Guía de configuración de Oracle® Solaris Trusted Extensions

Referencia: E22522
Agosto de 2011

ORACLE

111013@25097

Contenido

Lista de figuras

Lista de tablas

Prefacio

La *Guía de configuración de Oracle Solaris Trusted Extensions* proporciona los procedimientos para configurar Trusted Extensions en el sistema operativo Solaris (SO Solaris). En esta guía también se describe la preparación del sistema Solaris para que admita una instalación segura de Trusted Extensions.

Nota – Esta versión de Oracle Solaris es compatible con sistemas que usen arquitecturas de las familias de procesadores SPARC y x86. Los sistemas compatibles aparecen en las Listas de compatibilidad del sistema operativo Oracle Solaris (`http://www.oracle.com/webfolder/technetwork/hcl/index.html`). Este documento indica las diferencias de implementación entre los tipos de plataforma.

En este documento, estos términos relacionados con x86 significan lo siguiente:

- x86 hace referencia a la familia más grande de productos compatibles con x86 de 64 bits.
- x64 hace referencia específicamente a CPU compatibles con x86 de 64 bits.

Para saber cuáles son los sistemas admitidos, consulte las *listas de compatibilidad del sistema operativo Oracle Solaris*.

Usuarios a los que está destinada esta guía

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

Implementación de la seguridad del sitio

Para configurar Trusted Extensions correctamente en un sistema de una manera que sea coherente con la seguridad del sitio, es necesario comprender las funciones de seguridad de Trusted Extensions y la política de seguridad de su sitio. Antes de empezar, lea el Capítulo 1, “Planificación de la seguridad para Trusted Extensions” para obtener información sobre cómo garantizar la seguridad del sitio al configurar el software.

Trusted Extensions y el sistema operativo Solaris

Trusted Extensions se ejecuta en el SO Solaris. Como el software de Trusted Extensions puede modificar el SO Solaris, Trusted Extensions puede necesitar una configuración específica para las opciones de instalación de Solaris. Para obtener detalles, consulte el Capítulo 3, "Adición del software de Trusted Extensions al SO Solaris (tareas)". Además, las guías de Trusted Extensions complementan las guías de Solaris. Como administrador, necesita tener acceso a las guías de Solaris y a las guías de Trusted Extensions.

Organización de este manual

En el Capítulo 1, "Planificación de la seguridad para Trusted Extensions" se describen los problemas de seguridad que debe tener en cuenta al configurar el software de Trusted Extensions en uno o varios sistemas de Solaris.

El Capítulo 2, "Guía básica de configuración de Trusted Extensions" contiene mapas de tareas para agregar el software de Trusted Extensions a los sistemas de Solaris.

El Capítulo 3, "Adición del software de Trusted Extensions al SO Solaris (tareas)" proporciona instrucciones para la preparación de un sistema de Solaris para el software de Trusted Extensions. También incluye instrucciones sobre la habilitación de Trusted Extensions.

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

El Capítulo 5, "Configuración de LDAP para Trusted Extensions (tareas)" proporciona instrucciones sobre la configuración de LDAP para Trusted Extensions.

En el Capítulo 6, "Configuración de Trusted Extensions en un sistema sin periféricos (tareas)" se describe cómo configurar y administrar el software de Trusted Extensions en un sistema sin periféricos.

En el Apéndice A, "Política de seguridad del sitio" se aborda la política de seguridad del sitio y se coloca a Trusted Extensions en el contexto de una seguridad de sitio y organizativa más amplia.

En el Apéndice B, "Uso de acciones de CDE para instalar zonas en Trusted Extensions" se describe cómo configurar zonas con etiquetas con acciones de Trusted CDE.

El Apéndice C, "Lista de comprobación de configuración de Trusted Extensions" proporciona una lista de comprobación de configuración para el equipo de configuración inicial.

En el Glosario se definen los términos y las frases que se utilizan en esta guía.

Cómo se organizan las guías de Trusted Extensions

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

Título de la guía	Temas	Destinatarios
Solaris Trusted Extensions Transition Guide	Obsoleto. Proporciona una descripción general de las diferencias entre el software de Trusted Solaris 8, el software de Solaris 10 y el software de Trusted Extensions. En esta versión, el documento *Novedades* de SO Solaris proporciona una descripción general de los cambios de Trusted Extensions.	Todos
Manual de referencia de Solaris Trusted Extensions	Obsoleto. Proporciona páginas del comando man de Trusted Extensions para las versiones Solaris 10 11/06 y Solaris 10 8/07 de Trusted Extensions. Para esta versión, se incluyen páginas del comando man de Trusted Extensions con las páginas del comando man de Solaris.	Todos
Guía del usuario de Oracle Solaris Trusted Extensions	Describe las funciones básicas de Trusted Extensions. Esta guía contiene un glosario.	Usuarios finales, administradores y desarrolladores
Solaris Trusted Extensions Installation and Configuration for Solaris 10 11/06 and Solaris 10 8/07 Releases	Obsoleto. Describe cómo planificar, instalar y configurar Trusted Extensions para las versiones Solaris 10 11/06 y Solaris 10 8/07 de Trusted Extensions.	Administradores y desarrolladores
Guía de configuración de Oracle Solaris Trusted Extensions	A partir de la versión Solaris 10 5/08, describe cómo habilitar y configurar inicialmente Trusted Extensions. Sustituye *Solaris Trusted Extensions Installation and Configuration*.	Administradores y desarrolladores
Procedimientos de administradores de Oracle Solaris Trusted Extensions	Muestra cómo realizar tareas de administración específicas.	Administradores y desarrolladores
Oracle Solaris Trusted Extensions Developer's Guide	Describe cómo desarrollar aplicaciones con Trusted Extensions.	Desarrolladores y administradores
Oracle Solaris Trusted Extensions Label Administration	Proporciona información sobre cómo especificar componentes de etiquetas en el archivo de codificaciones de etiqueta.	Administradores
Compartmented Mode Workstation Labeling: Encodings Format	Describe la sintaxis utilizada en el archivo de codificaciones de etiqueta. La sintaxis aplica distintas reglas para dar un formato correcto a las etiquetas de un sistema.	Administradores

Guías de instalación relacionadas

Las siguientes guías contienen información que resulta útil en el momento de realizar los preparativos para el software de Trusted Extensions.

Oracle Solaris 10 8/11 Installation Guide: Basic Installations : ofrece indicaciones sobre las opciones de instalación para el SO Solaris

Oracle Solaris 10 8/11 Installation Guide: Custom JumpStart and Advanced Installations: proporciona indicaciones sobre métodos de instalación y opciones de configuración

Oracle Solaris 10 8/11 Installation Guide: Planning for Installation and Upgrade: proporciona indicaciones sobre la instalación de una actualización del SO Solaris

Referencias relacionadas

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

Entorno de escritorio común de Solaris: guía para usuarios avanzados y administradores del sistema: describe Common Desktop Environment (CDE, entorno de escritorio común)

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

Referencias relacionadas con el sitio web de otras empresas

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

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

Documentación, asistencia y formación

Encontrará recursos adicionales en estos sitios web:

- Documentación (`http://www.oracle.com/technetwork/indexes/documentation/index.html`)
- Asistencia (`http://www.oracle.com/us/support/systems/index.html`)
- Formación (`http://www.oracle.com/global/us/education/sun_select_country.html`) - Elija el país para el que desea información de formación para los antiguos productos de Sun.

Recursos de software de Oracle

Oracle Technology Network (`http://www.oracle.com/technetwork/index.html`) ofrece diversos recursos relacionados con el software Oracle:

- Para discutir problemas técnicos y sus soluciones, utilice los foros de discusión (`http://forums.oracle.com`).
- Para practicar procedimientos paso a paso, utilice Oracle By Example (`http://www.oracle.com/technetwork/tutorials/index.html`).
- Puede descargar código de muestra (`http://www.oracle.com/technology/sample_code/index.html`).

Convenciones tipográficas

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

TABLA P–1 Convenciones tipográficas

Tipos de letra	Significado	Ejemplo
`AaBbCc123`	Los nombres de los comandos, los archivos, los directorios y los resultados que el equipo muestra en pantalla.	Edite el archivo `.login`. Utilice el comando `ls -a` para mostrar todos los archivos. `nombre_sistema% tiene correo.`
`AaBbCc123`	Lo que se escribe, en contraposición con la salida del equipo en pantalla	`nombre_sistema%` **`su`** `Contraseña:`
aabbcc123	Marcador de posición: sustituir por un valor o nombre real	El comando necesario para eliminar un archivo es `rm` *nombrearchivo*.

TABLA P–1 Convenciones tipográficas *(Continuación)*

Tipos de letra	Significado	Ejemplo
AaBbCc123	Títulos de los manuales, términos nuevos y palabras destacables	Consulte el capítulo 6 de la *Guía del usuario*. Una *copia en caché* es aquella que se almacena localmente. *No* guarde el archivo. **Nota:** algunos elementos destacados aparecen en negrita en línea.

Indicadores de los shells en los ejemplos de comandos

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

TABLA P–2 Indicadores de shell

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

◆ ◆ ◆ CAPÍTULO 1

1 Planificación de la seguridad para Trusted Extensions

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

Planificación de la seguridad en Trusted Extensions

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

Para obtener una lista de comprobación de las tareas de configuración de Trusted Extensions, consulte el Apéndice C, "Lista de comprobación de configuración de Trusted Extensions". Si está interesado en la localización de su sitio, consulte "Para clientes internacionales de Trusted Extensions" en la página 22. Si está interesado en la ejecución de una configuración evaluada, consulte "Comprensión de la política de seguridad del sitio" en la página 20.

Comprensión de Trusted Extensions

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

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

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

Comprensión de la política de seguridad del sitio

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

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

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

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

- Cambiar la configuración de la conmutación de núcleo en el archivo `/etc/system`.
- Desactivar la auditoría o la asignación de dispositivos.
- Cambiar las entradas predeterminadas en los siguientes archivos configurables:
  - `/usr/openwin/server/etc/*`
  - `/usr/dt/app-defaults/C/Dt`
  - `/usr/dt/app-defaults/C/Dtwm`
  - `/usr/dt/app-defaults/C/SelectionManager`
  - `/usr/dt/bin/Xsession`
  - `/usr/dt/bin/Xtsolsession`
  - `/usr/dt/bin/Xtsolusersession`
  - `/usr/dt/config/sel_config`
  - `/usr/X11/lib/X11/xserver/TrustedExtensionsPolicy`

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

Diseño de una estrategia de administración para Trusted Extensions

El usuario `root` o el rol de administrador del sistema es el responsable de la habilitación de 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.
- El administrador principal es el responsable de crear el perfil de derechos para el administrador de la seguridad, y de solucionar los problemas cuando los administradores de la seguridad y el sistema no tienen privilegios suficientes.
- 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 de Trusted Extensions. También podría modificar uno de los archivos suministrados o crear un nuevo archivo `label_encodings` específico para su sitio. El archivo debe incluir las extensiones locales específicas de Oracle, al menos la sección `COLOR NAMES`.

Precaución – Si proporciona un archivo `label_encodings`, debe tener la versión final del archivo lista antes de que el sistema verifique las etiquetas. El archivo debe estar en un medio extraíble. Las etiquetas se verifican durante el primer inicio, una vez que el servicio de Trusted Extensions está habilitado.

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

Para obtener más información, consulte *Oracle Solaris 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`.

Trusted Extensions admite menos configuraciones regionales que SO Oracle Solaris. Cuando se trabaja en una configuración regional que Trusted Extensions no admite, el texto que es

específico de Trusted Extensions, como los mensajes de error acerca de las etiquetas, no se traduce en su configuración regional. El software Oracle Solaris permanece traducido en su configuración regional.

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 la instalación de una versión de Oracle Solaris, como se describe en "System Requirements and Recommendations" de *Solaris 10 5/09 Installation Guide: Basic Installations*.
- 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 Solaris Management Console, se requiere una interfaz gráfica de usuario administrativa
    - 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

Si desea obtener ayuda para la planificación de hardware de red, consulte el Capítulo 2, "Planning Your TCP/IP Network (Tasks)" de *System Administration Guide: IP Services*.

Como en cualquier red cliente-servidor, debe identificar los hosts por su función, es decir, servidor o cliente, y configurar el software adecuadamente. Para obtener ayuda para la planificación, consulte la *Solaris 10 5/09 Installation Guide: Custom JumpStart and Advanced Installations*.

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

TABLA 1–1 Plantillas de host predeterminadas en Trusted Extensions

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

Si otras redes pueden acceder a la red, debe especificar los hosts y dominios a los que se puede acceder. También debe identificar qué hosts de Trusted Extensions van a servir 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.

La página del comando man `smtnrhtp(1M)` proporciona una descripción completa de cada tipo de host y varios ejemplos.

Planificación de zonas en Trusted Extensions

El software de Trusted Extensions se agrega al SO Oracle Solaris en la zona global. A continuación, debe configurar las zonas no globales con etiquetas. Puede crear una zona con etiquetas para cada etiqueta única, aunque no es necesario crear una zona para cada la etiqueta en el archivo `label_encodings`.

Una parte de la configuración de zona es la configuración de la red. De manera predeterminada, las zonas con etiquetas están configuradas para comunicarse con la zona global. Además, puede configurar las zonas del sistema para que se comuniquen con otras zonas de la red.

- El servidor X en el que se ejecuta la visualización del escritorio sólo está disponible desde la zona global. A partir de la versión Solaris 10 10/08, la interfaz de bucle de retorno, `lo0`, se pueden utilizar para comunicarse con la zona global. Por lo tanto, la visualización del escritorio está disponible para las zonas no globales mediante `lo0`.
- De manera predeterminada, las zonas no globales no se pueden comunicar con hosts que no son de confianza. A partir de la versión Solaris 10 10/08, puede configurar cada zona no global con una ruta predeterminada única que no utilice la zona global.

Zonas de Trusted Extensions y zonas de Oracle Solaris

Las zonas con etiquetas difieren de las zonas típicas de Oracle Solaris. 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. La única manera de acceder a una interfaz interactiva con una zona con etiquetas es mediante la consola de zona. Sólo el usuario root puede acceder a la consola de zona.

Creación de zonas en Trusted Extensions

Para crear una zona con etiquetas es necesario copiar todo el SO Oracle Solaris y, a continuación, iniciar los servicios para el SO Oracle Solaris en cada zona. El proceso puede durar bastante tiempo. Un proceso más rápido es crear una zona y, a continuación, copiar dicha zona o clonar su contenido. En la siguiente tabla se describen las opciones para la creación de zonas en Trusted Extensions.

Método de creación de zona	Esfuerzo necesario	Características de este método
Cree cada zona con etiquetas desde el principio.	Configure, inicialice, instale, personalice e inicie cada zona con etiquetas.	■ Este método se admite y resulta útil para crear una o dos zonas adicionales. Las zonas se pueden actualizar. ■ Este método puede llevar bastante tiempo.
Cree más zonas con etiquetas a partir de una copia de la primera zona con etiquetas.	Configure, inicialice, instale y personalice una zona. Utilice esta zona como plantilla para obtener más las zonas con etiquetas.	■ Este método se admite y es más rápido que crear zonas desde el principio. Las zonas se pueden actualizar. Utilice el método de copia de zona si desea que Oracle Support lo ayude a resolver cualquier dificultad relacionada con la zona. ■ Este método utiliza UFS. UFS no ofrece el aislamiento adicional para las zonas que ofrece Oracle Solaris ZFS.
Cree más zonas con etiquetas a partir de una instantánea de ZFS de la primera zona con etiquetas.	Configure una agrupación ZFS a partir de una partición que dejó a un lado durante la instalación de Oracle Solaris. Configure, inicialice, instale y personalice una zona. Utilice esta zona como una instantánea de ZFS para obtener más las zonas con etiquetas.	■ Este método utiliza Oracle Solaris ZFS y es el método más rápido. Este método convierte a cada zona en un sistema de archivos y, por lo tanto, proporciona más aislamiento que UFS. ZFS utiliza mucho menos espacio en el disco. ■ Si está probando Trusted Extensions y puede volver a instalar las zonas en lugar de actualizarlas, este método puede ser una buena elección. Este método puede ser útil en los sistemas cuyo contenido no es volátil, puesto que el sistema se puede volver a instalar rápidamente con un estado utilizable. ■ Este método *no* se admite. Las zonas que se creen con este método *no se podrán actualizar* cuando surja una versión posterior del sistema operativo.

Las zonas de Oracle Solaris afectan la instalación del paquete y la aplicación de parches. Para obtener más información, consulte las siguientes referencias:

- El Capítulo 25, "About Packages and Patches on a Solaris System With Zones Installed (Overview)" de *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*
- Preguntas frecuentes sobre zonas y contenedores de Solaris (`http://hub.opensolaris.org/bin/view/community+group+zones/faq`)

Planificación de acceso de varios niveles

Normalmente, los servicios de impresión y NFS están configurados como servicios de varios niveles. Para acceder a los servicios de varios niveles, un sistema bien configurado requiere que cada zona pueda acceder a una o varias direcciones de red. Las siguientes configuraciones proporcionan servicios de varios niveles:

- **Pila IP exclusiva**: como en el SO Oracle Solaris, se asigna una dirección IP a cada zona, incluida la zona global. De manera predeterminada, una tarjeta de información de red virtual (VNIC) se crea para cada zona etiquetada.

  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.
- **Pila IP compartida**: se asigna una dirección `all-zones`. En esta configuración, el sistema no puede ser un servidor NFS de varios niveles. Una o varias zonas pueden tener direcciones específicas de la zona.

Un sistema que reúna las dos condiciones siguientes no puede proporcionar servicios de varios niveles:

- Se asigna una dirección IP compartida entre la zona global y las zonas con etiquetas.
- No se asigna ninguna dirección específica de la zona.

Consejo – Si los usuarios de las zonas con etiquetas supuestamente no tienen acceso a una impresora local de varios niveles y usted no necesita exportaciones NFS de los directorios principales, entonces puede asignar una dirección IP a un sistema en el que haya configurado Trusted Extensions. En un sistema de este tipo, no se admite la impresión de varios niveles, y los directorios principales no se pueden compartir. Generalmente esta configuración 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 piensa ejecutar Trusted Extensions en una red de sistemas, utilice LDAP como servicio de nombres. Para Trusted Extensions se requiere un servidor LDAP (Sun Java System Directory Server) 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 de Trusted Extensions. Los procedimientos se describen en el Capítulo 5, "Configuración de LDAP para Trusted Extensions (tareas)".

Planificación de la auditoría en Trusted Extensions

Al instalar Trusted Extensions la auditoría está habilitada de manera predeterminada. Por lo tanto, de manera predeterminada, se audita el inicio de sesión, el bloqueo de pantalla y el cierre de sesión del usuario `root`. Para auditar a los usuarios que están configurando el sistema, puede crear roles en una fase temprana del proceso de configuración. Cuando estos roles configuran el sistema, los registros de auditoría incluyen al usuario de inicio de sesión que asume el rol. Consulte "Creación de roles y usuarios en Trusted Extensions" en la página 90.

La planificación de la auditoría en Trusted Extensions es igual que en el SO Oracle Solaris. Para obtener detalles, consulte la Parte VII, "Oracle Solaris Auditing" de *System Administration Guide: Security Services*. Mientras que Trusted Extensions agrega tokens de clases, eventos y auditoría, el software no cambia el modo en que se administra la auditoría. Para obtener información sobre las adiciones de Trusted Extensions a la auditoría, consulte el Capítulo 18, "Auditoría de Trusted Extensions (descripción general)" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.

Planificación de la seguridad del usuario en Trusted Extensions

El software de Trusted Extensions proporciona valores predeterminados de seguridad razonable para los usuarios. Estos valores predeterminados de seguridad se muestran en la Tabla 1–2. Cuando se muestran dos valores, el primero es el valor predeterminado. El administrador de la seguridad puede modificar estos valores predeterminados para reflejar la política de seguridad del sitio. Una vez que el administrador de la seguridad define los valores predeterminados, el administrador del sistema puede crear todos los usuarios, que heredan los

valores predeterminados establecidos. Para obtener descripciones de las palabras clave y los valores predeterminados, consulte las páginas del comando man `label_encodings(4)` y `policy.conf(4)`.

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

Nombre del archivo	Palabra clave	Valor
`/etc/security/policy.conf`	`IDLECMD`	`lock | logout`
	`IDLETIME`	`30`
	`CRYPT_ALGORITHMS_ALLOW`	`1,2a,md5,5,6`
	`CRYPT_DEFAULT`	`_unix_`
	`LOCK_AFTER_RETRIES`	`no | yes`
	`PRIV_DEFAULT`	`basic`
	`PRIV_LIMIT`	`all`
	`AUTHS_GRANTED`	`solaris.device.cdrw`
	`PROFS_GRANTED`	`Basic Solaris User`
Sección de DEFINICIONES LOCALES 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 en vigencia para ese rol.

El administrador del sistema puede configurar una plantilla de usuario estándar que defina los valores predeterminados del sistema adecuados para cada usuario. Por ejemplo, de manera predeterminada el shell inicial de cada usuario es Bourne. El administrador del sistema puede configurar una plantilla que ofrezca a cada usuario un shell C. Para obtener más información, consulte la ayuda en pantalla de Solaris Management Console para las cuentas de usuario.

Diseño de una estrategia de configuración para Trusted Extensions

Permitir que el usuario `root` configure el software de Trusted Extensions no es una estrategia segura. A continuación se describen las estrategias de configuración, de la estrategia más segura a la menos segura:

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

  Dos personas están en el equipo cuando se habilita el software. En una fase temprana del proceso de configuración, este equipo crea roles y usuarios locales que pueden asumir dichos roles. El equipo también configura la auditoría para auditar los eventos ejecutados por los roles. Una vez que se asignan los roles a los usuarios y se reinicia el equipo, 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.

  Nota – Si la seguridad del sitio requiere la separación de tareas, un administrador de confianza completa la sección "Creación de perfiles de derechos que aplican la separación de tareas" en la página 90 antes de crear usuarios o roles. En esta configuración personalizada, un rol gestiona la seguridad, incluidos los atributos de seguridad de los usuarios. El otro rol gestiona los atributos no relacionados con la seguridad de los sistemas y los usuarios.

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

  En una etapa temprana del proceso de configuración, el usuario `root` crea un usuario local y roles. Este usuario también configura la auditoría para auditar los eventos ejecutados por los roles. Una vez que se asignan los roles al usuario local y se reinicia el equipo, el software aplica la división de tareas por rol. La pista de auditoría proporciona un registro del proceso de configuración.

- Una persona habilita y configura el software asumiendo el rol adecuado. El proceso de configuración no es auditado.

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

- El usuario `root` habilita y configura el software. El proceso de configuración es auditado.

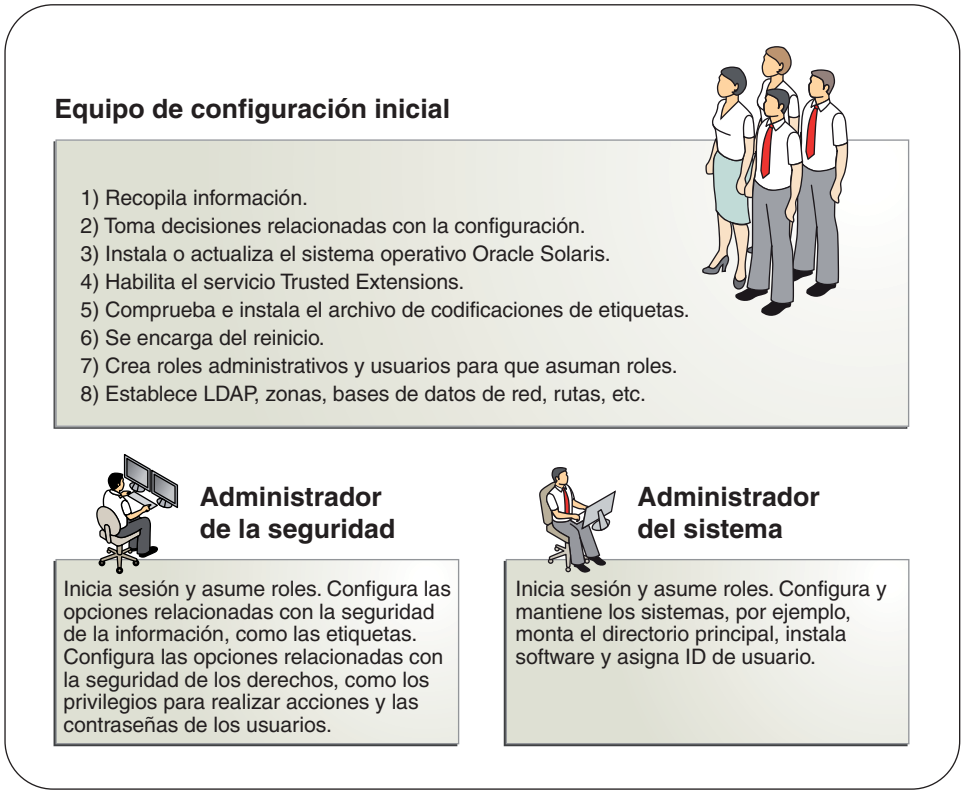
  El equipo configura la auditoría para auditar todos los eventos que realice el usuario `root` durante la configuración. Con esta estrategia, el equipo debe determinar qué eventos se auditarán. La pista de auditoría no incluye el nombre del usuario que está actuando como usuario `root`.

- El usuario `root` habilita y configura el software.

En la figura siguiente se muestra la división de tareas por rol. El administrador de la seguridad configura la auditoría, protege los sistemas de archivos, establece la política de dispositivos,

determina qué programas requieren privilegio para la ejecución y protege a los usuarios, entre otras tareas. El administrador del sistema comparte y monta sistemas de archivos, instala paquetes de software y crea usuarios, entre otras tareas.

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



Resolución de problemas adicionales antes de habilitar Trusted Extensions

Antes de configurar Trusted Extensions, debe proteger físicamente los sistemas, decidir qué etiquetas adjuntará a las zonas y resolver otras cuestiones de seguridad. Para obtener información sobre los procedimientos, consulte "Recopilación de información y toma de decisiones antes de habilitar Trusted Extensions" en la página 43.

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

Si el sistema tiene archivos que se deben guardar, realice una copia de seguridad antes de habilitar el servicio Trusted Extensions. La forma más segura de realizar una copia de seguridad de los archivos es realizar un volcado de nivel 0. Si no tiene un procedimiento de copia de seguridad en el lugar, consulte la guía del administrador de su sistema operativo actual para obtener instrucciones.

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

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

- La auditoría está habilitada.
- Se instala y configura un archivo label_encodings de Oracle.
- Se agregan dos escritorios de confianza. Solaris Trusted Extensions (CDE) es la versión de confianza de CDE. Solaris Trusted Extensions (JDS) es la versión de confianza de Sun Java Desktop System. Cada entorno de ventanas crea espacios de trabajo de Trusted Path en la zona global.
- Como en el SO Oracle Solaris, los perfiles de derechos para los roles están definidos. Como en el SO Oracle Solaris, los roles no están definidos.

  Para utilizar los roles para administrar Trusted Extensions, debe crear los roles. Durante la configuración, debe crear el rol de administrador de la seguridad.
- Se agregan tres bases de datos de red Trusted Extensions, `tnrhdb`, `tnrhtp` y `tnzonecfg`. Las bases de datos se administran mediante la herramienta Security Templates y la herramienta Trusted Network Zones de Solaris Management Console.
- Trusted Extensions proporciona las interfaces gráficas de usuario para administrar el sistema. Algunas interfaces gráficas de usuario son extensiones de una interfaz gráfica de usuario de Oracle Solaris.
  - En Trusted CDE, se proporcionan acciones administrativas en la carpeta Trusted_Extensions. Algunas de estas acciones se utilizan al configurar Trusted Extensions por primera vez. Las herramientas se presentan en el Capítulo 2, “Herramientas de administración de Trusted Extensions” de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.
  - La secuencia de comandos `txzonemgr` permite a los administradores configurar las zonas y las redes de Trusted Extensions. Para obtener más información, consulte la página del comando man `txzonemgr(1M)`.

- Un editor de confianza permite a los administradores modificar los archivos administrativos locales. En Trusted CDE, la acción Admin Editor invoca a un editor de confianza.
- Device Allocation Manager gestiona los dispositivos conectados.
- Solaris Management Console proporciona herramientas basadas en Java para gestionar bases de datos administrativas locales y de red. El uso de estas herramientas es necesario para gestionar la red, las zonas y los usuarios de confianza.

◆ ◆ ◆ CAPÍTULO 2

Guía básica de configuración de Trusted Extensions

En este capítulo se detallan las tareas para habilitar y configurar el software de Trusted Extensions.

Mapa de tareas: preparación de un sistema Solaris para Trusted Extensions

Asegúrese de que el SO Solaris en el que tiene previsto ejecutar Trusted Extensions admita las funciones de Trusted Extensions que piensa utilizar. Complete una de las dos tareas que se describen en el siguiente mapa de tareas.

Tarea	Para obtener instrucciones
Prepare la instalación de un sistema Solaris existente o actualizado para Trusted Extensions.	"Preparación de un sistema Solaris instalado para Trusted Extensions" en la página 41
Instale el SO Solaris teniendo en mente las funciones de Trusted Extensions.	"Instalación de un sistema Solaris para la compatibilidad con Trusted Extensions" en la página 40

Mapa de tareas: preparación para Trusted Extensions y activación del producto

Para preparar un sistema Trusted Extensions antes de configurarlo, complete las tareas que se describen en el siguiente mapa de tareas.

Tarea	Para obtener instrucciones
Complete la preparación del sistema Solaris.	"Mapa de tareas: preparación de un sistema Solaris para Trusted Extensions" en la página 33

Tarea	Para obtener instrucciones
Realice una copia de seguridad del sistema.	Para un sistema Trusted Solaris 8, realice una copia de seguridad del sistema como se describe en la documentación para la versión. Una copia de seguridad con etiquetas se puede restaurar a cada zona con etiquetas de la misma manera.
	Para obtener información sobre un sistema Solaris, consulte la *Guía de administración del sistema: administración básica*.
Reúna información y tome decisiones relacionadas con el sistema y la red de Trusted Extensions.	"Recopilación de información y toma de decisiones antes de habilitar Trusted Extensions" en la página 43
Habilite Trusted Extensions.	"Habilitación de Trusted Extensions" en la página 46
Configure el sistema.	Para un sistema con un monitor, consulte "Mapa de tareas: configuración de Trusted Extensions" en la página 35.
	Para un sistema sin periféricos, consulte "Configuración de un sistema sin periféricos en Trusted Extensions (mapa de tareas)" en la página 135.
	Para Sun Ray, consulte la *Sun Ray Server Software 4.1 Installation and Configuration Guide for the Solaris Operating System*. Para la versión Sun Ray 5, consulte el sitio web de la documentación de Sun Ray Server 4.2 y Sun Ray Connector 2.2 (`http://wikis.sun.com/display/SRS/Home`). Juntos, este servidor y cliente componen el paquete *Sun Ray 5*. Para configurar la comunicación inicial de cliente-servidor, consulte "Configuración de bases de datos de red de confianza (mapa de tareas)" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.
	Para un equipo portátil, vaya a la página web de seguridad de la comunidad de OpenSolaris (`http://hub.opensolaris.org/bin/view/Community+Group+security/`). Haga clic en Trusted Extensions. En la página de Trusted Extensions en la sección Laptop Configurations, haga clic en `Laptop instructions`.
	Para evitar que las redes se comuniquen con la zona global, configure la interfaz `vni0`. Para ver un ejemplo, consulte `Laptop instructions`. A partir de la versión Solaris 10 10/08, no es necesario configurar la interfaz `vni0`. De manera predeterminada, la interfaz `lo0` es una interfaz `all-zones`. Para que dhcp funcione con Trusted Extensions, aún se aplican otras instrucciones de equipos portátiles.

Mapa de tareas: configuración de Trusted Extensions

Para un proceso de configuración seguro, cree roles en una etapa temprana del proceso. Cuando los roles configuran el sistema, el orden de las tareas se muestra en el siguiente mapa de tareas.

1. Configure la zona global.

Tareas	Para obtener instrucciones
Proteja el hardware del equipo mediante la solicitud de una contraseña para cambiar la configuración del hardware.	"Controlling Access to System Hardware" de *System Administration Guide: Security Services*
Configure etiquetas. Las etiquetas se *deben* configurar para el sitio. Si tiene previsto utilizar el archivo `label_encodings` predeterminado, puede omitir esta tarea.	"Revisión e instalación del archivo de codificaciones de etiquetas" en la página 50
Si está ejecutando una red IPv6, puede modificar el archivo `/etc/system` para permitirle a la IP reconocer los paquetes con etiquetas.	"Habilitación de redes IPv6 en Trusted Extensions" en la página 54
Si el dominio de interpretación (DOI) CIPSO de los nodos de la red es distinto de 1, especifique el dominio de interpretación en el archivo `/etc/system`.	"Configuración del dominio de interpretación" en la página 54
Si tiene previsto utilizar una instantánea de ZFS de Solaris para clonar zonas, cree la agrupación ZFS.	"Creación de agrupación ZFS para clonar zonas" en la página 56
Inicie para habilitar un entorno con etiquetas. Al iniciar sesión, se encuentra en la zona global. El archivo `label_encodings` del sistema aplica el control de acceso obligatorio (MAC).	"Reinicie e inicie sesión en Trusted Extensions" en la página 57
Inicialice Solaris Management Console. Esta interfaz gráfica de usuario se utiliza para etiquetar zonas, entre otras tareas.	"Inicialización del servidor de Solaris Management Console en Trusted Extensions" en la página 59
Cree el rol de administrador de la seguridad y otros roles que desee utilizar localmente. Debe crear estos roles tal como lo haría en el SO Solaris. Puede dejar esta tarea para el final. Para ver las consecuencias, consulte "Diseño de una estrategia de configuración para Trusted Extensions" en la página 29.	"Creación de roles y usuarios en Trusted Extensions" en la página 90 "Verificación del funcionamiento de los roles de Trusted Extensions" en la página 99

Si está utilizando archivos locales para administrar el sistema, omita el siguiente conjunto de tareas.

2. Configure un servicio de nombres.

Tareas	Para obtener instrucciones
Si tiene previsto utilizar archivos para administrar Trusted Extensions, puede omitir las siguientes tareas.	Para el servicio de nombres, no se requiere ninguna configuración.
Si tiene un servidor LDAP (Sun Java System Directory Server) existente, agregue bases de datos de Trusted Extensions al servidor. A continuación, convierta el primer sistema Trusted Extensions en un proxy del servidor LDAP. Si no tiene un servidor LDAP, configure el primer sistema como servidor.	Capítulo 5, "Configuración de LDAP para Trusted Extensions (tareas)"
Configure de forma manual una caja de herramientas LDAP para Solaris Management Console. La caja de herramientas se puede utilizar para modificar los atributos de Trusted Extensions en objetos de red.	"Configuración de Solaris Management Console para LDAP (mapa de tareas)" en la página 128
A los sistemas que no son el servidor LDAP o el servidor proxy, conviértalos en clientes LDAP.	"Conversión de la zona global en un cliente LDAP en Trusted Extensions" en la página 62
En el ámbito LDAP, cree el rol de administrador de la seguridad y otros roles que desee utilizar. Puede dejar esta tarea para el final. Para ver las consecuencias, consulte "Diseño de una estrategia de configuración para Trusted Extensions" en la página 29.	"Creación de roles y usuarios en Trusted Extensions" en la página 90 "Verificación del funcionamiento de los roles de Trusted Extensions" en la página 99

3. Cree zonas con etiquetas.

Tareas	Para obtener instrucciones
Ejecute el comando `txzonemgr`. Siga los menús para configurar las interfaces de red y, a continuación, cree y personalice la primera zona con etiquetas. A continuación, copie o clone el resto de las zonas.	"Creación de zonas con etiquetas" en la página 66
O bien, utilice las acciones de Trusted CDE.	Apéndice B, "Uso de acciones de CDE para instalar zonas en Trusted Extensions"
(Opcional) Una vez que se hayan personalizado correctamente todas las zonas, agregue las direcciones de red específicas de la zona y la ruta predeterminada a las zonas con etiquetas.	"Adición de interfaces de red y rutas a zonas con etiquetas" en la página 81

Las siguientes tareas podrían ser necesarias en su entorno.

4. Complete la configuración del sistema.

Tareas	Para obtener instrucciones
Identifique los hosts remotos adicionales que requieren una etiqueta, uno o varios puertos de varios niveles, o una política de mensajes de control diferente.	"Configuración de bases de datos de red de confianza (mapa de tareas)" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*
Cree un servidor de directorio principal de varios niveles y, a continuación, monte automáticamente las zonas instaladas.	"Creación de directorios principales en Trusted Extensions" en la página 101
Configure la auditoría, monte sistemas de archivos y realice otras tareas antes de habilitar a los usuarios para que inicien sesión en el sistema.	*Procedimientos de administradores de Oracle Solaris Trusted Extensions*
Agregue usuarios de un entorno NIS al servidor LDAP.	"Adición de un usuario NIS al servidor LDAP" en la página 104
Agregue un host y sus zonas con etiquetas al servidor LDAP.	"Configuración de bases de datos de red de confianza (mapa de tareas)" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*

◆ ◆ ◆ CAPÍTULO 3

Adición del software de Trusted Extensions al SO Solaris (tareas)

En este capítulo se describe cómo preparar el SO Solaris para el software de Trusted Extensions. En este capítulo también se describe la información que necesita antes de habilitar Trusted Extensions. También se proporcionan instrucciones sobre cómo habilitar Trusted Extensions.

Responsabilidades del equipo de configuración inicial

El software de Trusted Extensions está diseñado para ser habilitado y configurado por dos personas con distintas responsabilidades. Sin embargo, el programa de instalación de Solaris no aplica esta división de tareas entre dos roles. En cambio, la división de tareas se aplica por roles. Como los roles y los usuarios se crean después de la instalación, se considera una buena práctica que un equipo de configuración inicial de al menos dos personas esté presente para habilitar y configurar el software de Trusted Extensions.

Instalación o actualización del SO Solaris para Trusted Extensions

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

- Para obtener una compatibilidad adecuada para Trusted Extensions, debe instalar el SO Solaris subyacente de manera segura. Para las opciones de instalación de Solaris que afectan a Trusted Extensions, consulte "Instalación de un sistema Solaris para la compatibilidad con Trusted Extensions" en la página 40.
- Si ha utilizado el SO Solaris, compare la configuración actual con los requisitos para Trusted Extensions. Para las opciones de configuración que afectan a Trusted Extensions, consulte "Preparación de un sistema Solaris instalado para Trusted Extensions" en la página 41.

▼ Instalación de un sistema Solaris para la compatibilidad con Trusted Extensions

Esta tarea se aplica a las instalaciones realizadas desde cero del SO Solaris. Si va a realizar una actualización, consulte "Preparación de un sistema Solaris instalado para Trusted Extensions" en la página 41.

- **Al instalar el SO Solaris, realice la acción recomendada en las siguientes opciones de instalación.**

  Las opciones siguen el orden de las preguntas de instalación de Solaris. Las preguntas de instalación que no se mencionan en esta tabla no afectan a Trusted Extensions.

Opción de Solaris	Comportamiento de Trusted Extensions	Acción recomendada
Servicio de nombres NIS Servicio de nombres NIS+	Trusted Extensions admite archivos y LDAP para un servicio de nombres. Para la resolución de nombre de host, se puede utilizar DNS.	No elija NIS ni NIS+. Puede no elegir ninguno, lo que equivale a elegir archivos. Más adelante, puede configurar LDAP para que funcione con Trusted Extensions.
Actualizar	Trusted Extensions instala zonas con etiquetas con características de seguridad específicas.	Si va a realizar una actualización, vaya a "Preparación de un sistema Solaris instalado para Trusted Extensions" en la página 41.
Contraseña del usuario `root`	Las herramientas de administración de Trusted Extensions requieren contraseñas. Si el usuario `root` no dispone de una contraseña, el usuario `root` no puede configurar el sistema.	Proporcione una contraseña para el usuario `root`. No cambie el método de cifrado de contraseña `crypt_unix` predeterminado. Para obtener detalles, consulte "Managing Password Information" de *System Administration Guide: Security Services*.

Opción de Solaris	Comportamiento de Trusted Extensions	Acción recomendada
Grupo de desarrolladores	Trusted Extensions utiliza Solaris Management Console para administrar la red. El grupo de usuarios finales y los grupos más pequeños no instalan los paquetes para Solaris Management Console.	En cualquier sistema que desee utilizar para administrar otros sistemas, no instale el grupo de usuarios finales, el grupo de núcleo ni el grupo de redes reducido.
Instalación personalizada	Como Trusted Extensions instala zonas, es posible que necesite más espacio en el disco en las particiones del que proporciona la instalación predeterminada.	Seleccione Instalación personalizada y diseñe las particiones. Considere la posibilidad de agregar espacio de intercambio adicional para los roles. Si tiene pensado clonar zonas, cree una partición de 2000 MB para la agrupación ZFS. Para los archivos de auditoría, es recomendable crear una partición dedicada.

▼ Preparación de un sistema Solaris instalado para Trusted Extensions

Esta tarea se aplica a los sistemas Solaris que se han estado utilizando y en los que tiene previsto ejecutar Trusted Extensions. Además, para ejecutar Trusted Extensions en un sistema Solaris actualizado, siga este procedimiento. Otras tareas que pueden modificar un sistema Solaris instalado se pueden realizar durante la configuración de Trusted Extensions.

Antes de empezar

Trusted Extensions no se puede habilitar en algunos entornos Solaris:

- Si el sistema forma parte de un clúster, Trusted Extensions no se puede habilitar en el sistema.
- No se admite la habilitación de Trusted Extensions en un entorno de inicio alternativo (EI). Trusted Extensions sólo se puede habilitar en el entorno de inicio actual.

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

O bien, puede volver a instalar el SO Solaris. Si va a volver a instalar el SO Solaris, siga las instrucciones de "Instalación de un sistema Solaris para la compatibilidad con Trusted Extensions" en la página 40.

Trusted Extensions utiliza las zonas con marca.

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

Las herramientas de administración de Trusted Extensions requieren contraseñas. Si el usuario `root` no dispone de una contraseña, el usuario `root` no puede configurar el sistema.

Utilice el método de cifrado de contraseña `crypt_unix` predeterminado para el usuario `root`. Para obtener detalles, consulte "Managing Password Information" de *System Administration Guide: Security Services*.

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. El SO Solaris ofrece protección contra contraseñas inseguras, pero no puede evitar que el usuario revele su contraseña o la escriba.

---

3 Si tiene previsto administrar el sitio desde este sistema, agregue los paquetes de Solaris para Solaris Management Console.

Trusted Extensions utiliza Solaris Management Console para administrar la red. Si el sistema se instaló con el grupo de usuarios finales o un grupo más pequeño, el sistema no tiene los paquetes para Solaris Management Console.

4 Si ya ha creado un archivo `xorg.conf`, debe modificarlo.

Agregue la siguiente línea al final de la sección de módulo en el archivo `/etc/X11/xorg.conf`.

```
load "xtsol"
```

Nota – De manera predeterminada, el archivo `xorg.conf` no existe. Si este archivo no existe, no haga nada.

---

5 En las versiones Solaris 10 9/09 y Solaris 10 9/10, si el sistema forma parte de una configuración de Oracle Solaris Cluster, puede habilitar Trusted Extensions en el clúster.

Nota – Las aplicaciones se deben ejecutar sólo en los clústeres de zona de Oracle Solaris Cluster.

Para obtener más información sobre la compatibilidad de Oracle Solaris Cluster con Trusted Extensions, consulte "Cómo prepararse para utilizar Trusted Extensions con clústeres de zona", en el Capítulo 7, y "Creación de zonas no globales y clústeres de zona" en la *Oracle Solaris Cluster Software Installation Guide*.

6 Antes de actualizar un sistema Trusted Extensions, lea lo siguiente:

- Capítulo 1, "Novedades de la versión Solaris 10 10/08," en *Novedades de Solaris 10*
- *Notas de la versión Solaris 10 10/08*

Consejo – Para encontrar información pertinente, busque la cadena `Trusted Extensions`.

---

7 **Si tiene previsto clonar zonas, cree una partición para la agrupación ZFS.**

Para tomar decisiones sobre el método de creación de zona, consulte "Planificación de zonas en Trusted Extensions" en la página 24.

8 **Si tiene previsto instalar zonas con etiquetas en este sistema, compruebe que las particiones tengan suficiente espacio en el disco para las zonas.**

En la mayoría de los sistemas en los que está configurado Trusted Extensions se instalan zonas con etiquetas. Es posible que las zonas con etiquetas requieran más espacio en el disco que el que tiene reservado el sistema instalado.

Sin embargo, algunos sistemas Trusted Extensions no requieren la instalación de zonas con etiquetas. Por ejemplo, un servidor de impresión de varios niveles, un servidor LDAP de varios niveles o un servidor proxy LDAP de varios niveles no requieren la instalación de zonas con etiquetas. Es posible que estos sistemas no requieran espacio adicional en el disco.

9 **(Opcional) Agregue espacio de intercambio adicional para los roles.**

Los roles administran Trusted Extensions. Considere la adición de espacio de intercambio para los procesos de los roles.

10 **(Opcional) Dedique una partición a archivos de auditoría.**

Trusted Extensions habilita la auditoría de manera predeterminada. Para los archivos de auditoría, es recomendable crear una partición dedicada.

11 **(Opcional) Para ejecutar una configuración protegida, ejecute el comando `netservices limited` antes de habilitar Trusted Extensions.**

```
# netservices limited
```

Recopilación de información y toma de decisiones antes de habilitar Trusted Extensions

Para cada sistema en el que se va a configurar Trusted Extensions, debe conocer cierta información y tomar algunas decisiones relacionadas con la configuración. Por ejemplo, como va a crear zonas con etiquetas, es posible que desee reservar espacio en el disco donde se puedan clonar las zonas como un sistema de archivos Solaris ZFS. Solaris ZFS proporciona aislamiento adicional para las zonas.

▼ Recopilación de información del sistema antes de habilitar Trusted Extensions

1 **Determine la dirección IP y el nombre de host principal del sistema.**

El nombre de host es el nombre del host de la red y es la zona global. En un sistema Solaris, el comando `getent` devuelve el nombre de host, como en el siguiente ejemplo:

```
# getent hosts machine1
192.168.0.11   machine1
```

2 **Determine las asignaciones de dirección IP para las zonas con etiquetas.**

Un sistema con dos direcciones IP puede funcionar como un servidor de varios niveles. Un sistema con una dirección IP debe tener acceso a un servidor de varios niveles para poder imprimir o realizar tareas de varios niveles. Para obtener una explicación de las opciones de dirección IP, consulte "Planificación de acceso de varios niveles" en la página 26.

La mayoría de los sistemas requieren una segunda dirección IP para las zonas con etiquetas. Por ejemplo, el siguiente es un host con una segunda dirección IP para zonas con etiquetas:

```
# getent hosts machine1-zones
192.168.0.12   machine1-zones
```

3 **Recopile la información de la configuración de LDAP.**

Para el servidor LDAP que está ejecutando el software de Trusted Extensions se necesita la siguiente información:

- El nombre del dominio de Trusted Extensions al que presta servicio el servidor LDAP
- La dirección IP del servidor LDAP
- El nombre del perfil LDAP que se cargará

Para un servidor proxy LDAP, también necesita la contraseña para el proxy LDAP.

▼ Toma de decisiones relacionadas con el sistema y la seguridad antes de habilitar Trusted Extensions

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

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

En un sitio seguro, este paso se realiza para cada sistema Solaris instalado.

- Para los sistemas basados en SPARC, se ha proporcionado una contraseña y un nivel de seguridad PROM.
- Para los sistemas x86, el BIOS está protegido.

- En todos los sistemas, el usuario `root` está protegido 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 Sun. Sun también suministra otros archivos `label_encodings`, que puede encontrar en el directorio `/etc/security/tsol`. Los archivos de Sun son archivos de demostración. Es posible que no sean adecuados para los sistemas de producción.

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

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

En la siguiente tabla se muestran los nombres de etiqueta y los nombres de zona sugeridos para el archivo `label_encodings` predeterminado.

Etiqueta	Nombre de zona
`PUBLIC`	`public`
`CONFIDENTIAL : INTERNAL`	`internal`
`CONFIDENTIAL : NEED TO KNOW`	`needtoknow`
`CONFIDENTIAL : RESTRICTED`	`restricted`

Para facilitar el montaje de NFS, el nombre de zona de una etiqueta determinada debe ser idéntico en todos los sistemas. En algunos sistemas, como los servidores de impresión de varios niveles, no es necesario instalar zonas con etiquetas. No obstante, si instala zonas con etiquetas en un servidor de impresión, los nombres de zona deben ser idénticos a los nombres de zona que figuran en los demás sistemas de la red.

4 Decida cuándo crear roles.

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

Si no es necesario que configure el sistema mediante el uso de roles, puede configurar el sistema como superusuario. Este método de configuración es menos seguro. Los registros de auditoría no indican qué usuario fue superusuario durante la configuración. El superusuario puede realizar todas las tareas en el sistema, mientras que un rol puede realizar un conjunto de tareas más limitado. Por lo tanto, la configuración es más controlada cuando es realizada por roles.

5 **Seleccione un método de creación de zona.**

Puede crear zonas desde el principio, copiar zonas o clonar zonas. Estos métodos difieren en la velocidad de creación, los requisitos de espacio en el disco y la solidez. Para las compensaciones, consulte "Planificación de zonas en Trusted Extensions" en la página 24.

6 **Planifique la configuración de LDAP.**

Utilizar archivos locales para la administración es práctico para los sistemas no conectados en red.

LDAP es el servicio de nombres para un entorno de red. Un servidor LDAP relleno es necesario al configurar varios equipos.

- Si tiene un servidor LDAP (Sun Java System Directory Server) existente, puede crear un servidor proxy LDAP en un sistema que esté ejecutando Trusted Extensions. El servidor proxy de varios niveles maneja las comunicaciones con el servidor LDAP sin etiquetas.
- Si no tiene un servidor LDAP, puede configurar un sistema que ejecute el software de Trusted Extensions como servidor LDAP de varios niveles.

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

Por ejemplo, quizás desee tener en cuenta los siguientes problemas de seguridad:

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

Habilitación del servicio de Trusted Extensions

A partir de la versión Solaris 10 5/08, Trusted Extensions es un servicio gestionado por la utilidad de gestión de servicios (SMF, Service Management Facility). El nombre del servicio es `svc:/system/labeld:default`. De manera predeterminada, el servicio `labeld` está inhabilitado.

▼ Habilitación de Trusted Extensions

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

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

- Todas las comunicaciones de red

Antes de empezar

Debe haber completado las tareas de "Instalación o actualización del SO Solaris para Trusted Extensions" en la página 40 y "Recopilación de información y toma de decisiones antes de habilitar Trusted Extensions" en la página 43.

1 En un sistema Solaris, habilite el servicio `labeld`.

```
# svcadm enable -s svc:/system/labeld:default
```

El servicio `labeld` agrega etiquetas al sistema e inicia la asignación de dispositivos y el servicio de auditoría de Solaris. No realice ninguna otra tarea hasta que el cursor haya vuelto a la pregunta.

2 Compruebe que el servicio esté habilitado.

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

Nota – Las etiquetas aparecerán una vez que haya reiniciado el sistema. La sección "Configuración de la zona global en Trusted Extensions" en la página 49 incluye las tareas que quizás desee llevar a cabo antes de reiniciar.

Errores más frecuentes

El siguiente mensaje indica que no está ejecutando una versión de Solaris que admite Trusted Extensions como un servicio: `svcs: Pattern 'labeld' doesn't match any instances`.

Para ejecutar Trusted Extensions en un sistema Solaris que no admite el servicio `labeld`, siga las instrucciones de la guía *Solaris Trusted Extensions Installation and Configuration*.

◆ ◆ ◆ CAPÍTULO 4

Configuración de Trusted Extensions (tareas)

En este capítulo se explica cómo configurar Trusted Extensions en un sistema con un supervisor. Para que el software de Trusted Extensions funcione correctamente es necesario configurar los elementos siguientes: etiquetas, zonas, red, usuarios que puedan asumir roles, roles y herramientas.

- "Configuración de la zona global en Trusted Extensions" en la página 49
- "Creación de zonas con etiquetas" en la página 66
- (Opcional) "Adición de interfaces de red y rutas a zonas con etiquetas" en la página 81
- "Creación de roles y usuarios en Trusted Extensions" en la página 90
- "Creación de directorios principales en Trusted Extensions" en la página 101
- "Adición de usuarios y hosts a una red de confianza existente" en la página 104
- "Resolución de los problemas de configuración de Trusted Extensions" en la página 106
- "Tareas adicionales de configuración de Trusted Extensions" en la página 110

Para otras tareas de configuración, consulte *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.

Configuración de la zona global en Trusted Extensions

Antes de configurar la zona global, se deben tomar decisiones sobre la configuración. Para obtener información sobre las decisiones, consulte "Recopilación de información y toma de decisiones antes de habilitar Trusted Extensions" en la página 43.

Tarea	Descripción	Para obtener instrucciones
Proteja el hardware.	El hardware se puede proteger mediante solicitud de una contraseña para cambiar la configuración del hardware.	"Controlling Access to System Hardware" de *System Administration Guide: Security Services*
Configure etiquetas.	Las etiquetas se *deben* configurar para el sitio. Si tiene previsto utilizar el archivo `label_encodings` predeterminado, puede omitir este paso.	"Revisión e instalación del archivo de codificaciones de etiquetas" en la página 50

Tarea	Descripción	Para obtener instrucciones
Para IPv6, modifique el archivo `/etc/system`.	Si está ejecutando una red IPv6, puede modificar el archivo `/etc/system` para permitirle a la IP reconocer los paquetes con etiquetas.	"Habilitación de redes IPv6 en Trusted Extensions" en la página 54
Para un dominio de interpretación cuyo valor no sea `1`, modifique el archivo `/etc/system`.	Si el dominio de interpretación CIPSO de los nodos de la red es distinto de `1`, especifique el dominio de interpretación en el archivo `/etc/system`.	"Configuración del dominio de interpretación" en la página 54
Cree espacio para una instantánea de ZFS de Solaris.	Si tiene previsto utilizar una instantánea de ZFS de Solaris para clonar zonas, cree la agrupación ZFS. Realice esta tarea si va a clonar la primera zona para crear el resto de las zonas con etiquetas.	"Creación de agrupación ZFS para clonar zonas" en la página 56
Reinicie e inicie sesión.	Al iniciar sesión, se encuentra en la zona global, que es un entorno que reconoce y aplica el control de acceso obligatorio (MAC).	"Reinicie e inicie sesión en Trusted Extensions" en la página 57
Inicialice Solaris Management Console.	Trusted Extensions agrega herramientas a Solaris Management Console para la administración de los usuarios, los roles, las zonas y la red.	"Inicialización del servidor de Solaris Management Console en Trusted Extensions" en la página 59
Configure LDAP.	Si está utilizando el servicio de nombres LDAP, configure el servicio LDAP.	Capítulo 5, "Configuración de LDAP para Trusted Extensions (tareas)"
	Si configuró el servicio LDAP, convierta este sistema en un cliente LDAP.	"Conversión de la zona global en un cliente LDAP en Trusted Extensions" en la página 62

▼ Revisión e instalación del 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 *Oracle Solaris Trusted Extensions Label Administration* para ver los requisitos, los procedimientos y los ejemplos.

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

Antes de empezar

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

1. **Inserte los medios con el archivo `label_encodings` en el dispositivo adecuado.**
2. **Copie el archivo `label_encodings` en el disco.**
3. **Compruebe la sintaxis del archivo y conviértalo en el archivo `label_encodings` activo.**

   - **En Trusted JDS, compruebe e instale el archivo desde la línea de comandos.**

     a. **Abra una ventana de terminal.**

     b. **Ejecute el comando `chk_encodings`.**

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

     c. **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, "Making a Label Encodings File (Tasks)" de *Oracle Solaris Trusted Extensions Label Administration*

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

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

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

   - **En Trusted CDE, utilice la acción Check Encodings.**

     a. **Abra la carpeta Trusted_Extensions.**

        Haga clic con el tercer botón del mouse en el fondo.

b. Desde el menú Workspace, seleccione Applications → Application Manager.

c. Haga doble clic en el icono de la carpeta Trusted_Extensions.

d. Haga doble clic en la acción Check Encodings.

En el cuadro de diálogo, escriba el nombre de la ruta completa del archivo:

/full-pathname-of-label-encodings-file

Se invoca el comando `chk_encodings` para comprobar la sintaxis del archivo. Los resultados se muestran en el cuadro de diálogo Check Encodings.

e. Lea el contenido de este cuadro de diálogo y realice una de las siguientes acciones:

- **Corrija los errores.**

  Si la acción Check Encodings informa errores, éstos se *deben* corregir antes de continuar. Para obtener ayuda, consulte el Capítulo 3, "Making a Label Encodings File (Tasks)" de *Oracle Solaris Trusted Extensions Label Administration*.

- **Haga clic en `Yes` para convertir el archivo en el archivo `label_encodings` activo.**

  La acción Check Encodings crea una copia de seguridad del archivo original y, a continuación, instala la versión comprobada en `/etc/security/tsol/label_encodings`. La acción, luego, reinicia el daemon de etiqueta.

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

4 Compruebe la sintaxis del archivo y conviértalo en el archivo `label_encodings` activo.

Use la línea de comandos.

a. Abra una ventana de terminal.

b. Ejecute el comando `chk_encodings`.

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

c. 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, "Making a Label Encodings File (Tasks)" de *Oracle Solaris Trusted Extensions Label Administration*

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

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

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

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

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

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

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

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

---> VERSION = MYCOMPANY LABEL ENCODINGS  2.0 10/10/2006

---> CLASSIFICATIONS <---

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

---> COMPARTMENTS AND MARKINGS USAGE ANALYSIS <---
...
---> SENSITIVITY LABEL to COLOR MAPPING <---
...
```

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

```
# cp /var/encodings/label_encodings2 /etc/security/tsol/label.encodings.10.10.06
# cd /etc/security/tsol
# cp label_encodings label_encodings.tx.orig
# cp label.encodings.10.10.06 label_encodings
```

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

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

```
---> VERSION = MYCOMPANY LABEL ENCODINGS  2.0 10/10/2006
```

▼ Habilitación de redes IPv6 en Trusted Extensions

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

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

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

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

Errores más frecuentes

- Si los mensajes de error durante el inicio indican que la configuración de IPv6 es incorrecta, corrija la entrada:
  - Compruebe que la entrada esté escrita correctamente.
  - Compruebe que el sistema se haya reiniciado después de haber agregado la entrada correcta al archivo `/etc/system`.
- Si instala Trusted Extensions en un sistema Solaris que actualmente tiene IPv6 habilitado, pero no agrega la entrada de IP en `/etc/system`, verá el siguiente mensaje de error: `t_optmgmt: System error: Cannot assign requested address` *indicación de hora*
- Si instala Trusted Extensions en un sistema Solaris que no tiene IPv6 habilitado, y no agrega la entrada de IP en `/etc/system`, verá los siguientes tipos de mensajes de error:
  - `WARNING: IPv6 not enabled via /etc/system`
  - `Failed to configure IPv6 interface(s): hme0`
  - `rpcbind: Unable to join IPv6 multicast group for rpc broadcast` *número de difusión*

▼ Configuración del dominio de interpretación

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

Si su dominio de interpretación no es 1, debe agregar una entrada en el archivo `/etc/system` y modificar el valor `doi` en las plantillas de seguridad predeterminadas.

1. **Escriba la entrada de dominio de interpretación en el archivo `/etc/system`:**

   ```
   set default_doi = n
   ```

   Este número positivo distinto de cero debe coincidir con el número de dominio de interpretación de la base de datos `tnrhtp` para el nodo y los sistemas con los que se comunica el nodo.

2. **Antes de agregar la base de datos `tnrhtp` al servidor LDAP, modifique el valor `doi` en las entradas predeterminadas y en todas las entradas para las direcciones locales.**

   Trusted Extensions proporciona dos plantillas en la base de datos `tnrhtp`, `cipso` y `admin_low`. Si agregó entradas para las direcciones locales, también modifique estas entradas.

   a. **Abra la base de datos `tnrhtp` en el editor de confianza.**

      ```
      # /usr/dt/bin/trusted_edit /etc/security/tsol/tnrhtp
      ```

      En Solaris Trusted Extensions (CDE), puede utilizar la acción Admin Editor en la carpeta Trusted_Extensions, en el gestor de aplicaciones.

   b. **Copie la entrada de la plantilla `cipso` en otra línea.**

      ```
      cipso:host_type=cipso;doi=1;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
      cipso:host_type=cipso;doi=1;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
      ```

   c. **Comente una de las entradas de `cipso`.**

      ```
      #cipso:host_type=cipso;doi=1;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
      cipso:host_type=cipso;doi=1;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
      ```

   d. **Modifique el valor `doi` en la entrada sin comentarios de `cipso` .**

      Este valor debe ser igual al valor `default_doi` del archivo `/etc/system`.

      ```
      #cipso:host_type=cipso;doi=1;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
      cipso:host_type=cipso;doi=n;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
      ```

   e. **Cambie el valor `doi` para la entrada `admin_low`.**

```
#admin_low:host_type=unlabeled;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH;doi=1;def_label=ADMIN_LOW
admin_low:host_type=unlabeled;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH;doi=n;def_label=ADMIN_LOW
```

   Una vez que todos los valores `doi` de todas las entradas de la base de datos `tnrhtp` sean iguales, habrá terminado.

Errores más frecuentes

Si el archivo `/etc/system` establece un valor`default_doi` distinto de `1` y una plantilla de seguridad para este sistema define un valor que no coincide con este valor `default_doi`, aparecerán mensajes similares a los siguientes en la consola del sistema durante la configuración de la interfaz:

- `NOTICE: er10 failed: 10.17.1.12 has wrong DOI 4 instead of 1`
- `Failed to configure IPv4 interface(s): er10`

Un error en la configuración de la interfaz puede dar como resultado un error en el inicio de sesión:

- `Hostname: unknown`
- `unknown console login: root`
- `Oct 10 10:10:20 unknown login: pam_unix_cred: cannot load hostname Error 0`

Para corregir el problema, inicie el sistema en modo de usuario único y corrija las plantillas de seguridad como se describe en este procedimiento.

Véase también

Para obtener información sobre el dominio de interpretación, consulte "Atributos de seguridad de red en Trusted Extensions" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.

Para cambiar el valor `doi` en las plantillas de seguridad que cree, consulte "Cómo crear una plantilla de host remoto" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.

Para utilizar el editor que prefiere como editor de confianza, consulte "Cómo asignar el editor de su elección como editor de confianza" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.

▼ Creación de agrupación ZFS para clonar zonas

Si tiene previsto utilizar una instantánea de ZFS de Solaris como la plantilla de zona, debe crear una agrupación ZFS a partir de un archivo ZFS o un dispositivo ZFS. Esta agrupación contiene la instantánea para clonar cada zona. Puede utilizar el dispositivo `/zone` para la agrupación ZFS.

Antes de empezar

Debe haber reservado espacio en el disco durante la instalación de Solaris para un sistema de archivos ZFS. Para obtener detalles, consulte "Planificación de zonas en Trusted Extensions" en la página 24.

1 Desmonte la partición `/zone`.

Durante la instalación, usted creó una partición `/zone` con suficiente espacio en el disco de aproximadamente 2.000 MBytes.

```
# umount /zone
```

2. **Elimine el punto de montaje `/zone`.**

   ```
   # rmdir /zone
   ```

3. **Comente la entrada `/zone` en el archivo `vfstab`.**

   a. **Evite que la entrada `/zone` sea leída.**

      Abra el archivo `vfstab` en un editor. Agregue un signo de comentario delante de la entrada `/zone`.

      ```
      #/dev/dsk/cntndnsn  /dev/dsk/cntndnsn  /zone  ufs  2  yes  -
      ```

   b. **Copie el segmento de disco, `cn tndn sn`, en el portapapeles.**

   c. **Guarde el archivo y cierre el editor.**

4. **Utilice el segmento de disco para volver a crear `/zone` como una agrupación ZFS.**

   ```
   # zpool create -f zone cntndnsn
   ```

   Por ejemplo, si la entrada `/zone` utiliza el segmento de disco `c0t0d0s5`, el comando es el siguiente:

   ```
   # zpool create -f zone c0t0d0s5
   ```

5. **Verifique que la agrupación ZFS se encuentre en buen estado.**

   Utilice uno de los siguientes comandos:

   ```
   # zpool status -x zone
   pool 'zone' is healthy

   # zpool list
   NAME     SIZE     USED   AVAIL   CAP   HEALTH   ALTROOT
   /zone    5.84G    80K    5.84G    7%   ONLINE   -
   ```

   En este ejemplo, el equipo de configuración inicial reservó una partición de 6.000 MB para las zonas. Para obtener más información, consulte la página del comando man `zpool(1M)`.

▼ Reinicie e inicie sesión en Trusted Extensions

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

Antes de empezar

Antes de iniciar sesión por primera vez, familiarícese con las opciones de etiqueta y el escritorio de Trusted Extensions. Para obtener detalles, consulte el Capítulo 2, "Inicio de sesión en Trusted Extensions (tareas)" de *Guía del usuario de Oracle Solaris Trusted Extensions*.

1. **Reinicie el sistema.**

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

Si el sistema no tiene una visualización gráfica, vaya al Capítulo 6, “Configuración de Trusted Extensions en un sistema sin periféricos (tareas)”.

2 Inicie sesión como superusuario en el escritorio de Solaris Trusted Extensions (CDE) o Solaris Trusted Extensions (JDS).

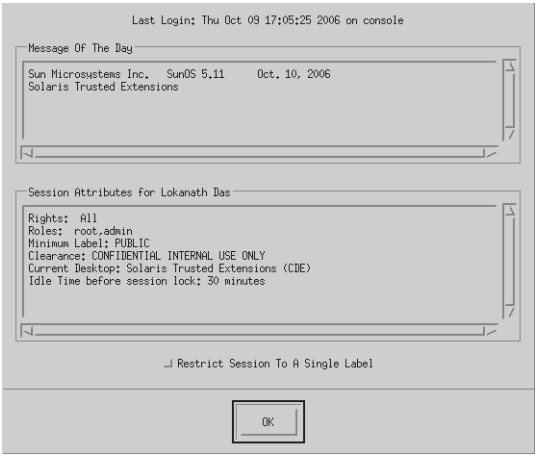
a. En la ventana de inicio de sesión, seleccione uno de los escritorios de confianza.

El escritorio de Trusted CDE contiene acciones que son útiles para la configuración del sistema. A partir de la versión Solaris 10 10/08, la secuencia de comandos `txzonemgr` es el programa preferido para la configuración del sistema.

b. En el cuadro de diálogo de inicio de sesión, escriba el usuario `root` y la contraseña de usuario root.

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

3 Lea la información en el cuadro de diálogo Last Login.



A continuación, haga clic en OK para cerrar el cuadro.

4 Lea el generador de etiquetas.

Haga clic en OK para aceptar la etiqueta predeterminada.

Una vez que se haya completado el proceso de inicio de sesión, aparecerá brevemente la pantalla Trusted Extensions y se abrirá una sesión de escritorio con cuatro espacios de trabajo. El símbolo `Trusted Path` se muestra en la banda de confianza.

Nota – Antes de alejarse del sistema, debe cerrar 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.

▼ Inicialización del servidor de Solaris Management Console en Trusted Extensions

Este procedimiento le permite administrar los usuarios, los roles, los hosts, las zonas y la red en este sistema. En el primer sistema que configure, sólo estará disponible el ámbito `files`.

Antes de empezar

Debe ser superusuario.

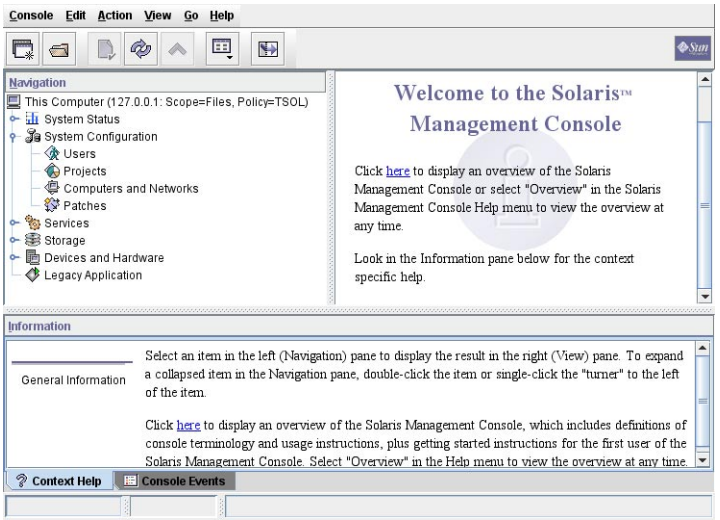
Para utilizar la caja de herramientas LDAP en el servidor LDAP desde una consola Solaris Management Console que se está ejecutando en un cliente, debe completar todas las tareas de "Configuración de Solaris Management Console para LDAP (mapa de tareas)" en la página 128.

1 Inicie Solaris Management Console.

```
# /usr/sbin/smc &
```

Nota – La primera vez que se inicia, Solaris Management Console realiza varias tareas de registro. Estas tareas pueden tardar unos minutos.

FIGURA 4–1 Ventana inicial de Solaris Management Console



2 Si los iconos de la caja de herramientas no aparecen en Solaris Management Console, realice una de las siguientes acciones:

- **Si el panel Navigation no se puede ver:**

  a. En el cuadro de diálogo Open Toolbox que aparece, haga clic en la opción Load ubicada junto al nombre de este sistema, debajo de Server.

  Si este sistema no dispone de la cantidad de memoria y de espacio de intercambio recomendada, es posible que la caja de herramientas tarde unos minutos en aparecer. Para ver las recomendaciones, consulte "Instalación o actualización del SO Solaris para Trusted Extensions" en la página 40.

  b. De la lista de cajas de herramientas, seleccione una caja de herramientas con `Policy=TSOL`.

  En la Figura 4–2 se muestra una caja de herramientas This Computer (*este host*: `Scope=Files, Policy=TSOL`). Trusted Extensions modifica las herramientas del nodo de configuración del sistema.

Precaución – No seleccione una caja de herramientas que no tenga ninguna política. La cajas de herramientas sin una política no admiten Trusted Extensions.

La elección de la caja de herramientas depende de qué ámbito desea influenciar.

- Para editar archivos locales, seleccione el ámbito Files.
- Para editar bases de datos LDAP, seleccione el ámbito LDAP.

Una vez que haya completado todas de las tareas de "Configuración de Solaris Management Console para LDAP (mapa de tareas)" en la página 128, el ámbito LDAP estará disponible.

c. Haga clic en Open.

- **Si el panel Navigation se puede ver, pero los iconos de la caja de herramientas son señales de detención:**

  a. Salga de Solaris Management Console.

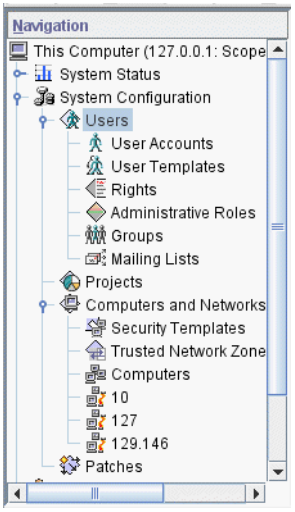
  b. Reinicie Solaris Management Console.

  ```
  # /usr/sbin/smc &
  ```

3 Si aún no lo ha hecho, seleccione una caja de herramientas con `Policy=TSOL`.

En la siguiente figura se muestra una caja de herramientas This Computer (*este host*: `Scope=Files, Policy=TSOL`). Trusted Extensions modifica las herramientas del nodo de configuración del sistema.

FIGURA 4–2 Herramientas de Trusted Extensions en Solaris Management Console



4 **(Opcional) Guarde la caja de herramientas actual.**

Al guardar una caja de herramientas `Policy=TSOL`, permite que una caja de herramientas de Trusted Extensions se cargue de manera predeterminada. Las preferencias se guardan por rol, por host. El host es el servidor de Solaris Management Console.

a. **En el menú Console, elija Preferences.**

La caja de herramientas de inicio está seleccionada.

b. **Defina una caja de herramientas con `Policy=TSOL` como la caja de herramientas de inicio.**

Coloque la caja de herramientas actual en el campo Location haciendo clic en el botón Use Current Toolbox.

c. **Haga clic en OK para guardar las preferencias.**

5 **Salga de Solaris Management Console.**

Véase también Para obtener una descripción general de las adiciones de Trusted Extensions a Solaris Management Console, consulte "Herramientas de Solaris Management Console" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*. Para utilizar Solaris Management Console para crear plantillas de seguridad, consulte "Configuración de bases de datos de red de confianza (mapa de tareas)" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.

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

Para LDAP, este procedimiento establece la configuración del servicio de nombres para la zona global. Si no está utilizando LDAP, puede omitir este procedimiento.

A partir de la versión Solaris 10 5/08, si está en un espacio de trabajo de Solaris Trusted Extensions (CDE), puede usar la secuencia de comandos `txzonemgr` o una acción de Trusted CDE para crear un cliente LDAP. Si está en un espacio de trabajo de Solaris Trusted Extensions (JDS) o Solaris Trusted Extensions (GNOME), debe utilizar 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 Sun Java System Directory Server, es decir, el servidor LDAP, debe existir. El servidor se debe rellenar con las bases de datos de Trusted Extensions y este sistema se debe poder contactar con

el servidor. Por lo tanto, el sistema que se está configurando debe tener una entrada en la base de datos `tnrhdb` del servidor LDAP o debe estar incluido en una entrada de comodín antes de realizar este procedimiento.

Si un servidor LDAP en el que está configurado Trusted Extensions no existe, debe completar los procedimientos del Capítulo 5, "Configuración de LDAP para Trusted Extensions (tareas)", antes de realizar este procedimiento.

1 Si está utilizando DNS, modifique el archivo `nsswitch.ldap`.

a. Guarde una copia del archivo `nsswitch.ldap` original.

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

```
# cd /etc
# cp nsswitch.ldap nsswitch.ldap.orig
```

b. Cambie las entradas del archivo `nsswitch.ldap` para los siguientes servicios.

Las entradas correctas son similares a las siguientes:

```
hosts:    files dns ldap

ipnodes:    files dns ldap

networks:   ldap files
protocols:  ldap files
rpc:        ldap files
ethers:     ldap files
netmasks:   ldap files
bootparams: ldap files
publickey:  ldap files

services:   files
```

Tenga en cuenta que Trusted Extensions añade dos entradas:

```
tnrhtp:    files ldap
tnrhdb:    files ldap
```

c. Copie el archivo `nsswitch.ldap` modificado en `nsswitch.conf`.

```
# cp nsswitch.ldap nsswitch.conf
```

2 Realice uno de los siguientes pasos para crear un cliente LDAP.

- **Ejecute la secuencia de comandos `txzonemgr` y responda a las peticiones de datos sobre LDAP.**

  La opción de menú Create LDAP Client sólo permite configurar la zona global.

  a. **Siga las instrucciones de "Ejecución de la secuencia de comandos `txzonemgr`" en la página 67.**

     El título del cuadro de diálogo es Labeled Zone Manager.

  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` agrega el cliente LDAP. A continuación, aparece una ventana con el resultado del comando.

- **En un espacio de trabajo de Trusted CDE, busque y utilice la acción Create LDAP Client.**

  a. **Navegue hasta la carpeta Trusted_Extensions haciendo clic con el tercer botón del mouse en el fondo.**

  b. **Desde el menú Workspace, seleccione Applications → Application Manager.**

  c. **Haga doble clic en el icono de la carpeta Trusted_Extensions.**

     Esta carpeta contiene acciones que configuran interfaces, clientes LDAP y zonas con etiquetas.

  d. **Haga doble clic en la acción Create LDAP Client.**

     Responda a las siguientes las peticiones de datos:

     ```
     Domain Name:                    Type the domain name
     Hostname of LDAP Server:        Type the name of the server
     IP Address of LDAP Server:      Type the IP address
     LDAP Proxy Password:            Type the password to the server
     ```

```
Profile Name:                   Type the profile name
```

e. Haga clic en OK.

Aparece el siguiente mensaje de finalización:

```
global zone will be LDAP client of LDAP-server
System successfully configured.

*** Select Close or Exit from the window menu to close this window ***
```

f. Cierre la ventana de la acción.

3 En una ventana de terminal, establezca el parámetro `enableShadowUpdate` en `TRUE`.

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

La acción Create LDAP Client y la secuencia de comandos `txzonemgr` ejecutan sólo el comando `ldapclient init`. En Trusted Extensions, también debe modificar un cliente LDAP inicializado para habilitar actualizaciones de shadow.

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, cree el cliente LDAP de nuevo y proporcione los valores correctos. 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.

Ejemplo 4–2 Uso de nombres de host después de cargar un archivo `resolv.conf`

En este ejemplo, el administrador quiere que un conjunto determinado de servidores DNS esté disponible para el sistema. El administrador copia un archivo `resolv.conf` de un servidor en una red de confianza. Como DNS aún no está activo, el administrador utiliza la dirección IP del servidor para localizar el servidor.

```
# cd /etc
# cp /net/10.1.1.2/export/txsetup/resolv.conf resolv.conf
```

Una vez que el archivo `resolv.conf` se copia y el archivo `nsswitch.conf` incluye `dns` en la entrada de `hosts`, el administrador puede utilizar nombres de host para localizar sistemas.

Creación de zonas con etiquetas

La secuencia de comandos `txzonemgr` lo guía a lo largo de todas las siguientes tareas para configurar las zonas con etiquetas.

Precaución – Para utilizar los procedimientos de `txzonemgr`, debe estar ejecutando la versión Solaris 10 8/07 de Trusted Extensions, o una versión posterior. O bien, debe instalar todos los parches para la versión Solaris 10 11/06.

Si está ejecutando la versión Solaris 10 11/06 sin los parches actuales, utilice los procedimientos de Apéndice B, "Uso de acciones de CDE para instalar zonas en Trusted Extensions" para configurar las zonas con etiquetas.

Las instrucciones de esta sección permiten configurar zonas con etiquetas en un sistema al que se le han asignado un máximo de dos direcciones IP. Para otras configuraciones, consulte las opciones de configuración en "Mapa de tareas: preparación para Trusted Extensions y activación del producto" en la página 33.

Tarea	Descripción	Para obtener instrucciones
1. Ejecute la secuencia de comandos `txzonemgr`.	La secuencia de comandos `txzonemgr` crea una interfaz gráfica de usuario que presenta las tareas correspondientes a medida que configura las zonas.	"Ejecución de la secuencia de comandos `txzonemgr`" en la página 67
2. Gestione las interfaces de red en la zona global.	Configure las interfaces en la zona global, o cree las interfaces lógicas y configúrelas en la zona global.	"Configuración de las interfaces de red en Trusted Extensions" en la página 68
3. Asigne un nombre a la zona y etiquétela.	Asigne un nombre a la zona con una versión de su etiqueta y asigne la etiqueta.	"Asignación de nombre y etiquetado de zona" en la página 72
4. Instale e inicie la zona.	Instale los paquetes en la zona. Configure los servicios en la zona. Zone Terminal Console le permite ver la actividad en la zona.	"Instalación de la zona con etiquetas" en la página 74 "Inicie la zona con etiquetas" en la página 75
5. Verifique el estado de la zona.	Verifique que la zona con etiquetas esté en ejecución y que la zona pueda comunicarse con la zona global.	"Verificación del estado de la zona" en la página 77

Tarea	Descripción	Para obtener instrucciones
6. Personalice la zona.	Elimine los servicios no deseados de la zona. Si la zona se va a utilizar para crear otras zonas, elimine la información que sea específica de esta zona solamente.	"Personalización de la zona con etiquetas" en la página 78
7. Cree el resto de las zonas.	Utilice el método que ha elegido para crear la segunda zona. Para ver una explicación de los métodos de creación de zonas, consulte "Planificación de zonas en Trusted Extensions" en la página 24.	"Copia o clonación de una zona en Trusted Extensions" en la página 80
8. (Opcional) Agregue las interfaces de red específicas de la zona.	Para que se aplique el aislamiento de red, agregue una o varias interfaces de red a una zona con etiquetas. Generalmente, estas configuraciones se utilizan para aislar subredes con etiquetas.	"Adición de interfaces de red y rutas a zonas con etiquetas" en la página 81

▼ Ejecución de la secuencia de comandos `txzonemgr`

Esta secuencia de comandos lo guiará a lo largo de las tareas para configurar, instalar, inicializar e iniciar las zonas con etiquetas correctamente. En la secuencia de comandos, asigne un nombre a cada zona, asocie el nombre con una etiqueta, instale los paquetes para crear un sistema operativo virtual y, a continuación, inicie la zona para iniciar los servicios en dicha zona. La secuencia de comandos incluye las tareas de copia de zona y clonación de zona. También puede detener una zona, cambiar el estado de una zona y agregar interfaces de red específicas de la zona.

Esta secuencia de comandos presenta un menú determinado dinámicamente que sólo muestra las opciones válidas para las circunstancias actuales. Por ejemplo, si la zona está configurada, la opción de menú de Install zone no se muestra. Las tareas finalizadas no aparecen en la lista.

Antes de empezar

Debe ser superusuario.

Si tiene previsto clonar zonas, debe haber terminado la preparación para clonar zonas. Si tiene previsto utilizar sus propias plantillas de seguridad, debe haber creado las plantillas.

1 Abra una ventana de terminal en la zona global.

2 Ejecute la secuencia de comandos `txzonemgr`.

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

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

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

Consejo – Para ver el estado actual de finalización de la zona, haga clic en Return to Main Menu, en Labeled Zone Manager.

▼ Configuración de las interfaces de red en Trusted Extensions

Nota – Si va a configurar el sistema para utilizar DHCP, consulte las instrucciones para equipos portátiles de la sección de Trusted Extensions de la página web de seguridad de la comunidad de OpenSolaris (`http://hub.opensolaris.org/bin/view/Community+Group+security/`).

A partir de la versión Solaris 10 10/08, si está configurando un sistema en el que cada zona con etiquetas está en su propia subred, puede omitir este paso y continuar con "Asignación de nombre y etiquetado de zona" en la página 72. Una vez que haya terminado de instalar y personalizar las zonas, agregue las interfaces de red para todas las zonas con etiquetas según lo explicado en "Adición de una interfaz de red para enrutar una zona con etiquetas existente" en la página 82.

Mediante esta tarea, se configuran las redes en la zona global. Debe crear exactamente una interfaz `all-zones`. Una interfaz `all-zones` es compartida por las zonas con etiquetas y la zona global. La interfaz compartida se usa para enrutar el tráfico entre las zonas con etiquetas y la zona global. Para configurar esta interfaz, realice una de las siguientes acciones:

- Cree una interfaz lógica a partir de una interfaz física y, a continuación, comparta la interfaz física.

  Esta configuración es la más fácil para administrar. Elija esta configuración cuando se hayan asignado dos direcciones IP a su sistema. En este procedimiento, la interfaz lógica se convierte en la dirección específica de la zona global, y la interfaz física se comparte entre la zona global y las zonas con etiquetas.

- Comparta una interfaz física.

  Elija esta configuración cuando se haya asignado una dirección IP a su sistema. En esta configuración, la interfaz física se comparte entre la zona global y las zonas con etiquetas.

- Comparta una interfaz de red virtual, `vni0`.

  Elija esta configuración cuando esté configurando DHCP, o cuando cada subred esté en una etiqueta diferente. Para un procedimiento de muestra, consulte las instrucciones para equipos portátiles de la sección de Trusted Extensions de la página web de seguridad de la comunidad de OpenSolaris (`http://hub.opensolaris.org/bin/view/Community+Group+security/`).

A partir de la versión Solaris 10 10/08, la interfaz de bucle de retorno en Trusted Extensions se crea como una interfaz all-zones. Por lo tanto, no hace falta crear una interfaz compartida `vni0`.

Para agregar interfaces de red específicas de la zona, finalice y verifique la creación de la zona antes de agregar las interfaces. Para conocer el procedimiento, consulte "Adición de una interfaz de red para enrutar una zona con etiquetas existente" en la página 82.

Antes de empezar

Debe ser superusuario de la zona global.

Aparece Labeled Zone Manager. Para abrir esta interfaz gráfica de usuario, consulte "Ejecución de la secuencia de comandos `txzonemgr`" en la página 67.

1 En Labeled Zone Manager, seleccione Manage Network Interfaces y haga clic en OK.

Aparece una lista de interfaces.

Nota – En este ejemplo, durante la instalación se asignó un nombre de host y una dirección IP a la interfaz física.

---

2 Seleccione la interfaz física.

Un sistema con una interfaz muestra un menú similar al siguiente. La anotación se agrega para obtener asistencia:

```
vni0                          Down      Virtual Network Interface
eri0 global 10.10.9.9 cipso Up      Physical Interface
```

a. Seleccione la interfaz `eri0`.

b. Haga clic en OK.

3 Seleccione la tarea adecuada para esta interfaz de red.

Se le ofrecen tres opciones:

```
View Template       Assign a label to the interface
Share       Enable the global zone and labeled zones to use this interface
Create Logical Interface       Create an interface to use for sharing
```

- **Si el sistema tiene una dirección IP, vaya al Paso 4.**
- **Si el sistema tiene dos direcciones IP, vaya al Paso 5.**

4 En un sistema con una dirección IP, comparta la interfaz física.

En esta configuración, la dirección IP del host se aplica a todas las zonas. Por lo tanto, la dirección del host es la dirección `all-zones`. Este host no se puede utilizar como un servidor de

varios niveles. Por ejemplo, los usuarios no pueden compartir archivos de este sistema. El sistema no puede ser un servidor proxy LDAP, un servidor de directorio principal NFS ni un servidor de impresión.

a. Seleccione Share y haga clic en OK.

b. Haga clic en OK en el cuadro de diálogo que muestra la interfaz compartida.

```
eri0  all-zones  10.10.9.8  cipso  Up
```

Si realizó todo correctamente, la interfaz física será una interfaz `all-zones`. Continúe con "Asignación de nombre y etiquetado de zona" en la página 72.

5 En un sistema con dos direcciones IP, cree una interfaz lógica.

A continuación, comparta la interfaz física.

Ésta es la configuración de red de Trusted Extensions más sencilla. En esta configuración, la dirección IP principal puede ser utilizada por otros sistemas para llegar a cualquier zona de este sistema, y la interfaz lógica es específica de la zona para la zona global. La zona global se puede utilizar como un servidor de varios niveles.

a. Seleccione Create Logical Interface y haga clic en OK.

Cierre el cuadro de diálogo que confirma la creación de una interfaz lógica nueva.

b. Seleccione Set IP address y haga clic en OK.

c. En la petición de datos, especifique el nombre de host para la interfaz lógica y haga clic en OK.

Por ejemplo, especifique `machine1-services` como nombre de host para la interfaz lógica. El nombre indica que este host ofrece servicios de varios niveles.

d. En la petición de datos, especifique la dirección IP para la interfaz lógica y haga clic en OK.

Por ejemplo, especifique `10.10.9.2` como la dirección IP de la interfaz lógica.

e. Seleccione la interfaz lógica de nuevo y haga clic en OK.

f. Seleccione Bring Up y haga clic en OK.

La interfaz aparece como `Up`.

```
eri0    global       10.10.9.1   cipso   Up
eri0:1  global       10.10.9.2   cipso   Up
```

g. Comparta la interfaz física.

i. Seleccione la interfaz física y haga clic en OK.

ii. Seleccione Share y haga clic en OK.

```
eri0    all-zones    10.10.9.1   cipso   Up
eri0:1  global       10.10.9.2   cipso   Up
```

Si realizó todo correctamente, al menos una interfaz será `all-zones`.

Ejemplo 4–3 Visualización del archivo `/etc/hosts` en un sistema con una interfaz lógica compartida

En un sistema en el que la zona global tiene una interfaz única y las zonas con etiquetas comparten una segunda interfaz con la zona global, aparece un archivo `/etc/hosts` similar al siguiente:

```
# cat /etc/hosts
...
127.0.0.1  localhost
192.168.0.11 machine1 loghost
192.168.0.12 machine1-services
```

En la configuración predeterminada, aparece un archivo `tnrhdb` similar al siguiente:

```
# cat /etc/security/tsol/tnrhdb
...
127.0.0.1:cipso
192.168.0.11:cipso
192.168.0.12:cipso
0.0.0.0:admin_low
```

Si la interfaz `all-zones` no está en el archivo `tnrhdb`, de manera predeterminada se establece `cipso` para la interfaz.

Ejemplo 4–4 Visualización de la interfaz compartida en un sistema Trusted Extensions con una dirección IP

En este ejemplo, el administrador no tiene previsto utilizar el sistema como un servidor de varios niveles. Para conservar las direcciones IP, la zona global se configura para que comparta su dirección IP con todas las zonas con etiquetas.

El administrador selecciona Share para la interfaz `hme0` en el sistema. El software configura todas las zonas para que tengan NIC lógicas. Estas NIC lógicas comparten una NIC física única en la zona global.

El administrador ejecuta el comando **`ifconfig -a`** para verificar que la interfaz física `hme0` de la interfaz de red `192.168.0.11` esté compartida. Aparece el valor `all-zones`:

```
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        all-zones
        inet 192.168.0.11 netmask fffffe00 broadcast 192.168.0.255
```

A partir de la versión Solaris 10 10/08, la interfaz de bucle de retorno en Trusted Extensions se crea como una interfaz all-zones.

```
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
        all-zones
        inet 127.0.0.1 netmask ff000000
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        all-zones
        inet 192.168.0.11 netmask fffffe00 broadcast 192.168.0.255
```

El administrador también examina el contenido del archivo `/etc/hostname.hme0`:

```
192.168.0.11 all-zones
```

▼ Asignación de nombre y etiquetado de zona

No es necesario que cree una zona para cada la etiqueta del archivo `label_encodings`, pero puede hacerlo. Las interfaces gráficas de usuario administrativas enumeran las etiquetas para las que se pueden crear zonas en este sistema.

Antes de empezar

Debe ser superusuario de la zona global. Aparece el cuadro de diálogo Labeled Zone Manager. Para abrir esta interfaz gráfica de usuario, consulte "Ejecución de la secuencia de comandos `txzonemgr`" en la página 67. Ha configurado las interfaces de red en la zona global.

Ha creado todas las plantillas de seguridad que necesita. Una plantilla de seguridad define, entre otros atributos, el rango de etiqueta que se puede asignar a una interfaz de red. Las plantillas de seguridad predeterminadas pueden satisfacer sus necesidades.

- Para obtener una descripción general de las plantillas de seguridad, consulte "Atributos de seguridad de red en Trusted Extensions" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.
- Para utilizar Solaris Management Console para crear plantillas de seguridad, consulte "Configuración de bases de datos de red de confianza (mapa de tareas)" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.

1 En Labeled Zone Manager, seleccione Create a new zone y haga clic en OK.

Se le pedirá un nombre.

a. Escriba el nombre de la zona.

Consejo – Asigne a la zona un nombre que sea similar a la etiqueta de la zona. Por ejemplo, el nombre de una zona cuya etiqueta es `CONFIDENTIAL: RESTRICTED` sería `restricted`.

Por ejemplo, el archivo `label_encodings` predeterminado contiene las siguientes etiquetas:

```
PUBLIC
CONFIDENTIAL: INTERNAL USE ONLY
CONFIDENTIAL: NEED TO KNOW
CONFIDENTIAL: RESTRICTED
SANDBOX: PLAYGROUND
MAX LABEL
```

Si bien puede crear una zona por etiqueta, considere la posibilidad de crear las siguientes zonas:

- En un sistema para todos los usuarios, cree una zona para la etiqueta `PUBLIC` y tres zonas para las etiquetas `CONFIDENTIAL`.
- En un sistema para desarrolladores, cree una zona para la etiqueta `SANDBOX: PLAYGROUND`. Como `SANDBOX: PLAYGROUND` se define como una etiqueta separada para los desarrolladores, sólo los sistemas que utilizan los desarrolladores necesitan una zona para esta etiqueta.
- No cree una zona para la etiqueta `MAX LABEL`, que se define como una acreditación.

b. Haga clic en OK.

El cuadro de diálogo muestra *nombre_zona* `:configured` encima de un lista de tareas.

2 Para etiquetar la zona, elija una de las siguientes opciones:

- **Si está utilizando un archivo `label_encodings` personalizado, etiquete la zona con la herramienta Trusted Network Zones.**

  a. Abra la herramienta Trusted Network Zones en Solaris Management Console.

  i. Inicie Solaris Management Console.

  ```
  # /usr/sbin/smc &
  ```

  ii. Abra la caja de herramientas de Trusted Extensions para el sistema local.

  Seleccione Console → Open Toolbox.

  Seleccione la caja de herramientas que se denomina This Computer (*este host*: `Scope=Files, Policy=TSOL`).

  Haga clic en Open.

  iii. En System Configuration, navegue hasta Computers and Networks.

  Escriba una contraseña cuando se le solicite.

iv. **Haga doble clic en la herramienta Trusted Network Zones.**

b. **Asocie la etiqueta correspondiente al nombre de zona de cada zona.**

i. **Elija Action → Add Zone Configuration.**

El cuadro de diálogo muestra el nombre de una zona que no tiene ninguna etiqueta asignada.

ii. **Fíjese en el nombre de la zona y, a continuación, haga clic en Edit.**

iii. **En el generador de etiquetas, haga clic sobre la etiqueta adecuada para el nombre de zona.**

Si hace clic en la etiqueta incorrecta, haga clic de nuevo en la etiqueta para anular la selección y, a continuación, haga clic en la etiqueta correcta.

iv. **Guarde la asignación.**

Haga clic en OK en el generador de etiquetas y, a continuación, haga clic en OK en el cuadro de diálogo Trusted Network Zones Properties.

Habrá terminado una vez que todas las zonas que desea aparezcan en el panel o cuando la opción de menú Add Zone Configuration abra un cuadro de diálogo que no tenga un valor para el nombre de zona.

- **Si utiliza el archivo `label_encodings` predeterminado, utilice Labeled Zone Manager.**

Haga clic en la opción de menú Select Label y, a continuación, en OK para mostrar la lista de etiquetas disponibles.

a. **Seleccione la etiqueta para la zona.**

Para una zona que se denomina `public`, tendría que seleccionar la etiqueta `PUBLIC` de la lista.

b. **Haga clic en OK.**

Aparecerá una lista de tareas.

▼ Instalación de la zona con etiquetas

Antes de empezar

Debe ser superusuario de la zona global. La zona debe estar configurada y tener asignada una interfaz de red.

Aparece el cuadro de diálogo Labeled Zone Manager con el subtítulo *nombre_zona*`:configured`. Para abrir esta interfaz gráfica de usuario, consulte "Ejecución de la secuencia de comandos `txzonemgr`" en la página 67.

1 **Desde Labeled Zone Manager, seleccione Install y haga clic en OK.**

Precaución – Este proceso demora algún tiempo en completarse. No realice otras tareas mientras se esté realizando esta tarea.

El sistema copia paquetes de la zona global a la zona no global. Esta tarea instala un sistema operativo virtual con etiquetas en la zona. Para continuar con el ejemplo, esta tarea instala la zona `public`. La interfaz gráfica de usuario muestra un resultado similar al siguiente.

```
# Labeled Zone Manager: Installing zone-name zone
Preparing to install zone <zonename>
Creating list of files to copy from the global zone
Copying <total> files to the zone
Initializing zone product registry
Determining zone package initialization order.
Preparing to initialize <subtotal> packages on the zone.
Initializing package <number> of <subtotal>: percent complete: percent

Initialized <subtotal> packages on zone.
Zone <zonename> is initialized.
The file /zone/internal/root/var/sadm/system/logs/install_log
contains a log of the zone installation.
```

Nota – Los mensajes como `cannot create ZFS dataset zone/` *nombre_zona*`: dataset already exists` son sólo informativos. La zona utiliza el conjunto de datos existente.

Cuando se complete la instalación, se le solicitará el nombre del host. Se proporciona un nombre.

2 **Acepte el nombre del host.**

El cuadro de diálogo muestra *nombre_zona*`:installed` encima de una lista de tareas.

Errores más frecuentes Si aparecen advertencias similares a la siguiente: `Installation of these packages generated errors: SUNW`*nombre_paquete*, lea el registro de instalación y termine de instalar los paquetes.

▼ Inicie la zona con etiquetas

Antes de empezar Debe ser superusuario de la zona global. La zona debe estar instalada y tener asignada una interfaz de red.

Aparece el cuadro de diálogo Labeled Zone Manager con el subtítulo *nombre_zona*`:installed`. Para abrir esta interfaz gráfica de usuario, consulte "Ejecución de la secuencia de comandos `txzonemgr`" en la página 67.

1 **En Labeled Zone Manager, seleccione Zone Console y haga clic en OK.**

Aparece una ventana de consola independiente para la zona con etiquetas actual.

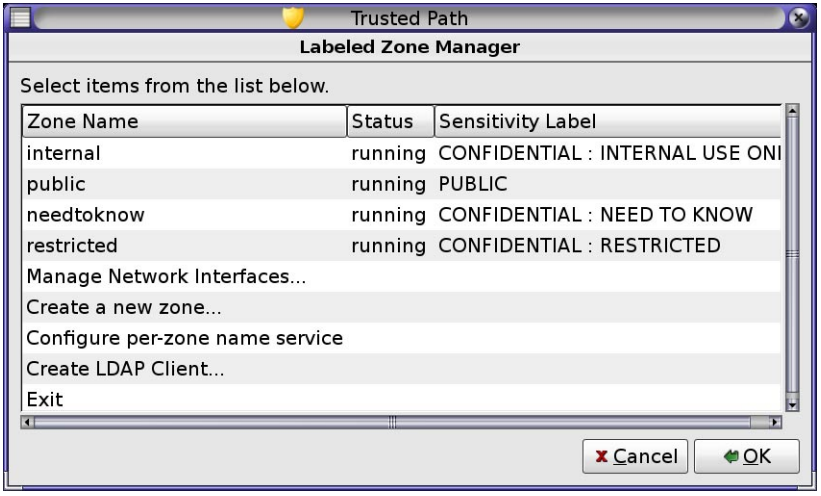
2 **Seleccione Boot.**

Zone Terminal Console realiza un seguimiento del progreso del inicio de la zona. Si la zona se crea desde el principio, en la consola aparecen mensajes similares a los siguientes:

```
[Connected to zone 'public' console]

[NOTICE: Zone booting up]
...
Hostname: zone-name
Loading smf(5) service descriptions: number/total
Creating new rsa public/private host key pair
Creating new dsa public/private host key pair

rebooting system due to change(s) in /etc/default/init

[NOTICE: Zone rebooting]
```

Precaución – No realice otras tareas mientras se esté realizando esta tarea.

Una vez que las cuatro zonas predeterminadas se configuran e inician, Labeled Zone Manager muestra las zonas de la siguiente manera:



Errores más frecuentes

A veces, aparecen mensajes de error y la zona no se reinicia. En Zone Terminal Console, presione la tecla de retorno. Si se le solicita que escriba y para reiniciar, escriba y. Luego, presione la tecla de retorno. La zona se reiniciará.

Pasos siguientes Si esta zona se copió o clonó de otra zona, continúe con "Verificación del estado de la zona" en la página 77.

Si esta zona es la primera zona, continúe con "Personalización de la zona con etiquetas" en la página 78.

▼ Verificación del estado de la zona

Nota – El servidor X se ejecuta en la zona global. Cada zona con etiquetas debe poder conectarse con la zona global para utilizar el servidor X. Por lo tanto, para poder utilizar una zona es necesario que las redes de la zona funcionen. Para acceder a información básica, consulte "Planificación de acceso de varios niveles" en la página 26.

1 Verifique que la zona se haya iniciado por completo.

a. En *nombre_zona*: Zone Terminal Console, inicie sesión como usuario root.

```
hostname console login: root
Password:      Type root password
```

b. En Zone Terminal Console, verifique que los servicios fundamentales estén en ejecución.

```
# svcs -xv
svc:/application/print/server:default (LP print server)
 State: disabled since Tue Oct 10 10:10:10 2006
Reason: Disabled by an administrator.
   See: http://sun.com/msg/SMF-8000-05
   See: lpsched(1M)
...
```

Los servicios `sendmail` y `print` no son servicios fundamentales.

c. Verifique que la zona tenga una dirección IP válida.

```
# ifconfig -a
```

Por ejemplo, el siguiente resultado muestra una dirección IP para la interfaz `hme0`.

```
# ...
 hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
         all-zones
         inet 192.168.0.11 netmask fffffe00 broadcast 192.168.0.255
```

d. (Opcional) Verifique que la zona puede comunicarse con la zona global.

i. Defina la variable `DISPLAY` para que haga referencia al servidor X.

```
# DISPLAY=global-zone-hostname:n.n
# export DISPLAY
```

ii. Desde la ventana de terminal, muestre una interfaz gráfica de usuario.

Por ejemplo, muestre un reloj.

```
# /usr/openwin/bin/xclock
```

Si el reloj no aparece en la etiqueta de la zona, las redes de la zona no se configuraron correctamente. Para ver sugerencias sobre depuración, consulte "La zona con etiquetas no puede acceder al servidor X" en la página 107.

iii. Antes de continuar, cierre la interfaz gráfica de usuario.

2 Desde la zona global, compruebe el estado de las zonas con etiquetas.

```
# zoneadm list -v
ID NAME         STATUS         PATH                BRAND   IP
 0 global       running        /                   native  shared
 3 internal     running        /zone/internal      native  shared
 4 needtoknow   running        /zone/needtoknow    native  shared
 5 restricted   running        /zone/restricted    native  shared
```

Pasos siguientes Ha terminado de configurar la zona con etiquetas. Para agregar interfaces de red específicas de la zona a las zonas, o establecer una ruta predeterminada por zona con etiquetas, continúe con "Adición de interfaces de red y rutas a zonas con etiquetas" en la página 81. De lo contrario, continúe con "Creación de roles y usuarios en Trusted Extensions" en la página 90.

▼ Personalización de la zona con etiquetas

Si va a clonar o a copiar zonas, este procedimiento permite configurar una zona para utilizarla como plantilla para otras zonas. Además, este procedimiento permite configurar una zona que no se ha creado a partir de una plantilla para su uso.

Antes de empezar Debe ser superusuario de la zona global. Debe haber completado la sección "Verificación del estado de la zona" en la página 77.

1 En Zone Terminal Console, deshabilite los servicios que no son necesarios en una zona con etiquetas.

Si está copiando o clonando esta zona, los servicios que deshabilite se inhabilitarán en las nuevas zonas. Los servicios que están en línea en el sistema dependen del manifiesto de servicio para la zona. Utilice el comando `netservices limited` para desactivar los servicios que las zonas con etiquetas no necesitan.

a. Elimine varios servicios innecesarios.

```
# netservices limited
```

b. Muestre los servicios restantes.

```
# svcs
...
STATE          STIME      FMRI
online         13:05:00   svc:/application/graphical-login/cde-login:default
...
```

c. Deshabilite el acceso gráfico.

```
# svcadm disable svc:/application/graphical-login/cde-login
# svcs cde-login
STATE          STIME      FMRI
disabled       13:06:22   svc:/application/graphical-login/cde-login:default
```

Para obtener información sobre la estructura de gestión de servicios, consulte la página del comando man `smf(5)`.

2 En Labeled Zone Manager, seleccione Halt para detener la zona.

3 Antes de continuar, verifique que la zona esté cerrada.

En *nombre_zona*: Zone Terminal Console, el siguiente mensaje indica que la zona está cerrada.

```
[ NOTICE: Zone halted]
```

Si usted no está copiando ni clonando esta zona, cree las demás zonas de la misma manera en que creó esta primera zona. De lo contrario, continúe con el paso siguiente.

4 Si está utilizando esta zona como una plantilla para las demás zonas, realice lo siguiente:

a. Elimine el archivo `auto_home_`*nombre_zona*.

En una ventana de terminal de la zona global, elimine este archivo de la zona *nombre_zona*.

```
# cd /zone/zone-name/root/etc
# ls auto_home*
auto_home  auto_home_zone-name
# rm auto_home_zone-name
```

Por ejemplo, si la zona `public` es la plantilla para la clonación de otras zonas, elimine el archivo `auto_home_public`:

```
# cd /zone/public/root/etc
# rm auto_home_public
```

b. Si tiene previsto clonar esta zona, cree la instantánea de ZFS en el paso siguiente y, luego, continúe con "Copia o clonación de una zona en Trusted Extensions" en la página 80.

c. Si va a copiar esta zona, complete el Paso 6 y, luego, continúe con "Copia o clonación de una zona en Trusted Extensions" en la página 80.

5 Para crear una plantilla de zona para clonar las demás zonas, seleccione Create Snapshot y haga clic en OK.

Precaución – La zona para la instantánea debe estar en un sistema de archivos ZFS. En la sección "Creación de agrupación ZFS para clonar zonas" en la página 56, creó un sistema de archivos ZFS para la zona.

6 **Para asegurarse de que la zona personalizada todavía se pueda utilizar, seleccione la opción Boot de Labeled Zone Manager.**

La acción Zone Terminal Console realiza un seguimiento del progreso del inicio de la zona. En la consola aparecen mensajes similares a los siguientes:

```
[Connected to zone 'public' console]

[NOTICE: Zone booting up]
...
Hostname: zonename
```

Presione la tecla de retorno para acceder a la petición de datos de inicio de sesión. Puede iniciar sesión como usuario root.

▼ Copia o clonación de una zona en Trusted Extensions

Antes de empezar Debe haber completado "Personalización de la zona con etiquetas" en la página 78.

Aparece el cuadro de diálogo Labeled Zone Manager. Para abrir esta interfaz gráfica de usuario, consulte "Ejecución de la secuencia de comandos `txzonemgr`" en la página 67.

1 **Cree la zona.**

Para obtener detalles, consulte "Asignación de nombre y etiquetado de zona" en la página 72.

2 **Continúe con la estrategia de creación de zona seleccionando uno de los siguientes métodos:**

Deberá repetir estos pasos para cada zona nueva.

- **Copie la zona que acaba de etiquetar.**

  a. **En Labeled Zone Manager, seleccione Copy y haga clic en OK.**

  b. **Seleccione la plantilla de zona y haga clic en OK.**

  Aparece una ventana en la que se muestra el proceso de copia. Una vez que termine el proceso, la zona estará instalada.

  Si Labeled Zone Manager muestra *nombre_zona* `:configured`, continúe con el paso siguiente. De lo contrario, continúe con el Paso e.

  c. **Seleccione la opción de menú Select another zone y, a continuación, haga clic en OK.**

  d. **Seleccione la zona que acaba de instalar y haga clic en OK.**

e. **Complete la sección "Inicie la zona con etiquetas" en la página 75.**

f. **Complete la sección "Verificación del estado de la zona" en la página 77.**

- **Clone la zona que acaba de etiquetar.**

a. **En Labeled Zone Manager, seleccione Clone y, a continuación, haga clic en OK.**

b. **Seleccione una instantánea de ZFS de la lista y haga clic en OK.**

Por ejemplo, si ha creado una instantánea a partir de `public`, seleccione `zone/public@snapshot`.

Una vez que termine el proceso de clonación, la zona estará instalada. Continúe con el Paso c.

c. **Abra una consola de zona e inicie la zona.**

Para obtener instrucciones, consulte "Inicie la zona con etiquetas" en la página 75.

d. **Complete la sección "Verificación del estado de la zona" en la página 77.**

Pasos siguientes

- Cuando haya completado la sección "Verificación del estado de la zona" en la página 77 para cada zona y desee que cada zona esté en una red física independiente, continúe con "Adición de una interfaz de red para enrutar una zona con etiquetas existente" en la página 82.
- Si aún no ha creado roles, continúe con "Creación de roles y usuarios en Trusted Extensions" en la página 90.
- Si ya ha creado roles, continúe con "Creación de directorios principales en Trusted Extensions" en la página 101.

Adición de interfaces de red y rutas a zonas con etiquetas

Las siguientes tareas se pueden realizar en entornos en los que cada zona está conectada a una red física independiente.

Tarea	Descripción	Para obtener instrucciones
PUEDE 1a: agregar una interfaz de red a cada zona con etiquetas y utilizar la zona global para llegar a la red externa.	Conecta cada zona con etiquetas a una red física independiente. Las zonas con etiquetas utilizan la ruta de red que proporciona la zona global.	"Adición de una interfaz de red para enrutar una zona con etiquetas existente" en la página 82

Tarea	Descripción	Para obtener instrucciones
O 1b: agregar una interfaz de red a cada zona con etiquetas con una ruta predeterminada.	Conecta cada zona a una red física independiente. Las zonas con etiquetas *no* utilizan la zona global para el enrutamiento.	"Adición de una interfaz de red que no utiliza la zona global para enrutar una zona con etiquetas existente" en la página 84
2. Cree una antememoria de servicio de nombres en cada zona con etiquetas.	Configura un daemon de servicio de nombres para cada zona.	"Configuración de una antememoria de servicio de nombres en cada zona con etiquetas" en la página 88

▼ Adición de una interfaz de red para enrutar una zona con etiquetas existente

Este procedimiento agrega interfaces de red específicas de la zona a las zonas con etiquetas existentes. Esta configuración se puede realizar en entornos en los que cada zona con etiquetas está conectada a una red física independiente. Las zonas con etiquetas utilizan la ruta de red que proporciona la zona global.

Nota – La zona global debe configurar una dirección IP para cada subred en la que esté configurada una dirección de zona no global.

Antes de empezar

Debe ser superusuario de la zona global.

Para cada zona, debe haber completado las tareas de la sección "Creación de zonas con etiquetas" en la página 66.

1 En la zona global, escriba las direcciones IP y los nombres de host para las interfaces de red adicionales en el archivo `/etc/hosts`.

Utilice una convención de denominación estándar, como la adición de *nombre_zona* al nombre del host.

```
## /etc/hosts in global zone
10.10.8.2    hostname-zone-name1
10.10.8.3    hostname-global-name1
10.10.9.2    hostname-zone-name2
10.10.9.3    hostname-global-name2
```

2 Para la red para cada interfaz, agregue entradas al archivo `/etc/netmasks`.

```
## /etc/netmasks in global zone
10.10.8.0 255.255.255.0
10.10.9.0 255.255.255.0
```

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

3 En la zona global, conecte las interfaces físicas específicas de la zona.

a. Identifique las interfaces físicas que ya están conectadas.

```
# ifconfig -a
```

b. Configure las direcciones de la zona global en cada interfaz.

```
# ifconfig interface-nameN1 plumb
# ifconfig interface-nameN1 10.10.8.3 up
# ifconfig interface-nameN2 plumb
# ifconfig interface-nameN2 10.10.9.3 up
```

c. Para cada dirección de zona global, cree un archivo `hostname.`*nombre_interfazN*.

```
# /etc/hostname.interface-nameN1
10.10.8.3
# /etc/hostname.interface-nameN2
10.10.9.3
```

Las direcciones de la zona global se configuran inmediatamente cuando se inicia el sistema. Las direcciones específicas de la zona se configuran cuando se inicia la zona.

4 Asigne una plantilla de seguridad a cada interfaz de red específica de la zona.

Si la puerta de enlace a la red no está configurada con etiquetas, asigne la plantilla de seguridad `admin_low`. Si la puerta de enlace a la red tiene etiquetas, asigne una plantilla de seguridad `cipso`.

Puede crear plantillas de seguridad de tipo de host `cipso` que reflejen la etiqueta de cada red. Para ver los procedimientos para crear y asignar plantillas, consulte "Configuración de bases de datos de red de confianza (mapa de tareas)" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.

5 Detenga todas las zonas con etiquetas a las que desea agregar una interfaz específica de la zona.

```
# zoneadm -z zone-name halt
```

6 Inicie Labeled Zone Manager.

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

7 Para cada zona a la que desea agregar una interfaz específica de zona, realice las siguientes acciones:

a. Seleccione la zona.

b. Seleccione Add Network.

c. Asigne un nombre a la interfaz de red.

d. Escriba la dirección IP de la interfaz.

8 **En el cuadro de diálogo Labeled Zone Manager de cada zona completada, seleccione Zone Console.**

9 **Seleccione Boot.**

10 **En la consola de zona, verifique que se hayan creado las interfaces.**

```
# ifconfig -a
```

11 **Verifique que la zona tenga una ruta a la puerta de enlace para la subred.**

```
# netstat -rn
```

Errores más frecuentes

Para depurar la configuración de la zona, consulte lo siguiente:

- El Capítulo 30, "Troubleshooting Miscellaneous Solaris Zones Problems" de *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*
- "Resolución de los problemas de configuración de Trusted Extensions" en la página 106
- "Resolución de problemas de la red de confianza (mapa de tareas)" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*

▼ Adición de una interfaz de red que no utiliza la zona global para enrutar una zona con etiquetas existente

Este procedimiento establece rutas predeterminadas específicas de la zona para las zonas con etiquetas existentes. En esta configuración, las zonas con etiquetas *no* utilizan la zona global para el enrutamiento.

La zona con etiquetas debe estar conectada a la zona global antes de que se inicie la zona. Sin embargo, para aislar la zona con etiquetas de la zona global, cuando se inicie la zona, la interfaz debe estar en el estado `down`. Para obtener más información, véase el Capítulo 17, "Non-Global Zone Configuration (Overview)" de *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*.

Nota – Se debe configurar una única ruta predeterminada para cada zona no global que se inicie.

Antes de empezar

Debe ser superusuario de la zona global.

Para cada zona, debe haber completado las tareas de la sección "Creación de zonas con etiquetas" en la página 66. Está utilizando la interfaz `vni0` o la interfaz `lo0` para conectar las zonas con etiquetas a la zona global.

1. **Para cada interfaz de red, determine la dirección IP, la máscara de red y el enrutador predeterminado.**

   Utilice el comando `ifconfig -a` para determinar la dirección IP y la máscara de red. Utilice el comando `zonecfg -z zonename info net` para determinar si se ha asignado un enrutador predeterminado.

2. **Cree un archivo `/etc/hostname.`*interfaz* vacío para cada zona con etiquetas.**

   ```
   # touch /etc/hostname.interface
   # touch /etc/hostname.interface:n
   ```

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

3. **Conecte las interfaces de red de las zonas con etiquetas.**

   ```
   # ifconfig zone1-network-interface plumb
   # ifconfig zone2-network-interface plumb
   ```

4. **Verifique que las interfaces de la zona con etiquetas tengan el estado `down`.**

   ```
   # ifconfig -a
   zone1-network-interface zone1-IP-address down
   zone2-network-interface zone2-IP-address down
   ```

   Las direcciones específicas de la zona se configuran cuando se inicia la zona.

5. **Para la red para cada interfaz, agregue entradas al archivo `/etc/netmasks`.**

   ```
   ## /etc/netmasks in global zone
   192.168.2.0 255.255.255.0
   192.168.3.0 255.255.255.0
   ```

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

6. **Asigne una plantilla de seguridad a cada interfaz de red específica de la zona.**

   Cree plantillas de seguridad de tipo de host `cipso` que reflejen la etiqueta de cada red. Para crear y asignar plantillas, consulte "Configuración de bases de datos de red de confianza (mapa de tareas)" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.

7. **Ejecute la secuencia de comandos `txzonemgr` y abra una ventana de terminal independiente.**

   En Labeled Zone Manager, agregará las interfaces de red para las zonas con etiquetas. En la ventana de terminal, visualizará la información de la zona y definirá el enrutador predeterminado.

8. **Para cada zona a la que va a agregar una interfaz de red específica de la zona y un enrutador, realice los siguientes pasos:**

   a. **En la ventana de terminal, detenga la zona.**

      ```
      # zoneadm -z zone-name halt
      ```

b. En Labeled Zone Manager, realice las siguientes acciones:

i. Seleccione la zona.

ii. Seleccione Add Network.

iii. Asigne un nombre a la interfaz de red.

iv. Escriba la dirección IP de la interfaz.

v. En la ventana de terminal, verifique la configuración de la zona.

```
# zonecfg -z zone-name info net
net:    address: IP-address
        physical: zone-network-interface
        defrouter not specified
```

c. En la ventana de terminal, configure el enrutador predeterminado para la red de la zona con etiquetas.

```
# zonecfg -z zone-name
zonecfg:zone-name > select net address=IP-address
zonecfg:zone-name:net> set defrouter=router-address
zonecfg:zone-name:net> end
zonecfg:zone-name > verify
zonecfg:zone-name > commit
zonecfg:zone-name > exit
#
```

Para obtener más información, consulte la página del comando man `zonecfg`(1M) y "How to Configure the Zone" de *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*.

d. Inicie la zona con etiquetas.

```
# zoneadm -z zone-name boot
```

e. En la zona global, verifique que la zona con etiquetas tenga una ruta a la puerta de enlace para la subred.

```
# netstat -rn
```

Aparece una tabla de enrutamiento. El destino y la interfaz para la zona con etiquetas es diferente de la entrada para la zona global.

9 Para eliminar la ruta predeterminada, seleccione la dirección IP de la zona y, a continuación, elimine la ruta.

```
# zonecfg -z zone-name

zonecfg:zone-name > select net address=zone-IP-address
zonecfg:zone-name:net> remove net defrouter=zone-default-route
zonecfg:zone-name:net>  info net
net:
```

```
address: zone-IP-address
physical: zone-network-interface
defrouter not specified
```

Ejemplo 4–5 Definición de una ruta predeterminada para una zona con etiquetas

En este ejemplo, el administrador enruta la zona Secret a una subred física independiente. El tráfico desde y hacia la zona Secret no se enruta por medio de la zona global. El administrador utiliza Labeled Zone Manager y el comando `zonecfg`, y, a continuación, verifica que el enrutamiento funcione.

El administrador determina que `qfe1` y `qfe1:0` actualmente no están en uso, y crea una asignación para dos zonas con etiquetas. `qfe1` es la interfaz designada para la zona Secret.

```
Interface IP Address    Netmask        Default Router
qfe1     192.168.2.22 255.255.255.0 192.168.2.2
qfe1:0   192.168.3.33 255.255.255.0 192.168.3.3
```

En primer lugar, el administrador crea el archivo `/etc/hostname.qfe1` y configura el archivo `/etc/netmasks`.

```
# touch /etc/hostname.qfe1

# cat /etc/netmasks
## /etc/netmasks in global zone
192.168.2.0 255.255.255.0
```

A continuación, el administrador conecta la interfaz de red y verifica que la interfaz esté inactiva.

```
# ifconfig qfe1 plumb
# ifconfig -a
```

A continuación, en Solaris Management Console, el administrador crea una plantilla de seguridad con una única etiqueta, Secret, y asigna la dirección IP de la interfaz a la plantilla.

El administrador detiene la zona.

```
# zoneadm -z secret halt
```

El administrador ejecuta la secuencia de comandos `txzonemgr` para abrir Labeled Zone Manager.

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

En Labeled Zone Manager, el administrador selecciona la zona Secret, luego, Add Network y, por último, una interfaz de red. El administrador cierra Labeled Zone Manager.

En la línea de comandos, el administrador selecciona la dirección IP de la zona y, a continuación, define la ruta predeterminada. Antes de salir del comando, el administrador verifica la ruta y la confirma.

```
# zonecfg -z secret
zonecfg: secret > select net address=192.168.6.22
zonecfg: secret:net> set defrouter=192.168.6.2
zonecfg: secret:net> end
zonecfg: secret > verify
zonecfg: secret > commit
zonecfg: secret > info net
  net:
     address: 192.168.6.22
     physical: qfe1
     defrouter: 192.168.6.2
zonecfg: secret > exit
#
```

El administrador inicia la zona.

```
# zoneadm -z secret boot
```

En una ventana de terminal independiente, en la zona global, el administrador verifica el envío y la recepción de paquetes.

```
# netstat -rn
Routing Table: IPv4
  Destination           Gateway           Flags  Ref     Use  Interface
-------------------- -------------------- ----- ----- ------- ---------
default              192.168.5.15         UG        1    2664 qfe0
192.168.6.2          192.168.6.22         UG        1     240 qfe1
192.168.3.3          192.168.3.33         U         1     183 qfe1:0
127.0.0.1            127.0.0.1            UH        1     380 lo0
...
```

▼ Configuración de una antememoria de servicio de nombres en cada zona con etiquetas

Este procedimiento permite configurar por separado un daemon de servicio de nombres (`nscd`) en cada zona con etiquetas. Esta configuración admite entornos en los que cada zona se conecta a una subred que se ejecuta en la etiqueta de la zona y la subred dispone de su propio servidor de nombres para esa etiqueta.

Nota – Esta configuración no cumple con los criterios de una configuración evaluada. En una configuración evaluada, el daemon `nscd` sólo se ejecuta en la zona global. Las puertas de cada zona con etiquetas conectan la zona al daemon `nscd` global.

Antes de empezar

Debe ser superusuario de la zona global. El usuario `root` todavía no debe ser un rol. Debe haber completado satisfactoriamente la sección "Adición de una interfaz de red para enrutar una zona con etiquetas existente" en la página 82.

Para utilizar esta configuración, es necesario tener conocimientos avanzados sobre redes. Si tiene el servicio de nombres LDAP, debe establecer la conexión de cliente LDAP a cada zona con etiquetas. El daemon `nscd` almacena la información del servicio de nombres en la antememoria, pero no la envía.

1. **Si está utilizando LDAP, verifique una ruta al servidor LDAP desde la zona con etiquetas.**

   En una ventana de terminal de cada zona con etiquetas, ejecute el siguiente comando:

   zone-name `# netstat -rn`

2. **En la zona global, inicie Labeled Zone Manager.**

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

3. **Seleccione la opción Configure per-zone name service y haga clic en OK.**

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

4. **Configure el servicio `nscd` de cada zona.**

   Para obtener ayuda, consulte las páginas del comando man `nscd(1M)` y `nscd.conf(4)`.

5. **Reinicie el sistema.**

6. **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 October 10, 2010  10:10:10 AM PDT
         See: nscd(1M)
         See: /etc/svc/volatile/system-name-service-cache:default.log
      Impact: None.
      ```

   b. **Verifique la ruta a la subred.**

      zone-name `# netstat -rn`

7. **Para eliminar los daemons de servicio de nombres específicos de la zona, realice las siguientes acciones en la zona global:**

   a. **Abra Labeled Zone Manager.**

   b. **Seleccione la opción Unconfigure per-zone name service y haga clic en OK.**

      Esta selección elimina el daemon `nscd` de cada zona con etiquetas.

   c. **Reinicie el sistema.**

Creación de roles y usuarios en Trusted Extensions

Si ya está usando roles administrativos, es posible que desee agregar un rol de administrador de la seguridad. Para los sitios que aún no han implementado los roles, el procedimiento para crearlos es similar al procedimiento utilizado en el SO Solaris. Trusted Extensions agrega el rol de administrador de la seguridad y requiere el uso de Solaris Management Console para administrar un dominio de Trusted Extensions.

Si la seguridad del sitio requiere que dos personas creen las cuentas de usuario y de rol, cree perfiles de derechos personalizados y asígnelos a los roles para aplicar la *separación de tareas*.

Tarea	Descripción	Para obtener instrucciones
Cree tres perfiles de derechos que sean más restrictivos que los perfiles predeterminados.	Crea perfiles de derechos para gestionar usuarios. Estos perfiles son más restrictivos que los perfiles predeterminados para gestionar a los usuarios.	"Creación de perfiles de derechos que aplican la separación de tareas" en la página 90
Cree un rol de administrador de la seguridad.	Crea un rol de administrador de la seguridad que maneja las tareas relacionadas con la seguridad.	"Creación del rol de administrador de la seguridad en Trusted Extensions" en la página 93
Cree un rol de administrador del sistema que no pueda definir una contraseña de usuario.	Crea un rol de administrador del sistema y le asigna un perfil de derechos de administración del sistema restringido.	"Creación de un rol de administrador del sistema restringido" en la página 96
Cree usuarios para que asuman roles administrativos.	Crea uno o varios usuarios que puedan asumir roles.	"Creación de usuarios que puedan asumir roles en Trusted Extensions" en la página 96
Verifique que los roles puedan realizar sus tareas.	Pone a los roles a prueba en diferentes situaciones.	"Verificación del funcionamiento de los roles de Trusted Extensions" en la página 99
Habilite a los usuarios para que puedan iniciar sesión en una zona con etiquetas.	Inicia el servicio `zones` para que los usuarios comunes puedan iniciar sesión.	"Habilitación de los usuarios para que inicien sesión en una zona con etiquetas" en la página 101

▼ Creación de perfiles de derechos que aplican la separación de tareas

Si la separación de tareas no es un requisito de seguridad del sitio, omita este procedimiento. Si el sitio requiere la separación de tareas, debe crear estos perfiles de derechos y roles antes rellenar el servidor LDAP.

Este procedimiento permite crear perfiles de derechos con capacidades discretas para gestionar a los usuarios. Al asignar estos perfiles a roles distintos, se requieren dos roles para crear y

configurar usuarios. Un rol puede crear usuarios, pero no puede asignar atributos de seguridad. El otro rol puede asignar atributos de seguridad, pero no puede crear usuarios. Al iniciar sesión en Solaris Management Console en un rol que tiene asignado uno de estos perfiles, sólo están disponibles las fichas y los campos adecuados para el rol.

Antes de empezar Debe ser superusuario, en el rol `root` o en el rol de administrador principal. Al iniciar este procedimiento, Solaris Management Console debe estar cerrada.

1 Cree copias de los perfiles de derechos predeterminados que afectan la configuración del usuario.

a. Copie el archivo `prof_attr` en el archivo `prof_attr.orig`.

b. Abra el archivo `prof_attr` en el editor confianza.

```
# /usr/dt/bin/trusted_edit /etc/security/prof_attr
```

c. Copie los tres perfiles de derechos y cambie el nombre de las copias.

```
System Administrator:::Can perform most non-security...
Custom System Administrator:::Can perform most non-security...

User Security:::Manage passwords...
Custom User Security:::Manage passwords...

User Management:::Manage users, groups, home...
Custom User Management:::Manage users, groups, home...
```

d. Guarde los cambios.

e. Verifique los cambios.

```
# grep ^Custom  /etc/security/prof_attr
Custom System Administrator:::Can perform most non-security...
Custom User Management:::Manage users, groups, home...
Custom User Security:::Manage passwords...
```

Copiar un perfil de derechos en lugar de modificarlo permite actualizar el sistema a una versión posterior de Solaris y conservar los cambios. Como estos perfiles de derechos son complejos, es menos probable que se produzca un error si se modifica una copia del perfil predeterminado que si se crea un perfil más restrictivo desde el principio.

2 Inicie Solaris Management Console.

```
# /usr/sbin/smc &
```

3 Seleccione la caja de herramientas This Computer (*este host*: `Scope=Files, Policy=TSOL`).

4 Haga clic en System Configuration y, a continuación, en Users.

Se le solicitará la contraseña.

5. **Escriba la contraseña correspondiente.**

6. **Haga doble clic en Rights.**

7. **Modifique el perfil de derechos de seguridad de usuarios personalizada.**

   Restrinja este perfil para que no pueda crear usuarios.

   a. **Haga doble clic en Custom User Security.**

   b. **Haga clic en la ficha Authorizations y, a continuación, realice los siguientes pasos:**

      i. **Desde la lista Included, elimine la autorización `Manage Users and Roles`.**

         Permanecen los siguientes derechos de User Accounts:

         ```
         Audit Controls
         Label and Clearance Range
         Change Password
         View Users and Roles
         Modify Extended Security Attributes
         ```

      ii. **Agregue el derecho Manage Privileges a la lista Included.**

   c. **Haga clic en OK para guardar los cambios.**

8. **Modifique el perfil de gestión de usuarios personalizada.**

   Restrinja este perfil para que no pueda definir una contraseña.

   a. **Haga doble clic en Custom User Management.**

   b. **Haga clic en la ficha Authorizations y, a continuación, realice los siguientes pasos:**

      i. **Arrastre la barra de desplazamiento de la lista Included hasta User Accounts.**

      ii. **Desde la lista Included, elimine la autorización `Modify Extended Security Attributes`.**

         Permanecen los siguientes derechos de User Accounts:

         ```
         Manage Users and Roles
         View Users and Roles
         ```

   c. **Guarde los cambios.**

9 **Modifique el perfil de derechos de administración del sistema personalizada.**

El perfil de gestión de usuarios es un perfil complementario en este perfil. Impida que el administrador del sistema defina una contraseña.

a. **Haga doble clic en Custom System Administrator.**

b. **Haga clic en la ficha Supplementary Rights y, a continuación, realice los siguientes pasos:**

i. **Elimine el perfil de derechos de gestión de usuarios.**

ii. **Agregue el perfil de derechos de gestión de usuarios personalizada.**

iii. **Coloque el perfil de derechos de gestión de usuarios personalizada encima del perfil de derechos de todos.**

c. **Guarde los cambios.**

Pasos siguientes Para evitar que se utilicen los perfiles predeterminados, consulte el Paso 7 en "Verificación del funcionamiento de los roles de Trusted Extensions" en la página 99 después de verificar que los perfiles personalizados apliquen la separación de tareas.

▼ Creación del rol de administrador de la seguridad en Trusted Extensions

La creación de roles en Trusted Extensions es idéntica a la creación de roles en el SO Solaris. Sin embargo, en Trusted Extensions, se requiere un rol de administrador de la seguridad. Para crear un rol de administrador de la seguridad local, también puede utilizar la interfaz de la línea de comandos, como se muestra en el Ejemplo 4–6.

Antes de empezar Debe ser superusuario, en el rol `root` o en el rol de administrador principal.

Para crear el rol en la red, debe haber completado la sección "Configuración de Solaris Management Console para LDAP (mapa de tareas)" en la página 128.

1 **Inicie Solaris Management Console.**

```
# /usr/sbin/smc &
```

2 **Seleccione la caja de herramientas adecuada.**

- **Para crear el rol de manera local, utilice This Computer (*este host*: `Scope=Files, Policy=TSOL`).**

- **Para crear el rol en el servicio LDAP, utilice This Computer (*servidor ldap*: `Scope=LDAP`, `Policy=TSOL`).**

3. **Haga clic en System Configuration y, a continuación, en Users.**

   Se le solicitará la contraseña.

4. **Escriba la contraseña correspondiente.**

5. **Haga doble clic en Administrative Roles.**

6. **En el menú Action, seleccione Add Administrative Role.**

7. **Cree el rol de administrador de la seguridad.**

   Utilice la siguiente información como guía:

   - Role name: `secadmin`
   - Full name: `Security Administrator`
   - Description: oficial de seguridad del sitio, *aquí no se introduce información de propiedad exclusiva*.
   - Role ID Number: ≥100
   - Role shell: Bourne del administrador (shell de perfil)
   - Create a role mailing list: deje la casilla de verificación seleccionada.
   - Password and confirm: asigne una contraseña de al menos 6 caracteres alfanuméricos.

     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.

     Nota – Para todos los roles administrativos, elija la opción Always Available para la cuenta y no establezca fechas de caducidad para las contraseñas.

   - Available and Granted Rights: Information Security, User Security
     - Si la seguridad del sitio no requiere la separación de tareas, seleccione el perfil de derechos de seguridad de la información y el perfil de derechos predeterminado de seguridad de usuarios.
     - Si la seguridad del sitio requiere la separación de tareas, seleccione el perfil de derechos de seguridad de la información y el perfil de derechos de seguridad de usuarios personalizada.
   - Home Directory Server: *servidor de directorio de inicio*
   - Home Directory Path: /*ruta de montaje*

- Assign Users: este campo se rellena automáticamente al asignar un rol a un usuario.

8 Después de crear el rol, compruebe que los valores sean correctos.

Seleccione el rol y, a continuación, haga doble clic en él.

Revise los valores de los siguientes campos:

- Available Groups: si es necesario, agregue grupos.
- Trusted Extensions Attributes: los valores predeterminados son correctos.

  Para un sistema de una sola etiqueta en el que las etiquetas no deben estar visibles, elija Hide para Label: Show or Hide.
- Audit Excluded and Included: establezca indicadores auditoría sólo si los indicadores de auditoría del rol son excepciones a la configuración del sistema en el archivo `audit_control`.

9 Para crear otros roles, utilice el rol de administrador de la seguridad como guía.

Para obtener ejemplos, consulte "How to Create and Assign a Role by Using the GUI" de *System Administration Guide: Security Services*. Asigne a cada rol un ID único y asigne al rol el perfil de derechos correcto. Entre los posibles roles se incluyen los siguientes:

- Rol de administrador: derechos otorgados de `System Administrator`
- Rol de administrador principal: derechos otorgados de `Primary Administrator`
- Rol de operador: derechos otorgados de `Operator`

Ejemplo 4–6 Uso del comando `roleadd` para crear un rol de administrador de la seguridad local

En este ejemplo, el usuario `root` agrega el rol de administrador de la seguridad a un sistema local con el comando `roleadd`. Para obtener detalles, consulte la página del comando man `roleadd(1M)`. Antes de crear el rol, el usuario `root` consulta la Tabla 1–2. En este sitio, no se requiere la separación de tareas para crear un usuario.

```
# roleadd -c "Local Security Administrator" -d /export/home1 \
-u 110 -P "Information Security,User Security" -K lock_after_retries=no \
-K idletime=5 -K idlecmd=lock -K labelview=showsl \
-K min_label=ADMIN_LOW -K clearance=ADMIN_HIGH secadmin
```

El usuario `root` proporciona una contraseña inicial para el rol.

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

Para asignar el rol a un usuario local, consulte el Ejemplo 4–7.

▼ Creación de un rol de administrador del sistema restringido

Si la separación de tareas no es un requisito de seguridad del sitio, omita este procedimiento.

Mediante este procedimiento, se asigna un perfil de derechos más restrictivo al rol de administrador del sistema.

Antes de empezar

Debe ser superusuario, en el rol `root` o en el rol de administrador principal.

Debe haber completado "Creación de perfiles de derechos que aplican la separación de tareas" en la página 90. Debe utilizar la misma caja de herramientas que utilizó para crear el perfil de derechos.

1. **En Solaris Management Console, cree el rol de administrador del sistema.**

   Para obtener ayuda, consulte "Creación del rol de administrador de la seguridad en Trusted Extensions" en la página 93.

2. **Asigne el perfil de derechos de administración del sistema personalizada al rol.**

3. **Guarde los cambios.**

4. **Cierre Solaris Management Console.**

▼ Creación de usuarios que puedan asumir roles en Trusted Extensions

Para crear un usuario local, puede utilizar la interfaz de línea de comandos, como se muestra en el Ejemplo 4–7, en lugar de realizar el siguiente procedimiento. Si la política de seguridad del sitio lo permite, puede elegir crear un usuario que pueda asumir más de un rol administrativo.

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

Antes de empezar

Debe ser superusuario en el rol `root`, en el rol de administrador de la seguridad o en el rol de administrador principal. El rol de administrador de la seguridad debe tener la menor cantidad de privilegios necesaria para la creación de usuarios.

Aparece Solaris Management Console. Para obtener detalles, consulte "Creación del rol de administrador de la seguridad en Trusted Extensions" en la página 93.

1. **Haga doble clic en User Accounts, en Solaris Management Console.**

2 **En el menú Action, seleccione Add User → Use Wizard.**

Precaución – Los nombres y los ID de los roles y usuarios provienen de la misma agrupación. No utilice nombres ni ID existentes para los usuarios que agregue.

3 **Siga la ayuda en pantalla.**

También puede seguir los procedimientos descritos en "How to Add a User With the Solaris Management Console's Users Tool" de *System Administration Guide: Basic Administration*.

4 **Después de crear el usuario, haga doble clic en el usuario creado para modificar los valores.**

Nota – Para los usuarios que puedan asumir roles, elija la opción Always Available para la cuenta y no establezca fechas de caducidad para las contraseñas.

Asegúrese de que los siguientes campos estén definidos correctamente:

- Description: aquí no se introduce información de propiedad exclusiva.
- Password and confirm: asigne una contraseña de al menos 6 caracteres alfanuméricos.

  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.

- Account Availability: Always Available.
- Trusted Extensions Attributes: los valores predeterminados son correctos.

  Para un sistema de una sola etiqueta en el que las etiquetas no deben estar visibles, elija Hide para Label: Show or Hide.
- Account Usage: defina Idle time y Idle action.

  Lock account: defina No para cualquier usuario que pueda asumir un rol.

5 **Cierre Solaris Management Console.**

6 **Personalice el entorno de 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, puede permitir que los usuarios asignen dispositivos, impriman archivos PostScript, impriman sin etiquetas, inicien sesión de manera remota y cierren el sistema. Para crear el

perfil, consulte "Cómo crear perfiles de derechos para autorizaciones convenientes" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.

b. Personalice los archivos de inicialización de usuario.

Consulte el Capítulo 7, "Gestión de usuarios, derechos y roles en Trusted Extensions (tareas)" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.

Consulte también "Gestión de usuarios y derechos con Solaris Management Console (mapa de tareas)" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.

c. Cree archivos de copia y enlace de varias etiquetas.

En un sistema de varias etiquetas, 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" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.

Ejemplo 4–7 Uso del comando `useradd` para crear un usuario local

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

En primer lugar, el 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 usuario `root` consulta la Tabla 1–2 y crea el usuario.

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

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

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

Por último, el usuario `root` agrega el rol de administrador de la seguridad a la definición del usuario. El rol fue creado en la sección "Creación del rol de administrador de la seguridad en Trusted Extensions" en la página 93.

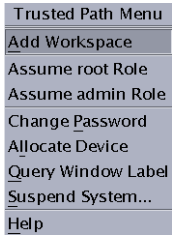
```
# usermod -R secadmin jandoe
```

Verificación del funcionamiento de los roles de Trusted Extensions

Para verificar cada rol, asuma el rol. A continuación, realice tareas que sólo ese rol puede realizar.

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. **Abra el menú Trusted Path.**
   - **En Trusted CDE, haga clic en el área de selección de espacios de trabajo.**

     Desde el menú, asuma el rol.
   - **En Trusted JDS, haga clic en su nombre de usuario, en la banda de confianza.**
     En la siguiente banda de confianza, el nombre de usuario es `tester`.

     De la lista de roles asignados, seleccione un rol.
3. **En el espacio de trabajo del rol, inicie Solaris Management Console.**

   ```
   $ /usr/sbin/smc &
   ```
4. **Seleccione el ámbito adecuado para el rol que está probando.**
5. **Haga clic en System Services y navegue hasta Users.**
   Se le solicitará una contraseña.
   a. **Escriba la contraseña del rol.**

b. Haga doble clic en User Accounts.

6 Haga clic en un usuario.

- El rol de administrador del sistema debería poder modificar los campos de las fichas General, Home Directory y Group.

  Si configuró los roles para aplicar la separación de tareas, el rol de administrador del sistema no puede establecer la contraseña inicial del usuario.
- El rol de administrador de la seguridad debería poder modificar los campos de todas las fichas.

  Si configuró los roles para aplicar la separación de tareas, el rol de administrador de la seguridad no puede crear un usuario.
- El rol de administrador principal debería poder modificar los campos de todas las fichas.

7 (Opcional) Si está aplicando la separación de tareas, impida la utilización de los perfiles de derechos predeterminados.

Nota – Cuando el sistema se actualiza a una versión más reciente del SO Solaris, los perfiles predeterminados de administrador del sistema, gestión de usuarios y seguridad del usuario se sustituyen.

En el editor confianza, realice uno de los siguientes pasos:

- **Elimine los tres perfiles de derechos del archivo `prof_attr`.**

  La eliminación impide que un administrador visualice o asigne estos perfiles. También elimine el archivo `prof_attr.orig`.

- **Comente los tres perfiles de derechos en el archivo `prof_attr`.**

  Al comentar los perfiles de derechos evita que estos perfiles se visualicen en Solaris Management Console o se utilicen en comandos para gestionar usuarios. Los perfiles y su contenido todavía se pueden ver en el archivo `prof_attr`.

- **Escriba una descripción diferente para los tres perfiles de derechos en el archivo `prof_attr`.**

  Edite el archivo `prof_attr` para cambiar el campo de descripción de estos perfiles de derechos. Por ejemplo, puede reemplazar las descripciones por `Do not use this profile`. Este cambio le advierte a un administrador que no utilice el perfil, pero no impide el uso del perfil.

▼ Habilitación de los usuarios para que inicien sesión en una zona con etiquetas

Cuando se reinicia el host, 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. Dicha zona no se debe estar utilizando para la clonación.

1. **Reinicie el sistema.**
2. **Inicie sesión como usuario `root`.**
3. **Reinicie el servicio zones.**

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

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

4. **Cierre la sesión.**

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

Creación de directorios principales en Trusted Extensions

En Trusted Extensions, los usuarios necesitan tener acceso a sus directorios principales en cada etiqueta en la que trabajan. Para que todos los directorios principales estén disponibles para el usuario, es necesario crear un servidor de directorio principal de varios niveles, ejecutar el montador automático en el servidor y exportar los directorios principales. En el sitio del cliente, puede ejecutar secuencias de comandos para encontrar el directorio principal para cada zona de cada usuario, o puede hacer que el usuario inicie sesión en el servidor de directorio principal.

▼ Creación del servidor de directorio principal en Trusted Extensions

Antes de empezar Debe ser superusuario, en el rol `root` o en el rol de administrador principal.

1. **Instale y configure el software de Trusted Extensions en el servidor de directorio principal.**
   - Si va a clonar zonas, asegúrese de utilizar un instantánea de ZFS de Solaris que tenga directorios principales vacíos.

- Debido a que los usuarios necesitan un directorio principal en cada etiqueta en la que pueden iniciar sesión, cree todas las zonas en las que el usuario puede iniciar sesión. Por ejemplo, si utiliza el archivo predeterminado `label_encodings`, debe crear una zona para la etiqueta `PUBLIC`.

2 Si está utilizando UFS y no ZFS de Solaris, habilite el servidor NFS para que se preste servicio a sí mismo.

a. En la zona global, modifique la entrada `automount` en el archivo `nsswitch.conf`.

Utilice el editor de confianza para editar el archivo `/etc/nsswitch.conf`. Para conocer el procedimiento, consulte "Cómo editar archivos administrativos en Trusted Extensions" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.

```
automount: files
```

b. En la zona global, ejecute el comando `automount`.

3 Para cada zona con etiquetas, siga el procedimiento de montaje automático en "Cómo montar archivos en NFS en una zona con etiquetas" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*. A continuación, regrese a este procedimiento.

4 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.

5 Cierre la sesión del servidor de directorio principal.

▼ Habilitación de los usuarios para que accedan a sus directorios principales en Trusted Extensions

Los usuarios, en principio, pueden iniciar sesión en el servidor de directorio principal para crear un directorio principal que se pueda compartir con otros sistemas. Para crear un directorio principal en cada etiqueta, cada usuario debe iniciar sesión en el servidor de directorio principal, en cada etiqueta.

Como alternativa, usted, como administrador, puede crear una secuencia de comandos para crear un punto de montaje para directorios principales en el sistema principal de cada usuario, antes de que el usuario inicie sesión por primera vez. La secuencia de comandos crea puntos de montaje en cada etiqueta en la que el usuario está autorizado a trabajar.

Antes de empezar El servidor de directorio principal para su dominio de Trusted Extensions debe estar configurado.

- **Seleccione si se permite el inicio de sesión directo en el servidor o si se debe ejecutar una secuencia de comandos.**
  - **Habilite a los usuarios para que inicien sesión directamente en el servidor de directorio principal.**
    a. **Indique a cada usuario que inicie sesión en el servidor de directorio principal.**
       Una vez que el usuario haya iniciado sesión correctamente, deberá cerrar sesión.
    b. **Indique a cada usuario que vuelva a iniciar sesión y que, esta vez, seleccione una etiqueta de inicio de sesión diferente.**
       El usuario utiliza el generador de etiquetas para seleccionar una etiqueta de inicio de sesión diferente. Una vez que el usuario haya iniciado sesión correctamente, deberá cerrar sesión.
    c. **Indique a cada usuario que repita el proceso de inicio de sesión para cada etiqueta que el usuario tiene permitido utilizar.**
    d. **Indique a los usuarios que inicien sesión desde su estación de trabajo habitual.**
       El directorio principal para su etiqueta predeterminada está disponible. 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.
  - **Escriba una secuencia de comandos que cree un punto de montaje de directorio principal para cada usuario, y ejecute la secuencia de comandos.**

```
#!/bin/sh
#
```

```
for zoneroot in ‘/usr/sbin/zoneadm list -p | cut -d ":" -f4‘ ; do
    if [ $zoneroot != / ]; then
        prefix=$zoneroot/root/export

        for j in ‘getent passwd|tr ’ ’ _‘ ; do
            uid=‘echo $j|cut -d ":" -f3‘
            if [ $uid -ge 100 ]; then
                gid=‘echo $j|cut -d ":" -f4‘
                homedir=‘echo $j|cut -d ":" -f6‘
                mkdir -m 711 -p $prefix$homedir
                chown $uid:$gid $prefix$homedir
            fi
        done
    fi
done
```

a. Desde la zona global, ejecute esta secuencia de comandos en el servidor NFS.

b. A continuación, ejecute esta secuencia de comandos en cada escritorio de varios niveles en el que el usuario vaya a iniciar sesión.

Adición de usuarios y hosts a una red de confianza existente

Si tiene usuarios que están definidos en mapas NIS, puede agregarlos a la red.

Para agregar hosts y etiquetas a hosts, consulte los siguientes procedimientos:

- Para agregar un host, utilice la herramienta Computers and Networks definida en Solaris Management Console. Para obtener detalles, consulte “Cómo agregar hosts a la red conocida del sistema” de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.

  Al agregar un host al servidor LDAP, agregue todas las direcciones IP que están asociadas con el host. Las direcciones para todas las zonas, incluidas las direcciones para zonas con etiquetas, se deben agregar al servidor LDAP.
- Para etiquetar un host, consulte “Cómo asignar una plantilla de seguridad a un host o a un grupo de hosts” de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.

▼ Adición de un usuario NIS al servidor LDAP

Antes de empezar Debe ser superusuario, en el rol `root` o en el rol de administrador principal.

1 Desde la base de datos NIS, recopile la información que necesita.

a. Cree un archivo a partir de la entrada del usuario en la base de datos `aliases`.

```
% ypcat -k aliases | grep login-name > aliases.name
```

b. Cree un archivo a partir de la entrada del usuario en la base de datos `passwd`.

```
% ypcat -k passwd | grep "Full Name" > passwd.name
```

c. Cree un archivo a partir de la entrada del usuario en la base de datos `auto_home_`.

```
% ypcat -k auto_home | grep login-name > auto_home_label
```

2 Cambie el formato de la información para LDAP y Trusted Extensions.

a. Utilice el comando `sed` para cambiar el formato de la entrada `alias`.

```
% sed 's/ /:/g' aliases.login-name > aliases
```

b. Utilice el comando `nawk` para cambiar el formato de la entrada `passwd`.

```
% nawk -F: '{print $1":x:"$3":"$4":"$5":"$6":"$7}' passwd.name > passwd
```

c. Utilice el comando `nawk` para crear una entrada `shadow`.

```
% nawk -F: '{print $1":"$2":6445::::::"}' passwd.name > shadow
```

d. Utilice el comando `nawk` para crear una entrada `user_attr`.

```
% nawk -F: '{print $1"::::lock_after_retries=yes-or-no;profiles=user-profile, ...;
labelview=int-or-ext,show-or-hide;min_label=min-label;
clearance=max-label;type=normal;roles=role-name,...;
auths=auth-name,..."}' passwd.name > user_attr
```

3 Copie los archivos modificados en el directorio `/tmp`, en el servidor LDAP.

```
# cp aliases auto_home_internal passwd shadow user_attr /tmp/name
```

4 Agregue las entradas de los archivos del Paso 3 a las bases de datos en el servidor LDAP.

```
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/aliases aliases
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/auto_home_internal auto_home_internal
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/passwd passwd
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/shadow shadow
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/user_attr user_attr
```

Ejemplo 4–8 Adición de un usuario de una base de datos NIS al servidor LDAP

En el siguiente ejemplo, el administrador agrega un usuario nuevo a la red de confianza. La información del usuario se almacena originalmente en una base de datos NIS. Para proteger la contraseña del servidor LDAP, el administrador ejecuta el comando `ldapaddent` en el servidor.

En Trusted Extensions, el usuario nuevo puede asignar dispositivos y asumir el rol de operador. Como el usuario puede asumir un rol, la cuenta de usuario no se bloquea. La etiqueta mínima del usuario es `PUBLIC`. La etiqueta en la que trabaja el usuario es `INTERNAL`, por lo que se agrega

jan a la base de datos auto_home_internal. La base de datos auto_home_internal monta automáticamente el directorio principal de jan con permisos de lectura y escritura.

- En el servidor LDAP, el administrador extrae la información del usuario de las bases de datos NIS.

```
# ypcat -k aliases | grep jan.doe > aliases.jan
# ypcat passwd | grep "Jan Doe" > passwd.jan
# ypcat -k auto_home | grep jan.doe > auto_home_internal
```

- Luego, el administrador cambia el formato de las entradas para LDAP.

```
# sed 's/ /:/g' aliases.jan > aliases
# nawk -F: '{print $1":x:"$3":"$4":"$5":"$6":"$7}' passwd.jan > passwd
# nawk -F: '{print $1":"$2":6445::::::"}' passwd.jan > shadow
```

- A continuación, el administrador crea una entrada user_attr para Trusted Extensions.

```
# nawk -F: '{print $1"::::lock_after_retries=no;profiles=Media User;
labelview=internal,showsl;min_label=0x0002-08-08;
clearance=0x0004-08-78;type=normal;roles=oper;
auths=solaris.device.allocate"}' passwd.jan > user_attr
```

- Luego, el administrador copia los archivos en el directorio /tmp/jan.

```
# cp aliases auto_home_internal passwd shadow user_attr /tmp/jan
```

- Por último, el administrador rellena el servidor con los archivos del directorio /tmp/jan.

```
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/aliases aliases
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/auto_home_internal auto_home_internal
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/passwd passwd
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/shadow shadow
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/user_attr user_attr
```

Resolución de los problemas de configuración de Trusted Extensions

En Trusted Extensions, las zonas con etiquetas se comunican con el servidor X mediante la zona global. Por lo tanto, las zonas con etiquetas debe tener rutas utilizables a la zona global. Además, las opciones que se seleccionaron durante una instalación de Solaris pueden impedir que Trusted Extensions utilice interfaces para acceder a la zona global.

`netservices limited` se ejecutó después de que se habilitó Trusted Extensions

Descripción:

En lugar de ejecutar el comando `netservices limited` antes de habilitar Trusted Extensions, ejecutó el comando en la zona global posteriormente. Por lo tanto, las zonas con etiquetas no se pueden conectar al servidor X en la zona global.

Solución:

Ejecute los siguientes comandos para abrir los servicios que Trusted Extensions requiere para la comunicación entre zonas:

```
# svccfg -s x11-server setprop options/tcp_listen = true
# svcadm enable svc:/network/rpc/rstat:default
```

No se puede abrir la ventana de consola en una zona con etiquetas

Descripción:

Cuando intenta abrir una ventana de consola en una zona con etiquetas, aparece el siguiente error en un cuadro de diálogo:

```
Action:DttermConsole,*,*,*,0 [Error]
Action not authorized.
```

Solución:

Compruebe que las siguientes dos líneas estén presentes en todas las entradas de la zona en el archivo `/etc/security/exec_attr`:

```
All Actions:solaris:act:::*;*;*;*;*:
All:solaris:act:::*;*;*;*;*:
```

Si estas líneas no están presentes, el paquete de Trusted Extensions que agrega estas entradas no se instaló en las zonas con etiquetas. En este caso, vuelva a crear las zonas con etiquetas. Para conocer el procedimiento, consulte "Creación de zonas con etiquetas" en la página 66.

La zona con etiquetas no puede acceder al servidor X

Descripción:

Si una zona con etiquetas no puede acceder correctamente al servidor X, es posible que vea mensajes como los siguientes:

- `Action failed. Reconnect to Solaris Zone?`
- `No route available`
- `Cannot reach globalzone-`*`nombre_host`* `:0`

Causa:

Es posible que las zonas con etiquetas no puedan acceder al servidor X por cualquiera de los siguientes motivos:

- La zona no se ha inicializado y está esperando que finalice el proceso `sysidcfg`.
- El servicio de nombres que se ejecuta en la zona global no reconoce el nombre del host de la zona con etiquetas.
- No se especificó ninguna interfaz `all-zones`.
- La interfaz de red de la zona con etiquetas está inactiva.
- Las consultas de nombres de LDAP fallaron.
- Los montajes de NFS no funcionan.

Pasos para la resolución del problema:

Realice lo siguiente:

1. Inicie sesión en la zona.

   Puede utilizar el comando `zlogin` o la acción Zone Terminal Console.

   ```
   # zlogin -z zone-name
   ```

   Si no puede iniciar sesión como superusuario, utilice el comando `zlogin -S` para omitir la autenticación.
2. Compruebe que la zona se esté ejecutando.

   ```
   # zoneadm list
   ```

   Si una zona tiene el estado `running`, la zona está ejecutando al menos un proceso.
3. Solucione cualquier problema que impida el acceso de las zonas con etiquetas al servidor X.
   - Inicialice la zona mediante la finalización del proceso `sysidcfg`.

     Ejecute el programa `sysidcfg` de manera interactiva. Responda a las peticiones de datos en Zone Terminal Console o en la ventana de terminal en la que ejecutó el comando `zlogin`.

Para ejecutar el proceso `sysidcfg` de manera no interactiva, puede realizar una de las siguientes acciones:

- Especifique la opción Initialize para la secuencia de comandos `/usr/sbin/txzonemgr`.

  La opción Initialize permite proporcionar valores predeterminados para las preguntas de `sysidcfg`.
- Escriba su propia secuencia de comandos `sysidcfg`.

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

- Verifique que el servidor X esté disponible para la zona.

  Inicie sesión en la zona con etiquetas. Defina la variable `DISPLAY` para que apunte al servidor X, y abra una ventana.

  ```
  # DISPLAY=global-zone-hostname:n.n
  # export DISPLAY
  # /usr/openwin/bin/xclock
  ```

  Si no aparece una ventana con etiquetas, la configuración de las redes de zona no se realizó correctamente para esa zona con etiquetas.

  Nota – Si está ejecutando Trusted CDE, a partir de la versión Solaris 10 5/09, consulte "Resolución de enrutamiento de zona local a zona global en Trusted CDE" en la página 163.

- Configure el nombre de host de la zona con el servicio de nombres.

  El archivo `/etc/hosts` local de la zona no se utiliza. En su lugar, se debe especificar información equivalente en la zona global o en el servidor LDAP. La información debe incluir la dirección IP del nombre de host asignado a la zona.
- No se especificó ninguna interfaz `all-zones`.

  A menos que todas las zonas tengan direcciones IP en la misma subred que la zona global, es posible que deba configurar una interfaz `all-zones` (compartida). Esta configuración permite la conexión de una zona con etiquetas al servidor X de la zona global. Si desea restringir las conexiones remotas al servidor X de la zona global, puede usar `vni0` como dirección `all-zones`.

  Si *no* desea configurar una interfaz`all-zones`, debe proporcionar una ruta al servidor X de la zona global para cada zona. Estas rutas se deben configurar en la zona global.
- La interfaz de red de la zona con etiquetas está inactiva.

  ```
  # ifconfig -a
  ```

Utilice el comando `ifconfig` para verificar que la interfaz de red de la zona con etiquetas tenga los indicadores `UP` y `RUNNING`.

- Las consultas de nombres de LDAP fallaron.

  Utilice el comando `ldaplist` para verificar que cada zona pueda comunicarse con el servidor LDAP o el servidor proxy LDAP. En el servidor LDAP, compruebe que la zona aparezca en la base de datos `tnrhdb`.

- Los montajes de NFS no funcionan.

  Como superusuario, reinicie `automount` en la zona. O bien, agregue una entrada `crontab` para ejecutar el comando `automount` cada cinco minutos.

Tareas adicionales de configuración de Trusted Extensions

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

▼ Cómo copiar archivos en medios portátiles en Trusted Extensions

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

Nota – Durante la configuración de Trusted Extensions, el superusuario, o un rol equivalente, copia los archivos administrativos a un medio portátil y desde él. Etiquete los medios con `Trusted Path`.

Antes de empezar Para copiar los archivos administrativos, debe ser superusuario o un rol en la zona global.

1 Asigne el dispositivo adecuado.

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

- En Solaris Trusted Extensions (CDE), un *gestor de archivos* muestra el contenido del medio portátil.
- En Solaris Trusted Extensions (JDS), un *explorador de archivos* muestra el contenido.

En este procedimiento, el explorador de archivos se utiliza para hacer referencia a esta interfaz gráfica de usuario.

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

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

   Por ejemplo, puede haber copiado los archivos a una carpeta `/export/clientfiles`.

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

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

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

5. **Desasigne el dispositivo.**

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

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

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

Ejemplo 4–9 Mantenimiento de los mismos archivos de configuración en todos los sistemas

El administrador del sistema debe asegurarse de que todos los equipos estén configurados con los mismos valores. Por lo tanto, en el primer equipo que configura, 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, copia la caja de herramientas de Trusted Extensions que Solaris Management Console utiliza para el ámbito LDAP, `/var/sadm/smc/toolboxes/tsol_ldap/tsol_ldap.tbx`. El administrador personalizó las plantillas de host remoto en el archivo `tnrhtp`, tiene una lista de servidores DNS y archivos de configuración de auditoría. Asimismo, modificó el archivo `policy.conf` para su sitio. Entonces, copia los archivos al directorio permanente.

```
# mkdir /export/commonfiles
# cp  /etc/security/policy.conf \
/etc/security/audit_control \
/etc/security/audit_startup \
/etc/security/tsol/tnrhtp \
/etc/resolv.conf \
/etc/nsswitch.conf \
/export/commonfiles
```

Utiliza Device Allocation Manager para asignar un disquete en la zona global, y transfiere los archivos al disquete. En un disquete aparte, con etiqueta `ADMIN_HIGH`, coloca el archivo `label_encodings` para el sitio.

Cuando copia los archivos en un sistema, modifica las entradas `dir:` en el archivo `/etc/security/audit_control` para ese sistema.

▼ Cómo copiar archivos desde medios portátiles en Trusted Extensions

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

Antes de empezar Para copiar los archivos administrativos, debe ser superusuario o un rol en la zona global.

1. **Asigne el dispositivo adecuado.**

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

   - En Solaris Trusted Extensions (CDE), un *gestor de archivos* muestra el contenido del medio portátil.
   - En Solaris Trusted Extensions (JDS), un *explorador de archivos* muestra el contenido.

   En este procedimiento, el explorador de archivos se utiliza para hacer referencia a esta interfaz gráfica de usuario.

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

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

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

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

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

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

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

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

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

7 **Desasigne el dispositivo.**

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

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

Ejemplo 4–10 Carga de archivos de configuración de auditoría en Trusted Extensions

En este ejemplo, los roles aún no están configurados en el sistema. El usuario `root` necesita copiar archivos de configuración en el medio portátil. El contenido de los medios luego se copiará a otros sistemas. Estos archivos se copiarán en cada sistema en el que esté configurado el software de Trusted Extensions.

El usuario `root` asigna el dispositivo `floppy_0` en Device Allocation Manager y responde `yes` a la consulta de montaje. A continuación, el usuario `root` inserta el disquete con los archivos de configuración y los copia en el disco. El disquete tiene la etiqueta `Trusted Path`.

Para leer desde el medio, el usuario `root` asigna el dispositivo en el host de recepción y, a continuación, descarga el contenido.

Si los archivos de configuración están en una cinta, el usuario `root` asigna el dispositivo `mag_0`. Si los archivos de configuración están en un CD-ROM, el usuario `root` asigna el dispositivo `cdrom_0`.

▼ Cómo eliminar Trusted Extensions del sistema

Para eliminar Trusted Extensions del sistema Solaris, debe realizar pasos específicos para eliminar las personalizaciones de Trusted Extensions del sistema Solaris.

1 **Como en el SO Solaris, archive todos los datos de las zonas con etiquetas que desee mantener.**

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

Para obtener detalles, consulte "How to Remove a Non-Global Zone" de *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*.

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

```
# svcadm disable labeld
```

4 **Ejecute el comando `bsmunconv`.**

Para ver el efecto de este comando, consulte la página del comando man `bsmunconv(1M)`.

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

6 Configure el sistema.

Es posible que deba configurar varios servicios para su sistema Solaris. Entre los candidatos se incluyen la auditoría, las funciones básicas de redes, los servicios de nombres y los montajes de sistemas de archivos.

◆ ◆ ◆ CAPÍTULO 5

Configuración de LDAP para Trusted Extensions (tareas)

En este capítulo se trata cómo configurar Sun Java System Directory Server y Solaris Management Console para su uso con Trusted Extensions. El servidor de directorios proporciona los servicios LDAP. LDAP es el servicio de nombres admitido para Trusted Extensions. Solaris Management Console es la interfaz gráfica de usuario administrativa para base de datos locales y LDAP.

Al configurar el servidor de directorios, dispone de dos opciones. Puede configurar un servidor LDAP en un sistema Trusted Extensions, o puede utilizar un servidor existente y conectarse a él mediante un servidor proxy Trusted Extensions. Siga las instrucciones de *uno* de los siguientes mapas de tareas:

- "Configuración de un servidor LDAP en un host de Trusted Extensions (mapa de tareas)" en la página 115
- "Configuración de un servidor proxy LDAP en un host de Trusted Extensions (mapa de tareas)" en la página 116

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

Tarea	Descripción	Para obtener instrucciones
Configure un servidor LDAP de Trusted Extensions.	Si no tiene un servidor Sun Java System Directory Server existente, convierta su primer sistema Trusted Extensions en el servidor de directorios. Este sistema no tiene zonas con etiquetas instaladas. Los demás sistemas Trusted Extensions son clientes de este servidor.	"Recopilación de información para el servidor de directorios para LDAP" en la página 117 "Instalación de Sun Java System Directory Server" en la página 118 "Configuración de los registros para Sun Java System Directory Server" en la página 123

Tarea	Descripción	Para obtener instrucciones
Agregue las bases de datos de Trusted Extensions al servidor.	Rellene el servidor LDAP con los datos de los archivos del sistema de Trusted Extensions.	"Rellenado de Sun Java System Directory Server" en la página 125
Configure Solaris Management Console para que funcione con el servidor de directorios.	Configure de forma manual una caja de herramientas LDAP para Solaris Management Console. La caja de herramientas se puede utilizar para modificar los atributos de Trusted Extensions en objetos de red.	"Configuración de Solaris Management Console para LDAP (mapa de tareas)" en la página 128
Configure los demás sistemas Trusted Extensions como clientes de este servidor.	Al configurar Trusted Extensions en otro sistema, convierta el sistema en un cliente de este servidor LDAP.	"Conversión de la zona global en un cliente LDAP en Trusted Extensions" en la página 62

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

Utilice este mapa de tareas si tiene un servidor Sun Java System Directory Server existente que se está ejecutando en un sistema Oracle Solaris.

Tarea	Descripción	Para obtener instrucciones
Agregue las bases de datos de Trusted Extensions al servidor.	La bases de datos de red de Trusted Extensions, `tnrhdb` y `tnrhtp`, se deben agregar al servidor LDAP.	"Rellenado de Sun Java System Directory Server" en la página 125
Configure un servidor proxy LDAP.	Convierta un sistema Trusted Extensions en el servidor proxy de los demás sistemas Trusted Extensions. Los demás sistemas Trusted Extensions utilizan este servidor proxy para acceder al servidor LDAP.	"Creación de un servidor proxy LDAP" en la página 128
Configure el servidor proxy para que tenga un puerto de varios niveles para LDAP.	Habilite el servidor proxy Trusted Extensions para que se pueda comunicar con el servidor LDAP en etiquetas específicas.	"Configuración de puerto de varios niveles para Sun Java System Directory Server" en la página 124
Configure Solaris Management Console para que funcione con el servidor proxy LDAP.	Configure de forma manual una caja de herramientas LDAP para Solaris Management Console. La caja de herramientas se puede utilizar para modificar los atributos de Trusted Extensions en objetos de red.	"Configuración de Solaris Management Console para LDAP (mapa de tareas)" en la página 128
Configure los demás sistemas Trusted Extensions como clientes del servidor proxy LDAP.	Al configurar Trusted Extensions en otro sistema, convierta el sistema en un cliente del servidor proxy LDAP.	"Conversión de la zona global en un cliente LDAP en Trusted Extensions" en la página 62

Configuración de Sun Java System Directory Server 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 está ejecutado el servicio de nombres LDAP, configure un Sun Java System Directory Server (servidor de directorios) en un sistema en el que esté configurado Trusted Extensions.

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

Nota – si no utiliza este servidor LDAP como un servidor NFS o como un servidor para clientes Sun Ray, no necesita instalar ninguna zona con etiquetas en este servidor.

▼ Recopilación de información para el servidor de directorios para LDAP

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

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

Petición de datos del asistente de instalación	Acción o información
Sun Java System Directory Server *versión*	
ID de usuario de administrador	El valor predeterminado es `admin`.
Contraseña de administrador	Cree una contraseña, como `admin123`.
DN del gestor de directorios	El valor predeterminado es `cn=Directory Manager`.
Contraseña del gestor de directorios	Cree una contraseña, como `dirmgr89`.
Root de servidor de directorios	El valor predeterminado es `/var/Sun/mps`. Esta ruta también se utiliza posteriormente si se intala el software de proxy.
Identificador del servidor	El valor predeterminado es el sistema local.

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

▼ Instalación de Sun Java System Directory Server

Los paquetes del servidor de directorios están disponibles en el sitio web de la puerta de enlace de software de Sun (`http://www.oracle.com/solaris`).

Antes de empezar

Debe estar en un sistema Trusted Extensions con sólo una zona global instalada. El sistema no debe tener zonas con etiquetas.

Los servidores LDAP de Trusted Extensions están configurados para los clientes que usan `pam_unix` para autenticarse en el depósito LDAP. Con `pam_unix`, las operaciones de contraseña y, por consiguiente, las directivas de contraseña son determinadas por el cliente. En concreto, la política establecida por el servidor LDAP no se utiliza. Para los parámetros de contraseña que puede establecer en el cliente, consulte "Gestión de información de contraseñas" de *Guía de administración del sistema: servicios de seguridad*. Para obtener información sobre `pam_unix`, consulte la página del comando man `pam.conf(4)`.

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

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

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

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

   En un sistema que se ejecute en una versión anterior a Solaris 10 8/07, agregue entradas IPv4 e IPv6 en el archivo `/etc/inet/ipnodes`. Las entradas de un sistema deben ser contiguas en el archivo.

   Si no está ejecutando la última versión del SO Solaris, debe tener los siguientes parches instalados. El primer número es un parche para SPARC. El segundo número es un parche para X86.

   - 138874–05, 138875–05: parche de conmutación de servicio de nombres LDAP, PAM nativo
   - 119313-35, 119314-36: parche de WBEM
   - 121308-21, 121308-21: parche de Solaris Management Console
   - 119315-20, 119316-20: parche de las aplicaciones de gestión de Solaris

2. **Encuentre los paquetes de Sun Java System Directory Server en el sitio web de Oracle Sun.**

   a. **En la página de la puerta de enlace de software de Sun (`http://www.oracle.com/solaris`), haga clic en la ficha Get It.**

   b. **Haga clic en la casilla de verificación correspondiente a Sun Java Identity Management Suite.**

   c. **Haga clic en el botón Submit.**

   d. **Si no está registrado, regístrese.**

   e. **Inicie sesión para descargar el software.**

   f. **Haga clic en Download Center, en la parte superior izquierda de la pantalla.**

   g. **En Identity Management, descargue el software más reciente adecuado para su plataforma.**

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

   Responda a las preguntas utilizando la información de "Recopilación de información para el servidor de directorios para LDAP" en la página 117. Para obtener una lista completa de las

preguntas, los valores predeterminados y las respuestas sugeridas, consulte el Capítulo 11, "Configuración de Sun Java System Directory Server con clientes LDAP (tareas)" de *Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP)*, y el Capítulo 12, "Configuración de clientes LDAP (tareas)" de *Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y 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 Habilite el programa `cacaoadm` y verifique que el programa esté habilitado.

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

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

Las plantillas para los servicios SMF para el servidor de directorios están en los paquetes de Sun Java System Directory Server.

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

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

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

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

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

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

8 Verifique la instalación.

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

```
SMF application name:  ds--export-home-ds-instances-your-instance
Instance version:      D-A00
```

Errores más frecuentes

Para conocer estrategias de resolución de problemas de configuración LDAP, consulte el Capítulo 13, "LDAP Troubleshooting (Reference)" de *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

▼ Creación de un cliente LDAP para el servidor de directorios

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

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

1 Instale Trusted Extensions en un sistema.

Puede utilizar el servidor de directorios de Trusted Extensions o instalar Trusted Extensions en un sistema aparte.

Nota – Si no está ejecutando la última versión del SO Solaris, debe tener los siguientes parches instalados. El primer número es un parche para SPARC. El segundo número es un parche para X86.

- 138874–05, 138875–05: parche de conmutación de servicio de nombres LDAP, PAM nativo
- 119313-35, 119314-36: parche de WBEM
- 121308-21, 121308-21: parche de Solaris Management Console
- 119315-20, 119316-20: parche de las aplicaciones de gestión de Solaris

---

2 En el cliente, modifique el archivo `/etc/nsswitch.ldap` predeterminado.

Las entradas en negrita indican las modificaciones. El archivo tiene el siguiente aspecto:

```
# /etc/nsswitch.ldap
#
# An example file that could be copied over to /etc/nsswitch.conf; it
# uses LDAP in conjunction with files.
#
# "hosts:" and "services:" in this file are used only if the
# /etc/netconfig file has a "-" for nametoaddr_libs of "inet" transports.

# LDAP service requires that svc:/network/ldap/client:default be enabled
# and online.

# the following two lines obviate the "+" entry in /etc/passwd and /etc/group.
passwd:     files ldap
```

```
group:      files ldap

# consult /etc "files" only if ldap is down.
hosts:      files ldap dns [NOTFOUND=return] files

# Note that IPv4 addresses are searched for in all of the ipnodes databases
# before searching the hosts databases.
ipnodes:    files ldap [NOTFOUND=return] files

networks:   files ldap [NOTFOUND=return] files
protocols:  files ldap [NOTFOUND=return] files
rpc:        files ldap [NOTFOUND=return] files
ethers:     files ldap [NOTFOUND=return] files
netmasks:   files ldap [NOTFOUND=return] files
bootparams: files ldap [NOTFOUND=return] files
publickey:  files ldap [NOTFOUND=return] files

netgroup:   ldap

automount:  files ldap
aliases:    files ldap

# for efficient getservbyname() avoid ldap
services:   files ldap

printers:   user files ldap

auth_attr:  files ldap
prof_attr:  files ldap

project:    files ldap

tnrhtp:     files ldap
tnrhdb:     files ldap
```

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

Este comando copia el archivo `nsswitch.ldap` al archivo `nsswitch.conf`.

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 profileNmae=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 *Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP)* y en la página del comando man `ldapclient`(1M).

▼ Configuración de los registros para Sun Java System Directory Server

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

- Todos los registros se habilitan y almacenan en la memoria intermedia.
- Los registros se colocan en el directorio `/export/home/ds/instances/`*su_instancia*`/logs/`*REGISTRO_TIPO* adecuado.
- Los eventos se registran en el nivel de registro 256.
- Los registros están protegidos por `600` permisos de archivo.
- Los registros de acceso rotan diariamente.
- Los registros de errores rotan semanalmente.

La configuración de este procedimiento cumple con los siguientes requisitos:

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

1 Configure los registros de acceso.

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

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

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

2 Configure los registros de auditoría.

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

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

3 **Configure los registros de errores.**

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

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

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

También puede configurar los siguientes valores de configuración para cada 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 Sun Java System Directory Server

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

1 **Inicie Solaris Management Console.**

```
# /usr/sbin/smc &
```

2 **Seleccione la caja de herramientas This Computer (*este host*: `Scope=Files, Policy=TSOL`).**

3 **Haga clic en System Configuration y, a continuación, en Computers and Networks.**

Se le solicitará la contraseña.

4 **Escriba la contraseña correspondiente.**

5 **Haga doble clic en Trusted Network Zones.**

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

7 **Agregue un puerto de varios niveles en el protocolo TCP:**

a. **Haga clic en Add para Multilevel Ports for Zone's IP Addresses.**

b. **Escriba 389 para el número de puerto y haga clic en OK.**

8 **Agregue un puerto de varios niveles para el protocolo UDP:**

   a. **Haga clic en Add para Multilevel Ports for Zone's IP Addresses.**

   b. **Escriba 389 para el número de puerto.**

   c. **Seleccione el protocolo udp y haga clic en OK.**

9 **Haga clic en OK para guardar la configuración.**

10 **Actualice el núcleo.**

```
# tnctl -fz /etc/security/tsol/tnzonecfg
```

▼ Rellenado de Sun Java System Directory Server

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

Antes de empezar

Debe rellenar la base de datos desde un cliente LDAP en el que esté habilitada la actualización de shadow. Para conocer los requisitos previos, consulte "Creación de un cliente LDAP para el servidor de directorios" en la página 121.

Si la seguridad del sitio requiere la separación de tareas, realice lo siguiente antes de llenar el servidor de directorios:

- "Creación de perfiles de derechos que aplican la separación de tareas" en la página 90
- "Creación del rol de administrador de la seguridad en Trusted Extensions" en la página 93
- "Creación de un rol de administrador del sistema restringido" en la página 96

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

Si está ejecutando la versión Solaris 10 11/06 sin los parches, copie el archivo `ipnodes`.

```
# cd /etc/inet
# cp ipnodes /setup/files
```

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

4 Elimine la entrada `?:::::?` del archivo `/setup/files/auth_attr`.

5 Elimine la entrada `::::` del archivo `/setup/files/prof_attr`.

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

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 de Trusted Extensions.

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

```
/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/&
```

7 Agregue todos los sistemas de la red al archivo `/setup/files/tnrhdb`.

Aquí no se puede utilizar ningún mecanismo comodín. Las direcciones IP de todos los sistemas con los que se establecerá contacto, incluidas las direcciones IP de las zonas con etiquetas, *deben* estar en este archivo.

a. Abra el editor de confianza y edite `/setup/files/tnrhdb`.

b. Agregue todas las direcciones IP de un sistema con etiquetas al dominio de Trusted Extensions.

Los sistemas con etiquetas son del tipo `cipso`. Además, el nombre de la plantilla de seguridad para los sistemas con etiquetas es `cipso`. Por lo tanto, en la configuración predeterminada, una entrada `cipso` es similar a la siguiente:

```
192.168.25.2:cipso
```

Nota – Esta lista incluye las direcciones IP de las zonas globales y las zonas con etiquetas.

c. Agregue todos los sistemas sin etiquetas con los que el dominio puede comunicarse.

Los sistemas sin etiquetas son del tipo `unlabeled`. El nombre de la plantilla de seguridad para los sistemas sin etiquetas es `admin_low`. Por lo tanto, en la configuración predeterminada, una entrada para un sistema sin etiquetas es similar a la siguiente:

```
192.168.35.2:admin_low
```

d. Guarde el archivo y salga del editor.

e. Compruebe la sintaxis del archivo.

```
# tnchkdb -h /setup/files/tnrhdb
```

f. Antes de continuar, corrija todos los errores.

8 Copie el archivo `/setup/files/tnrhdb` en el archivo `/etc/security/tsol/tnrhdb`.

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

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

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

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

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

```
# ldapclient -v uninit
```

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

Creación de un proxy de Trusted Extensions para un servidor Sun Java System Directory Server existente

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

▼ Creación de un servidor proxy LDAP

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

Antes de empezar

Debe haber rellenado el servidor LDAP a partir de un cliente que haya sido modificado para establecer el parámetro `enableShadowUpdate` en `TRUE`. Para conocer los requisitos, consulte "Creación de un cliente LDAP para el servidor de directorios" en la página 121.

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 Sun Java System Directory Server" en la página 125.

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`.

Para obtener detalles, consulte el Capítulo 12, "Configuración de clientes LDAP (tareas)" de *Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y 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 estrategias de resolución de problemas de configuración LDAP, consulte el Capítulo 13, "LDAP Troubleshooting (Reference)" de *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

Configuración de Solaris Management Console para LDAP (mapa de tareas)

Solaris Management Console es la interfaz gráfica de usuario para administrar la red de los sistemas que ejecutan Trusted Extensions.

Tarea	Descripción	Para obtener instrucciones
Inicialice Solaris Management Console.	Inicialice Solaris Management Console. Este procedimiento se realiza una vez por sistema en la zona global.	"Inicialización del servidor de Solaris Management Console en Trusted Extensions" en la página 59

Tarea	Descripción	Para obtener instrucciones
Registre las credenciales.	Autentique Solaris Management Console en el servidor LDAP.	"Registro de las credenciales LDAP en Solaris Management Console" en la página 129
Habilite la administración remota en un sistema.	De manera predeterminada, un cliente de Solaris Management Console no se puede comunicar con un servidor de consola de otro sistema. Debe habilitar explícitamente la administración remota.	"Habilitación de comunicaciones de red en Solaris Management Console" en la página 130
Cree la caja de herramientas LDAP.	Cree la caja de herramientas LDAP en Solaris Management Console para Trusted Extensions.	"Edición de la caja de herramientas LDAP en Solaris Management Console" en la página 131
?Verifique las comunicaciones.	Verifique que los hosts de Trusted Extensions puedan convertirse en clientes LDAP.	"Verificación de que Solaris Management Console contenga la información de Trusted Extensions" en la página 132

▼ Registro de las credenciales LDAP en Solaris Management Console

Antes de empezar

Debe ser el usuario `root` en un servidor LDAP en el que se esté ejecutando Trusted Extensions. El servidor puede ser un servidor proxy.

Su Sun Java System Directory Server debe estar configurado. Ha realizado una de las siguientes configuraciones:

- "Configuración de un servidor LDAP en un host de Trusted Extensions (mapa de tareas)" en la página 115
- "Configuración de un servidor proxy LDAP en un host de Trusted Extensions (mapa de tareas)" en la página 116

1 Registre las credenciales administrativas LDAP.

```
LDAP-Server # /usr/sadm/bin/dtsetup storeCred
Administrator DN:       Type the value for cn on your system
Password:       Type the Directory Manager password
Password (confirm):       Retype the password
```

2 Muestre los ámbitos en el servidor de directorios.

```
LDAP-Server # /usr/sadm/bin/dtsetup scopes
Getting list of manageable scopes...
Scope 1 file:       Displays name of file scope
Scope 2 ldap:       Displays name of ldap scope
```

La configuración del servidor LDAP determina los ámbitos que se muestran en la lista. El ámbito LDAP no aparecerá en la lista hasta que se haya editado la caja de herramientas LDAP. La caja de herramientas no se podrá editar hasta que se haya registrado el servidor.

Ejemplo 5–1 Registro de las credenciales LDAP

En este ejemplo, el nombre del servidor LDAP es `LDAP1` y el valor para `cn` es el valor predeterminado, `Directory Manager`.

```
# /usr/sadm/bin/dtsetup storeCred
Administrator DN:cn=Directory Manager
Password:abcde1;!
Password (confirm):abcde1;!
# /usr/sadm/bin/dtsetup scopes
Getting list of manageable scopes...
Scope 1 file:/LDAP1/LDAP1
Scope 2 ldap:/LDAP1/cd=LDAP1,dc=example-domain,dc=com
```

▼ Habilitación de comunicaciones de red en Solaris Management Console

De manera predeterminada, los sistemas Solaris no están configurados para recibir puertos que presentan riesgos de seguridad. Por lo tanto, debe configurar explícitamente cualquier sistema que pretenda administrar de manera remota para que acepte las comunicaciones de red. Por ejemplo, para administrar las bases de datos de red del servidor LDAP desde un cliente, el servidor de SMC; del servidor LDAP debe aceptar las comunicaciones de red.

Para ver una ilustración de los requisitos de configuración de Solaris Management Console para una red con un servidor LDAP, consulte "Comunicación cliente-servidor con Solaris Management Console" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.

Antes de empezar Debe ser superusuario en la zona global en el sistema de servidor de SMC;. En este procedimiento, ese sistema se denomina remoto. Asimismo, debe tener acceso como superusuario mediante la línea comandos al sistema cliente.

1. **Habilite las conexiones remotas en el sistema remoto.**

   El daemon `smc` se controla mediante el servicio `wbem`. Si la propiedad `options/tcp_listen` del servicio `wbem` se establece en `true`, el servidor de Solaris Management Console acepta las conexiones remotas.

   ```
   # /usr/sbin/svcprop -p options wbem
   options/tcp_listen boolean false
   # svccfg -s wbem setprop options/tcp_listen=true
   ```

2. **Actualice y reinicie el servicio `wbem`.**

   ```
   # svcadm refresh wbem
   # svcadm restart wbem
   ```

3. **Verifique que el servicio `wbem` esté configurado para aceptar conexiones remotas.**

```
# svcprop -p options wbem
options/tcp_listen boolean true
```

4. **En el sistema remoto y en cualquier cliente que necesite acceder a Solaris Management Console, asegúrese de que las conexiones remotas estén habilitadas en el archivo `smcserver.config`.**

   a. **Abra el archivo `smcserver.config` en el editor de confianza.**

```
# /usr/dt/bin/trusted_edit /etc/smc/smcserver.config
```

   b. **Establezca el parámetro `remote.connections` en `true`.**

```
## remote.connections=false
remote.connections=true
```

   c. **Guarde el archivo y salga del editor de confianza.**

Errores más frecuentes

Si reinicia o habilita el servicio `wbem`, debe asegurarse de que el parámetro `remote.connections` del archivo `smcserver.config` permanezca establecido en `true`.

▼ Edición de la caja de herramientas LDAP en Solaris Management Console

Antes de empezar

Debe ser superusuario en el servidor LDAP. Las credenciales LDAP deben estar registradas en Solaris Management Console, y debe conocer el resultado del comando `/usr/sadm/bin/dtsetup scopes`. Para obtener detalles, consulte "Registro de las credenciales LDAP en Solaris Management Console" en la página 129.

1. **Encuentre la caja de herramientas LDAP.**

```
# cd /var/sadm/smc/toolboxes/tsol_ldap
# ls *tbx
tsol_ldap.tbx
```

2. **Proporcione el nombre del servidor LDAP.**

   a. **Abra el editor de confianza.**

   b. **Copie y pegue el nombre de ruta completo de la caja de herramientas `tsol_ldap.tbx` como argumento en el editor.**

      Por ejemplo, la siguiente ruta es la ubicación predeterminada de la caja de herramientas LDAP:

```
/var/sadm/smc/toolboxes/tsol_ldap/tsol_ldap.tbx
```

c. Reemplace la información del ámbito.

Reemplace las marcas `server` entre las marcas `<Scope>` y `</Scope>` por el resultado de la línea `ldap:/.....` del comando `/usr/sadm/bin/dtsetup scopes`.

```
<Scope>ldap:/<ldap-server-name>/<dc=domain,dc=suffix></Scope>
```

d. Reemplace todas las instancias de `<?server?>` o `<?server ?>` por el servidor LDAP.

```
<Name>This Computer (ldap-server-name: Scope=ldap, Policy=TSOL)</Name>
services and configuration of ldap-server-name.</Description>
and configuring ldap-server-name.</Description>
...
```

e. Guarde el archivo y salga del editor.

3 Actualice y reinicie el servicio `wbem`.

```
# svcadm refresh wbem
# svcadm restart wbem
```

Ejemplo 5–2 Configuración de la caja de herramientas LDAP

En este ejemplo, el nombre del servidor LDAP es `LDAP1`. Para configurar la caja de herramientas, el administrador reemplaza las instancias de `<?server ?>` por `LDAP1`.

```
# cd /var/sadm/smc/toolboxes/tsol_ldap
# /usr/dt/bin/trusted_edit /tsol_ldap.tbx
<Scope>ldap:/LDAP1/cd=LDAP1,dc=example-domain,dc=com</Scope

...
<Name>This Computer (LDAP1: Scope=ldap, Policy=TSOL)</Name>
services and configuration of LDAP1.</Description>
and configuring LDAP1.</Description>
...
```

▼ Verificación de que Solaris Management Console contenga la información de Trusted Extensions

Para ver una ilustración de los requisitos de configuración de Solaris Management Console para una red con un servidor LDAP y para una red sin un servidor LDAP, consulte "Comunicación cliente-servidor con Solaris Management Console" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.

Antes de empezar

Debe iniciar sesión en un cliente LDAP con un rol administrativo o como superusuario. Para convertir un sistema en un cliente LDAP, consulte "Conversión de la zona global en un cliente LDAP en Trusted Extensions" en la página 62.

Para administrar el sistema local, debe haber completado "Inicialización del servidor de Solaris Management Console en Trusted Extensions" en la página 59.

Para conectarse a un servidor de consola de un sistema remoto desde el sistema local, debe haber completado "Inicialización del servidor de Solaris Management Console en Trusted Extensions" en la página 59 en ambos sistemas. Además, en el sistema remoto, debe haber completado "Habilitación de comunicaciones de red en Solaris Management Console" en la página 130.

Para administrar las bases de datos del servicio de nombres LDAP desde el cliente LDAP, en el servidor LDAP debe haber completado "Edición de la caja de herramientas LDAP en Solaris Management Console" en la página 131, además de los procedimientos mencionados anteriormente.

1 Inicie Solaris Management Console.

```
# /usr/sbin/smc &
```

2 Abra una caja de herramientas de Trusted Extensions.

Una caja de herramientas de Trusted Extensions tiene el valor `Policy=TSOL`.

- **En una red de confianza que utiliza LDAP como servicio de nombres, realice las siguientes pruebas:**

  a. **Para verificar que se pueda acceder a las bases de datos administrativas locales, abra la siguiente caja de herramientas:**

     `This Computer (`*este host*`: Scope=Files, Policy=TSOL)`

  b. **Para verificar que se pueda acceder a las bases de datos administrativas locales del servidor LDAP, especifique la siguiente caja de herramientas:**

     `This Computer (`*servidor ldap*`: Scope=Files, Policy=TSOL)`

  c. **Para verificar que se pueda acceder a las bases de datos del servicio de nombres del servidor LDAP, especifique la siguiente caja de herramientas:**

     `This Computer (`*servidor ldap*`: Scope=LDAP, Policy=TSOL)`

- **En una red de confianza que no utiliza LDAP como servicio de nombres, realice las siguientes pruebas:**

  a. **Para verificar que se pueda acceder a las bases de datos administrativas locales, abra la siguiente caja de herramientas:**

     `This Computer (`*este host*`: Scope=Files, Policy=TSOL)`

  b. **Para verificar que se pueda acceder a las bases de datos administrativas locales de un sistema remoto, especifique la siguiente caja de herramientas:**

     `This Computer (`*sistema remoto*`: Scope=Files, Policy=TSOL)`

3. **En System Configuration, navegue hasta Computers and Networks y, luego, hasta Security Templates.**

4. **Compruebe que se hayan aplicado las plantillas y etiquetas correctas a los sistemas remotos.**

Nota – Si intenta acceder a la información de la base de datos de la red desde un sistema distinto del servidor LDAP, la operación fallará. La consola le permite iniciar sesión en el host remoto y abrir la caja de herramientas. Sin embargo, si intenta acceder a la información o modificarla, el siguiente mensaje de error le indicará que ha seleccionado `Scope=LDAP` en un sistema distinto del servidor LDAP:

```
Management server cannot perform the operation requested.
...
Error extracting the value-from-tool.
The keys received from the client were machine, domain, Scope.
Problem with Scope.
```

Errores más frecuentes

Para resolver problemas de configuración de LDAP, consulte el Capítulo 13, "LDAP Troubleshooting (Reference)" de *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

◆ ◆ ◆ CAPÍTULO 6

Configuración de Trusted Extensions en un sistema sin periféricos (tareas)

Para configurar y administrar el software de Trusted Extensions en sistemas sin periféricos, como la serie Netra, es necesario modificar los valores de seguridad en el sistema sin periféricos para habilitar el acceso remoto. Para la administración de un sistema Trusted Extensions remoto se requiere una configuración similar. Para ejecutar una interfaz gráfica de usuario administrativa, es posible que tenga que ejecutar el proceso en el sistema remoto y mostrar la interfaz gráfica de usuario en el sistema de escritorio.

Para obtener una explicación de los requisitos, consulte el Capítulo 8, "Administración remota en Trusted Extensions (tareas)" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*

Nota – Los métodos de configuración que requieren los sistemas sin periféricos y remotos no cumplen con los criterios de una configuración evaluada. Para obtener más información, consulte "Comprensión de la política de seguridad del sitio" en la página 20.

Configuración de un sistema sin periféricos en Trusted Extensions (mapa de tareas)

En los sistemas sin periféricos, se conecta una consola por medio de una línea de serie a una ventana del emulador de terminal. La línea generalmente se protege mediante el comando `tip`. Según el tipo de sistema secundario que esté disponible, podrá utilizar uno de los siguientes métodos para configurar un sistema sin periféricos. En la siguiente tabla, los métodos aparecen ordenados del más seguro al menos seguro. Estas instrucciones también se aplican a los sistemas remotos.

Tarea	Descripción	Para obtener instrucciones
Habilite el inicio de sesión remoto por parte del usuario `root`.	Si no está utilizando LDAP, en principio, debe iniciar sesión en el sistema sin periféricos como usuario `root`. Si está utilizando LDAP, puede omitir este procedimiento.	"Habilitación del inicio de sesión remoto por parte del usuario `root` en Trusted Extensions" en la página 137
Habilite el inicio de sesión remoto.	Habilite el inicio de sesión remoto para un usuario que pueda asumir el rol de usuario `root` u otro rol administrativo.	"Habilitación del inicio de sesión remoto por parte de un rol en Trusted Extensions" en la página 137
	Habilite la administración de los sistemas de Trusted Extensions desde un sistema sin etiquetas.	"Habilitación del inicio de sesión remoto desde un sistema sin etiquetas" en la página 139
	Habilite a un usuario para que acceda a la zona global en un sistema sin periféricos.	"Cómo habilitar a usuarios específicos para que inicien sesión de manera remota en la zona global en Trusted Extensions" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*
(Opcional) Habilite la visualización de interfaces gráficas de usuario administrativas.	Habilite la visualización de las interfaces gráficas de usuario administrativas que se ejecutan en el sistema sin periféricos en el sistema de escritorio.	"Habilitación de la visualización remota de interfaces gráficas de usuario administrativas" en la página 141
(Opcional) Habilite la informática en red virtual (VNC, Virtual Network Computing).	Desde cualquier cliente, utiliza el servidor Xvnc en el sistema Trusted Extensions remoto para mostrar una sesión de varios niveles al cliente.	"Cómo utilizar Xvnc para acceder de manera remota a un sistema Trusted Extensions" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*
Seleccione una configuración y un método de administración para configurar el sistema sin periféricos.	Asuma un rol o conviértase en superusuario para administrar el sistema remoto.	"Uso de los comandos `rlogin` o `ssh` para iniciar sesión y administrar un sistema sin periféricos en Trusted Extensions" en la página 142
	Utilice Solaris Management Console en el sistema sin periféricos.	"Uso de una consola Solaris Management Console remota para administrar dentro del ámbito Files" en la página 140
	Si no tiene ningún sistema de ventanas, puede utilizar el inicio de sesión en serie como superusuario. Este procedimiento no es seguro.	No es necesario realizar ninguna configuración.

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

▼ Habilitación del inicio de sesión remoto por parte del usuario `root` en Trusted Extensions

Como en el SO Solaris, el usuario `root` puede iniciar una sesión de manera remota desde un sistema con etiquetas cuando la entrada `CONSOLE` está inhabilitada.

Si tiene previsto administrar un sistema remoto mediante la edición archivos locales, utilice este procedimiento.

1. **En el editor de confianza, quite el comentario de la línea `CONSOLE=` en el archivo `/etc/default/login`.**

   ```
   # /usr/dt/bin/trusted_edit /etc/default/login
   ```

   La línea editada tiene el siguiente aspecto:

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

2. **Permita que el usuario `root` inicie sesión mediante una conexión `ssh`.**

   Modifique el archivo `/etc/ssh/sshd_config`. De manera predeterminada, el comando `ssh` está habilitado en los sistemas Solaris.

   ```
   # /usr/dt/bin/trusted_edit /etc/ssh/sshd_config
   ```

   La línea editada tiene el siguiente aspecto:

   ```
   PermitRootLogin yes
   ```

Pasos siguientes Para iniciar sesión como usuario `root` desde un sistema sin etiquetas, también debe completar la sección "Habilitación del inicio de sesión remoto desde un sistema sin etiquetas" en la página 139.

Para habilitar el inicio de sesión remoto por parte de un rol, continúe con "Habilitación del inicio de sesión remoto por parte de un rol en Trusted Extensions" en la página 137.

▼ Habilitación del inicio de sesión remoto por parte de un rol en Trusted Extensions

Siga este procedimiento *sólo si* debe administrar un sistema sin periféricos mediante el comando `rlogin` o `ssh`.

Los errores de configuración se pueden depurar de manera remota.

Antes de empezar Si está utilizando archivos locales para administrar el sistema remoto, debe haber completado la sección "Habilitación del inicio de sesión remoto por parte del usuario `root` en Trusted Extensions" en la página 137. Por lo tanto, como usuario `root`, realice esta tarea en ambos sistemas.

1 En ambos sistemas, identifique al otro sistema como un sistema con etiquetas.

El sistema de escritorio y el sistema sin periféricos deben poder identificar que ambos están utilizando la misma plantilla de seguridad. Para conocer el procedimiento, consulte "Cómo asignar una plantilla de seguridad a un host o a un grupo de hosts" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.

Para asignar una etiqueta temporal, consulte el Ejemplo 6–1.

2 En ambos sistemas, cree usuarios y roles idénticos.

Los nombres y los ID deben ser idénticos, y el rol debe ser asignado al usuario en ambos sistemas. Para crear usuarios y roles, consulte "Creación de roles y usuarios en Trusted Extensions" en la página 90.

3 Para ponerse en contacto con una consola Solaris Management Console remota, realice las siguientes operaciones en ambos sistemas:

a. Agregue la dirección IP y el nombre de host del otro sistema al archivo `/etc/hosts`.

```
# /usr/dt/bin/trusted_edit /etc/hosts

127.0.0.1    localhost
192.168.66.66    local-system-name    loghost
192.168.12    remote-system-name
```

b. Para permitir la asunción de roles remotos, modifique el archivo `pam.conf` para flexibilizar la política de módulos de autentificación enlazables (PAM, Plugable Authentication Modules).

i. Copie el archivo `/etc/pam.conf` en `/etc/pam.conf.orig`.

```
# cp /etc/pam.conf /etc/pam.conf.orig
```

ii. En el editor de confianza, abra el archivo `pam.conf`.

```
# /usr/dt/bin/trusted_edit /etc/pam.conf
```

iii. Copie las entradas predeterminadas en la sección de gestión de cuentas.

iv. En cada entrada copiada, cambie `other` por `smcconsole`.

v. A la entrada copiada `pam_roles.so.1`, agréguele `allow_remote`.

Utilice la tecla Tab entre los campos. Esta sección ahora tiene un aspecto similar al siguiente:

```
# Solaris Management Console definition for Account management
#
smcconsole   account requisite   pam_roles.so.1   allow_remote
smcconsole   account required    pam_unix_account.so.1
smcconsole   account required    pam_tsol_account.so.1

# Default definition for Account management
# Used when service name is not explicitly mentioned for account management
#
other   account requisite    pam_roles.so.1
other   account required     pam_unix_account.so.1
other   account required     pam_tsol_account.so.1
```

vi. Guarde el archivo y salga del editor.

vii. (Opcional) Copie el archivo en `/etc/pam.conf.site`.

```
# cp /etc/pam.conf /etc/pam.conf.site
```

Si actualiza el sistema a una versión posterior, deberá evaluar si debe copiar los cambios del archivo `/etc/pam.conf.site` en el archivo `pam.conf`.

Ejemplo 6–1 Creación de una definición temporal de un tipo de host de Trusted Extensions

En este ejemplo, el administrador desea empezar a configurar un sistema Trusted Extensions remoto antes de que se configuren las definiciones de tipo de host. Para ello, el administrador utiliza el comando `tnctl` en el sistema remoto con el objetivo de definir de manera temporal el tipo de host del sistema de escritorio:

```
remote-TX# tnctl -h desktop-TX:cipso
```

Más tarde, el administrador desea acceder al sistema Trusted Extensions remoto desde un sistema de escritorio en el que no está configurado Trusted Extensions. En este caso, el administrador utiliza el comando `tnctl` en el sistema remoto para definir de manera temporal el tipo de host del sistema de escritorio como un sistema sin etiquetas que se ejecuta en la etiqueta `ADMIN_LOW`:

```
remote-TX# tnctl -h desktop-TX:admin_low
```

▼ Habilitación del inicio de sesión remoto desde un sistema sin etiquetas

Antes de empezar Este procedimiento no es seguro.

Debe haber flexibilizado la política de PAM para permitir la asunción de roles remotos, como se describe en "Habilitación del inicio de sesión remoto por parte de un rol en Trusted Extensions" en la página 137.

1 **En el sistema de confianza, aplique la plantilla de seguridad adecuada al sistema sin etiquetas.**

Precaución – Si utiliza los valores predeterminados, otro sistema sin etiquetas podría iniciar sesión en el sistema remoto y administrarlo. Por lo tanto, debe cambiar el valor predeterminado de la red `0.0.0.0` de `ADMIN_LOW` a una etiqueta diferente. Para conocer el procedimiento, consulte "Cómo limitar los hosts que se pueden contactar en la red de confianza" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.

2 **En el editor de confianza, abra el archivo `/etc/pam.conf`.**

```
# /usr/dt/bin/trusted_edit /etc/pam.conf
```

3 **Busque las entradas `smcconsole`.**

4 **Agregue `allow_unlabeled` al módulo `tsol_account`.**

Utilice la tecla Tab entre los campos.

```
smcconsole   account required  pam_tsol_account.so.1 allow_unlabeled
```

Después de las ediciones, esta sección se verá similar a la siguiente:

```
# Solaris Management Console definition for Account management
#
smcconsole  account  requisite      pam_roles.so.1    allow_remote
smcconsole  account  required       pam_unix_account.so.1
smcconsole  account  required       pam_tsol_account.so.1 allow_unlabeled
```

▼ Uso de una consola Solaris Management Console remota para administrar dentro del ámbito Files

Si no está utilizando LDAP y desea utilizar Solaris Management Console en un sistema remoto, debe habilitar la conexión remota a la consola. Este procedimiento no es suficiente para permitir el acceso al ámbito LDAP.

Para habilitar el acceso al ámbito LDAP, debe completar todos los procedimientos de la sección "Configuración de Solaris Management Console para LDAP (mapa de tareas)" en la página 128.

Antes de empezar Ambos sistemas son sistemas con etiquetas.

Debe haber completado los siguientes procedimientos:

- "Inicialización del servidor de Solaris Management Console en Trusted Extensions" en la página 59
- "Habilitación del inicio de sesión remoto por parte de un rol en Trusted Extensions" en la página 137

1. **Complete la sección "Habilitación de comunicaciones de red en Solaris Management Console" en la página 130.**

2. **En el sistema de escritorio, conviértase en un usuario que esté definido de la misma manera en ambos sistemas.**

3. **En el sistema de escritorio, asuma el rol que se define de la misma manera en ambos sistemas.**

4. **En el sistema de escritorio, inicie Solaris Management Console.**

   ```
   # /usr/sbin/smc &
   ```

5. **En el cuadro de diálogo del servidor, escriba el nombre del sistema sin periféricos.**

   A continuación, seleccione la caja de herramientas `Scope=Files`.

   `This Computer (`*sistema remoto*`: Scope=Files, Policy=TSOL)`

▼ Habilitación de la visualización remota de interfaces gráficas de usuario administrativas

El procedimiento para la visualización remota en un escritorio es idéntico al procedimiento en un sistema Solaris en el que no está configurado Trusted Extensions. Este procedimiento se coloca aquí para su comodidad.

1. **En el sistema de escritorio, habilite la visualización de los procesos del sistema sin periféricos.**

   a. **Habilite el acceso del sistema sin periféricos al servidor X en el sistema de escritorio.**

      desktop `$ xhost +` *headless-host*

   b. **Determine el valor de la variable `DISPLAY` del escritorio.**

      desktop `$ echo $DISPLAY`
      `:`*n*`.`*n*

2. **En el sistema sin periféricos, establezca la variable `DISPLAY` en el sistema de escritorio.**

   headless `$ DISPLAY=`*desktop*`:`*n*`.`*n*
   headless `$ export DISPLAY=`*n*`:`*n*

▼ Uso de los comandos `rlogin` o `ssh` para iniciar sesión y administrar un sistema sin periféricos en Trusted Extensions

Este procedimiento le permite utilizar la línea de comandos y la interfaz gráfica de usuario `txzonemgr` para administrar un sistema sin periféricos como superusuario o como un rol.

Nota – El inicio de sesión remoto mediante el comando `rlogin` es menos seguro que el inicio de sesión remoto mediante el comando `ssh`.

Para utilizar Solaris Management Console para administrar un sistema remoto no necesita utilizar un comando de inicio de sesión remoto. Para conocer el procedimiento, consulte "Cómo administrar sistemas de manera remota con Solaris Management Console desde un sistema Trusted Extensions" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.

Antes de empezar

Debe haber completado la sección "Habilitación del inicio de sesión remoto por parte de un rol en Trusted Extensions" en la página 137.

Debe ser un usuario habilitado para iniciar sesión en el sistema sin periféricos con ese mismo nombre e ID de usuario, y debe poder asumir el mismo rol en el sistema sin periféricos y en el sistema de escritorio.

1 En el sistema de escritorio, habilite la visualización de los procesos del sistema sin periféricos.

```
desktop $ xhost + headless-host
desktop $ echo $DISPLAY
:n.n
```

2 Asegúrese de ser el usuario que está definido de la misma manera en ambos sistemas.

3 Desde una ventana de terminal, inicie sesión de manera remota en el sistema sin periféricos.

- **Utilice el comando `ssh` para iniciar sesión:**

```
desktop $ ssh -l identical-username headless
Password:       Type the user's password
headless $
```

- **O bien, utilice el comando `rlogin` para iniciar sesión:**

```
desktop # rlogin headless
Password:       Type the user's password
headless $
```

4 Asuma el rol que está definido de la misma manera en ambos sistemas.

Utilice la misma ventana de terminal. Por ejemplo, asuma el rol `root`.

```
headless $ su - root
Password:      Type the root password
```

Ahora está en la zona global. Ahora puede utilizar este terminal para administrar el sistema sin periféricos desde la línea de comandos.

5 Habilite la visualización de los procesos del sistema sin periféricos en el sistema de escritorio.

Nota – También puede visualizar las interfaces gráficas de usuario remotas iniciando sesión con el comando`ssh -X`. Para obtener más información, consulte la página del comando man `ssh(1)`. Si desea ver un ejemplo, consulte el Ejemplo 6–2.

```
headless $  DISPLAY desktop:n.n
headless $ export DISPLAY=n:n
```

Ahora puede administrar el sistema sin periféricos mediante las interfaces gráficas de usuario de Trusted Extensions. Por ejemplo, inicie la interfaz gráfica de usuario `txzonemgr`:

```
headless $ /usr/sbin/txzonemgr
```

Labeled Zone Manager se ejecuta en el sistema remoto y se visualiza en el sistema de escritorio.

6 (Opcional) Acceda a las acciones de Trusted CDE.

Para abrir y cerrar de manera segura el gestor de aplicaciones, consulte "Cómo administrar Trusted Extensions con dtappsession de manera remota" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.

Ejemplo 6–2 Configuración de zonas con etiquetas en un sistema sin periféricos

En este ejemplo, el administrador utiliza la interfaz gráfica de usuario `txzonemgr` para configurar zonas con etiquetas en un sistema sin periféricos con etiquetas desde un sistema de escritorio con etiquetas. Como en el SO Solaris, el administrador habilita el acceso del sistema de escritorio al servidor X utilizando la opción `-X` para el comando `ssh`. El usuario `install1` está definido de la misma manera en ambos sistemas y puede asumir el rol `remoterole`.

```
TXdesk1 $ xhost + TXnohead4
TXdesk1 $ whoami
install1

TXdesk1 $ ssh -X -l install1 TXnohead4
Password: Ins1PwD1
TXnohead4 $
```

Para acceder a la zona global, el administrador asume el rol `remoterole`. Este rol está definido de la misma manera en ambos sistemas.

```
TXnohead4 # su - remoterole
Password: abcd1EFG
```

A continuación, el administrador inicia la interfaz gráfica de usuario `txzonemgr`.

```
TXnohead4 $ /usr/sbin/txzonemgr &
```

Labeled Zone Manager se ejecuta en el sistema sin periféricos y se visualiza en el sistema de escritorio.

◆ ◆ ◆ APÉNDICE A

Política de seguridad del sitio

En este apéndice se explican los problemas de la política de seguridad del sitio, y se sugieren sitios web y manuales de referencia para obtener más información:

Creación y gestión de una política de seguridad

Cada sitio de Trusted Extensions es único y debe determinar su propia política de seguridad. Realice las siguientes tareas al crear y gestionar una política de seguridad.

- Establezca un equipo de seguridad. El equipo de seguridad debe tener representación de la gerencia superior, la gerencia de personal, los administradores y la gerencia de sistemas informáticos, y la gerencia de utilidades. El equipo debe revisar las políticas y los procedimientos de los administradores de Trusted Extensions y recomendar las políticas de seguridad generales que se aplican a todos los usuarios del sistema.
- Informe al personal de gestión y administración sobre la política de seguridad del sitio. Todo el personal que participa en la gestión y administración del sitio debe estar familiarizado con la política de seguridad. Las políticas de seguridad no se deben poner a disposición de los usuarios comunes porque esta información de la política está directamente relacionada con la seguridad de los sistemas informáticos.
- Informe a los usuarios sobre la política de seguridad y el software de Trusted Extensions. Todos los usuarios deben estar familiarizados con la *Guía del usuario de Oracle Solaris Trusted Extensions*. Debido a que los usuarios, generalmente, son los primeros en saber cuándo un sistema no está funcionando normalmente, el usuario debe familiarizarse con el

sistema e informar sobre los problemas a un administrador del sistema. Un entorno seguro requiere que los usuarios notifiquen a los administradores del sistema inmediatamente si notan alguna de las siguientes irregularidades:

- Una discrepancia en la fecha y hora del último inicio de sesión que se informa al principio de cada sesión
- Un cambio poco común en los datos de un archivo
- Una copia impresa legible perdida o robada
- La incapacidad de utilizar una función de usuario

- Aplique la política de seguridad. Si la política de seguridad no se respeta y no se aplica, los datos incluidos en el sistema en el que está configurado Trusted Extensions no estarán protegidos. Es preciso establecer procedimientos para registrar cualquier problema y las medidas que se han tomado para resolver los incidentes.
- Revise periódicamente la política de seguridad. El equipo de seguridad debe llevar a cabo una revisión periódica de la política de seguridad y de todos los incidentes que se produjeron desde la última revisión. Los ajustes en esta política pueden ayudar a aumentar la seguridad.

Política de seguridad del sitio y Trusted Extensions

El administrador de la seguridad debe diseñar la red de Trusted Extensions en función de la política de seguridad del sitio. La política de seguridad dicta las decisiones relacionadas con la configuración, como las siguientes:

- Cuántas auditorías se realizan para todos los usuarios y para qué clases de eventos
- Cuántas auditorías se realizan para los usuarios con roles y para qué clases de eventos
- Cómo se gestionan, archivan y revisan los datos de la auditoría
- Qué etiquetas se utilizan en el sistema y si las etiquetas `ADMIN_LOW` y `ADMIN_HIGH` estarán visibles para los usuarios comunes
- Qué acreditaciones de usuario se asignan a las personas
- Qué dispositivos (si los hay) se pueden asignar por qué usuarios comunes
- Qué rangos de etiqueta se definen para los sistemas, las impresoras y otros dispositivos
- Si Trusted Extensions se utiliza en una configuración evaluada o no

Recomendaciones de seguridad informática

Considere la siguiente lista de directrices cuando desarrolle una política de seguridad para el sitio.

- Asigne la etiqueta máxima de un sistema con Trusted Extensions para que no sea mayor que el nivel de máxima seguridad del trabajo que se está realizando en el sitio.
- Registre de forma manual los cierres, los fallos de energía y los reinicios del sistema en un registro del sitio.
- Documente el daño en el sistema de archivos y analice todos los archivos afectados para verificar posibles infracciones de la política de seguridad.
- Restrinja los manuales de funcionamiento y la documentación del administrador a aquellas personas que realmente tengan la necesidad de acceder a dicha información.
- Informe y documente el comportamiento inusual o inesperado de cualquier software de Trusted Extensions y determine la causa.
- Si es posible, asigne, al menos, dos personas para administrar los sistemas en los que esté configurado Trusted Extensions. Asigne a una persona la autorización de administrador de la seguridad para tomar las decisiones relacionadas con la seguridad. Asigne a la otra persona la autorización de administrador del sistema para realizar las tareas de gestión del sistema.
- Establezca una rutina de copia de seguridad regular.
- Asigne autorizaciones sólo a los usuarios que las necesiten y que sepa que las usarán adecuadamente.
- Asígneles privilegios sólo para los programas que necesitan para realizar su trabajo, y sólo una vez que se hayan examinado los programas y se haya comprobado que se les puede confiar el uso del privilegio. Revise los privilegios en los programas de Trusted Extensions existentes como guía para el establecimiento de privilegios en programas nuevos.
- Revise y analice la información de auditoría con regularidad. Investigue los eventos irregulares para determinar la causa del evento.
- Minimice el número de identificadores de administración.
- Minimice el número de programas de setuid y setgid. Utilice autorizaciones, privilegios y roles para ejecutar el programa y para evitar el uso indebido.
- Asegúrese de que un administrador verifique con regularidad que los usuarios comunes tengan un shell de inicio de sesión válido.
- Asegúrese de que un administrador verifique con regularidad que los usuarios comunes tengan valores de ID de usuario válidos en lugar de valores de ID de administración del sistema.

Recomendaciones de seguridad física

Considere la siguiente lista de directrices cuando desarrolle una política de seguridad para el sitio.

- Restrinja el acceso a los sistemas en los que está configurado Trusted Extensions. Las ubicaciones más seguras generalmente son cuartos interiores que no se encuentran en la planta baja.
- Supervise y documente el acceso a los sistemas en los que esté configurado Trusted Extensions.
- Sujete el equipo informático a objetos grandes como mesas y escritorios para impedir robos. Cuando fije un equipo a un objeto de madera, aumente la solidez del objeto agregando placas de metal.
- Evalúe la posibilidad de utilizar medios de almacenamiento extraíbles para la información confidencial. Bloquee todos los medios extraíbles cuando no se estén utilizando.
- Almacene los archivos y las copias de seguridad del sistema en una ubicación segura separada de la ubicación de los sistemas.
- Restrinja el acceso físico a los medios de archivo y las copias de seguridad en la misma forma en que restringe el acceso a los sistemas.
- Instale una alarma de alta temperatura en la instalación informática para indicar si la temperatura está fuera del rango de las especificaciones del fabricante. Un rango sugerido es de 10 °C a 32 °C (50 °F a 90 °F).
- Instale una alarma de agua en la instalación informática para que indique si hay agua en el piso, en la cavidad del subsuelo y en el techo.
- Instale una alarma de humo para indicar la presencia de fuego y un sistema de extinción de fuego.
- Instale una alarma de humedad para indicar si hay mucha o poca humedad.
- Si las máquinas no lo tienen, tenga en cuenta el aislamiento TEMPEST. El aislamiento TEMPEST puede ser adecuado para las paredes, el suelo y el techo de la instalación.
- Permita que sólo técnicos certificados abran y cierren el equipo TEMPEST para garantizar su capacidad para aislar la radiación electromagnética.
- Controle la existencia de huecos físicos que permitan la entrada a las instalaciones o a las salas que contienen equipo informático. Busque aberturas debajo de pisos elevados, en techos falsos, en el equipo de ventilación del techo y en paredes linderas entre las adiciones originales y secundarias.
- Prohíba comer, beber y fumar en las instalaciones informáticas o cerca del equipo informático. Establezca las áreas donde estas actividades se pueden realizar sin poner en peligro el equipo informático.
- Proteja los dibujos y diagramas arquitectónicos de la instalación informática.

- Restrinja el uso de diagramas del edificio, mapas de piso y fotografías de la instalación informática.

Recomendaciones de seguridad del personal

Considere la siguiente lista de directrices cuando desarrolle una política de seguridad para el sitio.

- Inspeccione los paquetes, los documentos y los medios de almacenamiento cuando lleguen al sitio protegido y antes de que lo abandonen.
- Exija que todo el personal y los visitantes utilicen credenciales de identificación en todo momento.
- Utilice credenciales de identificación que sean difíciles de copiar o falsificar.
- Establezca qué áreas están prohibidas para los visitantes y márquelas claramente.
- Acompañe a los visitantes en todo momento.

Infracciones de seguridad comunes

Dado que ningún equipo es completamente seguro, una instalación informática es tan segura como las personas que la utilizan. La mayoría de las acciones que infringen la seguridad se pueden resolver fácilmente con usuarios cuidadosos o equipos adicionales. Sin embargo, la siguiente lista proporciona ejemplos de los problemas que pueden producirse:

- Los usuarios proporcionan contraseñas a otras personas que no deberían tener acceso al sistema.
- Los usuarios anotan las contraseñas y, luego, las pierden o las dejan en ubicaciones inseguras.
- Los usuarios definen sus contraseñas con palabras o nombres que se pueden adivinar fácilmente.
- Los usuarios aprenden las contraseñas observando a otros usuarios escribir sus contraseñas.
- Los usuarios no autorizados extraen o sustituyen el hardware, o lo sabotean físicamente.
- Los usuarios se alejan de sus sistemas sin bloquear la pantalla.
- Los usuarios cambian los permisos en un archivo para permitir que otros usuarios lo lean.
- Los usuarios cambian las etiquetas de un archivo para permitir que otros usuarios lean el archivo.
- Los usuarios desechan documentos confidenciales impresos sin destruirlos, o los usuarios dejan documentos confidenciales impresos en ubicaciones inseguras.
- Los usuarios dejan las puertas de acceso sin traba.

- Los usuarios pierden sus llaves.
- Los usuarios no bloquean los medios de almacenamiento extraíbles.
- Las pantallas de los equipos se pueden ver a través de ventanas exteriores.
- Los cables de red tienen derivaciones.
- Una intercepción electrónica captura las señales emitidas por el equipo informático.
- Interrupciones, sobrevoltaje y picos de energía eléctrica destruyen los datos.
- Terremotos, inundaciones, tornados, huracanes y relámpagos destruyen los datos.
- La interferencia de la radiación electromagnética externa, como una mancha solar, desordena los archivos.

Referencias de seguridad adicionales

En las publicaciones del gobierno se describen detalladamente las normas, las políticas, los métodos y la terminología relacionados con la seguridad informática. Otras publicaciones que se muestran aquí son las guías para administradores de sistemas UNIX, y son muy útiles para entender cabalmente los problemas y las soluciones de seguridad de UNIX.

La Web también proporciona recursos. En particular, el sitio web de CERT (`http://www.cert.org`) alerta a las empresas y los usuarios sobre brechas de seguridad en el software. El sitio de SANS Institute (`http://www.sans.org/`) ofrece formación, un amplio glosario de términos y una lista actualizada de las principales amenazas de Internet.

Publicaciones del gobierno de los Estados Unidos

El gobierno estadounidense ofrece muchas de sus publicaciones en la Web. El Centro de Recursos de Seguridad Informática (CSRC) del Instituto Nacional de Estándares y Tecnología (NIST) publica artículos sobre seguridad informática. Los siguientes son algunos ejemplos de las publicaciones que se pueden descargar del sitio de NIST (`http://csrc.nist.gov/index.html`).

- *An Introduction to Computer Security: The NIST Handbook* (Introducción a la seguridad informática: El manual de NIST). SP 800-12, octubre de 1995.
- *Standard Security Label for Information Transfer* (Etiqueta de seguridad estándar para la transferencia de información). FIPS 188, septiembre de 1994.
- Swanson, Marianne y Barbara Guttman. *Generally Accepted Principles and Practices for Securing Information Technology Systems* (Principios y prácticas generalmente aceptados para proteger los sistemas de tecnología de la información). SP 800-14, septiembre de 1996.
- Tracy, Miles, Wayne Jensen y Scott Bisker. *Guidelines on Electronic Mail Security* (Directrices sobre la seguridad del correo electrónico). SP 800-45, septiembre de 2002. La sección E. 7 se refiere a la configuración segura de LDAP para el correo.

- Wilson, Mark y Joan Hash. *Building an Information Technology Security Awareness and Training Program* (Programa de formación y consciencia sobre la seguridad de la tecnología de la información). SP 800-61, enero de 2004. Incluye un glosario útil.
- Grace, Tim, Karen Kent y Brian Kim. *Computer Security Incident Handling Guidelines* (Directrices para el manejo de incidentes relacionados con la seguridad informática). SP 800-50, septiembre de 2002. La sección E. 7 se refiere a la configuración segura de LDAP para el correo.
- Scarfone, Karen,Wayne Jansen y Miles Tracy. *Guide to General Server Security* (Guía para la seguridad general del servidor). SP 800-123, julio de 2008.
- Souppaya, Murugiah, John Wack y Karen Kent. *Security Configuration Checklists Program for IT Products* (Programa de listas de comprobación de configuración de seguridad para productos de TI). SP 800-70, mayo de 2005.

Publicaciones de seguridad de UNIX

Ingenieros de seguridad de Sun Microsystems. *Solaris 10 Security Essentials*. Prentice Hall, 2009.

Chirillo, John y Edgar Danielyan. *Sun Certified Security Administration for Solaris 9 & 10 Study Guide* (Guía de estudio de administración de seguridad certificada por Sun para Solaris 9 y 10). McGraw-Hill/Osborne, 2005.

Garfinkel, Simson, Gene Spafford y Alan Schwartz. *Practical UNIX and Internet Security, 3rd Edition* (Seguridad práctica para Internet y UNIX, 3.ª edición). O'Reilly & Associates, Inc, Sebastopol, CA, 2006.

Publicaciones sobre seguridad informática general

Brunette, Glenn M. and Christoph L. *Toward Systemically Secure IT Architectures* (Hacia arquitecturas de TI seguras desde el punto de vista sistemático). Sun Microsystems, Inc, junio de 2005.

Kaufman, Charlie, Radia Perlman y Mike Speciner. *Network Security: Private Communication in a Public World, 2nd Edition* (Seguridad de la red: Comunicación privada en un mundo público, 2.ª edición). Prentice-Hall, 2002.

Pfleeger, Charles P. y Shari Lawrence Pfleeger. *Security in Computing* (Seguridad en el área informática). Prentice Hall PTR, 2006.

Privacy for Pragmatists: A Privacy Practitioner's Guide to Sustainable Compliance (Privacidad para pragmáticos: Una guía práctica sobre la privacidad para la conformidad sostenible). Sun Microsystems, Inc, agosto de 2005.

Rhodes-Ousley, Mark, Roberta Bragg y Keith Strassberg. *Network Security: The Complete Reference* (Seguridad de la red: La referencia completa). McGraw-Hill/Osborne, 2004.

Stoll, Cliff. *The Cuckoo's Egg* (El huevo del cuco). Doubleday, 1989.

Publicaciones generales de UNIX

Bach, Maurice J. *The Design of the UNIX Operating System* (El diseño del sistema operativo UNIX). Prentice Hall, Englewood Cliffs, NJ, 1986.

Nemeth, Evi, Garth Snyder y Scott Seebas. *UNIX System Administration Handbook* (Manual de administración del sistema UNIX). Prentice Hall, Englewood Cliffs, NJ, 1989.

◆ ◆ ◆ APÉNDICE B

Uso de acciones de CDE para instalar zonas en Trusted Extensions

En este apéndice se trata cómo configurar las zonas con etiquetas en Trusted Extensions utilizando acciones de Trusted CDE. Si está ejecutando la versión Solaris 10 11/06 sin los parches, o si está familiarizado con estas acciones, utilice las acciones de Trusted CDE. Para utilizar la secuencia de comandos `txzonemgr`, consulte "Creación de zonas con etiquetas" en la página 66.

Asociación de interfaces de red con zonas mediante acciones de CDE (mapa de tareas)

Realice sólo una de las siguientes tareas. Para las compensaciones, consulte "Planificación de acceso de varios niveles" en la página 26.

Tarea	Descripción	Para obtener instrucciones
Comparta una interfaz lógica.	Asigne la zona global a una dirección IP y asigne las zonas con etiquetas a una dirección IP distinta.	"Especificación de dos direcciones IP para el sistema mediante una acción de CDE" en la página 154
Comparta una interfaz física.	Asigne todas las zonas a una dirección IP.	"Especificación de una dirección IP para el sistema mediante una acción de CDE" en la página 155

▼ Especificación de dos direcciones IP para el sistema mediante una acción de CDE

En esta configuración, la dirección del host se aplica sólo a la zona global. Las zonas con etiquetas comparten una segunda dirección IP con la zona global.

Antes de empezar Es superusuario de la zona global. Al sistema ya se le han asignado dos direcciones IP. Se encuentra en un espacio de trabajo de Trusted CDE.

1 Navegue hasta la carpeta Trusted_Extensions.

a. Haga clic con el tercer botón del mouse en el fondo.

b. Desde el menú Workspace, seleccione Applications → Application Manager.

c. Haga doble clic en el icono de la carpeta Trusted_Extensions.

Esta carpeta contiene acciones que configuran interfaces, clientes LDAP y zonas con etiquetas.

2 Haga doble clic en la acción Share Logical Interface y responda a las peticiones de datos.

Nota – Al sistema ya se le deben haber asignado dos direcciones IP. Para esta acción, proporcione la segunda dirección y un nombre de host para esa dirección. La segunda dirección es la dirección compartida.

```
Hostname:       Type the name for your labeled zones interface
IP Address:     Type the IP address for the interface
```

Esta acción configura un host con más de una dirección IP. La dirección IP para la zona global es el nombre del host. La dirección IP de una zona con etiquetas tiene un nombre de host diferente. Además, la dirección IP de las zonas con etiquetas se comparte con la zona global. Cuando se utiliza esta configuración, las zonas con etiquetas se pueden conectar con una impresora de red.

Consejo – Utilice una convención de denominación estándar para las zonas con etiquetas. Por ejemplo, agregue `-zonas` al nombre del host.

---

3 (Opcional) En una ventana de terminal, verifique los resultados de la acción.

```
# ifconfig -a
```

Por ejemplo, el siguiente resultado muestra una interfaz lógica compartida, `hme0:3` en la interfaz de red `192.168.0.12` para las zonas con etiquetas. La interfaz `hme0` es la dirección IP única de la zona global.

```
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
        ether 0:0:00:00:00:0
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.0.11 netmask fffffe00 broadcast 192.168.0.255
hme0:3 flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        all-zones
        inet 192.168.0.12 netmask fffffe00 broadcast 192.168.0.255
```

A partir de la versión Solaris 10 10/08, la interfaz de bucle de retorno, `lo0`, también es una interfaz `all-zones`:

```
 lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
        all-zones
        inet 127.0.0.1 netmask ff000000
        ether 0:0:00:00:00:0
...
```

▼ Especificación de una dirección IP para el sistema mediante una acción de CDE

En esta configuración, la dirección del host se aplica a todas las zonas, incluidas las zonas con etiquetas.

Antes de empezar Debe ser superusuario de la zona global. Se encuentra en un espacio de trabajo de Trusted CDE.

1. **Navegue hasta la carpeta Trusted_Extensions.**
   a. **Haga clic con el tercer botón del mouse en el fondo.**
   b. **Desde el menú Workspace, seleccione Applications → Application Manager.**
   c. **Haga doble clic en el icono de la carpeta Trusted_Extensions.**

      Esta carpeta contiene acciones que configuran interfaces, clientes LDAP y zonas con etiquetas.
2. **Haga doble clic en la acción Share Physical Interface.**

   Esta acción configura un host con una dirección IP. La zona global no tiene una dirección única. Este sistema no se puede utilizar como un servidor NFS ni como un servidor de impresión de varios niveles.

3 **(Opcional) En una ventana de terminal, verifique los resultados de la acción.**

```
# ifconfig -a
```

La acción Share Physical Interface configura todas las zonas para que tengan NIC lógicas. Estas NIC lógicas comparten una NIC física única en la zona global.

Por ejemplo, el siguiente resultado muestra la interfaz física compartida, `hme0` en la interfaz de red `192.168.0.11` para todas las zonas.

```
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
       inet 127.0.0.1 netmask ff000000
       ether 0:0:00:00:00:0
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
       all-zones
       inet 192.168.0.11 netmask fffffe00 broadcast 192.168.0.255
```

A partir de la versión Solaris 10 10/08, la interfaz de bucle de retorno, `lo0`, también es una interfaz `all-zones`:

```
  lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
         all-zones
         inet 127.0.0.1 netmask ff000000
         ether 0:0:00:00:00:0
...
```

Preparación para crear zonas mediante acciones de CDE (mapa de tareas)

En el mapa de tareas siguiente se describen las tareas que le permitirán preparar el sistema para la creación de zonas. Para ver una explicación de los métodos de creación de zonas, consulte "Planificación de zonas en Trusted Extensions" en la página 24.

Tarea	Descripción	Para obtener instrucciones
1. Asigne un nombre a cada zona y enlace el nombre de la zona a la etiqueta de la zona.	Asigne un nombre a cada zona con etiquetas con una versión de su etiqueta y, luego, asocie el nombre con la etiqueta en Solaris Management Console.	"Especificación de nombres y etiquetas de zona mediante una acción de CDE" en la página 157
2. Configure la red antes de crear las zonas.	Asigne una etiqueta a la interfaz de red en cada host y realice la configuración adicional.	"Configuración de bases de datos de red de confianza (mapa de tareas)" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*

▼ Especificación de nombres y etiquetas de zona mediante una acción de CDE

No es necesario que cree una zona para cada la etiqueta del archivo `label_encodings`, pero puede hacerlo. En la base de datos `tnzonecfg` se enumeran las etiquetas para las que se pueden crear zonas en este sistema.

1 Navegue hasta la carpeta Trusted_Extensions.

a. Haga clic con el tercer botón del mouse en el fondo.

b. Desde el menú Workspace, seleccione Applications → Application Manager.

c. Haga doble clic en el icono de la carpeta Trusted_Extensions.

2 Asigne un nombre a cada zona.

a. Haga doble clic en la acción Configure Zone.

b. En la petición de datos, proporcione un nombre.

Consejo – Asigne a la zona un nombre similar a la etiqueta de la zona. Por ejemplo, el nombre de una zona cuya etiqueta es `CONFIDENTIAL : INTERNAL USE ONLY` sería `internal`.

---

3 Repita la acción Configure Zone con cada zona.

Por ejemplo, el archivo predeterminado `label_encodings` contiene las siguientes etiquetas:

```
PUBLIC
CONFIDENTIAL: INTERNAL USE ONLY
CONFIDENTIAL: NEED TO KNOW
CONFIDENTIAL: RESTRICTED
SANDBOX: PLAYGROUND
MAX LABEL
```

Si bien podría ejecutar la acción Configure Zone seis veces para crear una zona por etiqueta, considere la posibilidad de crear las zonas siguientes:

- En un sistema para todos los usuarios, cree una zona para la etiqueta `PUBLIC` y tres zonas para las etiquetas `CONFIDENTIAL`.
- En un sistema para desarrolladores, cree una zona para la etiqueta `SANDBOX: PLAYGROUND`. Como `SANDBOX: PLAYGROUND` se define como una etiqueta separada para los desarrolladores, sólo los sistemas que utilizan los desarrolladores necesitan una zona para esta etiqueta.
- No cree una zona para la etiqueta `MAX LABEL`, que se define como una acreditación.

4. **Abra la herramienta Trusted Network Zones.**

   Las herramientas de Solaris Management Console están diseñadas para evitar errores de usuario. Estas herramientas buscan errores de sintaxis y automáticamente ejecutan los comandos en el orden correcto para actualizar las bases de datos.

   a. **Inicie Solaris Management Console.**

      ```
      # /usr/sbin/smc &
      ```

   b. **Abra la caja de herramientas de Trusted Extensions para el sistema local.**

      i. **Seleccione Console → Open Toolbox.**

      ii. **Seleccione la caja de herramientas que se denomina This Computer (***este host***: `Scope=Files, Policy=TSOL`).**

      iii. **Haga clic en Open.**

   c. **En System Configuration, navegue hasta Computers and Networks.**

      Escriba una contraseña cuando se le solicite.

   d. **Haga doble clic en la herramienta Trusted Network Zones.**

5. **Asocie la etiqueta correspondiente a un nombre de zona para cada zona.**

   a. **Elija Action → Add Zone Configuration.**

      El cuadro de diálogo muestra el nombre de una zona que no tiene ninguna etiqueta asignada.

   b. **Fíjese en el nombre de la zona y, a continuación, haga clic en Edit.**

   c. **En el generador de etiquetas, haga clic sobre la etiqueta adecuada para el nombre de zona.**

      Si hace clic en la etiqueta incorrecta, haga clic de nuevo en la etiqueta para anular la selección y, a continuación, haga clic en la etiqueta correcta.

   d. **Guarde la asignación.**

      Haga clic en OK en el generador de etiquetas y, a continuación, haga clic en OK en el cuadro de diálogo Trusted Network Zones Properties.

   Habrá terminado una vez que todas las zonas que desea aparezcan en el panel o cuando la opción de menú Add Zone Configuration abra un cuadro de diálogo que no tenga un valor para el nombre de zona.

Errores más frecuentes

Si el cuadro de diálogo Trusted Network Zones Properties no aparece para una zona que desea crear, es posible que el archivo de configuración de red de zona no exista o que el archivo ya se haya creado.

- Compruebe que el archivo de configuración de red de zona no exista. Busque el nombre en el panel.
- Si el archivo no existe, ejecute la acción Configure Zone para proporcionar el nombre de zona. A continuación, repita el Paso 5 para crear el archivo.

Creación de zonas con etiquetas mediante acciones de CDE (mapa de tareas)

Se puede crear una zona para cada entrada de la base de datos de Trusted Network Zone Configuration. Realizó las entradas en "Especificación de nombres y etiquetas de zona mediante una acción de CDE" en la página 157, ejecutando la acción Configure Zone.

La carpeta Trusted_Extensions del gestor de aplicaciones contiene las siguientes acciones que permiten crear zonas con etiquetas:

- Configure Zone: crea un archivo de configuración de zona para cada nombre de zona
- Install Zone: agrega los sistemas de archivos y paquetes correctos a la zona
- Zone Terminal Console: ofrece una ventana para ver los eventos de una zona
- Initialize Zone for LDAP: convierte a la zona en un cliente LDAP y la prepara para el inicio
- Start Zone: inicia la zona y, a continuación, inicia todos los servicios de la estructura de gestión de servicios (SMF)
- Shut Down Zone: cambia el estado de la zona de Started a Halted

Las tareas se llevan a cabo en el orden siguiente.

Tarea	Descripción	Para obtener instrucciones
1. Instale e inicie una zona.	Cree la primera zona con etiquetas. Instale los paquetes, convierta la zona en un cliente LDAP e inicie todos los servicios en la zona.	"Instalación, inicialización e inicio de una zona con etiquetas mediante acciones de CDE" en la página 160
2. Personalice la zona.	Elimine los servicios no deseados. Si va a copiar o a clonar la zona, elimine la información específica de la zona.	"Personalización de una zona iniciada en Trusted Extensions" en la página 164

Tarea	Descripción	Para obtener instrucciones
3. Cree las otras zonas.	Utilice uno de los siguientes métodos para crear las otras zonas. Seleccionó el método en "Toma de decisiones relacionadas con el sistema y la seguridad antes de habilitar Trusted Extensions" en la página 44.	
	Cree cada zona desde el principio.	"Instalación, inicialización e inicio de una zona con etiquetas mediante acciones de CDE" en la página 160 "Resolución de enrutamiento de zona local a zona global en Trusted CDE" en la página 163 "Personalización de una zona iniciada en Trusted Extensions" en la página 164
	Copie la primera zona con etiquetas en otra etiqueta. Repita el procedimiento para todas las zonas.	"Uso del método de copia de zona en Trusted Extensions" en la página 166
	Utilice una instantánea de ZFS para clonar la otras zonas de la primera zona con etiquetas.	"Uso del método de clonación de zona en Trusted Extensions" en la página 167

▼ Instalación, inicialización e inicio de una zona con etiquetas mediante acciones de CDE

Como la creación de zonas incluye la copia de todo un sistema operativo, el proceso puede requerir bastante tiempo. Un proceso más rápido consiste en crear una zona, convertir la zona en una plantilla para las demás zonas y, a continuación, copiar o clonar dicha plantilla de zona.

Antes de empezar

Ha terminado la sección "Especificación de nombres y etiquetas de zona mediante una acción de CDE" en la página 157.

Si está utilizando LDAP como servicio de nombres, ha terminado la sección "Conversión de la zona global en un cliente LDAP en Trusted Extensions" en la página 62.

Si va a clonar zonas, ha terminado la sección "Creación de agrupación ZFS para clonar zonas" en la página 56. En el siguiente procedimiento, instalará la zona que preparó.

1 En la carpeta Trusted_Extensions, haga doble clic la acción Install Zone.

a. Escriba el nombre de la zona que está instalando.

Esta acción crea un sistema operativo virtual con etiquetas. Este paso demora algún tiempo en completarse. No realice otras tareas en el sistema mientras se esté ejecutando la acción Install Zone.

```
# zone-name: Install Zone
Preparing to install zone <zone-name>
Creating list of files to copy from the global zone
```

```
Copying <total> files to the zone
Initializing zone product registry
Determining zone package initialization order.
Preparing to initialize <subtotal> packages on the zone.
Initializing package <number> of <subtotal>: percent complete: percent

Initialized <subtotal> packages on zone.
Zone <zone-name> is initialized.
The file /zone/internal/root/var/sadm/system/logs/install_log
contains a log of the zone installation.

*** Select Close or Exit from the window menu to close this window ***
```

b. Abra una consola para supervisar los eventos de la zona instalada.

i. Haga doble clic en la acción Zone Terminal Console.

ii. Escriba el nombre de la zona que se acaba de instalar.

2 Inicialice la zona.

- **Si está utilizando LDAP, haga doble clic en la acción Initialize Zone for LDAP.**

  ```
  Zone name:                  Type the name of the installed zone
  Host name for the zone:     Type the host name for this zone
  ```

  Por ejemplo, en un sistema con una interfaz lógica compartida, los valores serían parecidos a los siguientes:

  ```
  Zone name:              public
  Host name for the zone: machine1-zones
  ```

  Esta acción convierte a la zona con etiquetas en un cliente LDAP del mismo servidor LDAP que presta servicio a la zona global. La acción se habrá completado una vez que aparezca la siguiente información:

  ```
  zone-name zone will be  LDAP client of IP-address
  zone-name is ready for booting
  Zone label is LABEL

  *** Select Close or Exit from the window menu to close this window ***
  ```

- **Si no utiliza LDAP, inicialice la zona manualmente realizando uno de los siguientes pasos.**

  El procedimiento manual en Trusted Extensions es idéntico al procedimiento para SO Solaris. Si el sistema tiene, al menos, una interfaz `all-zones`, el nombre de host para todas las zonas debe coincidir con el nombre de host de la zona global. En general, las respuestas a las preguntas durante la inicialización de la zona son las mismas que las respuestas para la zona global.

Proporcione la información del host realizando una de las siguientes acciones:

- **Después de iniciar la zona en el Paso 3, responda a las preguntas sobre las características del sistema en Zone Terminal Console.**

  Las respuestas se utilizan para rellenar el archivo `sysidcfg` en la zona.

  Nota – Debe asegurarse de que exista una ruta para el escritorio Trusted CDE desde la zona con etiquetas hasta la zona global. Para conocer el procedimiento, consulte "Resolución de enrutamiento de zona local a zona global en Trusted CDE" en la página 163.

- **Coloque un archivo personalizado `sysidcfg` en el directorio `/etc` de la zona antes de iniciar la zona en el Paso 3.**

3 Haga doble clic en la acción Start Zone.

Responda a la petición de datos.

`Zone name:` *Type the name of the zone that you are configuring*

Esta acción inicia la zona y, a continuación, inicia todos los servicios que se ejecutan en la zona. Para obtener detalles sobre los servicios, consulte la página del comando man `smf(5)`.

La acción Zone Terminal Console realiza un seguimiento del progreso del inicio de la zona. En la consola aparecen mensajes similares a los siguientes:

```
[Connected to zone 'public' console]

[NOTICE: Zone booting up]
...
Hostname: zonename
Loading smf(5) service descriptions: number/total
Creating new rsa public/private host key pair
Creating new dsa public/private host key pair

rebooting system due to change(s) in /etc/default/init

[NOTICE: Zone rebooting]
```

4 Supervise el resultado de la consola.

Antes de pasar a la sección "Personalización de una zona iniciada en Trusted Extensions" en la página 164, asegúrese de que la zona se haya reiniciado. La siguiente petición de datos de inicio de sesión en la consola indica que la zona se ha reiniciado.

hostname `console login:`

Errores más frecuentes

Para Install Zone: Si aparecen advertencias similares a la siguiente: `Installation of these packages generated errors: SUNW`*nombre_paquete*, lea el registro de instalación y termine de instalar los paquetes.

▼ Resolución de enrutamiento de zona local a zona global en Trusted CDE

Para cada zona que acceda a Trusted CDE, se debe resolver la variable `DISPLAY`. En Trusted CDE, para resolver la variable, el nombre de nodo de la zona con etiquetas, el nombre de nodo de la zona global y el nombre de nodo de una interfaz all-zones se deben resolver con el mismo nombre.

Antes de empezar Está utilizando Trusted CDE y está inicializando manualmente una zona con etiquetas.

1 Habilite Trusted CDE para que aparezca en la etiqueta de una zona utilizando uno de los métodos siguientes.

- **Método 1: Habilite el tráfico del servidor X con otros sistemas.**

  En esta configuración, las zonas con etiquetas pueden alcanzar otros sistemas mediante el servidor X en la zona global.

  a. **Asegúrese de que el archivo `/etc/nodename` especifique el nombre del sistema.**

  ```
  ## /etc/nodename
  machine1
  ```

  b. **Asegúrese de que el archivo `/etc/hosts` especifique el nombre del sistema.**

  ```
  ## /etc/hosts
  192.168.2.3  machine1 loghost
  ```

  Para que funcionen los servicios de ToolTalk, el nombre del sistema debe estar en la misma línea que `loghost`.

  c. **Asegúrese de que el archivo `/etc/hostname.`*interface* especifique el nombre del sistema.**

  En esta configuración, `machine1` es la interfaz all-zones para Trusted CDE.

  ```
  ## /etc/hostname.bge0
  machine1 all-zones
  ```

- **Método 2: Limite el tráfico del servidor X al sistema local.**

  En esta configuración, las zonas con etiquetas se pueden comunicar con el servidor X en el sistema local. Sin embargo, no existe ninguna ruta desde el servidor X local a otros sistemas de la red. La ruta debe utilizar otra interfaz.

  a. **Asegúrese de que el archivo `/etc/nodename` especifique el nombre del sistema.**

  ```
  ## /etc/nodename
  machine1
  ```

b. Asegúrese de que el archivo `/etc/hosts` especifique el nombre del sistema.

A partir de la versión Solaris 10 10/08, `lo0` es una interfaz all-zones. En este caso, el archivo aparece de una forma similar a la siguiente:

```
## /etc/hosts
127.0.0.1  localhost  machine1 loghost
```

También puede utilizar la interfaz `vni0`.

Para que funcionen los servicios de ToolTalk, el nombre del sistema debe estar en la misma línea que `loghost`.

- **Método 3: Resuelva la variable `DISPLAY` de otra manera, por ejemplo, como direcciones enrutables en interfaces lógicas por zona.**

  Para obtener información sobre este procedimiento, consulte "Adición de interfaces de red y rutas a zonas con etiquetas" en la página 81.

2 Para iniciar la zona, vuelva al Paso 3 en "Instalación, inicialización e inicio de una zona con etiquetas mediante acciones de CDE" en la página 160.

▼ Personalización de una zona iniciada en Trusted Extensions

Si va a clonar zonas, este procedimiento permite configurar una zona para utilizarla como plantilla para otras zonas. Además, este procedimiento permite configurar la zona para su uso.

1 Asegúrese de que la zona se haya iniciado por completo.

a. En *nombre_zona*: Zone Terminal Console, inicie sesión como usuario root.

```
hostname console login: root
Password:      Type root password
```

b. Compruebe que la zona se esté ejecutando.

El estado `running` indica que al menos un proceso se está ejecutando en la zona.

```
# zoneadm list -v
ID NAME        STATUS         PATH
 2 public      running        /
```

c. Compruebe que la zona puede comunicarse con la zona global.

El servidor X se ejecuta en la zona global. Cada zona con etiquetas debe poder conectarse con la zona global para utilizar este servicio. Por lo tanto, para poder utilizar la zona es necesario que las redes de la zona funcionen. Para obtener ayuda, consulte "La zona con etiquetas no puede acceder al servidor X" en la página 107.

2 En Zone Terminal Console, deshabilite los servicios que no son necesarios en una zona con etiquetas.

Si está copiando o clonando esta zona, los servicios que deshabilite se inhabilitarán en las nuevas zonas. Los servicios que están en línea en el sistema dependen del manifiesto de servicio para la zona. Utilice el comando `netservices limited` para desactivar los servicios que las zonas con etiquetas no necesitan.

a. Elimine varios servicios innecesarios.

```
# netservices limited
```

b. Muestre los servicios restantes.

```
# svcs
...
STATE        STIME      FMRI
online       13:05:00   svc:/application/graphical-login/cde-login:default
...
```

c. Deshabilite el acceso gráfico.

```
# svcadm disable svc:/application/graphical-login/cde-login
# svcs cde-login
STATE        STIME      FMRI
disabled     13:06:22   svc:/application/graphical-login/cde-login:default
```

Para obtener información sobre la estructura de gestión de servicios, consulte la página del comando man `smf(5)`.

3 Cierre la zona.

Elija uno de los siguientes métodos:

- **Ejecute la acción Shut Down Zone.**

  Proporcione el nombre de la zona.

- **En una ventana de terminal de la zona global, utilice el comando `zlogin`.**

  ```
  # zlogin zone-name init 0
  ```

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

4 Verifique que la zona se cierre.

En *nombre_zona*: Zone Terminal Console, el siguiente mensaje indica que la zona está cerrada:

```
[ NOTICE: Zone halted]
```

Si usted no está copiando ni clonando esta zona, cree las demás zonas de la misma manera en que creó esta primera zona.

5 Si está utilizando esta zona como una plantilla para las demás zonas, realice lo siguiente:

a. Elimine el archivo `auto_home_`*nombre_zona*.

En una ventana de terminal de la zona global, elimine este archivo de la zona *nombre_zona*.

```
cd /zone/zone-name/root/etc
# ls auto_home*
auto_home  auto_home_zone-name
# rm auto_home_zone-name
```

Por ejemplo, si la base para la clonación de otras zonas es la zona `public`, elimine su archivo `auto_home`:

```
# cd /zone/public/root/etc
# rm auto_home_public
```

Pasos siguientes

- Si va a copiar una zona, vaya a "Uso del método de copia de zona en Trusted Extensions" en la página 166.
- Si va a clonar una zona, vaya a "Uso del método de clonación de zona en Trusted Extensions" en la página 167.

▼ Uso del método de copia de zona en Trusted Extensions

Antes de empezar

- Ha terminado la sección "Especificación de nombres y etiquetas de zona mediante una acción de CDE" en la página 157.
- Ha personalizado una zona que utilizará como plantilla para la clonación en "Creación de zonas con etiquetas mediante acciones de CDE (mapa de tareas)" en la página 159.
- En este momento no está ejecutando la zona que utilizará como plantilla para la clonación.
- Aparece la carpeta Trusted_Extensions.

1 Para cada zona que desee crear, haga doble clic en la acción Copy Zone.

Responda a las peticiones de datos.

`New Zone Name:`	*Type name of target zone*
`From Zone Name:`	*Type name of source zone*

Precaución – No realice otras tareas mientras se esté realizando esta tarea.

2 Una vez que se hayan creado las zonas, compruebe el estado de cada zona.

a. Haga doble clic en la acción Zone Terminal Console.

b. Inicie sesión en la zona.

c. Complete la sección "Verificación del estado de la zona" en la página 77.

▼ Uso del método de clonación de zona en Trusted Extensions

Antes de empezar

- Ha terminado la sección "Especificación de nombres y etiquetas de zona mediante una acción de CDE" en la página 157.
- Ha terminado la sección "Creación de agrupación ZFS para clonar zonas" en la página 56.
- Ha creado la plantilla de zona al completar la sección "Creación de agrupación ZFS para clonar zonas" en la página 56.
- Ha personalizado una zona que utilizará como plantilla para la clonación en "Creación de zonas con etiquetas mediante acciones de CDE (mapa de tareas)" en la página 159.
- La zona que utilizará como plantilla para la clonación está cerrada.
- Aparece la carpeta Trusted_Extensions.

1 Cree una instantánea de ZFS de Solaris de la plantilla de zona.

```
# cd /
# zfs snapshot zone/zone-name@snapshot
```

Utilizará esta instantánea para clonar las demás zonas. Para una zona configurada denominada `public`, el comando de la instantánea es el siguiente:

```
# zfs snapshot zone/public@snapshot
```

2 Para cada zona que desee crear, haga doble clic en la acción Clone Zone.

Responda a las peticiones de datos.

```
New Zone Name:          Type name of source zone
ZFS Snapshot:             Type name of snapshot
```

3 Lea la información del cuadro de diálogo.

```
Zone label is <LABEL>
zone-name is ready for booting

*** Select Close or Exit from the window menu to close this window ***
```

4 Para cada zona, ejecute la acción Start Zone.

Inicie cada zona antes de ejecutar la acción para otra zona.

5 Una vez que se hayan creado las zonas, compruebe el estado de cada zona.

a. Haga doble clic en la acción Zone Terminal Console.

b. **Complete la sección "Verificación del estado de la zona" en la página 77.**

◆ ◆ ◆ APÉNDICE C

Lista de comprobación de configuración de Trusted Extensions

Esta lista de comprobación ofrece una visión general de las principales tareas de configuración para Trusted Extensions. Las tareas más pequeñas se detallan dentro de las tareas principales. La lista de comprobación no sustituye los siguientes pasos en esta guía.

Lista de comprobación para la configuración de Trusted Extensions

En la siguiente lista se resume qué se requiere para habilitar y configurar Trusted Extensions en su sitio. Para las tareas que se tratan en otro lugar existen referencias cruzadas.

1. Lea.
   - Lea los primeros cinco capítulos de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.
   - Comprenda los requisitos de seguridad del sitio.
   - Lea "Política de seguridad del sitio y Trusted Extensions" en la página 146.
2. Prepare.
   - Elija la contraseña del 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 etiqueta.
   - Elija el método de creación de zona.
3. Habilite Trusted Extensions.
   a. Instale el SO Oracle Solaris.
      - Para la administración remota, instale el grupo de desarrolladores o el grupo más grande de los paquetes de Solaris.

- Para el método de creación de clonación de zona, seleccione la opción de instalación personalizada y, a continuación, diseñe una partición `/zona`.

b. Habilite `svc:/system/labeld`, el servicio de Trusted Extensions.

4. Si utiliza IPv6, habilite IPv6 para Trusted Extensions.
5. Si utiliza un dominio de interpretación distinto de `1`, defina el dominio de interpretación en los archivos `/etc/system` y `/etc/security/tsol/tnrhtp`.
6. (Opcional) Cree una agrupación ZFS para clonar zonas.
7. Configure etiquetas.
   a. Finalice el archivo `label_encodings` de su sitio.
   b. Compruebe e instale el archivo.
   c. Reinicie.
8. Configure las interfaces para la zona global y para las zonas con etiquetas.
9. Configure Solaris Management Console.
10. Configure el servicio de nombres.
    - Utilice el servicio de nombres de archivos, que no necesita ninguna configuración.
    - O bien, configure LDAP.
      a. Cree un servidor proxy para Trusted Extensions o un servidor LDAP para Trusted Extensions.
      b. Permita que el servidor de Solaris Management Console acepte conexiones de red.
      c. Registre Solaris Management Console en LDAP.
      d. Cree una caja de herramientas LDAP para Solaris Management Console.
11. Configure las conexiones de red para LDAP.
    - Asigne un servidor LDAP o un servidor proxy al tipo de host `cipso` en una plantilla de host remoto.
    - Asigne el sistema local al tipo de host `cipso` en una plantilla de host remoto.
    - Convierta el sistema local en un cliente del servidor LDAP.
12. Cree zonas con etiquetas.
    - OPCIÓN 1: Utilice la secuencia de comandos txzonemgr.
    - OPCIÓN 2: Utilice la acciones de Trusted CDE.
      a. Configure las zonas con etiquetas.
         i. En Solaris Management Console, asocie los nombres de zonas con etiquetas específicas.
         ii. Ejecute la acción Configure Zone.
      b. Ejecute la acción Install Zone.
      c. Ejecute la acción Initialize for LDAP.

d. Ejecute la acción Start Zone.
e. Personalice la zona en ejecución.
f. Ejecute la acción Shut Down Zone.
g. Personalice la zona mientras la zona esté cerrada.
h. (Opcional) Cree una instantánea de ZFS.
i. Cree las demás zonas desde el principio, o mediante las acciones Copy Zone o Clone Zone.

13. Configure la red. Consulte "Configuración de bases de datos de red de confianza (mapa de tareas)" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.
    - 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 host remoto.
    - Asigne hosts individuales a las plantillas.
    - Asigne subredes a las plantillas.
14. Establezca un enrutamiento estático. Consulte "Configuración de rutas y comprobación de la información de red en Trusted Extensions (mapa de tareas)" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.
15. Configure los usuarios locales y los roles de administración locales.
    - Para aplicar la separación de tareas, cree perfiles de derechos personalizados.
    - 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.
16. Cree directorios principales en el servidor NFS.
    - Cree directorios principales para cada usuario en cada etiqueta a la que puede acceder el usuario.
    - (Opcional) Evite que los usuarios lean los directorios principales de nivel inferior.
17. Configure las opciones de impresión. Consulte "Gestión de impresión en Trusted Extensions (mapa de tareas)" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.
18. Configure los dispositivos. Consulte "Control de dispositivos en Trusted Extensions (mapa de tareas)" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*.
    a. Asigne el perfil de gestión de dispositivos o el perfil de administrador del sistema a un rol.
    b. 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.

19. Configure las funciones de Oracle Solaris.
    - Configure las opciones de auditoría.
    - Configure los valores de seguridad.
    - Permita que determinados clientes LDAP sean sistemas de administración LDAP.
    - Configure los usuarios en LDAP.
    - Configure los roles de red en LDAP.
    - Monte y comparta sistemas de archivos. Consulte el Capítulo 11, "Gestión y montaje de archivos en Trusted Extensions (tareas)" de *Procedimientos de administradores de Oracle Solaris Trusted Extensions*

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.

administrador principal La persona que se encarga de crear el perfil de derechos nuevo para la organización y de resolver las dificultades de los equipos que están fuera del alcance del administrador de la seguridad y el administrador del sistema combinados. Este rol se asumirá rara vez. Después de la configuración de seguridad inicial, los sitios más seguros pueden elegir no crear este rol y no asignar el perfil de administrador principal a ningún rol.

archivo .copy_files Un archivo de configuración opcional en un sistema de varias etiquetas. Este archivo contiene una lista de archivos de inicio, como `.cshrc` o `.mozilla`, que el entorno de usuario o las aplicaciones de usuario requieren para que el sistema o la aplicación funcionen bien. Los archivos que aparecen en `.copy_files` se *copian* en el directorio principal del usuario en etiquetas superiores cuando se crean dichos directorios. Consulte también archivo .link_files.

archivo .link_files Un archivo de configuración opcional en un sistema de varias etiquetas. Este archivo contiene una lista de archivos de inicio, como `.cshrc` o `.mozilla`, que el entorno de usuario o las aplicaciones de usuario requieren para que el sistema o la aplicación funcionen bien. Los archivos que aparecen en `.link_files` se *enlazan* al directorio principal del usuario en etiquetas superiores cuando se crean dichos directorios. Consulte también archivo .copy_files.

archivo label_encodings Archivo en el que se definen la etiqueta de sensibilidad completa, los rangos de acreditación, la vista de las etiquetas, la visibilidad predeterminada de las etiquetas, las acreditaciones de usuario predeterminadas y otros aspectos de las etiquetas.

asignación Un mecanismo mediante el que se controla el acceso a un dispositivo. Consulte asignación de dispositivos.

asignación de dispositivos Un mecanismo para impedir el acceso a la información almacenada en un dispositivo asignable a todos menos al usuario que asigna el dispositivo. Nadie, excepto el usuario que asignó el dispositivo, puede acceder a la información relacionada con el dispositivo hasta que se anula la asignación de éste. Para que un usuario pueda asignar un dispositivo el administrador de la seguridad le debe haber otorgado la autorización de asignación de dispositivos.

atributo de seguridad Un atributo que se utiliza para aplicar la política de seguridad de Trusted Extensions. Diversos conjuntos de atributos de seguridad se asignan a los procesos, los usuarios, las zonas, los hosts, los dispositivos asignables y otros objetos.

autorización Un derecho otorgado a un usuario o un rol para realizar una acción que, de lo contrario, no estaría permitida por la política de seguridad. Las autorizaciones se conceden en los perfiles de derechos. Determinados comandos requieren que el usuario cuente con ciertas autorizaciones para ejecutarse con éxito. Por ejemplo, para imprimir un archivo PostScript se requiere la autorización Print postscript.

banda de confianza Una región que no se pude suplantar. La banda de confianza se ubica en la parte inferior de la pantalla en Trusted CDE y en la parte superior de la pantalla en Trusted JDS. 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. Se puede acceder a la base de datos mediante un archivo en `/etc/security/tsol/tnrhdb` o mediante el servidor LDAP.

base de datos tnrhtp La plantilla del 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. Se puede acceder a la base de datos mediante un archivo en `/etc/security/tsol/tnrhtp` o mediante el servidor LDAP.

bases de datos de la red de confianza `tnrhtp`, la plantilla del 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.

caja de herramientas Una recopilación de programas en Solaris Management Console. En un host de Trusted Extensions, los administradores utilizan cajas de herramientas `Policy=TSOL`. Cada caja de herramientas tiene programas que se pueden utilizar en el ámbito de la caja de herramientas. Por ejemplo, la herramienta Trusted Network Zones que maneja la base de datos `tnzonecfg` del sistema sólo existe en la caja de herramientas `Files`, porque su ámbito siempre es local. El programa de cuentas de usuario existe en todas las cajas de herramientas. Para crear un usuario local el administrador utiliza la caja de herramientas `Files` y para crear un usuario de red el administrador utiliza la caja de herramientas `LDAP`.

CDE Consulte Common Desktop Environment.

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.

Common Desktop Environment El histórico entorno de ventanas para administrar el software de Trusted Extensions. Trusted Extensions modifica el entorno para crear Trusted CDE. Sun Java Desktop System también se modifica para crear un Trusted JDS.

compartimiento Un componente no jerárquico de una etiqueta que se utiliza con el componente de clasificación para formar una acreditación o una etiqueta. Un compartimiento representa una recopilación de información, como la que utilizaría un departamento de ingeniería o un equipo de proyecto multidisciplinario.

configuración de etiqueta Una opción de instalación de Trusted Extensions de etiquetas de sensibilidad de una sola etiqueta o de varias etiquetas. En la mayoría de los casos, la configuración de etiquetas es idéntica en todos los sistemas del sitio.

configuración evaluada Uno o varios hosts de Trusted Extensions que se están ejecutando en una configuración cuyo cumplimiento con los criterios específicos haya sido certificado por una autoridad de certificación. En Estados Unidos, esos criterios conforman los Criterios de Evaluación de Sistemas Informáticos Fiables (TCSEC, Trusted Computer System Evaluation Criteria). El organismo de evaluación y certificación es la Agencia de Seguridad Nacional (NSA, National Security Agency).

- El software de Trusted Extensions que se configura en la versión Solaris 10 11/06 está certificado según los criterios comunes v2.3 [agosto de 2005], una normativa ISO, con un nivel de seguridad (EAL) 4 y numerosos perfiles de protección.
- Mediante el proceso de continuidad de garantía, la NSA certificó el software de Trusted Extensions que se configura en la versión Solaris 10 5/09.

Los criterios comunes v2 (CCv2) y los perfiles de protección convierten a la norma de TCSEC de Estados Unidos en obsoleta hasta el nivel B1+. Se ha firmado un acuerdo de reconocimiento mutuo para CCv2 entre Estados Unidos, el Reino Unido, Canadá, Dinamarca, Países bajos, Alemania y Francia.

La configuración de Trusted Extensions ofrece una funcionalidad similar a los niveles C2 y B1 de TCSEC, con algunas funciones adicionales.

conjunto de etiquetas Consulte conjunto de etiquetas de seguridad.

conjunto de etiquetas de seguridad Especifica un conjunto discreto de etiquetas de seguridad para una entrada de la base de datos tnrhtp. Los hosts que se asignan a una plantilla con un conjunto de etiquetas de seguridad pueden enviar y recibir paquetes que coincidan con cualquiera de las etiquetas del conjunto de etiquetas.

control de acceso discrecional El tipo de acceso que es otorgado o denegado por el propietario de un archivo o un directorio según el criterio del propietario. Trusted Extensions proporciona dos tipos de control de acceso discrecional (DAC), listas de control de acceso (ACL) y bits de permiso de UNIX.

control de acceso obligatorio Control de acceso que se basa en la comparación de la etiqueta de sensibilidad de un archivo, directorio o dispositivo con la etiqueta de sensibilidad del proceso que está intentando acceder a él. La regla de MAC, lectura en el mismo nivel y en sentido descendente, se aplica cuando un proceso de una etiqueta intenta leer un archivo de una etiqueta inferior. La regla MAC, escritura en el mismo nivel y lectura en sentido descendente, se aplica cuando un proceso de una etiqueta intenta escribir en un directorio de otra etiqueta.

DAC Consulte control de acceso discrecional.

dirección IP Dirección de protocolo de Internet. Un número único que identifica un sistema en red para que éste pueda comunicarse por medio de protocolos de Internet. En IPv4, la dirección está compuesta por cuatro números separados por puntos. La mayoría de las veces, cada parte de la dirección IP es un número entre 0 y 225. Sin embargo, el primer número debe ser menor que 224 y el último número no puede ser 0.

Las direcciones IP se dividen lógicamente en dos partes: la red, y el sistema de la red. El número de red es similar a un código de área de teléfono. En relación con la red, el número de sistema es similar a un número de teléfono.

dispositivo Entre los dispositivos se incluyen impresoras, equipos, unidades de cinta, unidades de disquete, unidades de CD-ROM, unidades de DVD, dispositivos de audio y dispositivos pseudoterminales internos. Los dispositivos están sujetos a la política MAC de lectura y escritura en el mismo nivel. El acceso a los dispositivos extraíbles, como las unidades de DVD, está controlado por la asignación de dispositivos.

dominio Parte de la jerarquía de nombres de Internet. Representa un grupo de sistemas de una red local que comparten los archivos administrativos.

dominio de interpretación (DOI) En un sistema Solaris en el que está configurado Trusted Extensions, el dominio de interpretación se utiliza para distinguir los distintos archivos `label_encodings` que pueden tener etiquetas similares definidas. 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.

editor de confianza En un sistema Solaris en el que está configurado Trusted Extensions, el editor de confianza se utiliza para crear y modificar los archivos administrativos. El nombre de archivo no puede ser cambiado por el editor. Asimismo, el uso del editor se audita y los comandos de escape de shell están inhabilitados. En Trusted CDE, la acción Admin Editor inicia el editor de confianza. En Trusted JDS, el comando `/usr/dt/bin/trusted_edit` inicia el editor confianza.

equipo de configuración inicial Un equipo de, al menos, dos personas que juntas supervisan la habilitación y configuración del software de 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 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 Sun al final de la GFI. Para obtener detalles, consulte el Capítulo 5, "Customizing LOCAL DEFINITIONS" de *Oracle Solaris 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 está ejecutando el SO Solaris.

MAC Consulte control de acceso obligatorio.

nombre de dominio La identificación de un grupo de sistemas de una red local. 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 las acciones de comandos y de CDE, y para los atributos de seguridad que se asignan a estos ejecutables. Los perfiles de derechos permiten que los administradores de Solaris controlen quién puede ejecutar qué 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, las acciones de CDE y las autorizaciones asignados en todos los perfiles de derechos de ese usuario.

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 Solaris en el que está configurado Trusted Extensions, un MLP se utiliza para proporcionar un servicio de varios niveles en una zona. De manera predeterminada el servidor X es un servicio de varios niveles que se define en la zona global. Un MLP se especifica mediante número de puerto y protocolo. Por ejemplo, el MLP del servidor X para el escritorio de varios niveles se especifica mediante 6000-6003 y TCP.

rango de acreditación Un conjunto de etiquetas de sensibilidad que están aprobadas para una clase de usuarios o recursos. Un conjunto de etiquetas válidas. Consulte también rango de acreditación del sistema y rango de acreditación de usuario.

rango de acreditación de usuario El conjunto de todas las etiquetas posibles en las que un usuario común puede trabajar en el sistema. El administrador de la seguridad del sitio especifica el rango en el archivo label_encodings. Las reglas para etiquetas con formato correcto que definen el rango de acreditación del sistema también están restringidas por los valores de la sección `ACCREDITATION RANGE` del archivo: el límite superior, el límite inferior, la combinación de restricciones y otras restricciones.

rango de acreditación del sistema El conjunto de etiquetas válidas creadas según las reglas que define el administrador de la seguridad en el archivo label_encodings más las dos etiquetas administrativas que se utilizan en todos los sistemas en los que esté configurado Trusted Extensions. Las etiquetas administrativos son `ADMIN_LOW` y `ADMIN_HIGH`.

rango de etiquetas Un conjunto de etiquetas de sensibilidad que se asignan a comandos, zonas y dispositivos asignables. El rango se especifica designando una etiqueta máxima y una etiqueta mínima. Para los comandos, las etiquetas mínima y máxima limitan las etiquetas en las que se puede ejecutar el comando. A los hosts remotos que no reconocen las etiquetas se les asigna una sola etiqueta de sensibilidad, al igual que a cualquier otro host que el administrador de la seguridad desee restringir a una sola etiqueta. Un rango de etiquetas limita las etiquetas en las que se pueden asignar dispositivos y restringe las etiquetas en las que se puede almacenar o procesar información al utilizar el dispositivo.

red abierta Una red de hosts de Trusted Extensions que se conecta físicamente a otras redes y que utiliza el software de 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 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, autorizaciones y acciones de CDE. Consulte rol administrativo.

rol administrativo Un rol que ofrece las autorizaciones, los comandos con privilegios, las acciones con privilegios y el atributo de seguridad Trusted Path necesarios para permitir que el rol lleve a cabo tareas administrativas. Los roles tienen un subconjunto de capacidades de superusuario de Solaris, por ejemplo, realizan las copias de seguridad o la auditoría.

rol de confianza Consulte rol administrativo.

ruta de búsqueda de aplicaciones En CDE, la ruta de búsqueda es utilizada por el sistema para encontrar aplicaciones y cierta información de la configuración. La ruta de búsqueda de aplicaciones es controlada por un rol de confianza.

ruta de confianza En un sistema 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 redes y nombres de servicios, y establece la zona global como cliente de un servidor LDAP existente. 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. Con un servicio de nombres, es posible mantener y gestionar la información del sistema, y acceder a ella desde cualquier punto de la red. Sun admite el servicio de nombres LDAP. Sin este servicio, cada sistema debe mantener su propia copia de la información del sistema en los archivos `/etc` locales.

shell de perfil Un shell especial que reconoce atributos de seguridad, como privilegios, autorizaciones, y UID y GID especiales. Un shell de perfil generalmente limita a los usuarios a menos comandos, pero puede permitir que estos comandos se ejecuten con más derechos. El shell de perfil es el shell predeterminado de un rol de confianza.

sistema Nombre genérico de un equipo. Después de la instalación, a un sistema de una red generalmente se lo denomina host.

sistema con etiquetas Un sistema con etiquetas es un sistema que está ejecutando un sistema operativo de varios niveles, como Trusted Extensions o SELinux con MLS habilitado. El sistema puede enviar y recibir paquetes de red que están etiquetados con una opción de seguridad de IP común (CIPSO) en el encabezado del paquete.

sistema de archivos Una colección de archivos y directorios que, cuando se organiza en una jerarquía lógica, forma un conjunto de información organizado y estructurado. Los sistemas de archivos se pueden montar desde el sistema local o desde un sistema remoto.

sistema sin etiquetas Para un sistema Solaris en el que está configurado Trusted Extensions, un sistema sin etiquetas es un sistema que no está ejecutando un sistema operativo de varios niveles, como Trusted Extensions o SELinux con MLS habilitado. Un sistema sin etiquetas no envía paquetes con etiquetas. Si el sistema Trusted Extensions que se está comunicando ha asignado una sola etiqueta al sistema sin etiquetas, la comunicación de red entre el sistema Trusted Extensions y el sistema sin etiquetas se produce en esa etiqueta. Al sistema sin etiquetas también se lo denomina "sistema de un solo nivel".

sistemas conectados en red Un grupo de sistemas que están conectados mediante hardware y software, al que a veces se denomina red de área local (LAN). Cuando los sistemas están conectados en red, se suelen necesitar uno o varios servidores.

sistemas no conectados en red Equipos que no están conectados a una red o que no dependen de otros hosts.

Solaris Management Console Una interfaz gráfica de usuario administrativa basada en Java que contiene la caja de herramientas de cada programa administrativo. La mayor parte de la tareas de administración de los sistemas, la red y los usuarios se realiza mediante caja de herramientas de la consola.

zona con etiquetas En un sistema Solaris en el que está configurado Trusted Extensions, a cada zona se le asigna una etiqueta única. 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 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.

Índice

C

I

L

M

N

O

P

R

S

T

U

V

Z