Guía del usuario de Trusted Extensions

Referencia: E53985
Julio de 2014

Contenido

Lista de figuras

Lista de tablas

Uso de esta documentación

- **Descripción general:** describe cómo utilizar la función Trusted Extensions de Oracle Solaris en un sistema de escritorio.
- **Destinatarios:** usuarios de escritorio de Trusted Extensions.
- **Conocimiento requerido:** escritorio GNOME.

Biblioteca de documentación del producto

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

Acceso a My Oracle Support

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

Comentarios

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

♦ ♦ ♦ CAPÍTULO 1

Acerca de Trusted Extensions

En este capítulo, se presentan las etiquetas y otras funciones de seguridad que la función Trusted Extensions agrega al Sistema operativo Oracle Solaris (SO Oracle Solaris).

¿Qué es Trusted Extensions?

Trusted Extensions proporciona funciones de seguridad especiales para el sistema Oracle Solaris. Estas funciones permiten que una organización defina e implemente una política de seguridad en un sistema Oracle Solaris. Una *política de seguridad* es el conjunto de reglas y prácticas que ayudan a proteger la información y otros recursos, como hardware, en el sitio. Normalmente, las reglas de seguridad tratan cuestiones como quién tiene acceso a qué información o quién tiene permiso para escribir datos en medios extraíbles. Las *prácticas de seguridad* son los procedimientos recomendados para realizar tareas.

Las siguientes secciones describen algunas de las principales funciones de seguridad que Trusted Extensions proporciona. El texto indica las funciones de seguridad que se pueden configurar.

Protección contra intrusos de Trusted Extensions

Trusted Extensions agrega funciones al SO Oracle Solaris que ofrecen protección contra intrusos. Trusted Extensions también depende de algunas funciones de Oracle Solaris, como la protección con contraseña. Trusted Extensions agrega una interfaz gráfica de usuario de cambio de contraseña para los roles. De manera predeterminada, los usuarios deben estar autorizados para utilizar un dispositivo periférico, como un micrófono o una cámara.

Acceso limitado a la base de computación de confianza

El término *base de computación de confianza* (*TCB*) se refiere a la parte de Trusted Extensions que gestiona eventos que son relevantes para la seguridad. La TCB incluye software, hardware, firmware, documentación y procedimientos administrativos. Los programas de utilidad y de aplicación que pueden acceder a archivos relacionados con la seguridad son parte de la TCB. El administrador establece límites en todas las posibles interacciones que usted pueda tener con la TCB. Estas interacciones incluyen programas que necesita para llevar a cabo el trabajo, archivos a los que tiene permiso para acceder y utilidades que pueden afectar a la seguridad.

Información protegida por el control de acceso obligatorio

Si un intruso inicia sesión en el sistema, existen otros obstáculos que impiden el acceso a la información. Los archivos y otros recursos están protegidos por el control de acceso. Al igual que en el SO Oracle Solaris, el propietario de la información puede configurar el control de acceso. En Trusted Extensions, el acceso también está controlado por el sistema. Para obtener detalles, consulte “Trusted Extensions proporciona control de acceso discrecional y obligatorio” [15].

Protección de dispositivos periféricos

En Trusted Extensions, los administradores controlan el acceso a dispositivos periféricos, como unidades de cinta, unidades de CD-ROM, dispositivos USB, impresoras y micrófonos. Se puede conceder acceso por usuario. El software restringe el acceso a los dispositivos periféricos como se indica a continuación:

- De manera predeterminada, los dispositivos deben ser asignados para su uso.
- Debe estar autorizado a acceder a dispositivos que controlan los medios extraíbles.
- Los usuarios remotos no pueden utilizar dispositivos locales, como micrófonos o unidades de CD-ROM. Sólo los usuarios locales pueden asignar un dispositivo.

Evasión de programas de suplantación de usuarios

Suplantar significa imitar. Los intrusos, a veces, suplantan los programas de inicio de sesión u otros programas legítimos para interceptar contraseñas u otros datos confidenciales. Trusted

Extensions ofrece protección contra programas de suplantación hostiles y muestra el siguiente *símbolo de confianza*, un icono a prueba de falsificaciones claramente identificable en la parte superior de la pantalla.

FIGURA 1-1 Símbolo de confianza

Este símbolo se muestra siempre que interacciona con la base de computación de confianza (TCB). La presencia del símbolo garantiza la tranquilidad de realizar transacciones relacionadas con la seguridad. Si no hay ningún símbolo visible, esto indica una posible infracción de la seguridad. La Figura 1-1, “Símbolo de confianza” muestra el símbolo de confianza.

Trusted Extensions proporciona control de acceso discrecional y obligatorio

Trusted Extensions controla qué usuarios pueden acceder a qué información mediante el control de acceso obligatorio y discrecional.

Control de acceso discrecional

El control de acceso discrecional (DAC) es un mecanismo de software para controlar el acceso de usuarios a archivos y directorios. DAC deja que la configuración de protecciones para archivos y directorios las realice el propietario según su criterio. Las dos formas de DAC son los bits de permisos UNIX y las listas de control de acceso (ACL).

Los bits de permisos permiten que el propietario establezca protección de lectura, escritura y ejecución por propietario, grupo y otros usuarios. En sistemas UNIX tradicionales, el superusuario o usuario `root` puede sustituir la protección de DAC. Con Trusted Extensions, únicamente los administradores y los usuarios autorizados tienen la capacidad de sustituir DAC. Las ACL proporcionan una granularidad de control de acceso más específica. Las ACL permiten que los propietarios establezcan permisos independientes para usuarios y grupos específicos. Para obtener más información, consulte Capítulo 7, “Uso de listas de control de acceso y atributos para proteger archivos Oracle Solaris ZFS” de “Gestión de sistemas de archivos ZFS en Oracle Solaris 11.2 ”.

Control de acceso obligatorio

El control de acceso obligatorio (MAC) es un mecanismo de control de acceso aplicado por el sistema que se basa en relaciones de etiquetas. El sistema asocia una etiqueta de sensibilidad con todos los procesos que se crean para ejecutar programas. La política de MAC utiliza esta etiqueta en decisiones de control de acceso. En general, los procesos no pueden almacenar información o comunicarse con otros procesos, a menos que la etiqueta del destino sea igual a la etiqueta del proceso. La política de MAC permite que los procesos lean datos de objetos en la misma etiqueta o de objetos en una etiqueta inferior. Sin embargo, el administrador puede crear un entorno etiquetado en el que haya disponibles pocos objetos de nivel inferior, o ninguno.

De manera predeterminada, la política de MAC es invisible para el usuario. Los usuarios regulares no pueden ver objetos salvo que tengan acceso MAC a esos objetos. En todos los casos, los usuarios no pueden realizar ninguna acción contraria a la política de MAC.

Acreditaciones y etiquetas de sensibilidad

Una etiqueta tiene los siguientes dos componentes:

- Clasificación, también conocida como *nivel*.

  Este componente indica un nivel jerárquico de seguridad. Cuando se aplica a las personas, la clasificación representa una medida de confianza. Cuando se aplica a los datos, una clasificación es el grado de protección que se requiere.

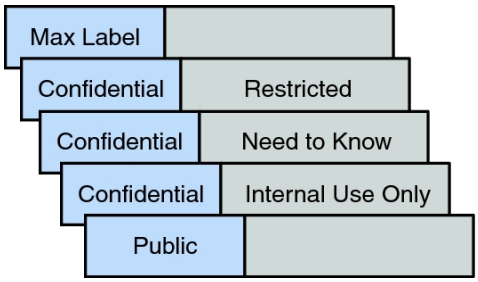
  En el Gobierno de los Estados Unidos, las clasificaciones son `TOP SECRET`, `SECRET`, `CONFIDENTIAL` y `UNCLASSIFIED`. Las clasificaciones de la industria no están tan estandarizadas. Una compañía puede establecer clasificaciones exclusivas. Para ver un ejemplo, consulte la Figura 1-2, “Etiquetas de sensibilidad típicas de la industria”. Los términos de la izquierda son clasificaciones. Los términos de la derecha son compartimientos.
- Compartimientos, también conocidos como *categorías*.

  Un compartimiento representa una agrupación, como un grupo de trabajo, un departamento, un proyecto o un tema. No es necesario que una clasificación tenga un compartimiento. En la Figura 1-2, “Etiquetas de sensibilidad típicas de la industria”, la clasificación `Confidential` tiene tres compartimientos exclusivos. `Public` y `Max Label` no tienen compartimientos. Como muestra la figura, esta organización define cinco etiquetas.

Trusted Extensions mantiene dos tipos de etiquetas: *etiquetas de sensibilidad* y *asignaciones*. Un usuario puede recibir una acreditación para trabajar en una o varias etiquetas de sensibilidad. Una etiqueta especial, conocida como *acreditación de usuario*, determina la etiqueta más alta en la que el usuario tiene permiso para trabajar. Además, cada usuario tiene una etiqueta de sensibilidad mínima. Esta etiqueta se utiliza de manera predeterminada durante el inicio de sesión para una sesión de escritorio de varios niveles. Después de iniciar sesión, el

usuario puede elegir trabajar en otras etiquetas dentro de este rango. A un usuario se le puede asignar la etiqueta `Public` como etiqueta de sensibilidad mínima y `Confidential: Need to Know` como acreditación. En el primer inicio de sesión, los espacios de trabajo del escritorio se encuentran en la etiqueta `Public`. Durante la sesión, el usuario puede crear espacios de trabajo en `Confidential: Internal Use Only` y `Confidential: Need to Know`.

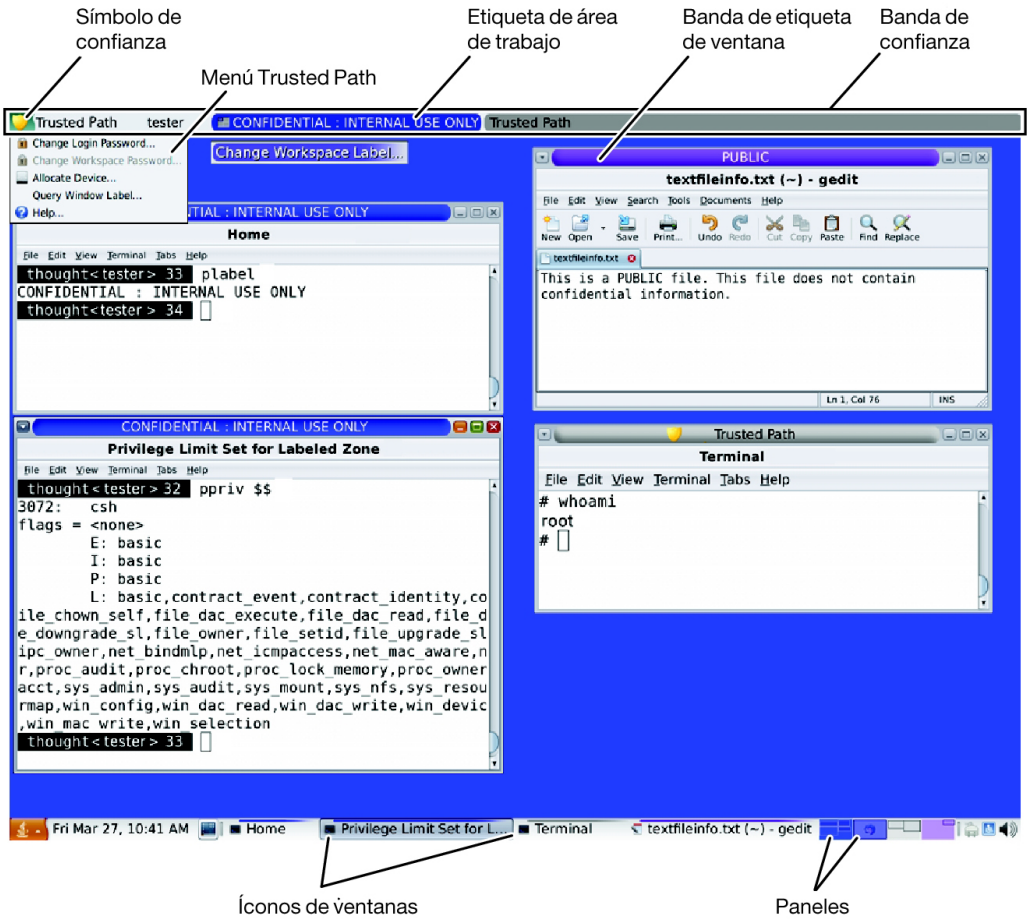
FIGURA 1-2 Etiquetas de sensibilidad típicas de la industria



Todos los sujetos y objetos tienen etiquetas en un sistema configurado con Trusted Extensions. Un *sujeto* es una entidad activa, generalmente, un proceso. El proceso hace que la información fluya entre los objetos; de lo contrario, cambia el estado del sistema. Un *objeto* es una entidad pasiva que contiene o recibe datos, como un archivo de datos, un directorio, una impresora u otro dispositivo. En algunos casos, un proceso puede ser un objeto, como cuando se utiliza el comando `kill` en un proceso.

En la Figura 1-3, “Sesión típica de varios niveles”, se muestra una sesión típica de varios niveles de Trusted Extensions. La banda de confianza se ubica en la parte superior. El menú Trusted Path se invoca desde la banda de confianza. Para asumir un rol, haga clic en el nombre de usuario para invocar al menú de roles. Los conmutadores de espacio de trabajo en el panel inferior muestran el color de la etiqueta del espacio de trabajo. La lista de ventanas en el panel inferior muestra el color de la etiqueta de la ventana.

FIGURA 1-3 Sesión típica de varios niveles



Contenedores y etiquetas

Trusted Extensions utiliza contenedores para etiquetar. Los contenedores también se denominan *zonas*. La *zona global* es una zona administrativa y no está disponible para los usuarios. Las zonas no globales se denominan *zonas etiquetadas*. Las zonas etiquetadas están disponibles para los usuarios. La zona global comparte algunos archivos del sistema con los usuarios. Cuando estos archivos están visibles en una zona con etiquetas, la etiqueta de estos archivos es `ADMIN_LOW`. Los usuarios pueden leer, pero no cambiar, el contenido de un archivo `ADMIN_LOW`.

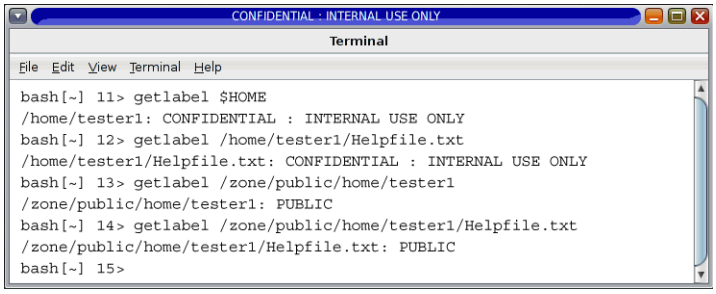
La comunicación de red está restringida por etiqueta. De manera predeterminada, las zonas no se pueden comunicar entre sí porque las etiquetas son diferentes. Por lo tanto, una zona no puede escribir en otra zona.

Sin embargo, el administrador puede configurar zonas específicas para que puedan leer directorios específicos de otras zonas. Las otras zonas pueden estar en el mismo host o en un sistema remoto. Por ejemplo, el directorio principal de un usuario en una zona de nivel inferior se puede montar mediante el servicio de montaje automático. La convención de nombre de ruta para estos montajes de directorio principal de nivel inferior incluyen el nombre de la zona de la siguiente manera:

`/zone/`*name-of-lower-level-zone*`/home/`*username*

La siguiente ventana de terminal ilustra la visibilidad del directorio principal de nivel inferior. Un usuario cuya etiqueta de inicio de sesión es `Confidential: Internal Use Only` puede ver el contenido de la zona `Public` cuando el servicio de montaje automático está configurado para hacer que las zonas de nivel inferior sean legibles. El archivo `textfileInfo.txt` tiene dos versiones. La versión de zona `Public` contiene información que se puede compartir con el público. La versión `Confidential: Internal Use Only` contiene información que se puede compartir sólo dentro de la compañía.

FIGURA 1-4 Visualización de información Public desde una zona de etiqueta superior



Etiquetas y transacciones

El software Trusted Extensions administra todas las transacciones relacionadas con la seguridad que se hayan intentado realizar. El software compara la etiqueta del sujeto con la del objeto y, luego, permite o no permite realizar la transacción según la etiqueta que sea *dominante*. Se dice que la etiqueta de una entidad *domina* a otra etiqueta de la entidad si se cumplen las dos condiciones siguientes:

- El componente de clasificación de la primera etiqueta de la entidad es mayor o igual que la clasificación del objeto.

- Todos los compartimientos de las segundas etiquetas de la entidad se incluyen en la primera etiqueta de la entidad.

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

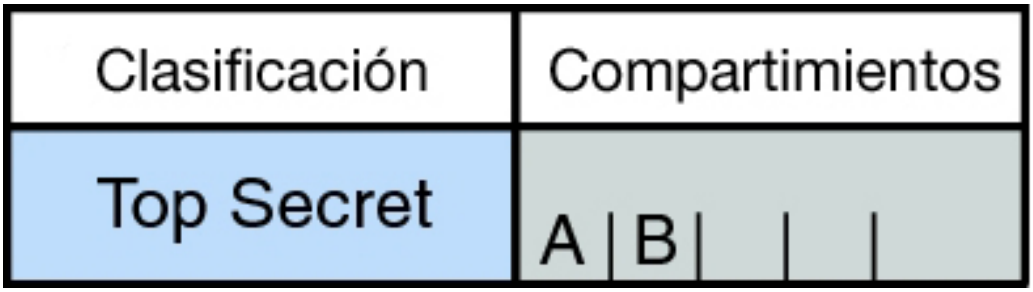
Si se cumple una de las siguientes condiciones, se dice que la primera etiqueta *domina estrictamente* a la segunda etiqueta:

- La primera etiqueta tiene una clasificación superior a la segunda etiqueta.
- La clasificación de la primera etiqueta es igual a la clasificación de una segunda etiqueta, la primera etiqueta incluye los compartimientos de la segunda etiqueta y la primera etiqueta tiene compartimientos adicionales.

Una etiqueta que domina estrictamente a una segunda etiqueta tiene permiso para acceder a la segunda etiqueta.

Se dice que dos etiquetas están *separadas* si ninguna de las etiquetas domina a la otra. El acceso no está permitido entre etiquetas separadas.

Por ejemplo, tenga en cuenta la siguiente figura.



A partir estos componentes, se pueden crear cuatro etiquetas:

- `TOP SECRET`
- `TOP SECRET A`
- `TOP SECRET B`
- `TOP SECRET AB`

`TOP SECRET AB` se domina a sí misma y domina estrictamente a las otras etiquetas. `TOP SECRET A` se domina a sí misma y domina estrictamente a `TOP SECRET`. `TOP SECRET B` se domina a sí misma y domina estrictamente a `TOP SECRET`. `TOP SECRET A` y `TOP SECRET B` están separadas.

En una transacción de lectura, la etiqueta del sujeto debe dominar a la etiqueta del objeto. Esta regla garantiza que el nivel de confianza del sujeto cumple con los requisitos de acceso al

objeto. Es decir que la etiqueta del sujeto incluye todos los compartimientos que tienen permiso para acceder al objeto. TOP SECRET A puede leer los datos de TOP SECRET A y TOP SECRET. Asimismo, TOP SECRET B puede leer los datos de TOP SECRET B y TOP SECRET. TOP SECRET A no puede leer los datos de TOP SECRET B. Ni TOP SECRET B puede leer los datos de TOP SECRET A. TOP SECRET AB puede leer los datos en todas las etiquetas.

En una transacción de escritura, es decir, cuando un sujeto crea o modifica un objeto, la zona con etiquetas del objeto resultante debe ser igual a la zona con etiquetas del sujeto. No se permiten las transacciones de escritura de una zona a otra zona diferente.

En la práctica, los sujetos y los objetos de transacciones de lectura y escritura, en general, tienen la misma etiqueta, y no es necesario tener en cuenta el dominio estricto. Por ejemplo, un sujeto TOP SECRET A puede crear o modificar un objeto TOP SECRET A. En Trusted Extensions, el objeto TOP SECRET A se encuentra en una zona con la etiqueta TOP SECRET A.

En la siguiente tabla se ilustran las relaciones de dominio entre las etiquetas del Gobierno de los Estados Unidos y entre un conjunto etiquetas de la industria.

TABLA 1-1 Ejemplos de relaciones de etiquetas en Trusted Extensions

	Etiqueta 1	Relación	Etiqueta 2
Etiquetas del Gobierno de los Estados Unidos	TOP SECRET AB	domina (estrictamente)	SECRET A
	TOP SECRET AB	domina (estrictamente)	SECRET A B
	TOP SECRET AB	domina (estrictamente)	TOP SECRET A
	TOP SECRET AB	domina (de igual modo)	TOP SECRET AB
	TOP SECRET AB	está separada de	TOP SECRET C
	TOP SECRET AB	está separada de	SECRET C
	TOP SECRET AB	está separada de	SECRET A B C
Etiquetas de la industria	Confidential: Restricted	domina a	Confidential: Need to Know
	Confidential: Restricted	domina a	Confidential: Internal Use Only
	Confidential: Restricted	domina a	Public
	Confidential: Need to Know	domina a	Confidential: Internal Use Only
	Confidential: Need to Know	domina a	Public
	Confidential: Internal	domina a	Public
	Sandbox	está separada de	todas las demás etiquetas

Al transferir información entre archivos con distintas etiquetas, Trusted Extensions muestra un cuadro de diálogo de confirmación si está autorizado a cambiar la etiqueta del archivo. Si no está autorizado a hacerlo, Trusted Extensions no permite realizar la transacción. El

administrador de la seguridad puede autorizarlo a actualizar o degradar la información. Para obtener más información, consulte “Realización de acciones de confianza” [45].

Responsabilidades del usuario para proteger datos

Como usuario, tiene la responsabilidad de configurar los permisos para proteger sus archivos y directorios. Las acciones que puede realizar para establecer permisos utilizan un mecanismo llamado control de acceso discrecional (DAC). Puede comprobar los permisos de sus archivos y directorios con el comando `ls -l` o con el explorador de archivos, como se describe en el Capítulo 3, Trabajo en Trusted Extensions.

El control de acceso obligatorio (MAC) es aplicado automáticamente por el sistema. Si está autorizado a actualizar o degradar información etiquetada, tiene la responsabilidad fundamental de garantizar que la necesidad de cambiar el nivel de la información es legítima.

Otro aspecto de la protección de datos se relaciona con el correo electrónico. Nunca siga las instrucciones de un administrador que reciba en un correo electrónico. Por ejemplo, si ha seguido instrucciones enviadas por correo electrónico para cambiar la contraseña por un valor específico, le daría al remitente la posibilidad de iniciar sesión en su cuenta. En algunos casos, puede verificar las instrucciones de manera independiente antes de seguir las instrucciones.

Trusted Extensions separa información por etiqueta

Trusted Extensions separa la información en las distintas etiquetas de la siguiente manera:

- El MAC se aplica para todas las transacciones, incluidas las transacciones de correo electrónico.
- Los archivos se almacenan en zonas independientes según la etiqueta.
- El escritorio proporciona espacios de trabajo etiquetados.
- Los usuarios pueden seleccionar una sesión de un solo nivel o de varios niveles.
- Los datos de los objetos se borran antes volver a utilizar el objeto.

Sesiones de un solo nivel o de varios niveles

Al iniciar sesión por primera vez en una sesión de Trusted Extensions, debe especificar si operará en una sola etiqueta o en varias etiquetas. Luego, debe establecer su *acreditación de sesión* o *etiqueta de sesión*. Ésta es la configuración del nivel de seguridad en el que pretende operar.

En una sesión de un solo nivel, únicamente se puede acceder a los objetos que son iguales a la etiqueta de sesión o que están dominados por la etiqueta.

En una sesión de varios niveles, puede acceder a la información en las etiquetas que son iguales o inferiores a la acreditación de sesión. Puede especificar distintas etiquetas para distintos espacios de trabajo. También puede haber varios espacios de trabajo en la misma etiqueta.

Ejemplo de selección de sesión

La Tabla 1-2, “Efecto de selección de la etiqueta inicial en las etiquetas de sesión disponibles” proporciona un ejemplo que muestra la diferencia entre una sesión de un solo nivel y una sesión de varios niveles. En este ejemplo, se compara un usuario que elige operar en una sesión de un solo nivel en `CONFIDENTIAL: NEED TO KNOW` (`CNF: NTK`) con un usuario que selecciona una sesión de varios niveles, también en `CNF: NTK`.

Las tres columnas de la izquierda muestran las selecciones de sesión de cada usuario en el momento del inicio de sesión. Tenga en cuenta que los usuarios establecen *etiquetas de sesión* para sesiones de un solo nivel y *acreditaciones de sesión* para sesiones de varios niveles. El sistema muestra el generador de etiquetas adecuado según la selección. Para ver un generador de etiquetas de ejemplo para una sesión de varios niveles, consulte la Figura 3-4, “Generador de etiquetas”.

Las dos columnas a la derecha muestran los valores de etiqueta que están disponibles en la sesión. La columna Etiqueta de espacio de trabajo inicial representa la etiqueta de cuando el usuario accede al sistema por primera vez. La columna Etiquetas disponibles muestra las etiquetas a las que el usuario tiene permiso para cambiar durante la sesión.

TABLA 1-2 Efecto de selección de la etiqueta inicial en las etiquetas de sesión disponibles

Selecciones del usuario			Valores de etiqueta de sesión	
Tipo de sesión	**Etiqueta de sesión**	**Acreditación de sesión**	**Etiqueta de espacio de trabajo inicial**	**Etiquetas disponibles**
de un solo nivel	`CNF: NTK`	-	`CNF: NTK`	`CNF: NTK`

de varios niveles	-	`CNF: NTK`	`Public`	`Public`
				`CNF: Internal Use Only`
				`CNF: NTK`

Como muestra la primera fila de la tabla, el usuario ha seleccionado una sesión de un solo nivel con una etiqueta de sesión `CNF: NTK`. El usuario tiene una etiqueta de espacio de trabajo inicial `CNF: NTK`, que es también la única etiqueta en la que el usuario puede operar.

Como muestra la segunda fila de la tabla, el usuario ha seleccionado una sesión de varios niveles con una acreditación de sesión `CNF: NTK`. La etiqueta de espacio de trabajo inicial del

usuario se establece en `Public` porque `Public` es la etiqueta inferior del rango de etiquetas de la cuenta del usuario. El usuario puede cambiar a cualquier etiqueta entre `Public` y `CNF: NTK`. `Public` es la etiqueta mínima y `CNF: NTK` es la acreditación de sesión.

Áreas de trabajo con etiquetas

En un escritorio de Trusted Extensions, se accede a los espacios de trabajo a través de los paneles del espacio de trabajo que se encuentran a la derecha del panel inferior.

FIGURA 1-5 Espacios de trabajo etiquetados en el panel

Cada espacio de trabajo tiene una etiqueta. Puede asignar la misma etiqueta a varios espacios de trabajo y puede asignar distintas etiquetas a distintos espacios de trabajo. Las ventanas que se inician en un espacio de trabajo tienen la etiqueta de ese espacio de trabajo. Cuando la ventana se mueve a un espacio de trabajo de una etiqueta diferente, la ventana conserva su etiqueta original. Por lo tanto, en una sesión de varios niveles, puede organizar las ventanas de distintas etiquetas en un espacio de trabajo.

Aplicación de MAC para transacciones de correo electrónico

Trusted Extensions aplica MAC para el correo electrónico. Puede enviar y leer correo electrónico en su etiqueta actual. Puede recibir correo electrónico en una etiqueta dentro del rango de su cuenta. En una sesión de varios niveles, puede cambiar a un espacio de trabajo en una etiqueta diferente para leer correo electrónico en esa etiqueta. Utiliza el mismo lector de correo electrónico y el mismo inicio de sesión. El sistema le permite leer correo sólo en su etiqueta actual.

Borrado de datos antes de reutilizar el objeto

Trusted Extensions impide la exposición accidental de información confidencial mediante el borrado automático de la información antigua de objetos a los que puede acceder el usuario

antes de reutilizarlos. Por ejemplo, la memoria y el espacio en el disco se borran antes de reutilizar el objeto. Si no se puede borrar la información confidencial antes de reutilizar el objeto, se pone en riesgo la exposición de la información a usuarios inadecuados. Mediante la desasignación del dispositivo, Trusted Extensions borra todos los objetos a los que el usuario puede acceder antes de asignar las unidades a los procesos. Tenga en cuenta, sin embargo, que debe borrar todos los medios de almacenamiento extraíbles, como los DVD y los dispositivos USB, antes de permitir que otro usuario acceda a la unidad.

Trusted Extensions permite la administración segura

A diferencia de los sistemas UNIX tradicionales, el superusuario (el usuario `root`) no se utiliza para administrar Trusted Extensions. En su lugar, administran el sistema roles administrativos con capacidades discretas. De este modo, ningún usuario puede comprometer la seguridad del sistema. Un *rol* es una cuenta de usuario especial que proporciona acceso a determinadas aplicaciones con los derechos necesarios para realizar las tareas específicas. Los derechos incluyen etiquetas, autorizaciones, privilegios y UID/GID efectivos.

Las siguientes prácticas de seguridad se aplican en un sistema configurado con Trusted Extensions:

- Se le ha otorgado acceso a aplicaciones y autorizaciones según su necesidad de uso.
- Puede ejecutar funciones que sustituyen a la política de seguridad sólo si los administradores le han otorgado autorizaciones o privilegios especiales.
- Las tareas de administración del sistema se dividen en varios roles.

Acceso a las aplicaciones en Trusted Extensions

En Trusted Extensions, sólo puede acceder a los programas que necesita para realizar su trabajo. Al igual que en el SO Oracle Solaris, un administrador proporciona acceso mediante la asignación de uno o más perfiles de derechos a su cuenta. Un *perfil de derechos* es una colección especial de programas y atributos de seguridad. Estos atributos de seguridad permiten el uso correcto del programa que se encuentra en el perfil de derechos.

El SO Oracle Solaris proporciona atributos de seguridad, como *privilegios* y *autorizaciones*. Trusted Extensions proporciona etiquetas. La falta de cualquiera de estos atributos puede evitar el uso del programa o de partes del programa. Por ejemplo, un perfil de derechos puede incluir una autorización que le permite leer una base de datos. Posiblemente se requiera un perfil de derechos con atributos de seguridad diferentes para modificar la base de datos o leer información clasificada como `Confidential`.

El uso de perfiles de derechos que contienen programas con atributos de seguridad asociados ayuda a evitar que los usuarios utilicen programas de manera indebida y perjudiquen los datos

del sistema. Si necesita realizar tareas que sustituyan la política de seguridad, el administrador puede asignarle un perfil de derechos que contenga los atributos de seguridad necesarios. Si no puede ejecutar una tarea determinada, póngase en contacto con el administrador. Es posible que falten atributos de seguridad obligatorios.

Además, el administrador puede asignarle un shell de perfil como su shell de inicio de sesión. Un *shell de perfil* es una versión especial de un shell común que proporciona acceso a un conjunto determinado de aplicaciones y capacidades. Los shells de perfil son una función del SO Oracle Solaris. Para obtener detalles, consulte la página del comando man `pfexec`(1).

Nota - Si intenta ejecutar un programa y recibe un mensaje de error `Not Found` o si intenta ejecutar un comando y recibe un mensaje de error `Not in Profile`, es posible que no se le permita utilizar este programa. Póngase en contacto con el administrador de la seguridad.

Administración por rol en Trusted Extensions

Trusted Extensions recomienda el uso de roles para la administración. Asegúrese de saber quién está realizando qué conjunto de tareas en su sitio. Los siguientes son roles comunes:

- Rol de usuario root: se utiliza principalmente para evitar que una sesión sea iniciada directamente por un superusuario.
- Rol de administrador de la seguridad: realiza tareas relacionadas con la seguridad, como autorizar asignaciones de dispositivos, asignar perfiles de derechos y evaluar programas de software.
- Rol de administrador del sistema: realiza tareas estándar de gestión del sistema, como crear usuarios, configurar directorios principales e instalar programas de software.
- Rol de operador: realiza copias de seguridad del sistema, administra impresoras y monta medios extraíbles.

♦ ♦ ♦ CAPÍTULO 2

Inicio de sesión en Trusted Extensions

En este capítulo, se describe el escritorio de confianza y el proceso de inicio de sesión en un sistema Trusted Extensions. En este capítulo, se tratan los siguientes temas:

Inicio de sesión en escritorio en Trusted Extensions

El escritorio que usted utiliza en Trusted Extensions está protegido. Las etiquetas proporcionan una indicación visible de la protección. Las aplicaciones, los datos y las comunicaciones están etiquetados. El escritorio es una versión de confianza del escritorio de Oracle Solaris.

La pantalla de inicio de sesión no está etiquetada. El proceso de inicio de sesión requiere que establezca una etiqueta para la sesión. Una vez que haya elegido una etiqueta, se etiquetarán el escritorio, sus ventanas y todas las aplicaciones. Además, las aplicaciones que afectan a la seguridad están visiblemente protegidas por el indicador de Trusted Path.

Proceso de inicio de sesión de Trusted Extensions

El proceso de inicio de sesión en un sistema configurado con Trusted Extensions es similar al proceso de inicio de sesión para Oracle Solaris. Sin embargo, antes de iniciar la sesión de escritorio en Trusted Extensions, se examinan varias pantallas de información relacionada con la seguridad. El proceso se describe de forma más detallada en las secciones que siguen. A continuación, puede ver una breve descripción general.

1. Identificación: escriba su nombre de usuario en el campo Username.
2. Autenticación: escriba su contraseña en el campo Password.

La finalización correcta de la identificación y la autenticación confirma su derecho a utilizar el sistema.

3. Comprobación de mensaje y selección de tipo de sesión: debe analizar la información del cuadro de diálogo Message Of The Day. Este cuadro de diálogo muestra la hora del último inicio de sesión, los mensajes del administrador y los atributos de seguridad de su sesión. Si tiene permiso para operar en más de una etiqueta, puede especificar el tipo de sesión, es decir, de un solo nivel o de varios niveles.

Nota - Si la cuenta sólo le permite operar en una etiqueta, no puede especificar el tipo de sesión. Esta restricción se denomina *etiqueta única* o configuración de un solo nivel. Si desea ver un ejemplo, consulte “Ejemplo de selección de sesión” [23].

---

4. Selección de etiqueta: en el generador de etiquetas, debe seleccionar el nivel de máxima seguridad con el que desea trabajar en su sesión.

Nota - De manera predeterminada, en Trusted Extensions no se admite el inicio de sesión remoto para los usuarios comunes. Si el administrador configuró el software Oracle Solaris Xvnc, usted puede usar un cliente VNC para visualizar remotamente un escritorio de varios niveles. Para conocer el procedimiento, consulte “Inicio de sesión remoto en Trusted Extensions” [32].

Identificación y autenticación durante el inicio de sesión

El SO Oracle Solaris gestiona la identificación y la autenticación durante el inicio de sesión. En la pantalla de inicio de sesión, en primer lugar, aparece la solicitud de nombre de usuario. Esta parte del proceso de inicio de sesión se denomina *identificación*.

Después de haber introducido el nombre de usuario, aparece la solicitud de contraseña. Esta parte del proceso se denomina *autenticación*. La contraseña autentica que usted realmente es el usuario autorizado para utilizar ese nombre de usuario.

Una *contraseña* es una combinación de teclas privada que valida su identidad en el sistema. Su contraseña se almacena en un formulario cifrado al cual ningún otro usuario del sistema puede acceder. Usted es responsable de proteger la contraseña para que otros usuarios no puedan utilizarla a fin de obtener acceso no autorizado. Nunca anote por escrito su contraseña ni la divulgue, ya que la persona que la obtenga, podrá acceder a todos los datos y no se la podrá identificar ni responsabilizar. La contraseña inicial es proporcionada por el administrador de la seguridad.

Revisión de atributos de seguridad durante el inicio de sesión

Trusted Extensions, no el SO Oracle Solaris, gestiona la revisión de los atributos de seguridad. Antes de que se complete el inicio de sesión, Trusted Extensions muestra el cuadro de diálogo Message Of The Day (MOTD). Este cuadro de diálogo proporciona información de estado para que usted revise. El estado incluye información pasada, por ejemplo, cuándo utilizó el sistema por última vez. También puede revisar los atributos de seguridad que se aplicarán en la próxima sesión. Si la cuenta está configurada para operar en más de una etiqueta, podrá seleccionar una sesión de un solo nivel o de varios niveles.

Luego, verá su etiqueta única o seleccionará una etiqueta y una acreditación del generador de etiquetas.

Inicio de sesión en Trusted Extensions

Las siguientes tareas lo guiarán para iniciar sesión en Trusted Extensions. Debe revisar y especificar la información de seguridad antes de alcanzar el escritorio.

▼ Identificación y autenticación en el sistema

1. **En el campo Username de la pantalla de inicio de sesión, introduzca su nombre de usuario.**
   Asegúrese de introducir el nombre de usuario exactamente como su administrador se lo ha asignado. Preste atención a la ortografía y al uso de mayúsculas.
   Si comete un error, escriba una contraseña falsa. Aparece el campo Username.

2. **Confirme la entrada.**
   Presione la tecla de retorno para confirmar el nombre de usuario.

Atención - *Nunca* se debe ver la banda de confianza cuando aparece la pantalla de inicio de sesión. Si ve la banda de confianza al intentar iniciar sesión o desbloquear la pantalla, no escriba la contraseña. Existe la posibilidad de que esté siendo suplantado. Una *suplantación* se produce cuando un programa intruso finge ser un programa de inicio de sesión a fin de capturar contraseñas. Póngase en contacto con el administrador de la seguridad inmediatamente.

3. **Introduzca su contraseña en el campo de entrada de la contraseña y presione Return.**
   Por motivos de seguridad, los caracteres no se muestran en el campo. El sistema compara el nombre de inicio de sesión y la contraseña con una lista de usuarios autorizados.

Errores más frecuentes

Si la contraseña proporcionada es incorrecta, la pantalla muestra un mensaje:

```
Authentication failed
```

Haga clic en OK para cerrar el cuadro de diálogo de error. Vuelva a escribir el nombre de usuario y, luego, la contraseña correcta.

▼ Comprobación de mensajes y selección de tipo de sesión

Si no se restringe a una sola etiqueta, puede ver datos en diferentes etiquetas. El rango en el que puede operar está limitado en el extremo superior por la acreditación de sesión y en el extremo inferior por la etiqueta mínima que el administrador le ha asignado.

1. **Revise el cuadro de diálogo MOTD.**

   a. **Compruebe que la hora de la última sesión sea precisa.**
   Siempre compruebe que no haya nada sospechoso en el último inicio de sesión, como una hora del día poco común. Si tiene motivos para creer que la hora no es precisa, póngase en contacto con el administrador de la seguridad.

   b. **Compruebe los mensajes del administrador.**
   El campo Message Of The Day puede contener advertencias sobre mantenimiento programado o problemas de seguridad. Siempre revise la información de este campo.

   c. **Examine los atributos de seguridad de la sesión.**

El cuadro de diálogo MOTD indica los roles que puede asumir, la etiqueta mínima y otras características de seguridad.

d. **(Opcional) Si tiene permiso para iniciar una sesión de varios niveles, decida si desea una sesión de un solo nivel.**

   Haga clic en el botón Restrict Session to a Single Label para iniciar una sesión de un solo nivel.

e. **Haga clic en Aceptar.**

2. **Confirme su selección de etiqueta.**

   Aparecerá un generador de etiquetas. Si inicia una sesión de una sola etiqueta, el generador de etiquetas describirá la etiqueta de la sesión. En un sistema de varios niveles, el generador de etiquetas le permite seleccionar la acreditación de sesión. Para ver un generador de etiquetas de ejemplo para una sesión de varios niveles, consulte la Figura 3-4, “Generador de etiquetas”.

   - **Acepte el valor predeterminado, a menos que tenga motivos para no hacerlo.**
   - **Para una sesión de varios niveles, seleccione una acreditación.**

     Para cambiar la acreditación, haga clic en la acreditación `Trusted Path` y, a continuación, haga clic en la acreditación que desea.
   - **Para una sesión de un solo nivel, seleccione una etiqueta.**

     Para cambiar la etiqueta, haga clic en la etiqueta `Trusted Path` y, a continuación, haga clic en la etiqueta que desea.

3. **Haga clic en Aceptar.**

   Aparece el escritorio de confianza.

▼ Resolución de problemas de inicio de sesión

1. **Si su nombre de usuario o contraseña no se reconocen, póngase en contacto con el administrador.**

2. **Si el rango de etiquetas no está permitido en su estación de trabajo, póngase en contacto con el administrador.**

   Las estaciones de trabajo se pueden restringir a un rango limitado de acreditaciones y etiquetas de sesión. Por ejemplo, una estación de trabajo en una sala de espera se puede limitar a etiquetas `PUBLIC` solamente. Si la etiqueta o la acreditación de sesión especificadas no se

aceptan, póngase en contacto con un administrador para determinar si la estación de trabajo está restringida.

3. **Si ha personalizado los archivos de inicialización de shell y no puede iniciar sesión, dispone de las siguientes dos opciones.**

   - **Póngase en contacto con el administrador del sistema para resolver el problema.**

   - **Si puede convertirse en `root`, inicie una sesión en modo a prueba de fallos.**

     En un inicio de sesión estándar, los archivos de inicialización de shell se originan al inicio para proporcionar un entorno personalizado. En un inicio de sesión en modo a prueba de fallos, los valores predeterminados se aplican al sistema y no se origina ningún archivo de inicialización de shell.

     En Trusted Extensions, el inicio de sesión en modo a prueba de fallos está protegido. Únicamente la cuenta `root` puede acceder a un inicio de sesión en modo a prueba de fallos.

     a. **Escriba el nombre de usuario en la pantalla de inicio de sesión.**

     b. **En la parte inferior de la pantalla, elija Solaris Trusted Extensions Failsafe Session en el menú del escritorio.**

     c. **Cuando se le solicite, proporcione su contraseña.**

     d. **Cuando se le solicite una contraseña adicional, proporcione la contraseña para `root`.**

Inicio de sesión remoto en Trusted Extensions

La informática en red virtual (VNC) proporciona una forma de acceder a un sistema Trusted Extensions central desde un equipo portátil o doméstico. El administrador del sitio debe configurar el software Oracle Solaris Xvnc para que se ejecute en un servidor Trusted Extensions y un visor de VNC para que se ejecute en los sistemas cliente. Puede trabajar en cualquier etiqueta del rango de etiquetas que instale en el servidor.

▼ Cómo iniciar sesión en un escritorio remoto de Trusted Extensions

Antes de empezar El administrador configuró un servidor Xvnc. Para obtener referencias, consulte “Cómo configurar un sistema Trusted Extensions con Xvnc para el acceso remoto” de “Configuración y administración de Trusted Extensions ”.

1. **En una ventana de terminal, conéctese con el servidor Xvnc.**

   Introduzca el nombre del servidor que el administrador ha configurado con Xvnc.

   ```
   % /usr/bin/vncviewer Xvnc-server
   ```

2. **Inicie sesión.**

   Siga los procedimientos descritos en “Inicio de sesión en Trusted Extensions” [29].

   Ahora puede trabajar en el escritorio de Trusted Extensions, en el visor de VNC.

♦ ♦ ♦ CAPÍTULO 3

Trabajo en Trusted Extensions

En este capítulo, se trata cómo trabajar en espacios de trabajo de Trusted Extensions. En este capítulo, se tratan los siguientes temas:

Seguridad de escritorio visible en Trusted Extensions

Trusted Extensions proporciona un escritorio de varios niveles.

Un sistema configurado con Trusted Extensions muestra la banda de confianza siempre, excepto durante el inicio de sesión y cuando se bloquea la pantalla. Todas las demás veces, la banda de confianza está visible.

La banda se ubica en la parte superior de la pantalla. El símbolo de confianza aparece en la banda de confianza al interaccionar con la base de computación de confianza (TCB). Cuando cambia la contraseña, por ejemplo, interacciona con la TCB.

Cuando los monitores de un sistema de varios encabezados de Trusted Extensions están configurados horizontalmente, aparece una banda de confianza a través de los monitores. Sin embargo, si el sistema de varios encabezados está configurado para mostrarse verticalmente, o tiene escritorios separados, uno por monitor, la banda de confianza aparecerá sólo en un monitor.

Atención - Si aparece una segunda banda de confianza en un sistema de varios encabezados, la banda no está generada por el sistema operativo. Es posible que tenga un programa no autorizado en el sistema.

Póngase en contacto con el administrador de la seguridad inmediatamente. Para determinar la banda de confianza adecuada, consulte Cómo encontrar el puntero del mouse [42].

Para obtener detalles sobre las aplicaciones, los menús, las etiquetas y las funciones del escritorio, consulte el Capítulo 4, Elementos de Trusted Extensions.

Proceso de cierre de sesión de Trusted Extensions

Una estación de trabajo cuya sesión está iniciada pero desatendida crea un riesgo de seguridad. Acostúmbrese a proteger la estación de trabajo antes de salir de ella. Si piensa volver pronto, bloquee la pantalla. En la mayoría de los sitios, la pantalla se bloquea automáticamente después de un período de inactividad determinado. Si prevé que se ausentará unos minutos, o que otra persona utilizará su estación de trabajo, cierre la sesión.

Trabajo en un sistema con etiquetas

Atención - Si en su área de trabajo falta la banda de confianza, póngase en contacto con el administrador de la seguridad. Los problemas del sistema pueden ser graves.

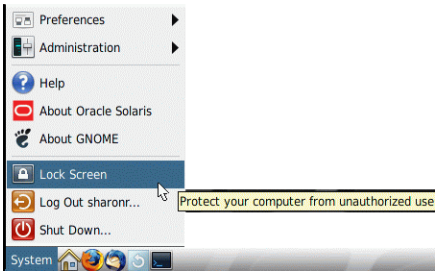
La banda de confianza no debe aparecer durante el inicio de sesión o cuando se bloquea la pantalla. Si aparece la banda de confianza, póngase en contacto inmediatamente con el administrador.

▼ Cómo bloquear y desbloquear la pantalla

Si sale de su estación de trabajo por unos instantes, bloquee la pantalla.

1. **Elija Lock Screen en el menú principal.**

FIGURA 3-1 Selección de bloqueo de pantalla



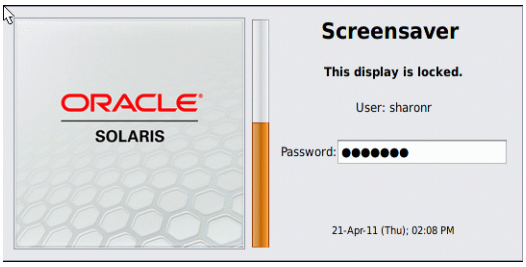
La pantalla se pondrá de color negro. En este punto, sólo podrá volver a iniciar sesión.

Nota - La banda de confianza no debe aparecer cuando la pantalla está bloqueada. Si la banda aparece, notifique al administrador de la seguridad inmediatamente.

---

2. **Para desbloquear la pantalla, realice lo siguiente:**

   a. **Mueva el mouse hasta que el cuadro de diálogo Screensaver sea visible.**



   Si no aparece el cuadro de diálogo Screensaver, presione la tecla de retorno.

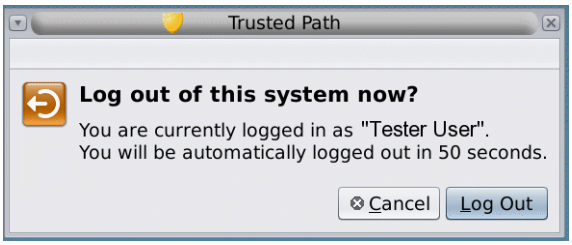
   b. **Introduzca su contraseña.**

   Esta acción lo hará volver a la sesión en su estado anterior.

▼ Cómo cerrar una sesión de Trusted Extensions

En la mayoría de los sitios, la pantalla se bloquea automáticamente después de un período de inactividad determinado. Si prevé que saldrá de la estación de trabajo por unos minutos, o que otra persona utilizará su estación de trabajo, cierre la sesión.

1. **Para cerrar una sesión de Trusted Extensions, elija Log Out** *su_nombre* **en el menú principal.**



2. **Confirme que desea cerrar la sesión o haga clic en Cancel.**

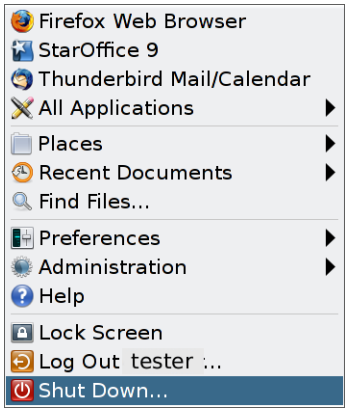
▼ Cómo cerrar el sistema

La manera normal de terminar una sesión de Trusted Extensions es mediante el cierre de sesión. Utilice el siguiente procedimiento si necesita desactivar su estación de trabajo.

Nota - Si no se encuentra en la consola, no puede cerrar el sistema. Por ejemplo, los clientes VNC no pueden cerrar el sistema.

Antes de empezar Se le debe asignar el perfil de derechos de mantenimiento y reparación.

- **Elija Shut Down en el menú principal.**



Confirme el cierre.

Nota - De manera predeterminada, la combinación de teclado Stop-A (L1-A) no está disponible en Trusted Extensions. El administrador de la seguridad puede cambiar este valor por defecto.

▼ Cómo ver los archivos en un espacio de trabajo etiquetado

Para ver los archivos, debe utilizar las mismas aplicaciones que utilizaría en el escritorio en un sistema Oracle Solaris. Si está trabajando en varias etiquetas, sólo son visibles los archivos que se encuentran en la etiqueta del espacio de trabajo.

- **Abra una ventana de terminal o el explorador de archivos.**

  - **Abra una ventana de terminal y enumere los contenidos del directorio principal.**

    Haga clic con el tercer botón del mouse en el fondo. En el menú, seleccione Open Terminal.

  - **Haga clic en la carpeta Home en el escritorio o el panel del escritorio.**

    La carpeta se abre en un explorador de archivos. La aplicación de explorador de archivos se abre en la misma etiqueta que el espacio de trabajo actual. La aplicación proporciona acceso sólo a los archivos que están en su etiqueta. Para obtener detalles sobre cómo ver archivos en distintas etiquetas, consulte “Contenedores y etiquetas” [18]. Para ver los

archivos de distintas etiquetas en un espacio de trabajo, consulte Cómo mover una ventana a un espacio de trabajo diferente [53].

▼ Cómo acceder a las páginas del comando man de Trusted Extensions

- **En la versión de Oracle Solaris, revise la página del comando man `trusted_extensions`(5) en una ventana de terminal.**

```
% man trusted_extensions
```

Para obtener una lista de los comandos específicos de Trusted Extensions, consulte Apéndice D, “Lista de las páginas del comando man de Trusted Extensions” de “Configuración y administración de Trusted Extensions ”. Las páginas del comando man también están disponibles en el sitio web de documentación (http://www.oracle.com/technetwork/indexes/documentation/index.html) de Oracle.

▼ Cómo acceder a los archivos de inicialización en cada etiqueta

Enlazar un archivo o copiar un archivo en otra etiqueta es útil cuando desea hacer visible un archivo con una etiqueta inferior en etiquetas superiores. El archivo enlazado sólo se puede escribir en una etiqueta inferior. El archivo copiado es único en cada etiqueta y se puede modificar en cada etiqueta. Para obtener más información, consulte “Archivos .copy_files y .link_files” de “Configuración y administración de Trusted Extensions ”.

Antes de empezar Debe iniciar una sesión de varios niveles. La política de seguridad de su sitio debe permitir el enlace.

Trabaje con el administrador al modificar estos archivos.

1. **Decida qué archivos de inicialización desea enlazar a otras etiquetas.**
2. **Cree o modifique el archivo `~/.link_files`.**

   Introduzca sus entradas de a un archivo por línea. Puede especificar las rutas a los subdirectorios en el directorio principal, pero no puede utilizar una barra inicial. Todas las rutas debe estar en su directorio principal.
3. **Decida qué archivos de inicialización desea copiar a otras etiquetas.**

Copiar un archivo de inicialización es útil cuando tiene una aplicación que siempre realiza escrituras en un archivo con un nombre específico y necesita separar los datos en distintas etiquetas.

4. **Cree o modifique el archivo `~/.copy_files`.**

   Introduzca sus entradas de a un archivo por línea. Puede especificar las rutas a los subdirectorios en el directorio principal, pero no puede utilizar una barra inicial. Todas las rutas debe estar en su directorio principal.

ejemplo 3-1 Creación de un archivo `.copy_files`

En este ejemplo, el usuario desea personalizar varios archivos de inicialización por etiqueta. En su organización, el servidor web de una compañía está disponible en el nivel `Restricted`. Por lo tanto, establece distintas configuraciones iniciales en el archivo `.mozilla`, en el nivel `Restricted`. Asimismo, tiene plantillas y alias especiales en el nivel `Restricted`. Por lo tanto, modifica los archivos de inicialización `.aliases` y `.soffice` en el nivel `Restricted`. Puede modificar fácilmente estos archivos después de crear el archivo `.copy_files` en su etiqueta inferior.

```
% vi .copy_files
# Copy these files to my home directory in every zone
.aliases
.mozilla
.soffice
```

ejemplo 3-2 Creación de un archivo `.link_files`

En este ejemplo, el usuario desea que los valores predeterminados del correo y del shell C sean idénticos en todas las etiquetas.

```
% vi .link_files
# Link these files to my home directory in every zone
.cshrc
.mailrc
```

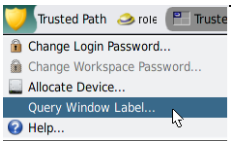
Errores más frecuentes

Estos archivos no tienen medidas de seguridad para tratar las anomalías. Las entradas duplicadas en ambos archivos o en ambas entradas del archivo que ya existen en otras etiquetas pueden provocar errores.

▼ Cómo mostrar de manera interactiva una etiqueta de ventana

Esta operación puede ser útil para identificar la etiqueta de una ventana parcialmente oculta.

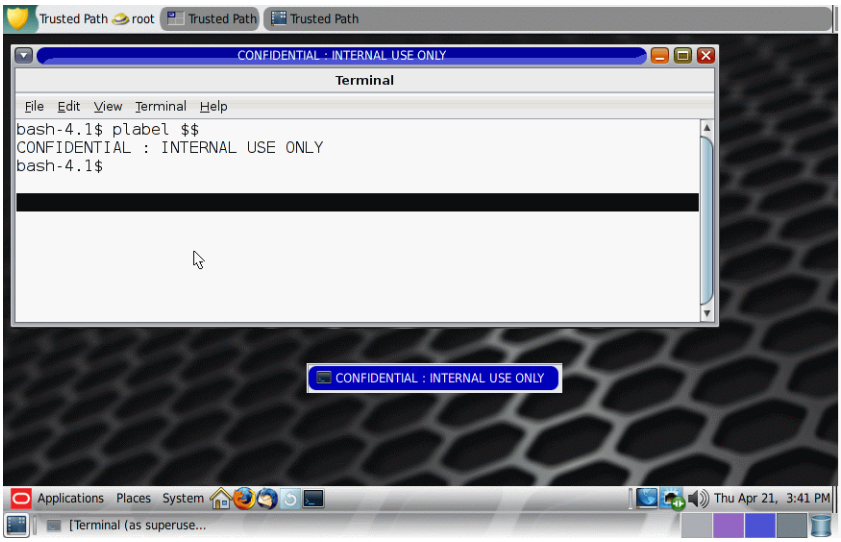
1. **Seleccione Query Window Label desde el menú Trusted Path.**



2. **Mueva el puntero por la pantalla.**

   Se muestra la etiqueta de la región debajo del puntero en un pequeño cuadro rectangular en el centro de la pantalla.

FIGURA 3-2 Operación de etiqueta de ventana de consultas



3. **Haga clic con el botón del mouse para finalizar la operación.**

▼ Cómo encontrar el puntero del mouse

Una aplicación que no es de confianza puede obtener el control del teclado o el puntero del mouse. Al encontrar este puntero, usted puede recuperar el control del enfoque del escritorio.

1. **Para recuperar el control de un teclado Sun, presione Meta y Stop.**

   Presione las teclas simultáneamente para recuperar el control del enfoque actual del escritorio. En el teclado Sun, la tecla de diamante a cada lado de la barra espaciadora es la tecla Meta.

   Si el arrastre del teclado o el puntero del mouse no son de confianza, el puntero se mueve a la banda de confianza. Si el puntero es de confianza, no se pasa a la banda de confianza.

2. **Si no está utilizando un teclado Sun, presione Alt-Break.**

ejemplo 3-3 Cómo forzar el puntero del mouse a la banda de confianza

En este ejemplo, un usuario no está ejecutando ningún proceso de confianza, pero no puede ver el puntero del mouse. Para ubicar el puntero en el centro de la banda de confianza, el usuario presiona simultáneamente las teclas Meta y Stop.

ejemplo 3-4 Cómo encontrar la banda de confianza real

En un sistema Trusted Extensions de varios encabezados cuyos monitores están configurados para mostrar un escritorio separado en cada monitor, los usuarios ven una banda de confianza por monitor. Por lo tanto, un programa que no es Trusted Extensions está generando una banda de confianza. Cuando un sistema de varios encabezados está configurado para mostrar un escritorio separado por monitor, se muestra una sola banda de confianza.

El usuario detiene el trabajo y se pone en contacto inmediatamente con el administrador de seguridad. Luego, el usuario encuentra la verdadera banda de confianza colocando el puntero del mouse en una ubicación que no es de confianza, por ejemplo, sobre el fondo del espacio de trabajo. Cuando el usuario presiona simultáneamente las teclas Alt-Break, el puntero se mueve a la banda de confianza generada por Trusted Extensions.

▼ Cómo realizar algunas tareas comunes de escritorio en Trusted Extensions

Algunas tareas comunes se ven afectadas por las etiquetas y la seguridad. En particular, las siguientes tareas se ven afectadas por Trusted Extensions:

- Vaciado de la papelera
- Búsqueda de eventos de calendario

1. **Vacíe la papelera.**

   Haga clic con el tercer botón del mouse en el icono de la papelera en el escritorio. Seleccione Empty Trash y, a continuación, confirme.

Nota - La papelera contiene archivos sólo en la etiqueta del espacio de trabajo. Suprima la información confidencial tan pronto como la información está en la papelera.

2. **Busque eventos de calendario en todas las etiquetas.**

   Los calendarios muestran sólo los eventos en la etiqueta del espacio de trabajo que abrió el calendario.

   - **En una sesión de varios niveles, abra el calendario desde cada espacio de trabajo que tenga una etiqueta diferente.**
   - **En una sesión de un solo nivel, cierre la sesión. Luego, inicie sesión en una etiqueta diferente para ver los eventos de calendario en esa etiqueta.**

3. **Guarde un escritorio personalizado en cada etiqueta.**

   Puede personalizar la configuración del espacio de trabajo para cada etiqueta en la que inicia sesión.

   a. **Configure el escritorio.**

   Nota - Los usuarios pueden guardar las configuraciones de escritorio. Los roles no pueden guardar las configuraciones de escritorio.

      i. **En el menú principal, haga clic en System > Preferences > Appearance.**

      ii. **Organice las ventanas, establezca el tamaño de la fuente y realice otras personalizaciones.**

   b. **Para guardar el escritorio actual, haga clic en el menú principal.**

      i. **Haga clic en System > Preferences > Startup Applications.**

      ii. **Haga clic en la ficha Options.**

      iii. **Haga clic en Remember Currently Running Applications y, a continuación, cierre el cuadro de diálogo.**

      El escritorio se restaurará en esta configuración cuando vuelva a iniciar sesión en esta etiqueta.

Realización de acciones de confianza

Las siguientes tareas relacionadas con la seguridad requieren la ruta de confianza.

Atención - Si cuando intenta realizar una acción relacionada con la seguridad falta el símbolo de confianza, póngase en contacto con el administrador de la seguridad inmediatamente. Los problemas del sistema pueden ser graves.

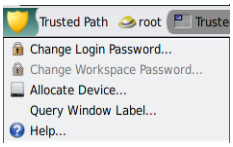
▼ Cómo cambiar la contraseña en Trusted Extensions

A diferencia del SO Oracle Solaris, Trusted Extensions proporciona una interfaz gráfica de usuario para cambiar la contraseña. La interfaz gráfica de usuario arrastra el puntero hasta que se haya completado la operación de la contraseña. Para detener un proceso que haya capturado el puntero, consulte el Ejemplo 3-5, “Comprobar si la petición de contraseña es de confianza”.

1. **Elija `Change Login Password` o `Change Workspace Password` en el menú Trusted Path.**

   Para seleccionar la opción de menú de contraseña, haga clic en la banda de confianza `Trusted Path`.

   FIGURA 3-3 Menú Trusted Path



Nota - La opción de menú `Change Workspace Password` de Trusted Path está activa cuando el sitio ejecuta un servicios de nombres separado por zona.

2. **Introduzca su contraseña actual.**

   Esta acción confirma que usted es el usuario legítimo de ese nombre de usuario. Por motivos de seguridad, la contraseña no se muestra cuando se introduce.

Atención - Al introducir la contraseña, asegúrese de que el cursor se encuentre sobre el cuadro de diálogo Change Password y de que se muestre el símbolo de confianza. Si el cursor no se encuentra sobre el cuadro de diálogo, es posible que, sin darse cuenta, introduzca su contraseña en una ventana diferente, donde otro usuario podría verla. Si el símbolo de confianza no se muestra, es posible que alguien esté intentando robar su contraseña. Póngase en contacto con el administrador de la seguridad inmediatamente.

3. **Introduzca la contraseña nueva.**

4. **Vuelva a introducirla para confirmarla.**

Nota - Si elige `Change Password` y el sitio está utilizando cuentas locales, la contraseña nueva no entrará en vigor hasta que se reinicie la zona o el sistema. Para reiniciar la zona, se le debe asignar el perfil de derechos de seguridad de la zona. Para reiniciar el sistema, se le debe asignar el perfil de derechos de mantenimiento y reparación. Si no se le asigna ninguno de estos perfiles, póngase en contacto con el administrador del sistema para programar un reinicio.

ejemplo 3-5 Comprobar si la petición de contraseña es de confianza

En un sistema x86 con un teclado Sun, se le solicita una contraseña al usuario. Se arrastró el puntero del mouse y se ubicó en el cuadro de diálogo de contraseña. Para comprobar que la solicitud sea de confianza, el usuario presiona simultáneamente las teclas Meta y Stop. Si el puntero permanece en el cuadro de diálogo, el usuario sabe que la petición de contraseña es de confianza.

Si el puntero no permanece en el cuadro de diálogo, el usuario sabe que la petición de contraseña no es de confianza. El usuario debe ponerse en contacto con el administrador.

▼ Cómo iniciar sesión en una etiqueta diferente

La etiqueta del primer espacio de trabajo que aparece en los inicios de sesión posteriores al primer inicio de sesión puede ser cualquier etiqueta que se encuentre dentro del rango de etiquetas.

Los usuarios pueden configurar las características de sesión de inicio para cada una de las etiquetas en las que inician sesión.

Antes de empezar Debe iniciar una sesión de varios niveles.

1. **Cree espacios de trabajo en cada etiqueta.**
   Para obtener detalles, consulte Cómo agregar un espacio de trabajo en una etiqueta mínima [51].

2. **Configure la apariencia de cada espacio de trabajo como desee.**

3. **Vaya al espacio de trabajo etiquetado que desea ver al iniciar sesión en esta etiqueta.**

4. **Guarde el espacio de trabajo actual.**

   Para obtener detalles, consulte Cómo realizar algunas tareas comunes de escritorio en Trusted Extensions [43].

▼ Cómo asignar un dispositivo en Trusted Extensions

La opción de menú Allocate Device le permite montar y asignar un dispositivo para su uso exclusivo. Si intenta utilizar un dispositivo sin asignarlo, obtendrá el mensaje de error “Permiso denegado”.

Antes de empezar Debe estar autorizado para asignar un dispositivo.

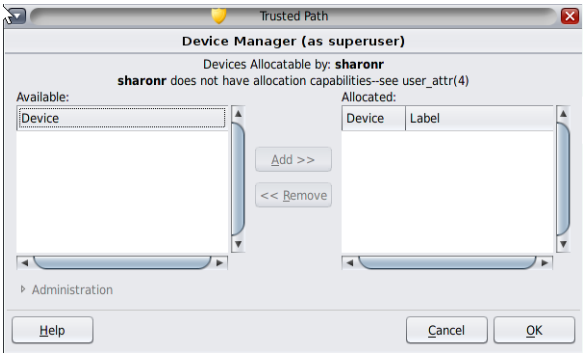
1. **Seleccione Allocate Device en el menú Trusted Path.**

2. **Haga doble clic en el dispositivo que desea utilizar.**

   Los dispositivos que tiene permitido asignar en su etiqueta actual aparecen en Available Devices:

   - `audio`*n*: indica un micrófono y un altavoz
   - `cdrom`*n*: indica una unidad de CD-ROM
   - `mag_tape`*n*: indica una unidad de cinta (transmisión por secuencias)
   - `rmdisk`*n*: indica un disco extraíble, como una unidad Jaz o Zip, o medios USB conectables

   El siguiente cuadro de diálogo indica que usted no está autorizado para asignar dispositivos:



3. **Seleccione el dispositivo.**

   Mueva el dispositivo de la lista de dispositivos disponibles a la lista de dispositivos asignados.

   - **Haga doble clic en el nombre del dispositivo en la lista de dispositivos disponibles.**
   - **O bien, seleccione el dispositivo y haga clic en el botón Allocate que apunta hacia la derecha.**

   Este paso inicia la secuencia de comandos de limpieza. La secuencia de comandos de limpieza garantiza que no queden datos de otras transacciones en los medios.

   Tenga en cuenta que la etiqueta del espacio de trabajo actual se aplica al dispositivo. Los datos transferidos a los medios del dispositivo o desde dichos medios deben ser dominados por esta etiqueta.

4. **Siga las instrucciones.**

   Las instrucciones garantizan que los medios tienen la etiqueta correcta. Por ejemplo, las siguientes instrucciones aparecen para el uso del micrófono:

Luego, se monta el dispositivo. El nombre del dispositivo ahora aparecerá en la lista de dispositivos asignados. Este dispositivo ahora está asignado para su uso exclusivo.

Errores más frecuentes

Si el dispositivo que desea utilizar no aparece en la lista, póngase en contacto con el administrador. Es posible que el dispositivo se encuentre en estado de error o esté siendo utilizado por otra persona. O bien, es posible que no tenga autorización para utilizar el dispositivo.

Si cambia a un espacio de trabajo de rol diferente o a un espacio de trabajo en una etiqueta diferente, es posible que el dispositivo asignado no funcione en esa etiqueta. Para utilizar el dispositivo en la etiqueta nueva, debe desasignar el dispositivo en la primera etiqueta y, luego, asignar el dispositivo en la etiqueta nueva. Cuando mueve el Device Manager a un espacio de trabajo en una etiqueta diferente, las listas de dispositivos disponibles y asignados cambian para reflejar el contexto correcto.

Si no aparece la ventana del explorador de archivos, abra la ventana manualmente y, luego, navegue hasta el directorio raíz: `/`. En este directorio, vaya hacia el dispositivo asignado para ver el contenido.

▼ Cómo desasignar un dispositivo en Trusted Extensions

1. **Desasigne el dispositivo.**
   a. **Vaya al espacio de trabajo donde aparece Device Manager.**
   b. **Mueva el dispositivo para desasignarlo de la lista de dispositivos asignados.**
2. **Extraiga el medio.**
3. **Haga clic en OK en el cuadro de diálogo Deallocation.**
   El dispositivo ya está disponible para que lo utilice otro usuario autorizado.

▼ Cómo asumir un rol en Trusted Extensions

A diferencia del SO Oracle Solaris, Trusted Extensions proporciona una interfaz gráfica de usuario para asumir un rol.

1. **Haga clic en su nombre de usuario a la derecha del símbolo de confianza.**

2. **Elija un nombre de rol en el menú.**

3. **Introduzca la contraseña del rol y presione Return.**

   Esta acción confirma que puede asumir este rol de manera legítima. Por motivos de seguridad, la contraseña no se muestra cuando se introduce.

Atención - Al introducir la contraseña, asegúrese de que el cursor se encuentre sobre el cuadro de diálogo Change Password y de que se muestre el símbolo de confianza. Si el cursor no se encuentra sobre el cuadro de diálogo, es posible que, sin darse cuenta, introduzca su contraseña en una ventana diferente, donde otro usuario podría verla. Si el símbolo de confianza no se muestra, es posible que alguien esté intentando robar su contraseña. Póngase en contacto con el administrador de la seguridad inmediatamente.

Después de que se acepta la contraseña del rol, el espacio de trabajo actual se convierte en el espacio de trabajo del rol. Debe encontrarse en la zona global. Puede realizar las tareas permitidas por los perfiles de derechos en el rol.

Cómo cambiar la etiqueta de un espacio de trabajo

La capacidad para configurar etiquetas de espacio de trabajo en Trusted Extensions proporciona una forma útil de trabajar en etiquetas diferentes dentro de la misma sesión de varios niveles.

Utilice este procedimiento para trabajar en el mismo espacio de trabajo, en una etiqueta diferente. Para crear un espacio de trabajo en una etiqueta diferente, consulte Cómo agregar un espacio de trabajo en una etiqueta mínima [51].

Antes de empezar Debe iniciar una sesión de varios niveles.

1. **Haga clic en la etiqueta de la ventana en la banda de confianza.**

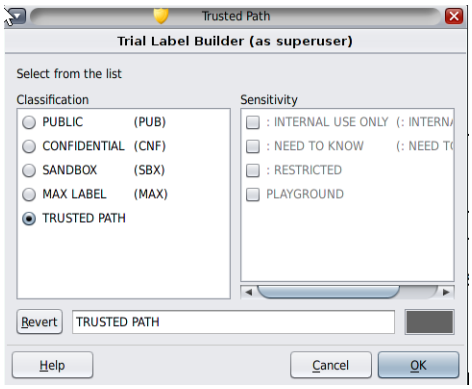
   También puede hacer clic en un panel del espacio de trabajo.

2. **Haga clic en Change Workspace Label.**

3. **Seleccione una etiqueta del generador de etiquetas.**

   En la ilustración siguiente, se muestra al usuario haciendo clic en el botón Trusted Path.

FIGURA 3-4 Generador de etiquetas



Después de hacer clic en este botón, el usuario puede seleccionar entre las etiquetas de usuario. La etiqueta del espacio de trabajo se cambia por la etiqueta nueva. En un sistema donde las etiquetas están codificadas con color, las ventanas nuevas están marcadas con el color nuevo.

4. **Proporcione la contraseña si se le solicita.**

   Si el sitio ejecuta un servicio de nombres separado por zona, se les solicita a los usuarios que proporcionen una contraseña al ingresar a un espacio de trabajo en una etiqueta nueva.

▼ Cómo agregar un espacio de trabajo en una etiqueta mínima

La capacidad para configurar etiquetas de espacio de trabajo en Trusted Extensions proporciona una forma útil de trabajar en etiquetas diferentes dentro de la misma sesión de varios niveles. Puede agregar espacios de trabajo en la etiqueta mínima.

Para cambiar la etiqueta del espacio de trabajo actual, consulte Cómo cambiar la etiqueta de un espacio de trabajo [50].

Antes de empezar Debe iniciar una sesión de varios niveles.

1. **Para crear un espacio de trabajo en la etiqueta mínima, realice lo siguiente:**

   a. **Haga clic con el tercer botón del mouse en un panel del espacio de trabajo.**

b. **En el menú, seleccione Preferences.**

c. **Aumente el número del campo Number of Workspaces.**

Los espacios de trabajo nuevos se crean en la etiqueta mínima. También puede utilizar este cuadro de diálogo para nombrar los espacios de trabajo. El nombre aparece en la pista.

d. **(Opcional) Asigne un nombre a las áreas de trabajo.**

Cuando el mouse se desplaza por encima del panel del espacio de trabajo, el nombre aparece en la pista.

2. **Para cambiar la etiqueta del espacio de trabajo, seleccione un panel del espacio de trabajo y cambie su etiqueta.**

Para obtener detalles, consulte Cómo cambiar la etiqueta de un espacio de trabajo [50].

▼ Cómo cambiar a un espacio de trabajo en una etiqueta diferente

Antes de empezar Debe iniciar una sesión de varios niveles.

1. **Haga clic en un panel del espacio de trabajo de un color distinto.**

2. **Proporcione la contraseña si se le solicita.**

Si el sitio ejecuta un servicio de nombres separado por zona, se les solicita a los usuarios que proporcionen una contraseña al ingresar a un espacio de trabajo en una etiqueta nueva.

Errores más frecuentes Si ha iniciado una sesión de un solo nivel, debe cerrar la sesión para trabajar en una etiqueta diferente. Luego, debe iniciar sesión en la etiqueta deseada. Si está autorizado, también puede iniciar una sesión de varios niveles.

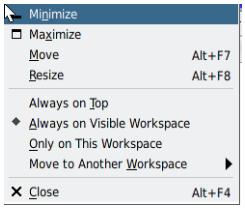
Cómo mover una ventana a un espacio de trabajo diferente

Si arrastra la ventana a un espacio de trabajo en una etiqueta diferente, la ventana conserva su etiqueta original. Las acciones de esa ventana se realizan en la etiqueta de la ventana, no en la etiqueta del espacio de trabajo que las contiene. Es útil mover una ventana si desea comparar la información. Es posible que también desee utilizar aplicaciones en distintas etiquetas sin necesidad de moverse entre espacios de trabajo.

1. **En la visualización de paneles, arrastre la ventana de un panel a un panel diferente.**

   La ventana arrastrada ahora aparece en el segundo espacio de trabajo.

2. **Para visualizar la ventana en todos los espacios de trabajo, elija Always Visible en el menú contextual en la barra de título.**



La ventana seleccionada ahora aparece en todos los espacios de trabajo.

Cómo determinar la etiqueta de un archivo

En general, la etiqueta de un archivo es evidente. Sin embargo, si tiene permiso para ver los archivos en una etiqueta inferior al espacio de trabajo actual, es posible que la etiqueta de un archivo no sea evidente. En concreto, la etiqueta de un archivo puede ser diferente de la etiqueta del explorador de archivos.

- **Utilice el explorador de archivos.**

Sugerencia - También puede utilizar la opción de menú Query Label del menú Trusted Path.

Cómo mover datos entre ventanas de etiquetas diferentes

Al igual que en un sistema Oracle Solaris, puede mover datos entre ventanas en Trusted Extensions. Sin embargo, los datos deben estar en la misma etiqueta. Al transferir información entre ventanas con distintas etiquetas, actualiza o degrada la sensibilidad de dicha información.

Antes de empezar La política de seguridad de su sitio debe permitir este tipo de transferencia, la zona contenedora debe permitir volver a etiquetar y usted debe estar autorizado a mover los datos entre las etiquetas.

Por lo tanto, el administrador debe haber realizado las siguientes tareas:

- "Cómo permitir que los archivos se vuelvan a etiquetar desde una zona con etiquetas" de "Configuración y administración de Trusted Extensions "
- "Cómo activar a un usuario para que cambie el nivel de seguridad de los datos" de "Configuración y administración de Trusted Extensions "

Debe iniciar una sesión de varios niveles.

1. **Cree espacios de trabajo en ambas etiquetas.**

   Para obtener detalles, consulte Cómo agregar un espacio de trabajo en una etiqueta mínima [51].

2. **Confirme la etiqueta del archivo de origen.**

   Para obtener detalles, consulte Cómo determinar la etiqueta de un archivo [53].

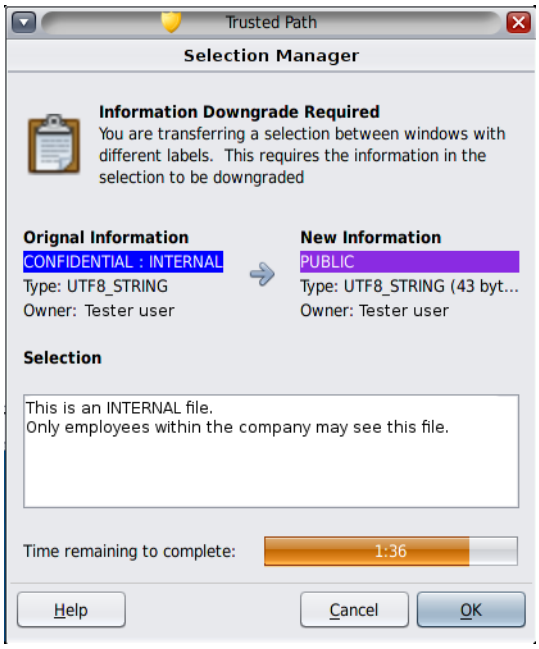
3. **Mueva la ventana con la información de origen a un espacio de trabajo en la etiqueta de destino.**

   Para obtener detalles, consulte Cómo mover una ventana a un espacio de trabajo diferente [53].

4. **Resalte la información que desea mover y pegue la selección en la ventana de destino.**

   Se muestra el cuadro de diálogo de confirmación de gestor de selecciones.

FIGURA 3-5 Cuadro de diálogo de confirmación del gestor de selecciones



5. **Revise el cuadro de diálogo de confirmación del gestor de selecciones y, luego, confirme o cancele la transacción.**

   Este cuadro de diálogo:

   - Describe por qué se necesita la confirmación de la transacción.
   - Identifica la etiqueta y el propietario del archivo de origen.
   - Identifica la etiqueta y el propietario del archivo de destino.
   - Identifica el tipo de datos seleccionados para transferir, el tipo de archivo de destino y el tamaño de los datos en bytes. De manera predeterminada, los datos seleccionados están visibles en formato de texto.
   - Indica el tiempo restante para completar la transacción. La cantidad de tiempo y el uso del temporizador depende de la configuración del sitio.

▼ Cómo actualizar los datos de un conjunto de datos con varios niveles

Los conjuntos de datos de varios niveles en Trusted Extensions facilitan la tarea de volver a etiquetar archivos. Para obtener más información sobre los conjuntos de datos de varios niveles, consulte "Conjuntos de datos de varios niveles para volver a etiquetar archivos" de "Configuración y administración de Trusted Extensions ".

Antes de empezar Debe estar autorizado para cambiar la etiqueta de los archivos. Puede operar en dos etiquetas o más, una de los cuales domina la otra.

Un conjunto de datos de varios niveles se monta en al menos una de las zonas con etiquetas, y el nombre de montaje es idéntico, por ejemplo, `/multi`, en todas las zonas que montan el conjunto de datos.

Para permitir volver a etiquetar, el administrador debe haber realizado las siguientes tareas:

- "Cómo crear y compartir un conjunto de datos de varios niveles" de "Configuración y administración de Trusted Extensions "
- "Cómo permitir que los archivos se vuelvan a etiquetar desde una zona con etiquetas" de "Configuración y administración de Trusted Extensions "
- "Cómo activar a un usuario para que cambie el nivel de seguridad de los datos" de "Configuración y administración de Trusted Extensions "

Debe iniciar una sesión de varios niveles.

1. **Cree un espacio de trabajo en una etiqueta superior.**

   Por ejemplo, para actualizar un archivo de `PUBLIC` a `INTERNAL`, cree un espacio de trabajo en la etiqueta `INTERNAL`.

   Para obtener detalles, consulte Cómo agregar un espacio de trabajo en una etiqueta mínima [51].

2. **Abra una ventana de terminal e indique el directorio que contiene el archivo que se va a actualizar.**

   En este ejemplo, el nombre de archivo es `temppub1`.

   ```
   $ ls /multi/public
   temppub1
   ```

3. **Cambie el nombre del archivo.**

   ```
   $ setlabel "cnf : internal" /multi/public/temppub1
   ```

4. **Verifique el cambio de etiqueta.**

```
$ getlabel  /multi/public/temppub1
/multi/public/temppub1: "CONFIDENTIAL : INTERNAL USE ONLY"
```

5. **(Opcional) Mueva el archivo a un directorio en la etiqueta de destino.**

```
$ mv /multi/public/temppub1 /multi/internal/temppub1
```

▼ Cómo disminuir de nivel los datos de un conjunto de datos con varios niveles

Para disminuir de nivel la fecha, primero mueva el archivo a su directorio de destino y, luego, cámbiele la fecha. Para obtener una explicación, consulte "Conjuntos de datos de varios niveles para volver a etiquetar archivos" de "Configuración y administración de Trusted Extensions ".

Antes de empezar Debe estar autorizado para disminuir el nivel de los archivos. El administrador ha montado un conjunto de datos de varios niveles en al menos una de las zonas con etiquetas y ha usado un nombre estándar, como `/multi`, para todos los montajes del conjunto de datos a los que puede tener acceso y ha permitido el cambio de etiqueta en esa zona.

Por lo tanto, el administrador debe haber realizado las siguientes tareas:

- "Cómo crear y compartir un conjunto de datos de varios niveles" de "Configuración y administración de Trusted Extensions "
- "Cómo permitir que los archivos se vuelvan a etiquetar desde una zona con etiquetas" de "Configuración y administración de Trusted Extensions "
- "Cómo activar a un usuario para que cambie el nivel de seguridad de los datos" de "Configuración y administración de Trusted Extensions "

Debe iniciar una sesión de varios niveles.

1. **Cree un área de trabajo en la etiqueta del archivo de origen.**

   Por ejemplo, cree un espacio de trabajo `internal`.

   Para obtener detalles, consulte Cómo agregar un espacio de trabajo en una etiqueta mínima [51].

2. **Abra una ventana de terminal y abra un shell de perfil.**

```
% pfbash
$
```

3. **(Opcional) Confirme la etiqueta del archivo de origen y el directorio que lo contiene.**

   Para obtener detalles, consulte Cómo determinar la etiqueta de un archivo [53].

Nota - Si el archivo de origen tiene la misma etiqueta que su directorio principal, no se puede bajar de nivel. Debe mover el archivo. Mover el archivo es una operación privilegiada.

4. **Mueva el archivo de origen a un directorio con la etiqueta de destino.**

   $ **mv /multi/***internal-directory/file* **/multi/***public-directory*

5. **Cambie la etiqueta a la etiqueta del directorio de destino.**

   $ **cd /multi/***public-directory*
   $ **setlabel public** *file*

6. **(Opcional) Verifique que se haya cambiado el nombre del archivo.**

   $ **getlabel /multi/***public-directory/file*
   /multi/*public-directory/file*: PUBLIC

   Puede editar el archivo en la etiqueta PUBLIC.

ejemplo 3-6 Cambio de la etiqueta de un directorio

En este ejemplo, un usuario autorizado cambia la etiqueta de un directorio.

En primer lugar, el usuario mueve o elimina todos los archivos del directorio.

```
$ getlabel /multi/conf
/multi/conf: CONFIDENTIAL : NEED TO KNOW
$ mv /multi/conf/* /multi/confNTK/temp
```

A continuación, el usuario establece la etiqueta del directorio y verifica la nueva etiqueta.

```
$ setlabel "Confidential : Internal Use Only" /multi/conf
getlabel /multi/conf
/multi/conf: "CONFIDENTIAL : INTERNAL USE ONLY"
```

♦ ♦ ♦ CAPÍTULO 4

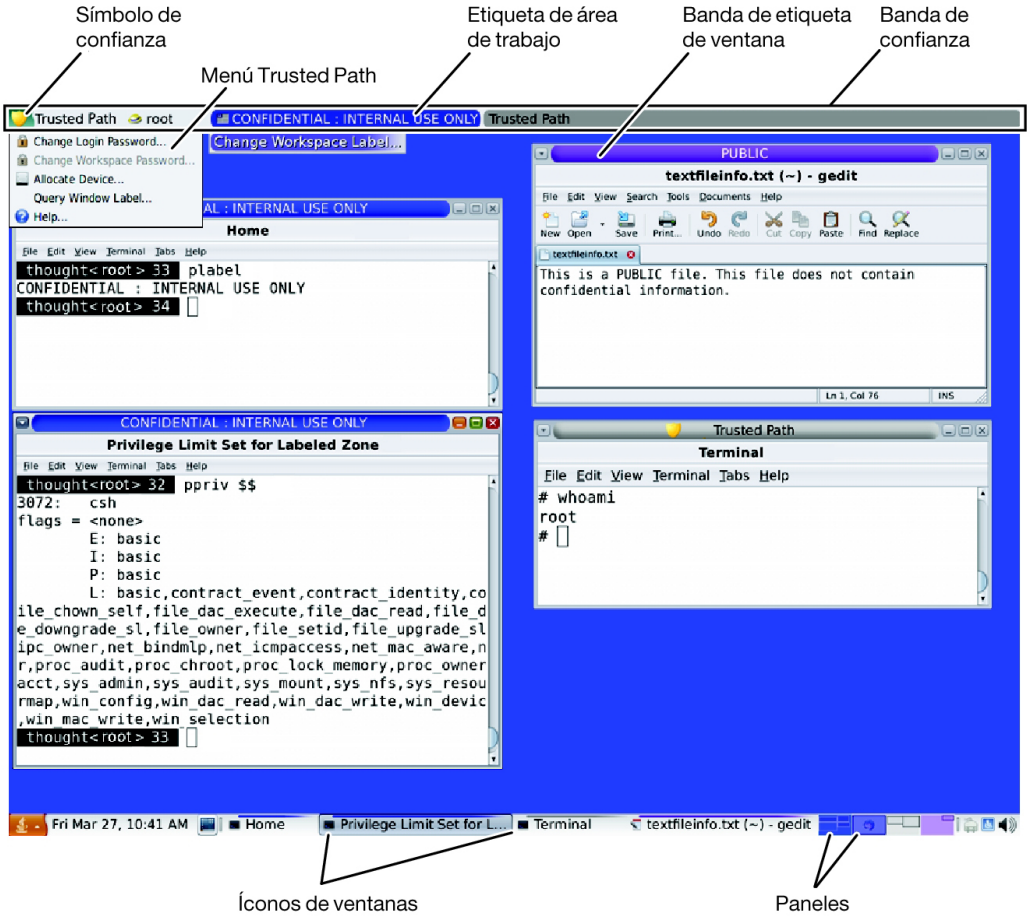
Elementos de Trusted Extensions

En este capítulo, se explican los elementos clave de Trusted Extensions. En este capítulo, se tratan los siguientes temas:

Funciones visibles de Trusted Extensions

Después de haber finalizado correctamente el proceso de inicio de sesión, como se explica en el Capítulo 2, Inicio de sesión en Trusted Extensions, puede trabajar con Trusted Extensions. El trabajo está sujeto a restricciones de seguridad. Las restricciones que son específicas de Trusted Extensions incluyen el rango de etiquetas del sistema, la acreditación y la elección de una sesión de un solo nivel o de varios niveles. Como se muestra en la siguiente figura, existen varias funciones que distinguen a un sistema configurado con Trusted Extensions de un sistema Oracle Solaris.

FIGURA 4-1 Escritorio de varios niveles de Trusted Extensions



- **Visualizaciones de etiquetas.** Todas las ventanas, los espacios de trabajo, los archivos y las aplicaciones tienen una etiqueta. El escritorio proporciona bandas de etiquetas y otros indicadores para ver la etiqueta de una entidad.
- **Banda de confianza.** Esta banda es una mecanismo de seguridad gráfica especial. En cada espacio de trabajo, la banda se muestra en la parte superior de la pantalla.
- **Acceso limitado a aplicaciones del espacio del trabajo.** El espacio de trabajo proporciona acceso únicamente a las aplicaciones permitidas en la cuenta.
- **Menú Trusted Path.** El símbolo de confianza proporciona acceso al menú.

Etiquetas de escritorios de Trusted Extensions

Como se ha explicado en “Control de acceso obligatorio” [16], todas las aplicaciones y los archivos de Trusted Extensions tienen etiquetas. Trusted Extensions muestra las etiquetas en las siguientes ubicaciones:

- Las bandas de etiqueta de la ventana se ubican arriba de la barra del título de la ventana.
- La banda en color de la etiqueta se ubica arriba del icono de la ventana en la lista de ventanas.
- El indicador de la etiqueta de la ventana se ubica en la banda de confianza.
- El indicador de etiqueta de ventana de consultas del menú Trusted Path que muestra la etiqueta de la ventana o del icono de ventana especificada por la ubicación del puntero.

Además, el color de los paneles indica la etiqueta del espacio de trabajo.

FIGURA 4-2 Paneles indicadores de espacios de trabajo con distintas etiquetas

En la Figura 4-1, “Escritorio de varios niveles de Trusted Extensions”, se muestra cómo se visualizan las etiquetas en un escritorio de Trusted Extensions. Además, la opción de menú de etiqueta de ventana de consultas se puede utilizar para mostrar la etiqueta de una ventana. Para ver una ilustración, consulte la Figura 3-2, “Operación de etiqueta de ventana de consultas”.

Banda de confianza

La banda de confianza aparece en la parte superior de la pantalla.

FIGURA 4-3 Banda de confianza en el escritorio

La finalidad de la banda de confianza es proporcionar una confirmación visual de que usted se encuentra en una sesión de Trusted Extensions legítima. La banda indica que está interaccionando con la base de computación de confianza (TCB). La banda también muestra las

etiquetas de su espacio de trabajo y ventana actuales. La banda de confianza no se puede mover, ni puede quedar oscurecida por otras ventanas o cuadros de diálogo.

La banda de confianza tiene los elementos siguientes:

- **El símbolo de confianza**, que se visualiza cuando el enfoque de la pantalla está relacionado con la seguridad
- **La etiqueta de la ventana**, que muestra la etiqueta de la ventana activa cuando el enfoque de la pantalla no está relacionado con la seguridad
- **Un marcador de rol**, ubicado a la derecha del símbolo de confianza antes del nombre de la cuenta, que muestra un icono con forma de sombrero si la cuenta es una cuenta de rol
- **El nombre de la cuenta actual**, ubicado a la derecha del símbolo de confianza, que muestra el nombre del propietario de procesos nuevos en el espacio de trabajo
- **Las ventanas etiquetadas**, que muestran las etiquetas de todas las ventanas en el espacio de trabajo

Símbolo de confianza

Cada vez que acceda a una parte de la TCB, aparecerá el símbolo de confianza a la izquierda del área de la banda de confianza.

El símbolo de confianza no se muestra cuando el puntero del mouse está dirigido a una ventana o un área de la pantalla que no afecta la seguridad. El símbolo confianza no se puede falsificar. Si ve el símbolo, significa que está interaccionando con la TCB de forma segura.

Atención - Si en su área de trabajo falta la banda de confianza, póngase en contacto con el administrador de la seguridad. Los problemas del sistema pueden ser graves.

La banda de confianza no debe aparecer durante el inicio de sesión o cuando se bloquea la pantalla. Si aparece la banda de confianza, póngase en contacto inmediatamente con el administrador.

Indicador de etiqueta de ventana

El indicador *Etiqueta de ventana* muestra la etiqueta de la ventana activa. En una sesión de varios niveles, el indicador puede ayudar a identificar ventanas con distintas etiquetas en el mismo espacio de trabajo. Además, el indicador puede mostrar que usted está interaccionando

con la TCB. Por ejemplo, cuando cambia la contraseña, aparece el indicador de Trusted Path en la banda de confianza.

Seguridad de dispositivos en Trusted Extensions

De manera predeterminada, en Trusted Extensions los dispositivos se protegen mediante requisitos de asignación de dispositivo. Los usuarios no pueden utilizar un dispositivo sin obtener la autorización explícita para asignar dispositivos. Además, un dispositivo asignado no puede ser utilizado por otro usuario. Un dispositivo en uso en una etiqueta no se puede utilizar en otra etiqueta hasta que se desasigne de la primera etiqueta y se asigne en la segunda.

Para utilizar un dispositivo, consulte Cómo asignar un dispositivo en Trusted Extensions [47].

Archivos y aplicaciones de Trusted Extensions

Todas las aplicaciones de Trusted Extensions tienen un nivel de sensibilidad indicado por su etiqueta. Las aplicaciones son *sujetos* en cualquier transacción de datos. Los sujetos deben dominar los *objetos* a los cuales los sujetos intentan acceder. Los objetos pueden ser archivos y, a veces, otros procesos. La información de etiqueta de una aplicación se muestra en la banda de la etiqueta de la ventana. La etiqueta es visible cuando una ventana está abierta y cuando una ventana está minimizada. La etiqueta de una aplicación también aparece en la banda de confianza cuando el puntero está en la ventana de la aplicación.

En Trusted Extensions, los archivos son objetos en transacciones de datos. Solamente pueden acceder a los archivos las aplicaciones cuyas etiquetas dominan las etiquetas de los archivos. Un archivo pueden verse desde las ventanas que tienen la misma etiqueta que el archivo.

Algunas aplicaciones utilizan archivos de inicialización para configurar el entorno del usuario. Existen dos archivos especiales en el directorio principal que lo ayudan a acceder a los archivos de inicialización en cada etiqueta. Estos archivos permiten que una aplicación en una etiqueta utilice un archivo de inicialización que se origina en un directorio en una etiqueta diferente. Los dos archivos especiales son `.copy_files` y `.link_files`.

Archivo `.copy_files`

El archivo `.copy_files` almacena nombres de archivos que se van a copiar cuando se cambie por primera vez a un espacio de trabajo con una etiqueta superior. Este archivo se almacena en el directorio principal en la etiqueta mínima. Este archivo es útil cuando tiene una aplicación

que siempre realiza escrituras en un archivo en el directorio principal con un nombre específico. El archivo `.copy_files` le permite especificar que la aplicación actualice el archivo en cada etiqueta.

Archivo `.link_files`

El archivo `.link_files` almacena nombres de archivos que se van a enlazar cuando se cambie por primera vez a un espacio de trabajo con una etiqueta superior. Este archivo se almacena en el directorio principal en la etiqueta mínima. El archivo `.link_files` es útil cuando un archivo específico debe estar disponible en varias etiquetas, pero el contenido debe ser idéntico en cada etiqueta.

Seguridad de contraseñas en el SO Oracle Solaris

Los usuarios que cambian las contraseñas frecuentemente reducen las posibilidades de que los intrusos utilicen contraseñas obtenidas de modo ilegal. Por lo tanto, la política de seguridad de su sitio puede solicitarle que cambie la contraseña con regularidad. El SO Oracle Solaris puede establecer requisitos de contenido para las contraseñas y aplicar requisitos de restablecimiento de contraseñas. A continuación, se indican los posibles requisitos de restablecimiento:

- **Número mínimo de días entre cambios:** evita que usted u otra persona cambien la contraseña durante un número de días determinado.
- **Número máximo de días entre cambios**: le solicita que cambie la contraseña después de un número de días determinado.
- **Número máximo de días inactivos**: bloquea la cuenta después de un número de días de inactividad establecido si la contraseña no se ha cambiado.
- **Fecha de caducidad**: le solicita que cambie la contraseña en una fecha específica.

Si el administrador ha implementado una de las opciones anteriores, usted recibirá un mensaje de correo electrónico donde se le advierte que debe cambiar la contraseña antes de la fecha límite.

Las contraseñas pueden tener criterios de contenido. Como mínimo, las contraseñas del SO Oracle Solaris deben cumplir con los siguientes criterios:

- La contraseña debe tener al menos ocho caracteres de longitud.
- La contraseña debe contener al menos dos caracteres alfabéticos y al menos un carácter numérico o un carácter especial.
- La contraseña nueva debe ser distinta de la contraseña anterior. No puede usar una contraseña que contenga los caracteres de la contraseña anterior en un orden inverso o circular. En esa comparación, no se hace distinción entre letras mayúsculas y minúsculas.

- La contraseña nueva debe tener al menos tres caracteres que sean diferentes de la contraseña anterior. En esa comparación, no se hace distinción entre letras mayúsculas y minúsculas.
- La contraseña debe ser difícil de adivinar. No utilice una palabra común o un nombre propio. Los programas y las personas que intentan acceder ilegalmente a una cuenta pueden utilizar listas para intentar adivinar las contraseñas de los usuarios.

Puede cambiar la contraseña mediante la opción de menú Change Password desde el menú Trusted Path. Para conocer los pasos, consulte Cómo cambiar la contraseña en Trusted Extensions [45].

Seguridad del área de trabajo en Trusted Extensions

En Trusted Extensions, los espacios de trabajo y las aplicaciones de escritorio reconocen etiquetas. Las aplicaciones se ejecutan en la etiqueta del espacio de trabajo actual y muestran información únicamente en la etiqueta del proceso que abrió la aplicación.

A continuación, se describe el comportamiento y la ubicación de las funciones de seguridad para los escritorios de confianza:

- El menú Trusted Path está disponible en la banda de confianza.
- El nombre de la etiqueta de una ventana en la lista de tareas del panel aparece en una pista cuando el mouse se desplaza por la ventana. De forma similar, el nombre de la etiqueta de un espacio de trabajo en el área de selección aparece en la pista.
- Para cambiar un rol, haga clic en el nombre de la cuenta en la banda de confianza y elija el rol.
- Para agregar un espacio de trabajo en una etiqueta determinada, seleccione un espacio de trabajo existente y cambie la etiqueta.
- El escritorio está configurado de modo que cada espacio de trabajo refleje el color de la etiqueta en la que está trabajando en ese espacio de trabajo. Los paneles de la banda inferior también muestran el color de la etiqueta.

Glosario

acreditación Una etiqueta que define el límite superior de un rango de etiquetas. Una acreditación tiene dos componentes: una clasificación y cero o más compartimientos. No es necesario que una acreditación sea una etiqueta bien formada. Una acreditación define un límite teórico, y no necesariamente una etiqueta real. Consulte también acreditación de usuario, acreditación de sesión y archivo de codificaciones de etiqueta.

acreditación de sesión Una acreditación establecida al iniciar sesión que define el límite superior de las etiquetas para una sesión de Trusted Extensions. Si el usuario tiene permiso para establecer la acreditación de sesión, puede especificar cualquier valor dentro del rango de etiquetas de cuenta del usuario. Si la cuenta del usuario está configurada para sesiones forzadas de un solo nivel, la acreditación de sesión se establece en el valor predeterminado especificado por el administrador de la seguridad. Consulte también acreditación.

acreditación de usuario Una acreditación asignada por el administrador de la seguridad. Una acreditación de usuario define el límite superior del rango de etiquetas de cuenta de un usuario. La acreditación de usuario determina la etiqueta más alta en la que el usuario tiene permiso para trabajar. Consulte también acreditación y acreditación de sesión.

administrador de la seguridad En un sistema que está configurado con Trusted Extensions, es el rol que se asigna a los usuarios responsables de definir y aplicar la política de seguridad. El administrador de la seguridad puede operar en cualquier etiqueta del rango de acreditación del sistema y es probable que tenga acceso a toda la información del sitio. El administrador de la seguridad configura los atributos de seguridad para todos los usuarios y equipos. Consulte también archivo de codificaciones de etiqueta.

administrador del sistema Una función de seguridad del SO Oracle Solaris.. El rol de administrador del sistema se puede asignar a los usuarios que son responsables de realizar tareas estándar de gestión del sistema, como configurar las partes no relevantes para la seguridad de las cuentas de usuario. Consulte también administrador de la seguridad.

aplicación de confianza Una aplicación a la que se han otorgado uno o varios privilegios.

archivo de codificaciones de etiqueta Un archivo gestionado por el administrador de la seguridad. El archivo de codificaciones contiene las definiciones de todas las etiquetas y acreditaciones válidas. El archivo también define el rango de acreditación del sistema y el rango de acreditación de usuario, y define la información de seguridad en las copias impresas del sitio.

área de trabajo Consulte área de trabajo con etiquetas.

área de trabajo con etiquetas Un espacio de trabajo que está asociado con una etiqueta. Un espacio de trabajo etiquetado etiqueta cada actividad que se inicia desde el espacio de trabajo con la etiqueta del espacio de trabajo. Cuando los usuarios mueven una ventana a un espacio de trabajo de una etiqueta diferente, la ventana movida conserva su etiqueta original. Cada espacio de trabajo en un escritorio de confianza está etiquetado. Dos espacios de trabajo pueden estar asociados con la misma etiqueta.

asignación de dispositivos Una función de seguridad del SO Oracle Solaris.. La asignación de dispositivos es un mecanismo para proteger la información de un dispositivo asignable contra el acceso de cualquier usuario, salvo el usuario que asigna el dispositivo. Cuando el dispositivo se desasigna, las secuencias de comandos device-clean se ejecutan para eliminar la información del dispositivo antes de que otro usuario pueda volver a acceder al dispositivo. En Trusted Extensions, Device Manager gestiona la asignación de dispositivos.

atributo de seguridad Una función de seguridad del SO Oracle Solaris.. Una propiedad de una entidad, como un proceso, una zona, un usuario o un dispositivo, que se relaciona con la seguridad. Los atributos de seguridad incluyen valores de identificación, como ID de usuario (UID) y ID de grupo (GID). Los atributos específicos de Trusted Extensions incluyen etiquetas y rangos de etiquetas. Tenga en cuenta que sólo determinados atributos de seguridad se aplican a un determinado tipo de entidad.

auditoría Una función de seguridad del SO Oracle Solaris.. La auditoría es un proceso para capturar la actividad del usuario y otros eventos del sistema, y, luego, almacenar esa información en un conjunto de archivos que se denomina *pista de auditoría*. La auditoría produce informes de actividades del sistema para cumplir con la política de seguridad del sitio.

autorización Una función de seguridad del SO Oracle Solaris.. Una autorización concede permiso a un usuario para realizar una acción que está prohibida conforme a la política de seguridad. El administrador de la seguridad asigna autorizaciones a los perfiles de derechos. Los perfiles de derechos luego se asignan a cuentas de usuario o rol. Algunos comandos y acciones no funcionan por completo, a menos que el usuario tenga las autorizaciones necesarias. Consulte también privilegio.

banda de confianza Un gráfico rectangular que aparece a lo ancho de la pantalla en un área reservada. La banda de confianza aparece en cada sesión de Trusted Extensions para confirmar que se trata de una sesión de Trusted Extensions válida. La banda de confianza tiene dos componentes: (1) un símbolo de confianza obligatorio para indicar interacción con la base de computación de confianza (TCB, Trusted Computing Base) y (2) una etiqueta para indicar la etiqueta de la ventana o el espacio de trabajo actual.

base de computación de confianza (TCB, Trusted La parte de un sistema que está configurada con Trusted Extensions que afecta a la seguridad. La TCB incluye software, hardware, firmware, documentación y procedimientos administrativos. Los programas de utilidad y los programas de aplicación que pueden acceder a archivos relacionados con la seguridad son parte de base de computación de confianza.

Computing Base)

canal oculto Un canal de comunicación que normalmente no está destinado a la comunicación de datos. Un canal oculto permite que un proceso transfiera información indirectamente de un modo que viola el objetivo de la política de seguridad.

clasificación Un componente de una acreditación o una etiqueta. Una clasificación indica un nivel jerárquico de seguridad, por ejemplo, `TOP SECRET` o `UNCLASSIFIED`.

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 un grupo de usuarios con una posible necesidad de acceder a esta información, como un departamento de ingeniería o un equipo de proyecto multidisciplinario.

configuración ampliada Un sistema informático que ya no es una configuración valorable debido a las modificaciones que han violado la política de seguridad.

configuración de un solo nivel Una cuenta de usuario que se ha configurado para operar en una sola etiqueta. También se denomina configuración de un solo nivel.

configuración valorable Un sistema informático que cumple con un conjunto de requisitos de seguridad del gobierno. Consulte también configuración ampliada.

control de acceso discrecional (DAC, Discretionary Access Control) Un mecanismo de control de acceso que permite al propietario de un archivo o directorio conceder o denegar el acceso a otros usuarios. El propietario asigna permisos de lectura, escritura y ejecución al propietario, al grupo de usuarios al que pertenece el propietario y a una categoría denominada Otros, que se refiere a todos los demás usuarios no especificados. El propietario también puede especificar una lista de control de acceso (ACL, Access Control List). Una ACL le permite al propietario asignar permisos específicamente a usuarios y grupos adicionales. Compárela con el control de acceso obligatorio (MAC, Mandatory Access Control).

control de acceso obligatorio (MAC, Mandatory Access Control) Un mecanismo de control de acceso aplicado por el sistema que utiliza acreditaciones y etiquetas para aplicar la política de seguridad. Una acreditación o una etiqueta es un nivel de seguridad. El MAC asocia los programas que un usuario ejecuta con el nivel de seguridad que el usuario elige para trabajar en la sesión. Además, el MAC permite el acceso a información, programas y dispositivos en el mismo nivel o sólo en un nivel inferior. El MAC también evita que los usuarios realicen escrituras en archivos en niveles inferiores. El MAC no se puede sustituir sin una autorización o un privilegio especial. Compárelo con control de acceso discrecional (DAC, Discretionary Access Control).

Device Manager Una aplicación de confianza de Trusted Extensions. Esta interfaz gráfica de usuario se utiliza para configurar, asignar y desasignar dispositivos. La configuración de dispositivos incluye la agregación de requisitos de autorización a un dispositivo.

dispositivo Consulte dispositivo asignable.

dispositivo asignable Una función de seguridad del SO Oracle Solaris.. Un dispositivo asignable puede ser utilizado por un usuario a la vez, y tiene la capacidad de importar o exportar datos del sistema. El administrador de la seguridad determina qué usuarios están autorizados a acceder a qué dispositivos asignables. Los dispositivos asignables incluyen unidades de cinta, dispositivos de audio y dispositivos de CD-ROM. Consulte también asignación de dispositivos.

dispositivo desasignado Una función de seguridad del SO Oracle Solaris.. Un dispositivo desasignado ya no está asignado a un usuario para uso exclusivo. Consulte también asignación de dispositivos.

dominio estricto Consulte etiqueta dominante.

estación de trabajo de modo compartimentado (CMW, Compartmented Mode Workstation) Un sistema informático que cumple con los requisitos gubernamentales para estaciones de trabajo de confianza, según lo indicado en el documento DIA número DDS-5502-2600-87, *Requisitos de seguridad para estaciones de trabajo de modo compartimentado y alta seguridad*. En concreto, define un sistema operativo basado en un sistema de ventanas X de confianza para estaciones de trabajo UNIX.

etiqueta También se denomina Etiqueta de sensibilidad. Una etiqueta indica el nivel de seguridad de una entidad. Una entidad es una interfaz de archivo, directorio, proceso, dispositivo o red. La etiqueta de una entidad se utiliza para determinar si se debe permitir el acceso en una transacción determinada. Las etiquetas tienen dos componentes: una clasificación que indica el nivel jerárquico de seguridad, y cero o más compartimientos para definir quién puede acceder a la entidad en una clasificación determinada. Consulte también archivo de codificaciones de etiqueta.

etiqueta actualizada La etiqueta de un objeto que se ha cambiado a un valor que domina el valor anterior de la etiqueta.

etiqueta bien formada Una etiqueta que se puede incluir en un rango, ya que todas las reglas aplicables del archivo de codificaciones de etiqueta permiten la etiqueta.

etiqueta de sensibilidad Consulte etiqueta.

etiqueta degradada La etiqueta de un objeto que se ha cambiado a un valor que no domina el valor anterior de la etiqueta.

etiqueta dominante En una comparación de dos etiquetas, se trata de la etiqueta cuyo componente de clasificación es mayor o igual que la clasificación de la segunda etiqueta y cuyos componentes de compartimiento incluyen todos los componentes de compartimiento de la segunda etiqueta. Si los componentes son los mismos, se dice que las etiquetas se dominan entre sí y son *iguales*. Si una etiqueta domina a la otra y las etiquetas no son iguales, se dice que la primera etiqueta

domina estrictamente a la otra. Dos etiquetas están *separadas* si no son iguales y ninguna de ellas es dominante.

etiqueta mínima Una etiqueta que se asignó a un usuario como el límite inferior del conjunto de etiquetas en las que ese usuario puede trabajar. Cuando un usuario inicia una sesión de Trusted Extensions por primera vez, la etiqueta mínima es la etiqueta predeterminada del usuario. En el inicio de sesión, el usuario puede elegir una etiqueta diferente para la etiqueta inicial.

También puede elegir la etiqueta más baja que se permite a cualquier usuario no administrativo. El administrador de la seguridad asigna la etiqueta mínima y define la parte inferior del rango de acreditación de usuario.

etiqueta separada Consulte etiqueta dominante.

etiquetas administrativas Dos etiquetas especiales destinadas solamente a archivos administrativos: `ADMIN_LOW` y `ADMIN_HIGH`. `ADMIN_LOW` es la etiqueta más baja del sistema sin compartimientos. Esta etiqueta está estrictamente dominada por todas las etiquetas del sistema. Todos pueden leer la información de `ADMIN_LOW`, pero sólo puede escribirla un usuario con un rol que esté trabajando en la etiqueta `ADMIN_LOW`. `ADMIN_HIGH` es la etiqueta más alta del sistema con todos los compartimientos. Esta etiqueta domina estrictamente todas las etiquetas del sistema. Sólo pueden leer la información de `ADMIN_HIGH` los usuarios con roles que operen en `ADMIN_HIGH`. Las etiquetas administrativas se utilizan como etiquetas o acreditaciones para roles y sistemas. Consulte también etiqueta dominante.

generador de etiquetas Una aplicación de confianza de Trusted Extensions. Esta interfaz gráfica de usuario permite a los usuarios seleccionar un permiso de sesión o una etiqueta de sesión. La acreditación o la etiqueta deben estar comprendidas dentro del rango de etiquetas de cuenta que el administrador de la seguridad ha asignado al usuario.

gestión de funciones de confianza Todas las actividades asociadas con la administración de un sistema UNIX convencional, más todas las actividades administrativas que son necesarias para mantener la seguridad de un sistema distribuido y los datos que contiene el sistema.

host Un equipo conectado a una red.

ID de auditoría (AUID) Una función de seguridad del SO Oracle Solaris.. Un ID de auditoría representa al usuario de inicio de sesión. El AUID no cambia después de que el usuario asume un rol; por lo tanto, se utiliza a fin de identificar al usuario para fines de auditoría. El ID de auditoría siempre representa al usuario para la auditoría, incluso cuando el usuario adquiere UID/GID efectivo. Consulte también ID de usuario (UID).

ID de grupo (GID) Una función de seguridad del SO Oracle Solaris.. Un GID es un número entero que identifica un grupo de usuarios que tienen permisos de acceso en común. Consulte también control de acceso discrecional (DAC, Discretionary Access Control).

ID de usuario (UID) Una función de seguridad del SO Oracle Solaris.. Un UID identifica un usuario para fines de control de acceso discrecional (DAC, Discretionary Access Control), control de acceso

obligatorio (MAC, Mandatory Access Control) y auditoría. Consulte también permiso de acceso.

lista de control de acceso (ACL, Access Control List) Una función de seguridad del SO Oracle Solaris.. Una ACL amplía el control de acceso discrecional (DAC, Discretionary Access Control) para utilizar una lista de especificaciones de permiso (entradas de ACL) que se aplican a usuarios y grupos específicos. Una ACL permite un control más específico que el control proporcionado por los permisos de UNIX estándar.

mecanismo de reserva Un método abreviado para especificar direcciones IP en la base de datos`tnrhtp`. Para las direcciones IPv4, el mecanismo de reserva reconoce el `0` como un comodín para una subred.

Menú Trusted Path Un menú de las operaciones de Trusted Extensions que aparece si se presiona el tercer botón del mouse en el área de selección del panel frontal. Las selecciones del menú se dividen en tres categorías: selecciones orientadas al espacio de trabajo, selecciones de asunción de un rol y tareas relacionadas con la seguridad.

objeto Una entidad pasiva que contiene o recibe datos, como un archivo de datos, un directorio, una impresora u otro dispositivo. Un sujeto es quien pone en funcionamiento un objeto. En algunos casos, un proceso puede ser un objeto, como cuando se envía una señal a un proceso.

operador Un rol que se le pueden asignar al usuario o a los usuarios responsables de realizar copias de seguridad de los sistemas.

perfil Consulte perfil de derechos.

perfil de derechos Una función de seguridad del SO Oracle Solaris.. Un perfil de derechos permite que el administrador de la seguridad de un sitio integre comandos con atributos de seguridad. Los atributos como las autorizaciones y los privilegios de usuario permiten que los comandos se ejecuten correctamente. Un perfil de derechos suele incluir tareas relacionadas. Un perfil se puede asignar a usuarios y roles.

permiso de acceso Una función de seguridad de la mayoría de los sistemas informáticos. El permiso de acceso proporciona al usuario el derecho a leer, escribir, ejecutar o ver el nombre de un archivo o de un directorio. Consulte también control de acceso discrecional (DAC, Discretionary Access Control) y control de acceso obligatorio (MAC, Mandatory Access Control).

permiso de acceso a nivel de seguridad igual o inferior La capacidad de un sujeto de ver un objeto cuya etiqueta domina. La política de seguridad, en general, concede el permiso de acceso a nivel de seguridad igual o inferior. Por ejemplo, un programa editor de texto que se ejecuta como `Secret` puede leer datos `Unclassified`. Consulte también control de acceso obligatorio (MAC, Mandatory Access Control).

permisos Un conjunto de códigos que indican los usuarios que tienen permiso para leer, escribir o ejecutar el archivo o el directorio (carpeta). Los usuarios se clasifican como propietario, grupo (el grupo del propietario) y otros (todos los demás). El permiso de lectura (indicado con la letra *r*) permite al usuario leer el contenido de un archivo o, si se trata de un directorio, enumerar los archivos de la carpeta. El permiso de escritura (*w*) permite al usuario realizar modificaciones en

un archivo o, si se trata de una carpeta, agregar o suprimir archivos. El permiso de ejecución (*e*) permite al usuario ejecutar el archivo si el archivo es ejecutable. Si el archivo es un directorio, el permiso de ejecución permite al usuario leer los archivos o buscarlos en el directorio. También se denomina permisos UNIX o bits de permiso.

plantilla de host Un registro en la base de datos `tnrhtp` que define los atributos de seguridad de una clase de hosts que puede acceder a la red de Trusted Extensions.

política de seguridad El conjunto de DAC, MAC y reglas de etiquetas que definen cómo se puede acceder a la información y quién puede acceder a ella. En un sitio de cliente, es el conjunto de reglas que definen la sensibilidad de la información que se procesa en ese sitio. La política incluye las medidas que se utilizan para proteger la información contra el acceso no autorizado.

principio de privilegio mínimo El principio de seguridad que restringe las funciones de los usuarios sólo a las funciones que son necesarias para realizar sus trabajos. El principio se aplica en el SO Oracle Solaris al poner los privilegios a disposición de los programas según sea necesario. Los privilegios están disponibles según sea necesario sólo para fines específicos.

privilegio Una función de seguridad del SO Oracle Solaris.. Un privilegio es un permiso que el administrador de la seguridad otorga a un programa. Un privilegio se puede requerir para sustituir algún aspecto de la política de seguridad. Consulte también autorización.

privilegio mínimo Consulte principio de privilegio mínimo.

proceso Un programa en ejecución. Los procesos de Trusted Extensions tienen atributos de seguridad Oracle Solaris, como ID de usuario (UID), ID de grupo (GID), el ID de auditoría (AUID) del usuario y privilegios. Trusted Extensions agrega una etiqueta a cada proceso.

proceso con privilegios Una función de seguridad del SO Oracle Solaris.. Un proceso con privilegios se ejecuta con privilegios asignados.

puerta de enlace Un host que tiene más de una interfaz de red. Este host se puede utilizar para conectar dos o más redes. Cuando la puerta de enlace es un host de Trusted Extensions, ésta puede restringir el tráfico a una etiqueta determinada.

rango de acreditación Un conjunto de etiquetas que se aprueban para una clase de usuarios o recursos. Consulte también rango de acreditación del sistema, rango de acreditación de usuario, archivo de codificaciones de etiqueta y rango de acreditación de red.

rango de acreditación de red El conjunto de etiquetas en el que se hospeda Trusted Extensions tiene permiso para comunicarse en una red. El conjunto puede ser una lista de cuatro etiquetas discretas.

rango de acreditación de usuario El mayor conjunto de etiquetas que el administrador de la seguridad puede asignar a un usuario en un sitio específico. El rango de acreditación de usuario excluye las etiquetas administrativas y cualquier combinación de etiquetas que estén disponibles solamente para los administradores. El rango de acreditación de usuario se define en el archivo de codificaciones de etiqueta.

rango de acreditación del sistema El conjunto de todas las etiquetas válidas para un sitio. El conjunto incluye las etiquetas administrativas que están disponibles para el administrador de la seguridad y el administrador del sistema del sitio. El rango de acreditación del sistema se define en el archivo de codificaciones de etiqueta.

rango de etiquetas Cualquier conjunto de etiquetas limitadas en el extremo superior por una acreditación o una etiqueta máxima y en el extremo inferior por una etiqueta mínima, y que consta de etiquetas bien formadas. Los rangos de etiqueta se utilizan para aplicar el control de acceso obligatorio (MAC, Mandatory Access Control). Consulte también archivo de codificaciones de etiqueta, rango de etiquetas de cuenta, rango de acreditación, rango de acreditación de red, rango de sesión, rango de acreditación del sistema y rango de acreditación de usuario.

rango de etiquetas de cuenta El conjunto de etiquetas que asigna el administrador de la seguridad a un usuario o rol para trabajar en un sistema en el que está configurado Trusted Extensions. Un rango de etiquetas está definido en el extremo superior por la acreditación de usuario y en el extremo inferior por la etiqueta mínima del usuario. El conjunto se limita a las etiquetas bien formadas.

rango de sesión El conjunto de etiquetas que están disponibles para un usuario durante una sesión de Trusted Extensions. El rango de sesión está delimitado por la acreditación de sesión del usuario en el extremo superior y por la etiqueta mínima en el extremo inferior.

rol Una función de seguridad del SO Oracle Solaris.. Un rol es una cuenta especial que concede al usuario que asume el rol acceso a determinadas aplicaciones y el atributo de seguridad que sea necesario para realizar las funciones específicas.

ruta de confianza Hace referencia al mecanismo para acceder a acciones y comandos que tienen permiso para interaccionar con la base de computación de confianza (TCB, Trusted Computing Base). Consulte también Menú Trusted Path, símbolo de confianza y banda de confianza.

Selection Manager Una aplicación de confianza de Trusted Extensions. Esta interfaz gráfica de usuario aparece cuando los usuarios autorizados intentan actualizar o degradar la información.

sesión El tiempo transcurrido entre la conexión con un host de Trusted Extensions y la desconexión del host. La banda de confianza aparece en todas las sesiones de Trusted Extensions para confirmar que un sistema falsificado no suplantará a los usuarios.

shell de perfil Una función de seguridad del SO Oracle Solaris.. Una versión del shell Bourne que permite al usuario ejecutar programas con más de un atributo de seguridad.

símbolo de confianza El símbolo que aparece a la izquierda del área de la banda de confianza. El símbolo se muestra cada vez que el usuario accede a una parte de la base de computación de confianza (TCB, Trusted Computing Base).

sujeto Una entidad activa; en general, un proceso que se ejecuta en nombre de un usuario o un rol. Un sujeto hace que la información fluya entre los objetos; de lo contrario cambia el estado del sistema.

suplantar Falsificar un programa de software para acceder ilegalmente a la información en un sistema.

tipo de host La clasificación de un host. La clasificación se utiliza para las comunicaciones de red. Las definiciones de tipos de host se almacenan en la base de datos `tnrhtp`. El tipo de host determina si el protocolo de red CIPSO se utiliza para comunicarse con otros hosts de la red. *Protocolo de red* hace referencia a las reglas de empaquetado de información de comunicación.

Trusted GNOME Un escritorio gráfico etiquetado que incluye un gestor de sesiones, un gestor de ventanas y distintas herramientas de escritorio. Se puede acceder por completo al escritorio.

UID/GID efectivo Una función de seguridad del SO Oracle Solaris.. Cuando es necesario, los ID efectivos sustituyen un ID real para ejecutar un programa determinado o la opción de un programa. El administrador de la seguridad asigna un UID efectivo a un comando o acción en un perfil de derechos cuando ese comando o acción deben ser ejecutados por un usuario específico, principalmente cuando el comando se debe ejecutar como root. Los ID de grupo efectivo se utilizan de la misma manera. Tenga en cuenta que, posiblemente, el uso del comando `setuid` como en los sistemas UNIX convencionales no funcione debido a que se necesitan privilegios.

usuario común Un usuario que no posee ninguna autorización especial que permite excepciones a las políticas de seguridad estándar del sistema. Normalmente, un usuario común no puede asumir un rol administrativo.

visualización de etiqueta Función de seguridad que muestra las etiquetas administrativas o sustituye los marcadores de posición sin clasificar por las etiquetas administrativas. Por ejemplo, si la política de seguridad prohíbe exponer las etiquetas `ADMIN_HIGH` y `ADMIN_LOW` , las etiquetas `RESTRICTED` y `PUBLIC` se pueden sustituir.

Índice

C

D

E

O

P

R

S

T

U

V

Z