para usuarios, 133
eliminación de `proc_info` del conjunto básico, 138
motivos no evidentes para el requerimiento, 313
restricción de usuarios, 144
procedimientos *Ver* tareas y mapas de tareas
procesos
etiquetas de, 99
etiquetas de procesos de usuario, 98
impedir que los usuarios vean los procesos de los demás, 138
programas *Ver* aplicaciones
programas de confianza, 312
agregación, 313
definidos, 312
propiedad `mlslabel`
etiqueta `ADMIN_HIGH` y, 179
protección
de archivos de etiquetas inferiores para que no se acceda a ellos, 166
dispositivos, 103, 281
dispositivos de asignación remota, 295
dispositivos no asignables, 294
hosts con etiquetas contra el acceso por hosts arbitrarios, 229
información con etiquetas, 99
proteger

sistemas de archivos con nombres no propietarios, 187
publicaciones
seguridad y UNIX, 319
puertas de enlace
comprobaciones de acreditaciones, 206
ejemplo de, 208
puertos de varios niveles (MLP)
administración, 237
ejemplo de MLP de NFSv3, 236
ejemplo de MLP de proxy web, 235

R

rango de sesión, 98
rangos de acreditación
archivo `label_encodings`, 97
rangos de etiquetas
configuración en búferes de trama, 282
configuración en impresoras, 282
restricción de acceso remoto, 147
recopilación de información
para el servicio LDAP, 77
recuperación del control del enfoque del escritorio, 121
red *Ver* red de confianza *Ver* red de Trusted Extensions
red de confianza
conceptos, 193
dirección de comodín `0.0.0.0/0`, 230
ejemplo de enrutamiento, 208
entrada `0.0.0.0 tnrhdb`, 229
etiquetas predeterminadas, 205
etiquetas y aplicación de MAC, 193
tipos de hosts, 199
uso de plantillas, 218
red de Trusted Extensions
activación de IPv6 para paquetes CIPSO, 42
agregación de daemon `nscd` específico de zona, 54
eliminación del daemon `nscd` específico de zona, 55
planificación, 21
Reducción de las restricciones de impresión en Trusted Extensions (mapa de tareas), 276
reetiquetado de datos
eliminación de ES, 69
reinicio
activación de etiquetas, 37
permitir inicio de sesión en zona con etiquetas, 62
reparación
etiquetas en bases de datos internas, 123
resolución de problemas
configuración de IPv6, 42
configuración de Trusted Extensions, 66
error en inicio de sesión, 141
LDAP, 247
reclamación de un dispositivo, 293
red, 242
red de confianza, 244
reparación de etiquetas en bases de datos internas, 123
sistemas de archivos montados, 190
verificar que la interfaz esté activa, 243
visualización de conjunto de datos ZFS montado en una zona de nivel inferior, 170
Resolución de problemas de la red de confianza (mapa de tareas), 242
responsabilidades del desarrollador, 313
restablecimiento del control del enfoque del escritorio, 121
restricción
acceso a archivos de nivel inferior, 166
acceso a dispositivos, 281
acceso a equipo basado en etiquetas, 282
acceso a impresoras con etiquetas, 260, 260, 261, 261
acceso a la zona global, 108
acceso remoto, 147
montajes de archivos de nivel inferior, 166
resultado de impresora *Ver* impresión
resultado de la impresión *Ver* impresión
rol de administrador de la seguridad
activación de las páginas del cuerpo sin etiquetas de un sistema público, 138
administración de la seguridad de las impresoras, 259
administración de usuarios, 141
aplicación de la seguridad, 285
asignación de autorizaciones a usuarios, 143
configuración de dispositivos, 289
creación, 56
creación de perfil de derechos de autorizaciones convenientes, 143
protección de dispositivos no asignables, 294

rol de administrador del sistema
  administración de las impresoras, 259
  creación, 58
  reclamación de un dispositivo, 293
  revisión de registros de auditoría, 304
rol de usuario root
  agregación de secuencia de comandos `device_clean`, 295
roles
  acceso a aplicación de confianza, 101
  administración de auditoría, 304
  agregación de rol LDAP con `roleadd`, 58
  agregación de rol local con `roleadd`, 56
  asignación de derechos, 133
  asunción, 107, 118
  creación, 108
  creación de administrador de la seguridad, 56
  decisión de si ARMOR, 35
  determinación del momento de creación, 35
  espacios de trabajo, 107
  salir del espacio de trabajo del rol, 118
  verificación del funcionamiento, 61
roles administrativos *Ver* roles
roles de ARMOR, 35, 56

S

secuencia de comandos `/usr/local/scripts/getmounts`, 164
secuencia de comandos `/usr/sbin/txzonemgr`, 44, 102, 162, 163
secuencia de comandos `getmounts`, 164
secuencia de comandos `txzonemgr`, 163
  opción `-c`, 44
secuencia de comandos `zenity`, 44
secuencias de comandos
  `/usr/bin/txzonemgr`, 163
  `/usr/sbin/txzonemgr`, 102, 162
  `getmounts`, 164
secuencias de comandos `device-clean`
  agregación a dispositivos, 295
  requisitos, 283
seguridad
  equipo de configuración inicial, 33
  política de seguridad del sitio, 315
  publicaciones, 319
selección
  registros de auditoría por etiqueta, 304
servicio `dpadm`, 79
servicio `dsadm`, 79
servicio `labeld`
  activación, 35
  desactivación, 74
servicios de nombres
  bases de datos exclusivas de Trusted Extensions, 251
  gestión de LDAP, 253
  LDAP, 251
servidor de varios niveles
  planificación, 24
servidor LDAP
  configuración de proxy para clientes de Trusted Extensions, 84
  configuración de un puerto de varios niveles, 82
  configuración del servicio de nombres, 77
  creación de proxy para clientes de Trusted Extensions, 85
  instalación en Trusted Extensions, 77
  protección de archivos log, 81
  recopilación de información para, 77
servidor proxy
  inicio y detención de LDAP, 254
servidores NFS
  servidores LDAP, y, 76
sesión en modo a prueba de fallos
  inicio de sesión, 141
sesiones
  modo a prueba de fallos, 141
similitudes
  entre la auditoría de Trusted Extensions y Oracle Solaris, 303
  entre Trusted Extensions y SO Oracle Solaris, 91
sistema de varios periféricos
  banda de confianza, 93
sistemas de archivos
  montaje en zonas globales y con etiquetas, 177
  montajes NFS, 177
  uso compartido, 174
  uso compartido en zonas globales y con etiquetas, 177
sistemas remotos

configuración para asunción de rol, 150
sistemas Sun Ray
activación del contacto inicial entre el cliente y el servidor, 233
dirección `0.0.0.0/32` para contacto de cliente, 230
impedir que los usuarios vean los procesos de los demás, 138
servidores LDAP, y, 76
sitio web para documentación, 30
sistemas Xvnc que ejecutan Trusted Extensions
acceso remoto a, 149, 152
SO Oracle Solaris
diferencias con el Trusted Extensions, 92
diferencias con la auditoría de Trusted Extensions, 303
similitudes con la auditoría de Trusted Extensions, 303
similitudes con Trusted Extensions, 91
software
administración de terceros, 311
importación, 311
`solaris.print.admin`
autorización, 268
`solaris.print.list`
autorización, 268
`solaris.print.nobanner`
autorización, 268
`solaris.print.unlabeled`
autorización, 268
Stop-A
activación, 124
subida de nivel de etiquetas
configuración de reglas para el confirmador de selección, 114
supresión
zonas con etiquetas, 74

T

tareas adicionales de configuración de Trusted Extensions, 67
tareas comunes en Trusted Extensions (mapa de tareas), 119
tareas y mapas de tareas
configuración de impresión con etiquetas (mapa de tareas), 269
configuración de IPsec con etiquetas (mapa de tareas), 237
configuración de la administración remota en Trusted Extensions (mapa de tareas), 149
configuración de LDAP en una red Trusted Extensions (mapa de tareas), 75
configuración de un servidor proxy LDAP en un sistema Trusted Extensions (mapa de tareas), 76
control de dispositivos en Trusted Extensions (mapa de tareas), 287
creación de zonas con etiquetas, 43
etiquetado de hosts y redes (tareas), 215
gestión de dispositivos en Trusted Extensions (mapa de tareas), 288
gestión de impresión en Trusted Extensions (mapa de tareas), 269
gestión de usuarios y derechos, 141
gestión de zonas (mapa de tareas), 162
mapa de tareas de introducción para administradores de Trusted Extensions, 117
mapa de tareas: configuración de Trusted Extensions con los valores predeterminados proporcionados, 30
mapa de tareas: configuración de Trusted Extensions según los requisitos del sitio, 30
mapa de tareas: preparación y activación de Trusted Extensions, 29
mapa de tareas: selección de una configuración de Trusted Extensions, 29
personalización de autorizaciones para dispositivos en Trusted Extensions (mapa de tareas), 296
Personalización del entorno de usuario para la seguridad (mapa de tareas), 135
Reducción de las restricciones de impresión en Trusted Extensions (mapa de tareas), 276
Resolución de problemas de la red de confianza (mapa de tareas), 242
tareas adicionales de configuración de Trusted Extensions, 67
tareas comunes en Trusted Extensions (mapa de tareas), 119
uso de dispositivos en Trusted Extensions (mapa de tareas), 287

visualización de plantillas de seguridad existentes (tareas), 216
tecla de acceso rápido
recuperación del control del enfoque del escritorio, 121
tipos de host
plantillas de host remoto, 199
redes, 194
tipos de hosts
redes, 199
tabla de plantillas y protocolos, 199
token de auditoría `label`, 307
token de auditoría `xatom`, 307
token de auditoría `xcolormap`, 307
token de auditoría `xcursor`, 307
token de auditoría `xfont`, 307
token de auditoría `xgc`, 308
token de auditoría `xpixmap`, 308
token de auditoría `xproperty`, 308
token de auditoría `xselect`, 308
token de auditoría `xwindow`, 309
tokens de auditoría de Trusted Extensions
lista de, 306
token `label`, 307
token `xatom`, 307
token `xcolormap`, 307
token `xcursor`, 307
token `xfont`, 307
token `xgc`, 308
token `xpixmap`, 308
token `xproperty`, 308
token `xselect`, 308
token `xwindow`, 309
traducción *Ver* localización
Trusted Extensions, 17
Ver también planificación de Trusted Extensions
acceso remoto a la pantalla, 154
activación, 35
agregación, 36
agregación a Oracle Solaris , 35
decisiones que se deben tomar antes de activar, 34
desactivación, 74
diferencias con el SO Oracle Solaris, 92
diferencias con la auditoría de Oracle Solaris, 303
diferencias desde la perspectiva de un administrador de Oracle Solaris, 28
estrategia de configuración de dos roles, 27
nuevas funciones de esta versión, 17
planificación de estrategia de configuración, 26
planificación de red, 21
planificación del hardware, 20
planificación para, 18
preparación para, 33
protecciones IPsec, 210
redes, 193
referencia rápida de páginas del comando man, 331
referencia rápida para administración, 327
requisitos de memoria, 21
resultados antes de la configuración, 28
similitudes con la auditoría de Oracle Solaris, 303
similitudes con SO Oracle Solaris, 91
Trusted Extensions (configuración)
procedimientos iniciales, 39
Trusted Path
Device Manager, 283

U

UID de root
necesario para las aplicaciones, 313
UID real de root
necesario para las aplicaciones, 313
una sola etiqueta
impresión en una zona, 272
inicio de sesión, 98
unidades de CD-ROM
acceso, 282
uso compartido
con Vino, 154
conjunto de datos ZFS de zona con etiquetas, 168
direcciones IP, 49
uso de dispositivos en Trusted Extensions (mapa de tareas), 287
usuarios
acceso a dispositivos, 281, 282
acceso a las impresoras, 259
agregación de usuario local con `useradd`, 60
archivo TrustedExtensionsPolicy, 109
archivos de inicio, 138
asignación de autorizaciones a, 132

asignación de contraseñas, 132
asignación de derechos, 133
asignación de etiquetas, 133
asignación de roles a, 132
autorizaciones para, 143
cambio de privilegios predeterminados, 133
configuración de directorios de estructura básica, 138
creación, 128
creación de usuarios iniciales, 58
cuadro de diálogo Selection Manager, 109
eliminación de algunos privilegios, 144
etiquetas de procesos, 98
formación sobre seguridad, 109, 112, 285
impedir bloqueo de cuentas, 144
impedir que se vean los procesos de los demás, 138
impresión, 259
inicio de sesión en modo a prueba de fallos, 141
modificación de valores predeterminados de seguridad, 136
modificación de valores predeterminados de seguridad para todos los usuarios, 137
opción de menú Change Password, 109
opción de menú Change Workspace Label, 109
personalización del entorno, 135
planificación para, 129
precauciones de seguridad, 112
precauciones de supresión, 112
rango de sesión, 98
restablecimiento del control del enfoque del escritorio, 121
uso de dispositivos, 287
uso del archivo `.copy_files`, 138
uso del archivo `.link_files`, 138
usuarios comunes *Ver* usuarios

V

verificación
archivo `label_encodings`, 40
de que la interfaz esté activa, 243
funcionamiento de roles, 61
Vino
uso compartido de escritorios, 154
visualización *Ver* acceso
estado de cada zona, 163
etiquetas de sistemas de archivos en zona con etiquetas, 165
volver a etiquetar información, 145

Z

ZFS
agregación de conjunto de datos a zona con etiquetas, 168
conjuntos de datos de varios niveles, 69, 173
método de creación de zonas rápido, 22
montaje de conjuntos de datos en Trusted Extensions, 173
montaje de lectura y escritura de conjunto de datos en zona con etiquetas, 168
visualización de conjunto de datos montado en sólo lectura desde una zona de nivel superior, 169
zona global
diferencia de las zonas con etiquetas, 157
entrar, 118
salir, 118
zonas
administración, 162
agregación de daemon `nscd` a cada zona con etiquetas, 54
creación de MLP, 235
creación de MLP para NFSv3, 236
creación de secundarias, 68
decisión de método de creación, 22
eliminación del daemon `nscd` de las zonas con etiquetas, 55
en Trusted Extensions, 157
especificación de etiquetas, 45
especificación de nombres, 45
gestión, 157
global, 157
para aislar servicios con etiquetas, 68
permitir inicio de sesión en, 62
primaria, 161
privilegio `net_mac_aware`, 189
procesos de zona global y, 160
secuencia de comandos `txzonemgr`, 44
secundaria, 161
supresión, 74
visualización de estado, 163

visualización de etiquetas de sistemas de archivos, 165
zonas con etiquetas *Ver* zonas