Guide de l'utilisateur Oracle® Solaris Trusted Extensions

Référence : E25056
Novembre 2011

ORACLE®

Copyright © 1997, 2011, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

U.S. GOVERNMENT RIGHTS

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée de The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation.

120424@25097

Table des matières

Liste des figures

Liste des tableaux

Préface

Le *Guide de l'utilisateur Oracle Solaris Trusted Extensions* est un guide d'utilisation du Système d'exploitation Oracle Solaris (SE Oracle Solaris) avec la fonction Trusted Extensions installée.

Utilisateurs de ce guide

Ce guide est destiné à tous les utilisateurs de Trusted Extensions. Vous devez être familiarisé avec l'utilisation du SE Oracle Solaris et du bureau GNOME Open Source.

Vous devez également être familiarisé avec la stratégie de sécurité de votre organisation.

Organisation des guides Trusted Extensions

Le tableau suivant répertorie les sujets abordés dans les guides Trusted Extensions et le public auxquels ils s'adressent.

Titre du guide	Sujets	Public visé
Guide de l'utilisateur Oracle Solaris Trusted Extensions	Décrit les fonctions de base de Trusted Extensions. Ce guide contient un glossaire.	Utilisateurs, administrateurs, développeurs
Configuration et administration d'Oracle Solaris Trusted Extensions	La partie I décrit la préparation, l'activation et la configuration initiale de Trusted Extensions. La partie II décrit l'administration d'un système Trusted Extensions. Ce guide contient un glossaire.	Administrateurs, développeurs
Trusted Extensions Developer's Guide	Décrit le développement d'applications avec Trusted Extensions.	Développeurs, administrateurs
Trusted Extensions Label Administration	Fournit des informations sur la manière de spécifier les composants d'étiquette dans le fichier label_encodings.	Administrateurs
Compartmented Mode Workstation Labeling: Encodings Format	Décrit la syntaxe utilisée dans le fichier label_encodings. La syntaxe applique les différentes règles permettant de créer des étiquettes bien formées pour un système.	Administrateurs

Organisation de ce guide

Le Chapitre 1, “Introduction à Trusted Extensions”, décrit les concepts de base mis en œuvre sur un système Oracle Solaris doté de la fonction Trusted Extensions.

Le Chapitre 2, “Connexion à Trusted Extensions (tâches)”, présente les procédures permettant d'accéder et de quitter un système Trusted Extensions.

Le Chapitre 3, “Utilisation de Trusted Extensions (tâches)”, décrit l'utilisation de Trusted Extensions.

Le Chapitre 4, “Eléments de Trusted Extensions (Référence)”, présente les éléments clés d'un système doté de la fonction Trusted Extensions.

Le Glossaire décrit les termes relatifs à la sécurité utilisés dans Trusted Extensions.

Accès au support technique Oracle

Les clients Oracle ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` adapté aux utilisateurs malentendants.

Conventions typographiques

Le tableau ci-dessous décrit les conventions typographiques utilisées dans ce manuel.

TABLEAU P–1 Conventions typographiques

Type de caractères	Signification	Exemple
`AaBbCc123`	Noms des commandes, fichiers et répertoires, ainsi que messages système.	Modifiez votre fichier `.login`. Utilisez `ls -a` pour afficher la liste de tous les fichiers. `nom_machine% Vous avez reçu du courrier.`
`AaBbCc123`	Ce que vous entrez, par opposition à ce qui s'affiche à l'écran.	`nom_machine%` **`su`** `Mot de passe :`
aabbcc123	Paramètre fictif : à remplacer par un nom ou une valeur réel(le).	La commande permettant de supprimer un fichier est `rm` *filename* .

TABLEAU P–1 Conventions typographiques *(Suite)*

Type de caractères	Signification	Exemple
AaBbCc123	Titres de manuel, nouveaux termes et termes importants.	Reportez-vous au chapitre 6 du *Guide de l'utilisateur*. Un *cache* est une copie des éléments stockés localement. *N'enregistrez pas* le fichier. **Remarque :** en ligne, certains éléments mis en valeur s'affichent en gras.

Invites de shell dans les exemples de commandes

Le tableau suivant présente l'invite système UNIX par défaut et l'invite superutilisateur pour les shells faisant partie du SE Oracle Solaris. L'invite système par défaut qui s'affiche dans les exemples de commandes dépend de la version Oracle Solaris.

TABLEAU P–2 Invites de shell

Shell	Invite
Shell Bash, shell Korn et shell Bourne	`$`
Shell Bash, shell Korn et shell Bourne pour superutilisateur	`#`
C shell	`nom_machine%`
C shell pour superutilisateur	`nom_machine#`

◆ ◆ ◆ CHAPITRE 1

1 Introduction à Trusted Extensions

Ce chapitre présente les étiquettes et autres fonctions de sécurité que la fonction Trusted Extensions ajoute au Système d'exploitation Oracle Solaris (SE Oracle Solaris)

Définition de Trusted Extensions

Trusted Extensions offre des fonctionnalités de sécurité particulières pour votre système Oracle Solaris. Ces fonctionnalités permettent à une organisation de définir et de mettre en œuvre une stratégie de sécurité sur un système Oracle Solaris. Une *stratégie de sécurité* correspond à l'ensemble de règles et de pratiques qui vous aident à protéger les informations et autres ressources telles que le matériel informatique sur votre site. En général, les règles de sécurité gèrent les autorisations d'accès de chacun aux différents types d'informations et définissent par exemple les personnes autorisées à écrire des données sur des médias amovibles. Les *pratiques de sécurité* sont des procédures recommandées pour l'exécution des tâches.

Les sections suivantes décrivent les principales fonctions de sécurité offertes par Trusted Extensions. Le texte indique les fonctionnalités de sécurité configurables.

Trusted Extensions vous protège contre les intrus

Trusted Extensions ajoute au SE Oracle Solaris des fonctionnalités qui vous protègent contre les intrusions. Trusted Extensions s'appuie également sur certaines fonctionnalités d'Oracle Solaris, telles que la protection par mot de passe. Trusted Extensions ajoute une interface graphique de changement de mot de passe pour les rôles. Par défaut, les utilisateurs doivent être autorisés à utiliser un périphérique, tel qu'un microphone ou une caméra.

L'accès à la base informatique sécurisée est limité

L'expression *base informatique de confiance* (*TCB, Trusted Computing Base*) fait référence à la partie du logiciel Trusted Extensions qui gère les événements liés à la sécurité. La TCB englobe les logiciels, le matériel, les microprogrammes, la documentation et les procédures administratives. Les utilitaires et programmes d'application pouvant accéder aux fichiers relatifs à la sécurité font tous partie de la TCB. Votre administrateur définit les limites de toutes les interactions potentielles que vous pouvez avoir avec la TCB. Ces interactions incluent les programmes dont vous avez besoin pour effectuer votre travail, les fichiers auxquels vous êtes autorisé à accéder et les utilitaires qui peuvent compromettre la sécurité.

Le contrôle d'accès obligatoire protège les informations

Si un intrus parvient à se connecter au système, d'autres d'obstacles l'empêchent d'accéder aux informations. Les fichiers et autres ressources sont protégés par le contrôle d'accès. Comme dans le SE Oracle Solaris, le contrôle d'accès peut être défini par le propriétaire des informations. Dans Trusted Extensions, l'accès est également contrôlé par le système. Pour plus d'informations, reportez-vous à la section "Trusted Extensions fournit des contrôles d'accès discrétionnaire et obligatoire" à la page 17.

Les périphériques sont protégés

Dans Trusted Extensions, les administrateurs contrôlent l'accès aux périphériques locaux tels que des lecteurs de bande, les lecteurs de CD-ROM, les périphériques USB, les imprimantes et les microphones. L'accès peut être accordé au cas par cas. Le logiciel limite l'accès aux périphériques, comme suit :

- Par défaut, les périphériques doivent être alloués pour être utilisés.
- Vous devez posséder des autorisations pour accéder aux périphériques contrôlant les médias amovibles.
- Les utilisateurs distants ne peuvent pas utiliser les périphériques locaux tels que les microphones ou les lecteurs de CD-ROM. Seuls les utilisateurs locaux peuvent allouer un périphérique.

Les programmes qui usurpent l'identité des utilisateurs sont bloqués

Usurper signifie emprunter une fausse identité. Les intrus usurpent parfois les identifiants de connexion ou d'autres programmes légitimes pour intercepter des mots de passe ou d'autres données sensibles. Trusted Extensions vous protège contre l'usurpation d'identité hostile en affichant le *symbole de confiance*, une icône d'inviolabilité facilement identifiable en haut de l'écran.

FIGURE 1–1 Symbole de confiance

Ce symbole s'affiche à chaque fois que vous interagissez avec la base informatique sécurisée (TCB). La présence du symbole garantit la sécurité des transactions. L'absence de symbole indique une faille de sécurité potentielle. La Figure 1–1 présente le symbole de confiance.

Trusted Extensions fournit des contrôles d'accès discrétionnaire et obligatoire

Trusted Extensions gère les utilisateurs qui peuvent accéder aux informations en proposant à la fois un contrôle d'accès discrétionnaire et un contrôle d'accès obligatoire.

Contrôle d'accès discrétionnaire

Le contrôle d'accès discrétionnaire (DAC) est un mécanisme logiciel qui permet de contrôler l'accès des utilisateurs aux fichiers et aux répertoires. Le DAC laisse à la discrétion du propriétaire la définition de la protection des fichiers et des répertoires. Les deux formes de DAC sont les bits d'autorisation UNIX et les listes de contrôle d'accès (ACL).

Les bits d'autorisation permettent au propriétaire de définir la protection en lecture, écriture et exécution en fonction du statut de l'utilisateur : propriétaire, groupe et autres utilisateurs. Sur les systèmes UNIX classiques, le superutilisateur ou l'utilisateur `root` peut passer outre à la protection DAC. Avec Trusted Extensions, les administrateurs et les utilisateurs autorisés peuvent passer outre au DAC. Les listes de contrôle d'accès (ACL) fournissent une granularité plus fine du contrôle d'accès. Les ACL permettent aux propriétaires de spécifier des permissions distinctes pour des utilisateurs et des groupes spécifiques. Pour plus d'informations, reportez-vous au Chapitre 8, “Utilisation des ACL et des attributs pour protéger les fichiers Oracle Solaris ZFS” du manuel *Administration d'Oracle Solaris : Systèmes de fichiers ZFS*.

Contrôle d'accès obligatoire

Le contrôle d'accès obligatoire (MAC) est un mécanisme de contrôle d'accès appliqué par le système et basé sur les relations entre les étiquettes. Le système associe une étiquette de sensibilité à tous les processus créés pour exécuter des programmes. La stratégie MAC utilise cette étiquette dans les décisions de contrôle d'accès. En général, les processus ne peuvent pas stocker d'informations ni communiquer avec d'autres processus, sauf si l'étiquette de la destination est égale à l'étiquette du processus. La stratégie MAC autorise les processus à lire des données d'objets de même niveau d'étiquette ou d'un niveau inférieur. Toutefois, l'administrateur peut créer un environnement étiqueté dans lequel peu d'objets de niveau inférieur, voire aucun, ne sont disponibles.

Par défaut, la stratégie MAC vous est invisible. Les utilisateurs standard ne peuvent pas voir d'objets sauf s'ils disposent d'un accès MAC à ces objets. Dans tous les cas, les utilisateurs ne peuvent pas effectuer d'action contraire à la stratégie MAC.

Etiquettes de sensibilité et autorisations

Une étiquette possède les deux composants suivants :

- Classification, également appelée *niveau*

  Ce composant indique un niveau de sécurité hiérarchique. Lorsqu'elle est appliquée à des personnes, la classification représente une mesure de confiance. Lorsqu'elle est appliquée à des données, la classification correspond au degré de protection requis.

  Au sein du gouvernement américain, les classifications sont `TOP SECRET`, `SECRET`, `CONFIDENTIAL` et `UNCLASSIFIED`. Les classifications industrielles ne sont pas normalisées. Une entreprise peut établir des classifications uniques. Pour obtenir un exemple, reportez-vous à la Figure 1–2. Les termes figurant sur la gauche sont les classifications. Les termes figurant sur la droite sont les compartiments.

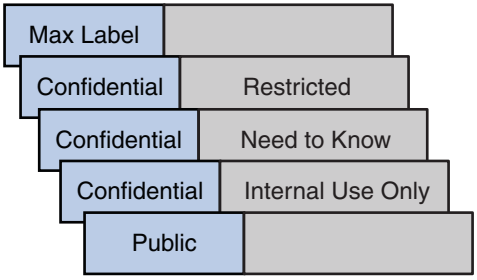
- Compartiments, également appelés *catégories*

  Un compartiment représente un groupement, tel qu'un groupe de travail, un service, un projet ou un sujet. Une classification n'a pas besoin d'avoir de compartiment. Dans la Figure 1–2, la classification `Confidential` possède trois compartiments exclusifs. Les classifications `Public` et `Etiquette maximale` n'ont aucun compartiment. Comme le montre cette figure, cinq étiquettes sont définies par cette organisation.

Trusted Extensions gère deux types d'étiquettes : les *étiquettes de sensibilité* et les *autorisations*. Un utilisateur peut être autorisé à travailler sur une ou plusieurs étiquettes de sensibilité. Une étiquette spéciale, appelée *autorisation de l'utilisateur*, détermine le plus haut niveau d'étiquette sur laquelle un utilisateur est autorisé à travailler. En outre, chaque utilisateur possède une étiquette de sensibilité minimum. Cette étiquette est utilisée par défaut lors de la connexion à une session de bureau multiniveau. Après la connexion, l'utilisateur peut choisir de travailler sur d'autres étiquettes dans cette plage. Un utilisateur peut posséder l'étiquette de sensibilité minimum `Public` et l'autorisation `Confidential : Need to Know`. A la première connexion,

les espaces de travail du bureau se trouvent au niveau d'étiquette `Public`. Au cours de la session, l'utilisateur peut créer des espaces de travail possédant les étiquettes `Confidential: Internal Use Only` et `Confidential: Need to Know`.

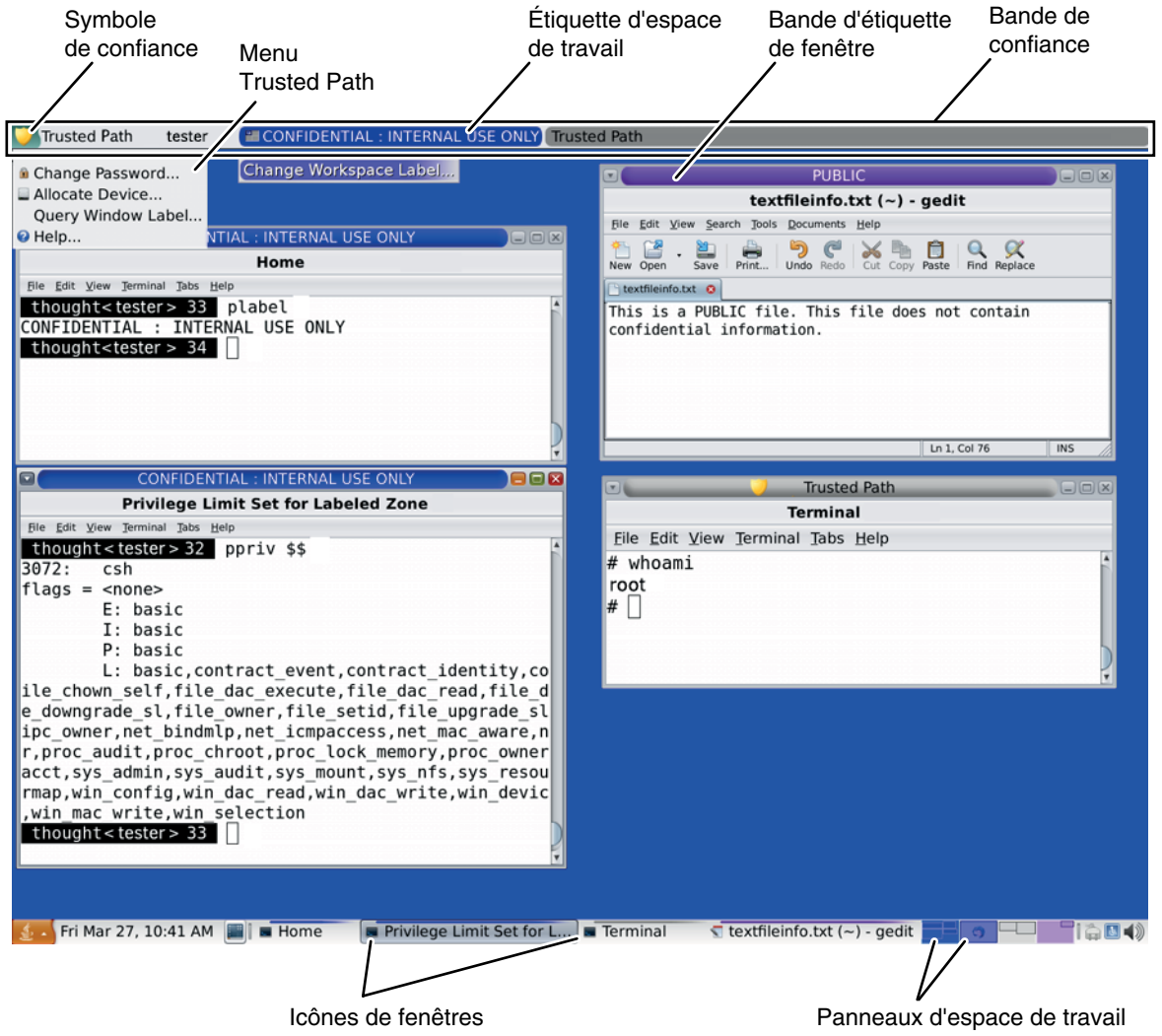
FIGURE 1–2 Etiquettes de sensibilité classiques dans l'industrie



Sur un système configuré avec Trusted Extensions, tous les sujets et les objets possèdent des étiquettes. Un *sujet* est une entité active, généralement un processus. Le processus fait circuler des informations entre les objets ou modifie l'état du système. Un *objet* est une entité passive qui contient ou reçoit des données, telle qu'un fichier de données, un répertoire, une imprimante ou un autre périphérique. Dans certains cas, un processus peut être un objet, par exemple lorsque vous utilisez la commande `kill` sur un processus.

La Figure 1–3 présente une session multiniveau classique de Trusted Extensions. La bande de confiance se trouve en haut. Le menu Trusted Path (Chemin de confiance) est appelé à partir de la bande de confiance. Pour assumer un rôle, cliquez sur le nom d'utilisateur pour afficher le menu des rôles. Les commutateurs de l'espace de travail du panneau inférieur affichent la couleur de l'étiquette de l'espace de travail. La liste de fenêtres en bas de l'écran affiche la couleur de l'étiquette de la fenêtre.

FIGURE 1–3 Session multiniveau classique



Conteneurs et étiquettes

Trusted Extensions utilise des conteneurs pour l'étiquetage. Les conteneurs sont également appelés *zones*. La *zone globale* est une zone d'administration et n'est pas disponible pour les utilisateurs. Les zones non globales sont appelées *zones étiquetées*. Les zones étiquetées sont disponibles pour les utilisateurs. La zone globale partage certains systèmes de fichiers avec des utilisateurs. Lorsque ces fichiers sont visibles dans une zone étiquetée, l'étiquette de ces fichiers est `ADMIN_LOW`. Les utilisateurs peuvent lire, mais ne peuvent pas accéder au contenu d'un fichier `ADMIN_LOW`.

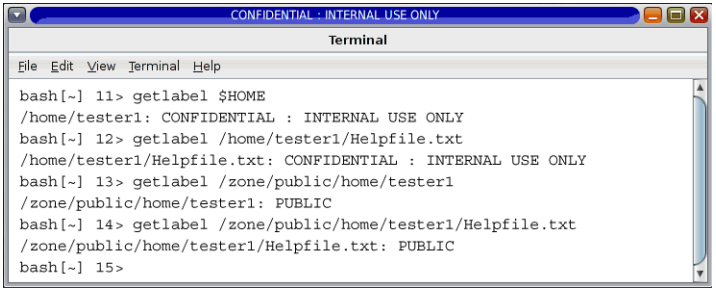
La communication réseau est limitée par étiquette. Par défaut, les zones ne peuvent pas communiquer les unes avec les autres car leurs étiquettes sont différentes. Par conséquent, une zone ne peut pas écrire dans une autre zone.

Toutefois, l'administrateur peut configurer des zones spécifiques afin qu'elles puissent lire des répertoires spécifiques d'autres zones. Les autres zones peuvent se trouver sur le même hôte ou sur un système distant. Par exemple, le répertoire personnel d'un utilisateur situé dans une zone de niveau inférieur peut être monté à l'aide du service de montage automatique. La convention de nommage du chemin d'accès pour ce type de montage de répertoires personnels de niveau inférieur comprend le nom de la zone, comme suit :

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

La fenêtre de terminal suivante illustre la visibilité du répertoire personnel de niveau inférieur. Un utilisateur dont l'étiquette de connexion est `Confidential: Internal Use Only` peut visualiser le contenu de la zone `Public` lorsque la commande de montage automatique est configurée de manière à rendre lisibles les zones de niveau inférieur. Il existe deux versions du fichier `textfileinfo.txt`. La version de la zone `Public` contient des informations qui peuvent être partagées avec le public. La version `Confidential: Internal Use Only` contient des informations qui ne peuvent être partagées qu'au sein de l'entreprise.

FIGURE 1–4 Affichage d'informations publiques à partir d'une zone d'étiquette supérieure



Etiquettes et transactions

Le logiciel Trusted Extensions gère toutes les transactions relevant de la sécurité tentées. Le logiciel compare l'étiquette du sujet à l'étiquette de l'objet, puis autorise ou interdit la transaction en fonction de l'étiquette *dominante*. L'étiquette d'une entité est dite *dominante* par rapport à l'étiquette d'une autre entité si les deux conditions suivantes sont remplies :

- Le composant de classification de l'étiquette de la première entité est égal à ou supérieur à la classification de l'objet.
- Tous les compartiments figurant dans les étiquettes de la deuxième entité sont inclus dans l'étiquette de la première entité.

Deux étiquettes sont considérées comme *égales* si elles possèdent la même classification et le même jeu de compartiments. Si les étiquettes sont égales, les étiquettes se dominent mutuellement. Par conséquent, l'accès est autorisé.

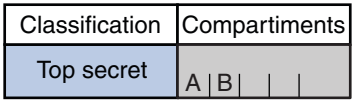
Si l'une des conditions suivantes est remplie, la première étiquette est dite *strictement dominante* par rapport à la deuxième étiquette.

- La première étiquette possède une classification supérieure à la deuxième.
- La classification de la première étiquette est égale à la classification de la deuxième, la première étiquette inclut les catégories de la deuxième étiquette et la première étiquette possède des catégories supplémentaires.

Une étiquette qui en domine strictement une autre peut accéder à la deuxième étiquette.

Deux étiquettes sont dites *disjointes* si aucune étiquette ne domine l'autre. L'accès n'est pas autorisé entre étiquettes disjointes.

Considérez par exemple la figure suivante.



Quatre étiquettes peuvent être créées à partir de ces composants :

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

`TOP SECRET AB` se domine elle-même et domine strictement les autres étiquettes. `TOP SECRET A` se domine elle-même et domine strictement `TOP SECRET`. `TOP SECRET B` se domine elle-même et domine strictement `TOP SECRET`. `TOP SECRET A` et `TOP SECRET B` sont disjointes.

Dans une transaction de lecture, l'étiquette du sujet doit dominer l'étiquette de l'objet. Cette règle garantit que le niveau de confiance du sujet est conforme aux exigences d'accès à l'objet. En d'autres termes, l'étiquette du sujet inclut tous les compartiments qui sont autorisés à accéder à l'objet. `TOP SECRET A` peut lire les données `TOP SECRET A` et `TOP SECRET`. De même, `TOP SECRET B` peut lire les données `TOP SECRET B` et `TOP SECRET`. `TOP SECRET A` ne peut pas lire les données `TOP SECRET B`. De même, `TOP SECRET B` ne peut pas lire les données `TOP SECRET A`. `TOP SECRET AB` peut lire les données de toutes les étiquettes.

Dans une transaction d'écriture, c'est-à-dire lorsqu'un sujet crée ou modifie un objet, la zone étiquetée de l'objet résultant doit être égale à la zone étiquetée du sujet. Les transactions d'écriture ne sont pas autorisées d'une zone vers une autre.

Dans la pratique, les sujets et les objets des transactions de lecture et d'écriture ont généralement la même étiquette et la domination stricte n'a pas à être envisagée. Par exemple, un sujet `TOP SECRET A` peut créer ou modifier un objet `TOP SECRET A`. Dans Trusted Extensions, l'objet `TOP SECRET A` se trouve dans une zone étiquetée `TOP SECRET A`.

Le tableau ci-après illustre les relations de domination entre les étiquettes du gouvernement et entre un ensemble d'étiquettes de l'industrie.

TABLEAU 1–1 Exemples de relations d'étiquettes dans Trusted Extensions

	Etiquette 1	Relation	Etiquette 2
Etiquettes du gouvernement américain	`TOP SECRET AB`	domine (strictement)	`SECRET A`
	`TOP SECRET AB`	domine (strictement)	`SECRET AB`
	`TOP SECRET AB`	domine (strictement)	`TOP SECRET A`
	`TOP SECRET AB`	domine (est égal à)	`TOP SECRET AB`
	`TOP SECRET AB`	est disjoint de	`TOP SECRET C`
	`TOP SECRET AB`	est disjoint de	`SECRET C`
	`TOP SECRET AB`	est disjoint de	`SECRET A B C`
Etiquettes de l'industrie	`Confidential: Restricted`	domine	`Confidential: Need to Know`
	`Confidential: Restricted`	domine	`Confidential: Internal Use Only`
	`Confidential: Restricted`	domine	`Public`
	`Confidential: Need to Know`	domine	`Confidential: Internal Use Only`
	`Confidential: Need to Know`	domine	`Public`
	`Confidential: Internal`	domine	`Public`
	`Sandbox`	est disjoint de	Toutes les autres étiquettes

Lorsque vous transférez des informations entre des fichiers possédant des étiquettes différentes, Trusted Extensions affiche une boîte de dialogue de confirmation vous demandant si vous êtes autorisé à modifier l'étiquette du fichier. Si vous n'êtes pas autorisé à le faire, Trusted Extensions n'autorise pas la transaction. L'administrateur de sécurité peut vous autoriser à augmenter ou réduire le niveau de sécurité d'informations. Pour plus d'informations, reportez-vous à la section "Réalisation d'actions sécurisées" à la page 46.

Responsabilités des utilisateurs concernant la protection des données

En tant qu'utilisateur, il vous incombe de définir les permissions destinées à protéger vos fichiers et répertoires. Les actions que vous pouvez effectuer pour définir les permissions utilisent un mécanisme appelé contrôle d'accès discrétionnaire (DAC). Vous pouvez vérifier les permissions sur vos fichiers et répertoires à l'aide de la commande `ls -l` ou à l'aide du navigateur de fichiers, comme décrit au Chapitre 3, “Utilisation de Trusted Extensions (tâches)”.

Le contrôle d'accès obligatoire (MAC) est automatiquement appliqué par le système. Si vous êtes autorisé à augmenter ou réduire le niveau de sécurité d'informations étiquetées, il vous incombe de vous assurer que le besoin de modifier le niveau de sécurité des informations est légitime.

Un autre aspect de la protection des données concerne les e-mails. Ne suivez jamais des instructions que vous recevez par e-mail de la part d'un administrateur. En suivant par exemple des instructions reçues par e-mail vous invitant à modifier votre mot de passe et à le remplacer par une valeur donnée, vous permettez à l'expéditeur de se connecter à votre compte. Dans de rares cas, vous pouvez vérifier les instructions de manière indépendante avant de les suivre.

Trusted Extensions sépare les informations en fonction des étiquettes

Trusted Extensions sépare les informations possédant des étiquettes différentes en procédant comme suit :

- MAC est appliqué à toutes les transactions, notamment les e-mails.
- Les fichiers sont stockés dans des zones séparées selon leur étiquette.
- Le bureau fournit des espaces de travail étiquetés.
- Les utilisateurs peuvent sélectionner une session à niveau unique ou multiniveau.
- Les données concernant les objets sont effacées avant la réutilisation des objets.

Sessions à niveau unique ou multiniveau

La première fois que vous vous ouvrez une session Trusted Extensions, vous choisissez une utilisation à étiquette unique ou à plusieurs étiquettes. Vous définissez ensuite l'*autorisation de session* ou l'*étiquette de session*. Ce paramètre correspond au niveau de sécurité auquel vous avez l'intention de travailler.

Dans une session à niveau unique, vous ne pouvez accéder qu'aux objets dont l'étiquette est égale à l'étiquette de votre session ou dominée par elle.

Dans une session multiniveau, vous avez accès à des informations possédant des étiquettes égales ou inférieures à votre autorisation de session. Vous pouvez spécifier différentes étiquettes pour différents espaces de travail. Vous pouvez également avoir plusieurs espaces de travail sous la même étiquette.

Exemple de sélection de session

L'exemple présenté dans le Tableau 1–2 met en évidence les différences entre une session à niveau unique et une session multiniveau. Cet exemple compare un utilisateur qui choisit de travailler dans une session à niveau unique avec l'étiquette `CONFIDENTIAL: NEED TO KNOW` (`CNF : NTK`) et un utilisateur qui choisit une session multiniveau, également avec l'étiquette `CNF : NTK`.

Les trois colonnes de gauche montrent la session de chaque utilisateur au moment de la connexion. Notez que les utilisateurs définissent une *étiquette de session* pour les sessions à niveau unique et une *autorisation de session* pour les sessions multiniveau. Le système affiche le générateur d'étiquettes (label builder) approprié en fonction de votre sélection. Pour voir un exemple de générateur d'étiquettes pour une session multiniveau, reportez-vous à la Figure 3–4.

Les deux colonnes de droite affichent les valeurs d'étiquettes disponibles au cours de la session. La colonne Etiquette d'espace de travail initiale représente l'étiquette active la première fois que l'utilisateur accède au système. La colonne Etiquettes disponibles répertorie les étiquettes vers lesquelles l'utilisateur est autorisé à basculer en cours de session.

TABLEAU 1–2 Effet de la sélection initiale de l'étiquette sur les étiquettes disponibles au cours de la session

Sélections de l'utilisateur			Valeurs d'étiquettes de la session	
Type de session	Etiquette de session	Autorisation de session	Etiquette d'espace de travail initiale	Etiquettes disponibles
niveau unique	`CNF: NTK`	-	`CNF: NTK`	`CNF: NTK`
multiniveau	-	`CNF: NTK`	`Public`	`Public`
				`CNF: Internal Use Only`
				`CNF: NTK`

Comme l'indique la première ligne du tableau, l'utilisateur a sélectionné une session à niveau unique avec une étiquette de session `CNF : NTK`. L'utilisateur a une étiquette d'espace de travail initiale `CNF : NTK`, qui est également la seule étiquette sur laquelle l'utilisateur peut travailler.

Comme l'indique la deuxième ligne du tableau, l'utilisateur a sélectionné une session multiniveau avec une autorisation de session `CNF : NTK`. L'étiquette d'espace de travail initiale de l'utilisateur est définie sur `Public`, car `Public` est l'étiquette la plus basse possible dans la

plage d'étiquettes du compte de l'utilisateur. L'utilisateur peut basculer vers toute étiquette comprise entre `Public` et `CNF : NTK`. `Public` est l'étiquette minimum et `CNF : NTK` est l'autorisation de session.

Espaces de travail étiquetés

Dans un bureau Trusted Extensions, les espaces de travail sont accessibles à l'aide des panneaux d'espace de travail situés à droite du panneau inférieur.

FIGURE 1–5 Espaces de travail étiquetés sur le panneau

Chaque espace de travail possède une étiquette. Vous pouvez affecter la même étiquette à plusieurs espaces de travail et vous pouvez affecter différentes étiquettes à différents espaces de travail. Les fenêtres qui sont lancées dans un espace de travail ont l'étiquette de cet espace de travail. Lorsqu'une fenêtre est déplacée vers un espace de travail d'une autre étiquette, elle conserve son étiquette d'origine. Par conséquent, vous pouvez, dans une session multiniveau, faire coexister des fenêtres possédant différentes étiquettes dans un même espace de travail.

Application du MAC pour les transactions par e-mail

Trusted Extensions applique le MAC pour les e-mails. Vous pouvez envoyer et lire des e-mails correspondant à votre étiquette active. Vous pouvez recevoir des e-mails correspondant à une étiquette comprise dans la plage d'étiquettes de votre compte. Dans une session multiniveau, vous pouvez passer à un espace de travail possédant une autre étiquette pour lire les e-mails de cette étiquette. Vous utilisez le même lecteur de courrier électronique et le même identifiant de connexion. Le système vous autorise à lire le courrier correspondant à votre étiquette active uniquement.

Suppression des données d'objets avant la réutilisation des objets

Trusted Extensions empêche la révélation involontaire d'informations sensibles en supprimant automatiquement les informations obsolètes des objets accessibles aux utilisateurs avant leur réutilisation. Par exemple, la mémoire et l'espace disque sont vidés avant d'être réutilisés. Si vous n'effacez pas les données sensibles avant la réutilisation d'un objet, les données risquent d'être révélées à des utilisateurs inappropriés. Par le biais de la libération de périphériques, Trusted Extensions efface tous les objets accessibles aux utilisateurs avant d'allouer les lecteurs à

des processus. Notez cependant que vous devez effacer tous les médias de stockage amovibles tels que les DVD et les périphériques USB avant d'autoriser un autre utilisateur à accéder au lecteur.

Trusted Extensions active l'administration sécurisée

Contrairement aux systèmes UNIX classiques, le superutilisateur (ou utilisateur `root`) n'est pas utilisé pour administrer Trusted Extensions. Des rôles d'administration avec fonctionnalités discrètes administrent le système. Ainsi, un utilisateur seul ne peut pas compromettre la sécurité du système. Un *rôle* est un compte utilisateur spécial qui donne accès à certaines applications avec les droits nécessaires à l'exécution de tâches spécifiques. Les droits comprennent les autorisations, les privilèges et les UID/GID effectifs.

Les pratiques de sécurité suivantes sont mises en oeuvre sur un système configuré avec Trusted Extensions :

- Vous disposez d'autorisations d'accès aux applications et d'autorisations en fonction de vos besoins d'utilisation.
- Vous pouvez uniquement exécuter des fonctions passant outre à la stratégie de sécurité si vous disposez d'autorisations spéciales ou de privilèges spéciaux octroyés par des administrateurs.
- Les tâches d'administration du système sont réparties entre plusieurs rôles.

Accès aux applications dans Trusted Extensions

Dans Trusted Extensions, vous ne pouvez accéder qu'aux programmes dont vous avez besoin pour faire votre travail. Comme dans le SE Oracle Solaris, l'administrateur autorise l'accès en assignant un ou plusieurs profils de droits à votre compte. Un *profil de droits* est une collection spéciale de programmes et d'attributs de sécurité. Ces attributs de sécurité permettent d'utiliser le programme figurant dans le profil de droits.

Le SE Oracle Solaris fournit des attributs de sécurité tels que des *privilèges* et des *autorisations*. Trusted Extensions fournit des étiquettes. N'importe lequel de ces attributs, s'il est manquant, peut empêcher l'utilisation de tout ou partie du programme. Par exemple, un profil de droits peut inclure une autorisation qui vous permette de lire une base de données. En revanche, un profil de droits doté d'attributs de sécurité différents peut être nécessaire pour vous permettre de modifier la base de données ou de lire les informations classées `Confidential`.

L'utilisation de profils de droits contenant des programmes auxquels sont associés des attributs de sécurité permet d'éviter aux utilisateurs de faire un mauvais usage des données et d'endommager les données sur le système. Si vous avez besoin d'effectuer des tâches qui contournent la stratégie de sécurité, l'administrateur peut vous attribuer un profil de droits

contenant les attributs de sécurité nécessaires. S'il vous est impossible d'exécuter une tâche en particulier, renseignez-vous auprès de votre administrateur. Il est possible que vous ne disposiez pas des attributs de sécurité requis.

En outre, l'administrateur peut vous attribuer un shell de profil en tant que shell de connexion. Un *shell de profil* est une version spéciale d'un shell commun qui permet d'accéder à un ensemble particulier d'applications et de fonctionnalités. Les shells de profil sont une fonction de SE Oracle Solaris. Pour plus d'informations, reportez-vous à la page de manuel `pfexec(1)`.

Remarque – Si vous tentez d'exécuter un programme et recevez le message d'erreur `Not Found` (introuvable) ou si vous tentez d'exécuter une commande et recevez un message d'erreur `Not in Profile` (non compris dans le profil), vous n'êtes peut-être pas autorisé à utiliser ce programme. Vérifiez auprès de votre administrateur de sécurité.

Administration par rôle dans Trusted Extensions

Trusted Extensions recommande l'utilisation de rôles pour l'administration. Assurez-vous que vous savez qui est en train d'exécuter quel ensemble de tâches sur votre site. Les rôles suivants sont les plus communs :

- Rôle root : principalement utilisé pour empêcher une connexion directe par un superutilisateur.
- Rôle d'administrateur de sécurité : effectue les tâches liées à la sécurité, telles que l'autorisation de l'allocation de périphériques, l'attribution des profils de droits et l'évaluation des programmes logiciels.
- Rôle d'administrateur système : effectue des tâches courantes de gestion du système, telles que la création des utilisateurs, la mise en place des répertoires personnels et l'installation des logiciels.
- Rôle d'opérateur : effectue les sauvegardes système, gère les imprimantes et monte les médias amovibles.

◆ ◆ ◆ CHAPITRE 2

Connexion à Trusted Extensions (tâches)

Ce chapitre décrit le bureau sécurisé et le processus de connexion sur un système Trusted Extensions. Ce chapitre comprend les sections suivantes :

Connexion au bureau dans Trusted Extensions

Le bureau que vous utilisez dans Trusted Extensions est protégé. Les étiquettes fournissent une indication visible de la protection. Les applications, les données et les communications sont étiquetées. Le bureau est une version sécurisée du bureau Oracle Solaris.

L'écran de connexion n'est pas étiqueté. Le processus de connexion impose que vous établissiez une étiquette pour votre session. Une fois que vous avez choisi une étiquette, le bureau, ses fenêtres et toutes les applications sont étiquetés. En outre, les applications qui affectent la sécurité sont visiblement protégées par un indicateur de chemin sécurisé.

Processus de connexion à Trusted Extensions

Le processus de connexion sur un système configuré avec Trusted Extensions est similaire au processus de connexion du Oracle Solaris. Toutefois, dans Trusted Extensions, vous examinez plusieurs écrans en recherchant les informations liées à la sécurité avant que la session de bureau ne puisse être lancée. Le processus est décrit plus en détails dans les sections qui suivent. Voici un bref aperçu.

1. Identification : tapez votre nom d'utilisateur dans le champ Username (Nom d'utilisateur).
2. Authentification : tapez votre mot de passe dans le champ Password (Mot de passe).

La réussite de l'identification et de l'authentification confirme que vous êtes autorisé à utiliser le système.

3. Vérification des messages et sélection du type de session : examinez les informations dans la boîte de dialogue Message Of The Day (Message du jour). Cette boîte de dialogue affiche l'heure de votre dernière connexion, les éventuels messages de l'administrateur et les attributs de sécurité de votre session. Si vous êtes autorisé à travailler sur plusieurs étiquettes, vous pouvez spécifier le type de session, à niveau unique ou multiniveau.

Remarque – Si votre compte vous empêche de travailler sur une étiquette, vous ne pouvez pas spécifier le type de session. Cette restriction est appelée *étiquette unique* ou configuration à niveau unique. Pour voir un exemple, reportez-vous à la section "Exemple de sélection de session" à la page 25.

---

4. Sélection d'étiquette : dans le générateur d'étiquettes (label builder), choisissez le niveau de sécurité le plus élevé auquel vous avez l'intention de travailler pendant votre session.

Remarque – Par défaut, la connexion à distance n'est pas prise en charge pour les utilisateurs standard dans Trusted Extensions. Si l'administrateur a configuré le logiciel Xvnc du Oracle Solaris, vous pouvez utiliser un client VNC pour afficher un bureau multiniveau à distance. Pour connaître la procédure, reportez-vous à la section "Connexion à distance à Trusted Extensions" à la page 34.

Identification et authentification lors de la connexion

L'identification et l'authentification lors de la connexion sont gérées par le SE Oracle Solaris. L'affichage de l'écran de connexion contient initialement une invite à saisir le nom d'utilisateur. Cette partie de la procédure de connexion est appelée *identification*.

Une fois que vous avez entré le nom d'utilisateur, l'invite de mot de passe s'affiche. Cette partie de la procédure est appelée *authentification*. Le mot de passe vous authentifie en tant qu'utilisateur autorisé à utiliser ce nom d'utilisateur.

Un *mot de passe* est une combinaison privée de touches du clavier qui valide votre identité sur le système. Votre mot de passe est stocké sous forme cryptée et n'est pas accessible par d'autres utilisateurs sur le système. Il vous incombe de protéger votre mot de passe, de façon à ce que d'autres utilisateurs ne puissent pas y accéder de manière non autorisée. N'écrivez jamais votre mot de passe et ne le divulguez à personne, car une personne possédant votre mot de passe aurait accès à toutes vos données sans être identifiable ni responsable. Votre mot de passe initial est fourni par votre administrateur de sécurité.

Vérification des attributs de sécurité lors de la connexion

La vérification des paramètres de sécurité est gérée par Trusted Extensions, et non par le SE Oracle Solaris. Avant la connexion, Trusted Extensions affiche la boîte de dialogue Message Of The Day (Message du jour). Cette boîte de dialogue fournit des informations relatives au statut que vous pouvez examiner. Le statut inclut des informations relatives au passé, par exemple l'heure de votre dernière utilisation du système. Vous pouvez également consulter les attributs de sécurité en vigueur pour la prochaine session. Si votre compte est configuré pour fonctionner sous plusieurs étiquettes, vous pouvez sélectionner une session à niveau unique ou multiniveau.

Vous pouvez ensuite visualiser votre étiquette unique ou sélectionner une étiquette et une autorisation à partir du générateur d'étiquettes (Label Builder).

Connexion à Trusted Extensions

Les tâches suivantes vous guident lors de la connexion à Trusted Extensions. Vous passez en revue et vous spécifiez les informations de sécurité avant d'atteindre le bureau.

▼ Identification et authentification auprès du système

1 **Dans le champ Username (Nom d'utilisateur) de l'écran de connexion, tapez votre nom d'utilisateur.**

Veillez à saisir le nom d'utilisateur exact que votre administrateur vous a attribué. Soyez particulièrement attentif à l'orthographe et aux majuscules.

Si vous faites une erreur, entrez un mot de passe fictif. Le champ Username (Nom d'utilisateur) s'affiche.

2 **Validez votre saisie.**

Appuyez sur la touche Entrée pour confirmer votre nom d'utilisateur.

Attention – Vous ne devez *jamais* voir la bande de confiance lorsque l'écran de connexion s'affiche. Si la bande de confiance apparaît lorsque vous essayez de vous connecter ou de déverrouiller l'écran, ne saisissez pas votre mot de passe. Il est possible que vous ayez été victime d'usurpation d'identité. Une *usurpation* se produit lorsqu'un programme intrus se fait passer pour un programme de connexion afin de récupérer des mots de passe. Contactez immédiatement votre administrateur de sécurité.

3 **Saisissez votre mot de passe dans le champ de mot de passe, puis appuyez sur la touche Entrée.**

Pour des raisons de sécurité, les caractères ne s'affichent pas dans le champ. Le système compare le nom de connexion et le mot de passe avec la liste des utilisateurs autorisés.

Erreurs fréquentes Si le mot de passe que vous avez fourni est incorrect, l'écran affiche un message :

```
Echec de l'authentification
```

Cliquez sur OK pour fermer la boîte de dialogue. Saisissez à nouveau votre nom d'utilisateur, puis le mot de passe correct.

▼ Consultation des messages et sélection du type de session

Si vous ne vous limitez pas à une étiquette unique, vous pouvez visualiser les données correspondant à différentes étiquettes. La plage dans laquelle vous pouvez travailler est limitée au niveau supérieur par l'autorisation de session et au niveau inférieur par l'étiquette minimum que votre administrateur vous a attribuée.

1 **Consultez la boîte de dialogue Message Of The Day.**

a. **Vérifiez que l'heure de votre dernière session est exacte.**

Vérifiez toujours que rien n'est suspect concernant l'heure de la dernière connexion, par exemple une heure inhabituelle dans la journée. Si vous avez des raisons de penser que l'heure n'est pas exacte, contactez votre administrateur de sécurité.

b. Vérifiez la présence d'éventuels messages de l'administrateur.

Le champ Message Of The Day (Message du jour) peut contenir des avertissements concernant les opérations de maintenance programmées ou des problèmes de sécurité. Consultez toujours les informations figurant dans ce champ.

c. Examinez les attributs de sécurité de votre session.

La boîte de dialogue Message Of The Day indique les rôles que vous pouvez assumer, votre étiquette minimale et d'autres caractéristiques de sécurité.

d. (Facultatif) Si vous êtes autorisé à vous connecter à une session multiniveau, décidez si vous souhaitez une session à étiquette unique.

Cliquez sur Restrict Session to a Single Label (Limiter la session à une étiquette) pour vous connecter à une session à étiquette unique.

e. Cliquez sur OK.

2 Confirmez votre choix d'étiquette.

Un générateur d'étiquettes (Label Builder) apparaît. Si vous ouvrez une session à étiquette unique, le générateur d'étiquettes décrit votre étiquette de session. Dans un système multiniveau, le générateur d'étiquettes vous permet de choisir votre autorisation de session. Pour voir un exemple de générateur d'étiquettes pour une session multiniveau, reportez-vous à la Figure 3–4.

- **Acceptez la valeur par défaut, sauf si vous avez une raison de ne pas le faire.**
- **Pour une session multiniveau, sélectionnez une autorisation.**

  Pour modifier l'autorisation, cliquez sur l'autorisation `Trusted Path` (Chemin de confiance), puis cliquez sur l'autorisation souhaitée.

- **Pour une session à niveau unique, sélectionnez une étiquette.**

  Pour modifier l'étiquette, cliquez sur l'autorisation `Trusted Path`, puis cliquez sur l'étiquette souhaitée.

3 Cliquez sur OK.

Le bureau sécurisé s'affiche.

▼ Résolution des problèmes de connexion

1 Si le nom d'utilisateur ou le mot de passe n'est pas reconnu, contactez votre administrateur.

2 **Si votre plage d'étiquettes n'est pas autorisée sur votre station de travail, consultez votre administrateur.**

Les stations de travail peuvent être limitées à une plage restreinte d'autorisations et d'étiquettes. Par exemple, une station de travail située dans un hall d'entrée peut être limitée aux étiquettes `PUBLIC`. Si l'étiquette ou l'autorisation de session que vous spécifiez n'est pas acceptée, vérifiez avec un administrateur pour déterminer si la station de travail est limitée.

3 **Si vous avez personnalisé vos fichiers d'initialisation du shell et que vous ne parvenez pas à vous connecter, les deux options suivantes sont disponibles :**

- **Contactez votre administrateur système pour résoudre le problème.**
- **Si vous pouvez devenir l'utilisateur `root`, ouvrez une session de secours.**

  Dans une connexion standard, les fichiers d'initialisation du shell sont fournis au démarrage, afin d'offrir un environnement personnalisé. Avec une connexion de secours, les valeurs par défaut sont appliquées à votre système et aucun fichier d'initialisation du shell n'est fourni.

  Dans Trusted Extensions, une connexion de secours est protégée. Seul le compte `root` peut accéder à une connexion de secours.

  a. **Saisissez votre nom d'utilisateur dans l'écran de connexion.**

  b. **En bas de l'écran, choisissez Solaris Trusted Extensions Failsafe Session (Session de secours Solaris) dans le menu du bureau.**

  c. **Lorsque vous y êtes invité, saisissez votre mot de passe.**

  d. **Lorsque vous êtes invité à indiquer un autre mot de passe, saisissez le mot de passe pour `root`.**

Connexion à distance à Trusted Extensions

Un VNC (Virtual network computing) offre un moyen d'accéder à un système Trusted Extensions central à partir de votre ordinateur portable ou d'un ordinateur personnel. L'administrateur de votre site doit configurer le logiciel Xvnc Oracle Solaris pour qu'il s'exécute sur le serveur Trusted Extensions et un visualiseur VNC pour qu'il s'exécute sur les systèmes clients. Vous pouvez choisir de travailler sur n'importe quelle étiquette dans la plage d'étiquettes installée sur le serveur.

▼ Procédure de connexion à un bureau Trusted Extensions distant

Avant de commencer L'administrateur a configuré un serveur Xvnc. Pour les pointeurs, reportez-vous à la section "Procédure de configuration d'un système Trusted Extensions à l'aide de Xvnc pour un accès à distance" du manuel *Configuration et administration d'Oracle Solaris Trusted Extensions*.

1. **Dans une fenêtre de terminal, connectez-vous au serveur Xvnc.**

   Saisissez le nom du serveur que l'administrateur a configuré avec Xvnc.

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

2. **Ouverture d'une session.**

   Suivez les procédures de la section "Connexion à Trusted Extensions" à la page 31.

   Vous pouvez à présent travailler sur le bureau Trusted Extensions dans VNC.

◆ ◆ ◆ CHAPITRE 3

Utilisation de Trusted Extensions (tâches)

Ce chapitre explique comment travailler dans les espaces de travail Trusted Extensions. Ce chapitre comprend les sections suivantes :

Sécurité visible du bureau dans Trusted Extensions

Trusted Extensions fournit un bureau multiniveau.

Un système configuré avec Trusted Extensions affiche la bande de confiance, sauf lors de l'ouverture de la session et du verrouillage de l'écran. Dans tous les autres cas, la bande de confiance est visible.

La bande apparaît en haut de l'écran. Le symbole de confiance apparaît sur la bande de confiance lorsque vous interagissez avec la base informatique sécurisée (TCB, Trusted Computing Base). Lorsque vous modifiez votre mot de passe, par exemple, vous pouvez interagir avec la TCB.

Lorsque les écrans d'un système Trusted Extensions multiécran sont configurés horizontalement, une bande de confiance apparaît en travers des écrans. Toutefois, si le système multiécran est configuré de manière à s'afficher verticalement ou possède un bureau par écran, la bande de confiance n'apparaît que sur un écran.

Attention – Si une deuxième la bande de confiance s'affiche sur un système multiécran, la bande n'est pas générée par le système d'exploitation. Il est possible qu'un programme non autorisé soit installé sur votre système.

Contactez immédiatement votre administrateur de sécurité. Pour déterminer quelle est la bande de confiance correcte, reportez-vous à la section "Procédure de recherche du pointeur de la souris" à la page 44.

Pour plus d'informations sur les applications, les menus, les étiquettes et les caractéristiques du bureau, reportez-vous au Chapitre 4, "Eléments de Trusted Extensions (Référence)".

Processus de déconnexion de Trusted Extensions

Une station de travail connectée mais laissée sans surveillance entraîne un risque pour la sécurité. Prenez l'habitude de sécuriser votre station de travail avant de vous absenter. Si vous avez l'intention de revenir bientôt, verrouillez votre écran. Sur la plupart des sites, l'écran se verrouille automatiquement après une période de veille spécifiée. Si vous prévoyez d'être absent plus longtemps ou si vous pensez qu'une autre personne va travailler sur votre poste, déconnectez-vous.

Travail sur un système étiqueté

Attention – Si la bande de confiance est absente de votre espace de travail, contactez l'administrateur de sécurité. Votre système pourrait avoir un problème sérieux.

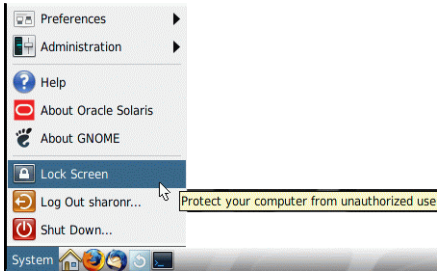
La bande de confiance ne doit pas apparaître lors de la procédure de connexion ni lorsque vous verrouillez votre écran. Si la bande de confiance apparaît, contactez immédiatement l'administrateur.

▼ Procédure de verrouillage et déverrouillage de l'écran

Si vous quittez brièvement votre station de travail, verrouillez l'écran.

1 **Choisissez Lock Screen (Verrouillage de l'écran) dans le menu principal.**

FIGURE 3–1 Sélection du verrouillage de l'écran



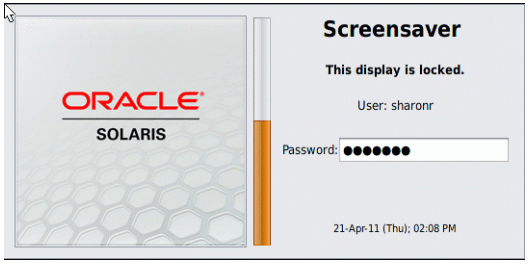
L'écran devient noir. A ce stade, vous seul pouvez vous connecter de nouveau.

Remarque – La bande de confiance ne doit pas apparaître lorsque l'écran est verrouillé. Si la bande s'affiche, informez-en immédiatement l'administrateur de sécurité.

---

2 Pour déverrouiller votre écran, procédez comme suit :

a. Déplacez le curseur de la souris jusqu'à ce que la boîte de dialogue Screensaver (Economiseur d'écran) soit visible.



Si la boîte de dialogue de l'économiseur d'écran n'apparaît pas, appuyez sur la touche Entrée.

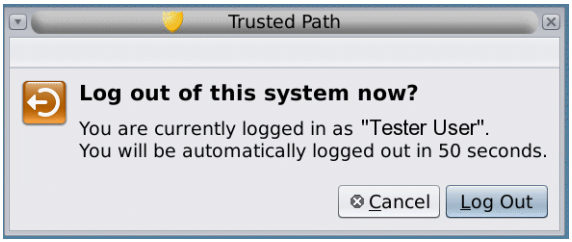
b. Saisissez votre mot de passe.

Cette action vous renvoie à votre session dans son état précédent.

▼ Procédure de déconnexion de Trusted Extensions

Sur la plupart des sites, l'écran se verrouille automatiquement après une période de veille spécifiée. Si vous prévoyez d'être absent plus longtemps ou si vous pensez qu'une autre personne va travailler sur votre poste, déconnectez-vous.

1. **Pour vous déconnecter de Trusted Extensions, choisissez Log Out (Déconnexion)** *votre-nom* **dans le menu principal.**



2. **Confirmez que vous souhaitez vous déconnecter, ou cliquez sur Annuler.**

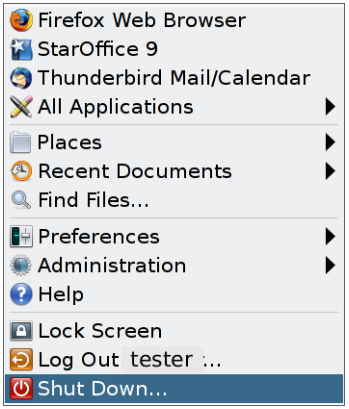
▼ Procédure d'arrêt du système

La déconnexion est la manière habituelle de mettre fin à une session Trusted Extensions. Utilisez la procédure suivante pour arrêter votre station de travail.

Remarque – Si vous n'êtes pas sur la console, vous ne pouvez pas arrêter le système. Par exemple, les clients VNC ne peuvent pas arrêter le système.

Avant de commencer Le profil de droits Maintenance and Repair (Maintenance et réparations) doit vous être assigné.

- **Choisissez Shut Down (Arrêt) dans le menu principal.**



Confirmez l'arrêt.

Remarque – Par défaut, la combinaison de touches Stop-A (L1-A) n'est pas disponible dans Trusted Extensions. L'administrateur de sécurité peut modifier cette valeur par défaut.

▼ Procédure d'affichage de vos fichiers dans un espace de travail étiqueté

Pour afficher vos fichiers, utilisez les mêmes applications que vous utiliseriez sur le bureau sur un système Oracle Solaris. Si vous travaillez sur plusieurs étiquettes, seuls les fichiers qui possèdent la même étiquette que l'espace de travail sont visibles.

- **Ouvrez une fenêtre de terminal ou le navigateur de fichiers.**
  - **Ouvrez une fenêtre de terminal et répertoriez le contenu de votre répertoire personnel.**

    Cliquez avec le bouton 3 de la souris sur l'arrière-plan. Dans le menu, choisissez Open Terminal (Ouvrir un terminal).
  - **Cliquez sur le dossier personnel sur le bureau ou sur le panneau du bureau.**

    Le dossier s'ouvre dans un navigateur de fichiers. Le navigateur de fichiers s'ouvre avec la même étiquette que l'espace de travail actif. L'application permet d'accéder uniquement aux fichiers qui possèdent la même étiquette. Pour plus de détails sur l'affichage de fichiers de différentes étiquettes, reportez-vous à la section "Conteneurs et étiquettes" à la page 20. Pour afficher des fichiers possédant différentes étiquettes dans un espace de travail, reportez-vous à la section "Procédure de déplacement d'une fenêtre vers un autre espace de travail" à la page 54.

▼ Procédure d'accès aux pages de manuel Trusted Extensions

- **Dans la version Oracle Solaris, ouvrez la page de manuel `trusted_extensions(5)` dans une fenêtre de terminal.**

  ```
  % man trusted_extensions
  ```

  Pour obtenir la liste des commandes utilisateur spécifiques à Trusted Extensions, reportez-vous à l'Annexe D, "Liste des pages de manuel Trusted Extensions" du manuel *Configuration et administration d'Oracle Solaris Trusted Extensions*. Les pages de manuel sont également disponibles à partir du site Web de documentation (`http://www.oracle.com/technetwork/indexes/documentation/index.html`) d'Oracle.

▼ Procédure d'accès aux fichiers d'initialisation de chaque étiquette

La liaison d'un fichier ou la copie d'un fichier vers une autre étiquette est utile lorsque vous souhaitez rendre un fichier d'étiquette inférieure visible depuis les niveaux supérieurs. Un fichier lié est uniquement accessible en écriture à l'étiquette inférieure. Un fichier copié est unique à chaque niveau d'étiquette et peut être modifié aux deux niveaux. Pour plus d'informations, reportez-vous à la section "Fichiers .copy_files et .link_files" du manuel *Configuration et administration d'Oracle Solaris Trusted Extensions*.

Avant de commencer Vous devez être connecté à une session multiniveau. La stratégie de sécurité de votre site doit permettre les liaisons.

Consultez votre administrateur lorsque vous modifiez ces fichiers.

1. **Choisissez les fichiers d'initialisation que vous souhaitez lier à d'autres étiquettes.**

2. **Créez ou modifiez le fichier `~/.link_files`.**

   Saisissez vos entrées à raison d'un fichier par ligne. Vous pouvez spécifier les chemins d'accès aux sous-répertoires dans votre répertoire personnel, mais vous ne pouvez pas utiliser de barre oblique initiale. Tous les chemins d'accès doivent se trouver dans votre répertoire personnel.

3. **Choisissez les fichiers d'initialisation que vous souhaitez copier vers d'autres étiquettes.**

   Copier un fichier d'initialisation est utile si vous disposez d'une application qui écrit toujours dans un fichier portant un nom donné et que vous avez besoin de séparer les données de différentes étiquettes.

4. **Créez ou modifiez le fichier `~/.copy_files`.**

   Saisissez vos entrées à raison d'un fichier par ligne. Vous pouvez spécifier les chemins d'accès aux sous-répertoires dans votre répertoire personnel, mais vous ne pouvez pas utiliser de barre oblique initiale. Tous les chemins d'accès doivent se trouver dans votre répertoire personnel.

Exemple 3–1 Création d'un fichier .copy_files

Dans cet exemple, l'utilisateur souhaite personnaliser plusieurs fichiers d'initialisation par étiquette. Dans son organisation, un serveur Web de l'entreprise est disponible au niveau `Restricted` (Restreint). Par conséquent, il définit différents paramètres initiaux dans le fichier `.mozilla` au niveau `Restricted`. De la même façon, il possède des modèles et des alias spéciaux au niveau `Restricted`. Il modifie les fichiers d'initialisation `.alias` et `.soffice` au niveau `Restricted`. Il peut facilement modifier ces fichiers après avoir créé le fichier `.copy_files` avec l'étiquette la plus basse.

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

Exemple 3–2 Création d'un fichier .link_files

Dans cet exemple, l'utilisateur souhaite que les valeurs par défaut de son courrier et les valeurs par défaut du shell C soient identiques pour toutes les étiquettes.

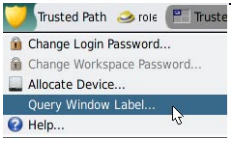
```
% vi .link_files
# Link these files to my home directory in every zone
.cshrc
.mailrc
```

Erreurs fréquentes Ces fichiers n'ont pas de sauvegardes pour gérer les anomalies. Les entrées en double dans les deux fichiers ou les entrées de fichier qui existent déjà sur d'autres étiquettes peuvent entraîner des erreurs.

▼ Procédure d'affichage interactif d'une étiquette de fenêtre

Cette opération peut être utile pour identifier l'étiquette d'une fenêtre partiellement masquée.

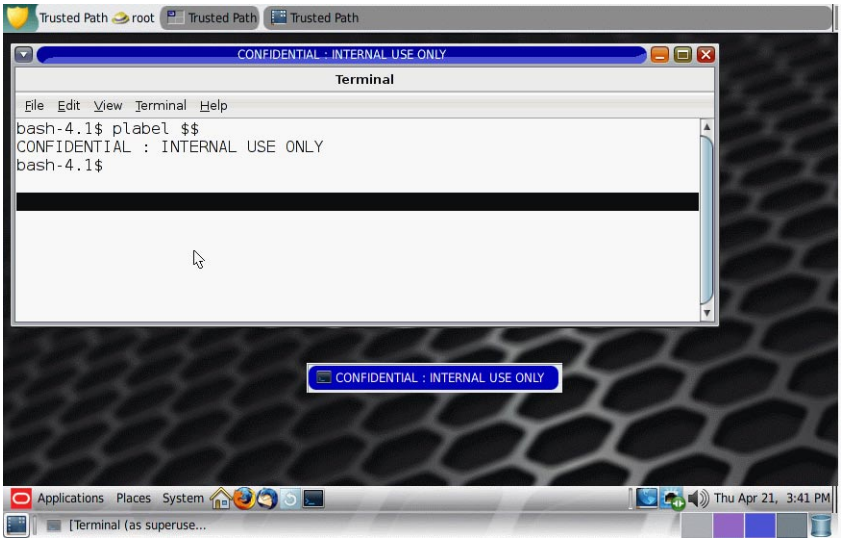
1. **Choisissez Query Window Label (Requête d'étiquette de fenêtre) dans le menu Trusted Path.**



2. **Déplacez le pointeur sur l'écran.**

   L'étiquette de la région sous le pointeur s'affiche dans une petite zone rectangulaire au centre de l'écran.

FIGURE 3–2 Opération de requête d'étiquette de fenêtre



3 **Cliquez sur le bouton de la souris pour mettre fin à l'opération.**

▼ Procédure de recherche du pointeur de la souris

Une application non sécurisée peut prendre le contrôle du pointeur de la souris. En recherchant le pointeur, vous pouvez reprendre le contrôle du focus du bureau.

1 **Pour reprendre le contrôle d'un clavier Sun, appuyez sur les touches Meta-Arrêt.**

Appuyez sur les touches simultanément pour reprendre le contrôle du focus du bureau actuel. Sur un clavier Sun, la touche Meta est la touche marquée d'un losange et placée de chaque côté de la barre d'espacement.

Si la préhension du clavier ou du pointeur de la souris n'est pas sécurisée, le pointeur se déplace vers la bande de confiance. Un pointeur de confiance ne se déplace pas vers la bande de confiance.

2 **Si vous n'utilisez pas un clavier Sun, appuyez sur les touches Alt-Pause/Attn.**

Exemple 3–3 Déplacement forcé du pointeur de la souris vers la bande de confiance

Dans cet exemple, l'utilisateur n'exécute aucun processus de confiance mais il ne peut pas voir le pointeur de la souris. Pour amener le pointeur au milieu de la bande de confiance, l'utilisateur appuie simultanément sur les touches Meta-Arrêt.

Exemple 3–4 Identification de la véritable bande de confiance

Sur un système Trusted Extensions multiécran dont les écrans sont configurés pour afficher un bureau distinct sur chaque écran, l'utilisateur voit une bande de confiance par écran. Ceci indique qu'un programme différent de Trusted Extensions génère une bande de confiance. Une seule bande de confiance s'affiche lorsqu'un système multiécran est configuré pour afficher un bureau par écran.

L'utilisateur cesse le travail et contacte immédiatement l'administrateur de sécurité. L'utilisateur identifie ensuite la véritable bande de confiance en plaçant le pointeur de la souris à un emplacement non sécurisé, par exemple sur l'arrière-plan de l'espace de travail. Lorsque l'utilisateur appuie simultanément sur les touches Alt-Pause/Attn, le pointeur de la souris se déplace vers la bande de confiance générée par Trusted Extensions.

▼ Exécution de certaines tâches de bureau courantes dans Trusted Extensions

Les étiquettes et la sécurité affectent certaines tâches courantes. Les tâches suivantes sont particulièrement affectées par Trusted Extensions :

- Vidage de la corbeille
- Recherche d'événements du calendrier

1 **Videz la corbeille.**

Cliquez avec le bouton 3 de la souris sur l'icône de corbeille sur le bureau. Choisissez Empty Trash (Vider la Corbeille), puis confirmez.

Remarque – La corbeille contient uniquement des fichiers possédant l'étiquette de l'espace de travail. Supprimez les informations sensibles dès qu'elles se trouvent dans la corbeille.

---

2 **Recherchez les événements du calendrier sur chaque étiquette.**

Les calendriers affichent uniquement les événements possédant l'étiquette de l'espace de travail qui a ouvert le calendrier.

- **Dans une session multiniveau, ouvrez votre calendrier depuis chaque espace de travail possédant une étiquette différente.**
- **Dans une session à niveau unique, déconnectez-vous. Ensuite, connectez-vous à une étiquette différente pour afficher les événements du calendrier de cette étiquette.**

3 **Enregistrez un bureau personnalisé sous chaque étiquette.**

Vous pouvez personnaliser la configuration de l'espace de travail pour chaque étiquette sur laquelle vous vous connectez.

a. **Configurez le bureau.**

Remarque – Les utilisateurs peuvent enregistrer les configurations du bureau. Les rôles ne peuvent pas enregistrer les configurations du bureau.

---

i. **Dans le menu principal, cliquez sur Système > Préférences > Apparence.**

ii. **Réorganisez les fenêtres, définissez la taille de la police et effectuez d'autres personnalisations.**

b. **Pour enregistrer le bureau actif, cliquez sur le menu principal.**

i. **Cliquez sur Système > Préférences > Applications au démarrage.**

ii. **Cliquez sur l'onglet Options.**

iii. **Cliquez sur Remember Currently Running Applications (Mémoriser les applications en cours d'exécution), puis fermez la boîte de dialogue.**

Votre bureau sera restauré dans cette configuration la prochaine fois que vous vous connecterez à cette étiquette.

Réalisation d'actions sécurisées

Les tâches suivantes liées à la sécurité nécessitent le chemin de confiance.

Attention – Si le symbole de confiance est absent lorsque vous tentez d'effectuer une action liée à la sécurité, contactez immédiatement votre administrateur de sécurité. Le problème de votre système pourrait être grave.

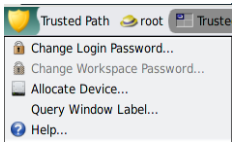
▼ Procédure de modification du mot de passe dans Trusted Extensions

Contrairement au SE Oracle Solaris, Trusted Extensions fournit une interface graphique permettant de modifier votre mot de passe. L'interface graphique prend le contrôle du pointeur jusqu'à ce que l'opération sur le mot de passe soit terminée. Pour arrêter un processus qui a saisi le pointeur de la souris, reportez-vous à l'Exemple 3–5.

1 **Choisissez `Change Login Password` (Modifier le mot de passe de connexion) ou `Change Workspace Password` (Modifier le mot de passe de l'espace de travail) dans le menu Trusted Path (Chemin de confiance).**

Pour sélectionner l'option de menu relative au mot de passe, cliquez sur `Trusted Path` dans la bande de confiance.

FIGURE 3–3 Menu Trusted Path



Remarque – L'option de menu `Change Workspace Password` (Modifier le mot de passe de l'espace de travail) du menu Trusted Path est active lorsque votre site exécute un service de nommage distinct dans chaque zone.

2 **Saisissez votre mot de passe actuel.**

Cette action confirme que vous êtes l'utilisateur légitime de ce nom d'utilisateur. Pour des raisons de sécurité, le mot de passe ne s'affiche pas lorsque vous le saisissez.

Attention – Lorsque vous saisissez votre mot de passe, assurez-vous que le curseur se trouve dans la boîte de dialogue Change Password (Modifier le mot de passe) et que le symbole de confiance est affiché. Si le curseur ne se trouve pas dans la boîte de dialogue, vous risquez de saisir par inadvertance votre mot de passe dans une autre fenêtre, dans laquelle le mot de passe pourrait être vu par un autre utilisateur. Si le symbole de confiance n'est pas affiché, il est possible qu'un autre utilisateur tente de voler votre mot de passe. Contactez immédiatement votre administrateur de sécurité.

3 **Saisissez le nouveau mot de passe.**

4 **Confirmez le mot de passe en le saisissant à nouveau.**

Remarque – Si vous choisissez `Change Password` (Modifier le mot de passe) et si votre site utilise des comptes locaux, votre nouveau mot de passe ne prendra effet qu'après le redémarrage de la zone ou du système. Vous ne pouvez redémarrer la zone que si le profil de droits Zone Security (Sécurité des zones) vous est affecté. Vous ne pouvez redémarrer le système que si le profil de droits Maintenance and Repair (Maintenance et réparations) vous est affecté. Si aucun de ces profils ne vous est affecté, contactez votre administrateur système pour programmer un redémarrage.

Exemple 3–5 Test permettant de vérifier si l'invite de mot de passe est de confiance

Sur un système x86 équipé d'un clavier Sun, l'utilisateur a été invité à saisir un mot de passe. Le pointeur de la souris a été capté et est placé dans la boîte de dialogue du mot de passe. Pour vérifier que l'invite est de confiance, l'utilisateur appuie simultanément sur les touches Meta-Arrêt. Si le pointeur reste dans la boîte de dialogue, l'utilisateur sait que l'invite du mot de passe est de confiance.

Si le pointeur ne reste pas dans la boîte de dialogue, l'utilisateur sait que l'invite du mot de passe n'est pas sécurisée. L'utilisateur doit alors contacter l'administrateur.

▼ Procédure de connexion à une étiquette différente

L'étiquette du premier espace de travail qui apparaît dans les sessions de connexion suivant la première connexion peut être définie sur toute étiquette de votre plage d'étiquettes.

Les utilisateurs peuvent configurer les caractéristiques de la session de démarrage pour chaque étiquette à laquelle ils se connectent.

Avant de commencer Vous devez être connecté à une session multiniveau.

1. **Créez des espaces de travail à chaque étiquette.**

   Pour plus d'informations, reportez-vous à la section "Procédure d'ajout d'un espace de travail sous votre étiquette minimale" à la page 53.

2. **Configurez chaque espace de travail comme vous souhaitez qu'il apparaisse.**

3. **Accédez à l'espace de travail que vous souhaitez afficher lorsque vous vous connectez.**

4. **Enregistrez l'espace de travail actif.**

   Pour plus d'informations, reportez-vous à la section "Exécution de certaines tâches de bureau courantes dans Trusted Extensions" à la page 45.

▼ Procédure d'allocation d'un périphérique dans Trusted Extensions

L'option de menu Allocate Device (Allouer le périphérique) permet de monter et d'allouer un périphérique pour votre usage exclusif. Si vous essayez d'utiliser un périphérique sans l'allouer, le message d'erreur Permission Denied (Autorisation refusée) apparaît.

Avant de commencer Vous devez être autorisé pour allouer un périphérique.

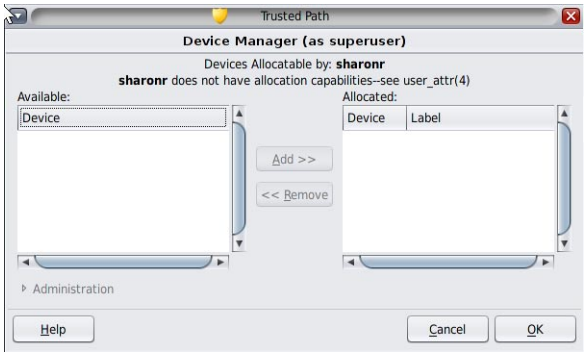
1 **Choisissez Allocate device dans le menu Trusted Path.**

2 **Double-cliquez sur le périphérique que vous souhaitez utiliser.**

Les périphériques que vous êtes autorisé à allouer avec votre étiquette active s'affichent dans la liste Available Devices (Périphériques disponibles) :

- `audio`*n* : représente un microphone et un haut-parleur ;
- `cdrom`*n* : représente une unité de CD-ROM ;
- `floppy`*n* : représente une unité de disquette ;
- `mag_tape`*n* : représente un lecteur de bande (transmission en continu) ;
- `rmdisk`*n* : représente un disque amovible, tel qu'un lecteur JAZ, ZIP ou un média USB enfichable à chaud.

La boîte de dialogue suivante indique que vous n'êtes pas autorisé à allouer des périphériques :



3 **Sélectionnez le périphérique.**

Déplacez le périphérique depuis la liste des périphériques disponibles (Available Devices) vers la liste des périphériques alloués (Allocated Devices).

- **Double-cliquez sur le nom du périphérique dans la liste des périphériques disponibles.**
- **Ou sélectionnez le périphérique et cliquez sur le bouton Allocate (Allouer) qui pointe vers la droite.**

Cette étape lance le script de nettoyage. Le script de nettoyage permet de s'assurer qu'aucune donnée issue d'autres transactions ne subsiste sur le média.

Notez que l'étiquette de l'espace de travail actif est appliquée au périphérique. Les éventuelles données transférées vers ou à partir du média du périphérique doivent être dominées par cette étiquette.

4 **Suivez les instructions.**

Les instructions garantissent que le média possède l'étiquette appropriée. Les instructions ci-après s'affichent par exemple pour l'utilisation d'un microphone :

Le périphérique est ensuite monté. Le nom du périphérique apparaît maintenant dans la liste des périphériques alloués. Ce périphérique est maintenant alloué pour votre usage exclusif.

Erreurs fréquentes

Si le périphérique que vous souhaitez utiliser ne figure pas dans la liste, contactez votre administrateur. Le périphérique peut être dans un état d'erreur ou être utilisé par quelqu'un d'autre. Ou vous n'êtes peut-être pas autorisé à utiliser le périphérique.

Si vous passez à l'espace de travail d'un rôle différent ou à un espace de travail d'étiquette différente, le périphérique alloué ne peut pas fonctionner. Pour utiliser le périphérique avec la nouvelle étiquette, vous devez libérer le périphérique au niveau de l'étiquette initiale, puis l'allouer à la nouvelle étiquette. Lorsque vous déplacez le gestionnaire de périphériques (Device Manager) vers un espace de travail sous une étiquette différente, la liste des périphériques disponibles et celle des périphériques alloués changent pour refléter le contexte correct.

Si une fenêtre du navigateur de fichiers n'apparaît pas, ouvrez la fenêtre manuellement, puis naviguez jusqu'au répertoire root, `/`. Dans ce répertoire, naviguez jusqu'au périphérique alloué pour afficher son contenu.

▼ Procédure de libération d'un périphérique dans Trusted Extensions

1 **Libérez le périphérique.**

   a. **Accédez à l'espace de travail dans lequel le gestionnaire de périphériques (Device Manager) est affiché.**

   b. **Déplacez le périphérique à libérer de la liste des périphériques alloués.**

2 **Retirez le média.**

3. **Cliquez sur OK dans la boîte de dialogue Deallocation (Libération).**

   Le périphérique peut maintenant être utilisé par un autre utilisateur autorisé.

▼ Procédure d'adoption d'un rôle dans Trusted Extensions

Contrairement au SE Oracle Solaris, Trusted Extensions fournit une interface graphique permettant d'assumer un rôle.

1. **Cliquez sur votre nom d'utilisateur à droite du symbole de confiance.**
2. **Choisissez le nom du rôle dans le menu.**
3. **Tapez le mot de passe du rôle et appuyez sur la touche Entrée.**

   Cette action confirme que vous pouvez légitimement assumer ce rôle. Pour des raisons de sécurité, le mot de passe ne s'affiche pas lorsque vous le saisissez.

Attention – Lorsque vous saisissez votre mot de passe, assurez-vous que le curseur se trouve dans la boîte de dialogue Change Password (Modifier le mot de passe) et que le symbole de confiance est affiché. Si le curseur ne se trouve pas dans la boîte de dialogue, vous risquez de saisir par inadvertance votre mot de passe dans une autre fenêtre, dans laquelle le mot de passe pourrait être vu par un autre utilisateur. Si le symbole de confiance n'est pas affiché, il est possible qu'un autre utilisateur tente de voler votre mot de passe. Contactez immédiatement votre administrateur de sécurité.

Une fois le mot de passe du rôle accepté, l'espace de travail actif devient l'espace de travail du rôle. Vous vous trouvez dans la zone globale. Vous pouvez effectuer les tâches autorisées par les profils de droits de votre rôle.

▼ Procédure de modification de l'étiquette d'un espace de travail

La possibilité de définir les étiquettes des espaces de travail dans Trusted Extensions offre un moyen pratique de travailler sous différentes étiquettes dans une même session multiniveau.

Utilisez la procédure décrite ci-dessous pour travailler avec une étiquette différente dans le même espace de travail. Pour créer un espace de travail sous une étiquette différente, reportez-vous à la section “Procédure d'ajout d'un espace de travail sous votre étiquette minimale” à la page 53.

Avant de commencer Vous devez être connecté à une session multiniveau.

1 **Cliquez sur l'étiquette de la fenêtre dans la bande de confiance.**

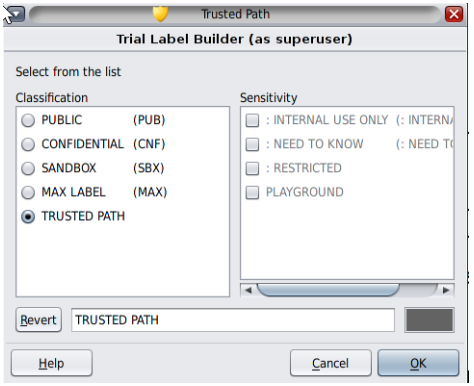
Vous pouvez également cliquer sur le panneau d'un espace de travail.

2 **Cliquez sur Change Workspace Label.**

3 **Sélectionnez une étiquette dans le générateur d'étiquettes (Label Builder).**

L'illustration suivante présente l'utilisateur en train de cliquer sur le bouton Trusted Path (Chemin de confiance).

FIGURE 3–4 Générateur d'étiquettes (Label Builder)



Après avoir cliqué sur ce bouton, l'utilisateur peut sélectionner une étiquette parmi les étiquettes de l'utilisateur. L'étiquette de l'espace de travail est remplacée par la nouvelle étiquette. Dans un système dans lequel les étiquettes sont assorties d'une couleur, les nouvelles fenêtres sont représentées à l'aide de la nouvelle couleur.

4 **Si vous êtes invité à saisir votre mot de passe, saisissez-le.**

Si votre site exécute un service de nommage distinct pour chaque zone, les utilisateurs sont invités à saisir un mot de passe lorsqu'ils accèdent à un espace de travail sous une nouvelle étiquette.

▼ Procédure d'ajout d'un espace de travail sous votre étiquette minimale

La possibilité de définir les étiquettes des espaces de travail dans Trusted Extensions offre un moyen pratique de travailler sous différentes étiquettes dans une même session multiniveau. Vous pouvez ajouter un espace de travail sous votre étiquette minimale.

Pour modifier l'étiquette de l'espace de travail actif, reportez-vous à la section "Procédure de modification de l'étiquette d'un espace de travail" à la page 51.

Avant de commencer Vous devez être connecté à une session multiniveau.

1 **Pour créer un espace de travail sous votre étiquette minimale, procédez comme suit :**

   a. **Cliquez avec le bouton 3 de la souris sur un panneau de l'espace de travail.**

   b. **Dans le menu, choisissez Preferences (Préférences).**

   c. **Augmentez le numéro figurant dans le champ Number of Workspaces (Nombre d'espaces de travail).**

      Les nouveaux espaces de travail créés possèdent votre étiquette minimum. Vous pouvez également utiliser cette boîte de dialogue pour nommer les espaces de travail. Le nom s'affiche dans l'info-bulle.

   d. **(Facultatif) Attribuez un nom aux espaces de travail.**

      Lorsque la souris se trouve sur le panneau d'un espace de travail, le nom de celui-ci s'affiche dans l'info-bulle.

2 **Pour modifier l'étiquette d'un espace de travail, sélectionnez le panneau de l'espace de travail et modifiez son étiquette.**

   Pour plus d'informations, reportez-vous à la section "Procédure de modification de l'étiquette d'un espace de travail" à la page 51.

▼ Procédure de basculement vers un espace de travail possédant une étiquette différente

Avant de commencer Vous devez être connecté à une session multiniveau.

1 **Cliquez sur le panneau d'un espace de travail de couleur différente.**

2 **Si vous êtes invité à saisir votre mot de passe, saisissez-le.**

Si votre site exécute un service de nommage distinct pour chaque zone, les utilisateurs sont invités à saisir un mot de passe lorsqu'ils accèdent à un espace de travail sous une nouvelle étiquette.

Erreurs fréquentes Si vous êtes connecté à une session à niveau unique, vous devez vous déconnecter pour travailler au niveau d'une autre étiquette. Ensuite, connectez-vous à l'étiquette souhaitée. Si vous y êtes autorisé, vous pouvez également ouvrir une session multiniveau.

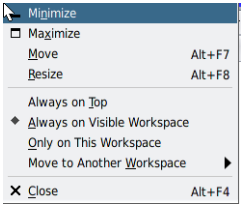
▼ Procédure de déplacement d'une fenêtre vers un autre espace de travail

Si vous faites glisser une fenêtre vers un espace de travail sous une étiquette différente, la fenêtre conserve son étiquette d'origine. Les actions effectuées dans cette fenêtre sont réalisées sous l'étiquette de la fenêtre, et non sous celle de l'espace de travail qui la contient. Le déplacement d'une fenêtre est utile pour comparer des informations. Vous pouvez aussi vouloir utiliser des applications à différents niveaux d'étiquette sans avoir à changer d'espace de travail.

1 **Dans l'affichage des panneaux, faites glisser la fenêtre d'un panneau vers un autre.**

La fenêtre déplacée apparaît maintenant dans le deuxième espace de travail.

2 **Pour afficher la fenêtre dans tous les espaces de travail, choisissez Always Visible (Toujours visible) dans le menu affiché d'un clic sur le bouton droit de la souris dans la barre de titre.**



La fenêtre sélectionnée apparaît à présent dans chaque espace de travail.

▼ Procédure de détermination de l'étiquette d'un fichier

En général, l'étiquette d'un fichier est évidente. Toutefois, si vous êtes autorisé à visualiser les fichiers possédant une étiquette inférieure à celle de votre espace de travail actif, l'étiquette d'un fichier peut ne pas être évidente. En particulier, l'étiquette d'un fichier peut être différente de l'étiquette du navigateur de fichiers.

- **Utilisation du navigateur de fichiers.**

Astuce – Vous pouvez également utiliser l'option de menu Query Labels (Requête d'étiquette) dans le menu Trusted Path.

▼ Procédure de déplacement de données entre les étiquettes

Comme dans un système Oracle Solaris, vous pouvez déplacer les données entre les fenêtres dans Trusted Extensions. Toutefois, les données doivent posséder la même étiquette. Lorsque vous transférez des informations entre des fenêtres possédant des étiquettes différentes, vous augmentez ou réduisez la sensibilité de ces informations.

Avant de commencer

La stratégie de sécurité de votre site doit autoriser ce type de transfert, la zone contenant les données doit autoriser le nouvel étiquetage et vous devez être autorisé à déplacer des données entre des étiquettes.

Par conséquent, l'administrateur doit avoir effectué les tâches suivantes :

- "Procédure d'octroi de l'autorisation à modifier l'étiquette de fichiers à un utilisateur" du manuel *Configuration et administration d'Oracle Solaris Trusted Extensions*
- "Procédure d'octroi de l'autorisation de modifier le niveau de sécurité de données à un utilisateur" du manuel *Configuration et administration d'Oracle Solaris Trusted Extensions*

Vous devez être connecté à une session multiniveau.

1. **Créez deux espaces de travail possédant chacun l'une des étiquettes.**

   Pour plus d'informations, reportez-vous à la section "Procédure d'ajout d'un espace de travail sous votre étiquette minimale" à la page 53.

2. **Confirmez l'étiquette du fichier source.**

   Pour plus d'informations, reportez-vous à la section "Procédure de détermination de l'étiquette d'un fichier" à la page 55.

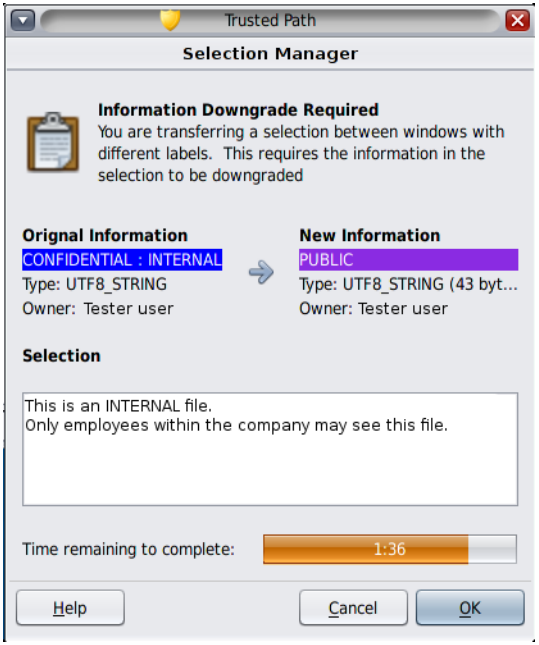
3 **Déplacez la fenêtre contenant les informations source vers un espace de travail possédant l'étiquette cible.**

Pour plus d'informations, reportez-vous à la section "Procédure de déplacement d'une fenêtre vers un autre espace de travail" à la page 54.

4 **Mettez en surbrillance les informations à déplacer et collez la sélection dans la fenêtre cible.**

La boîte de dialogue de confirmation du gestionnaire de sélection (Selection Manager) s'affiche.

FIGURE 3–5 Boîte de dialogue de confirmation du gestionnaire de sélection (Selection Manager)



5 **Examinez la boîte de dialogue de confirmation du gestionnaire de sélection, puis confirmez ou annulez la transaction.**

Cette boîte de dialogue :

- explique pourquoi la confirmation de la transaction est nécessaire ;
- identifie l'étiquette et le propriétaire du fichier source ;
- identifie l'étiquette et le propriétaire du fichier cible ;
- identifie le type de données sélectionnées pour le transfert, le type du fichier cible et la taille des données en octets. Par défaut, les données sélectionnées sont visibles sous forme de texte ;

- indique le temps restant jusqu'à l'achèvement de la transaction. La durée et l'utilisation du chronomètre dépendent de la configuration de votre site.

◆ ◆ ◆ CHAPITRE 4

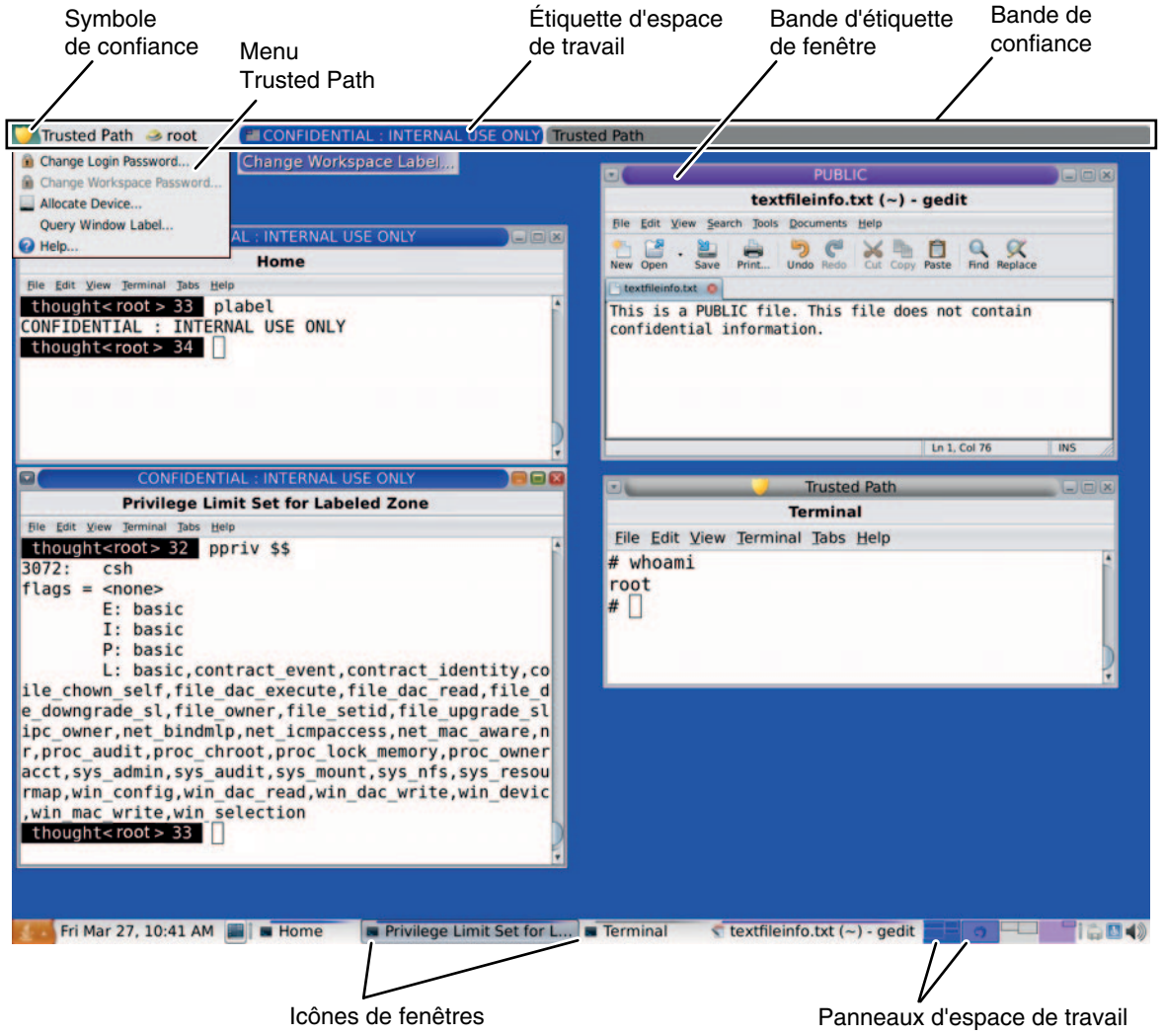
Eléments de Trusted Extensions (Référence)

Ce chapitre décrit les éléments clés de Trusted Extensions. Ce chapitre comprend les sections suivantes :

Caractéristiques visibles de Trusted Extensions

Une fois connecté selon la procédure indiquée au Chapitre 2, “Connexion à Trusted Extensions (tâches)”, vous pouvez travailler dans Trusted Extensions. Votre travail est soumis à certaines restrictions de sécurité. Les restrictions spécifiques à Trusted Extensions sont la plage d'étiquettes du système, vos autorisations et votre choix de session à niveau unique ou multiniveau. Comme illustré dans la figure suivante, quatre fonctions distinguent un système configuré avec Trusted Extensions d'un système Oracle Solaris.

FIGURE 4–1 Bureau Trusted Extensions multiniveau



- **Affichages des étiquettes** : toutes les fenêtres, les espaces de travail, les fichiers et les applications ont une étiquette. Le bureau fournit des bandes d'étiquettes et d'autres indicateurs permettant d'afficher l'étiquette d'une entité.
- **Bande de confiance** : cette bande est un mécanisme de sécurité graphique particulier. Dans chaque espace de travail, la bande s'affiche en haut de l'écran.
- **Accès limité à des applications à partir de l'espace de travail :** l'espace de travail vous permet uniquement d'accéder à des applications autorisées dans votre compte.

- **Menu Trusted Path (Chemin de confiance)** : le symbole de confiance permet d'accéder au menu.

Etiquettes sur les bureaux Trusted Extensions

Comme expliqué à la section "Contrôle d'accès obligatoire" à la page 18, toutes les applications et les fichiers Trusted Extensions portent des étiquettes. Trusted Extensions affiche les étiquettes aux emplacements suivants :

- Bandes d'étiquette de la fenêtre au-dessus de la barre de titre de la fenêtre
- Bande de couleur de l'étiquette au-dessus de l'icône de la fenêtre dans la liste de fenêtres
- Indicateur d'étiquette de la fenêtre dans la bande de confiance
- Indicateur de requête d'étiquette de fenêtre dans le menu Trusted Path qui affiche l'étiquette de la fenêtre ou l'icône de la fenêtre spécifiée par l'emplacement du pointeur

En outre, la couleur des panneaux indique l'étiquette de l'espace de travail.

FIGURE 4–2 Panneaux indiquant des espaces de travail possédant des étiquettes différentes

La Figure 4–1 présente l'affichage des étiquettes sur un bureau Trusted Extensions. En outre, l'option de menu Query Window Label (Requête d'étiquette de fenêtre) peut être utilisée pour afficher l'étiquette d'une fenêtre. Pour obtenir un exemple, reportez-vous à la Figure 3–2.

Bande de confiance

La bande de confiance s'affiche en haut de l'écran.

FIGURE 4–3 Bande de confiance sur le bureau

La bande de confiance sert à confirmer visuellement que vous vous trouvez dans une session légitime de Trusted Extensions. La bande vous indique que vous êtes en train d'interagir avec la base informatique sécurisée (TCB). La bande affiche également les étiquettes de l'espace de travail et de la fenêtre en cours. La bande de confiance ne peut pas être déplacée ni masquée par d'autres fenêtres ou boîtes de dialogue.

La bande de confiance comporte les éléments suivants :

- **Le symbole de confiance** : s'affiche lorsque l'élément affiché à l'écran relève de la sécurité.
- **L'étiquette de la fenêtre** : affiche l'étiquette de la fenêtre active lorsque l'élément affiché à l'écran relève de la sécurité.
- **Un marqueur de rôle** : à droite du symbole de confiance, avant le nom du compte, affiche une icône en forme de chapeau si le compte est un compte de rôle.
- **Le nom du compte actif** : à droite du symbole de confiance, affiche le nom du propriétaire du nouveau processus dans l'espace de travail.
- **Fenêtres étiquetées** : affichent les étiquettes de toutes les fenêtres de l'espace de travail.

Symbole de confiance

Chaque fois que vous accédez à une partie de la TCB, le symbole de confiance apparaît à gauche de la zone de la bande de confiance.

Le symbole de confiance n'est pas affiché lorsque le pointeur de la souris se trouve dans une fenêtre ou une zone de l'écran qui n'a pas d'impact sur la sécurité. Le symbole de confiance ne peut pas être falsifié. Si vous voyez le symbole, vous pouvez être assuré que vos interactions avec la TCB sont sécurisées.

Attention – Si la bande de confiance n'apparaît pas dans votre espace de travail, contactez l'administrateur de sécurité. Votre système pourrait avoir un problème sérieux.

La bande de confiance ne doit pas apparaître lors de la procédure de connexion, ni lorsque vous verrouillez votre écran. Si la bande de confiance apparaît, contactez immédiatement l'administrateur.

Indicateur d'étiquette de fenêtre

L'indicateur d'*étiquette de fenêtre* affiche l'étiquette de la fenêtre active. Dans une session multiniveau, l'indicateur peut aider à l'identification des fenêtres possédant des étiquettes différentes dans un même espace de travail. L'indicateur peut également signaler que vous interagissez avec la TCB. Lorsque vous modifiez votre mot de passe par exemple, l'indicateur Trusted Path apparaît dans la bande de confiance.

Sécurité des périphériques dans Trusted Extensions

Par défaut, dans Trusted Extensions, les périphériques sont protégés par des exigences d'allocation de périphériques. Un utilisateur ne peut pas utiliser un périphérique sans être explicitement autorisé à allouer des périphériques, et un périphérique alloué ne peut pas être utilisé par un autre utilisateur. Un périphérique en cours d'utilisation avec une étiquette ne peut pas être utilisé avec une autre étiquette tant que son allocation à la première étiquette n'a pas été annulée et remplacée par une allocation à la deuxième étiquette.

Pour utiliser un périphérique, reportez-vous à la section "Procédure d'allocation d'un périphérique dans Trusted Extensions" à la page 48.

Fichiers et applications dans Trusted Extensions

Le niveau de sensibilité de toutes les applications de Trusted Extensions est indiqué par leur étiquette. Les applications sont des *sujets* dans les transactions de données. Les sujets doivent dominer les *objets* auxquels ils tentent d'accéder. Les objets peuvent être des fichiers ; quelquefois, d'autres processus peuvent être des objets. Les informations d'étiquette d'une application s'affichent dans la bande d'étiquette de la fenêtre. L'étiquette est visible lorsqu'une fenêtre est ouverte ou réduite. L'étiquette d'une application peut aussi apparaître dans la bande de confiance lorsque le pointeur se trouve dans la fenêtre de l'application.

Dans Trusted Extensions, les fichiers sont des objets dans des transactions de données. Les fichiers ne sont accessibles que par les applications dont les étiquettes dominent les étiquettes des fichiers. Un fichier peut être consulté à partir de fenêtres possédant la même étiquette que le fichier.

Certaines applications utilisent les fichiers d'initialisation pour configurer l'environnement de l'utilisateur. Deux fichiers spéciaux dans votre répertoire personnel vous permettent d'accéder aux fichiers d'initialisation de chaque niveau d'étiquette. Ces fichiers permettent à une application correspondant à une étiquette d'utiliser un fichier d'initialisation provenant d'un répertoire dont l'étiquette est différente. Ces deux fichiers spéciaux sont `.copy_files` et `.link_files` .

Fichier .copy_files

Le fichier `.copy_files` stocke les noms des fichiers à copier la première fois que vous passez à un espace de travail d'un niveau d'étiquette plus élevé. Ce fichier est stocké dans votre répertoire personnel avec votre étiquette minimale. Ce fichier est utile si vous disposez d'une application qui écrit toujours dans un fichier portant un nom donné dans votre répertoire personnel. Le fichier `.copy_files` vous permet de spécifier que l'application doit mettre à jour le fichier au niveau de chaque étiquette.

Fichier .link_files

Le fichier `.link_files` stocke les noms des fichiers à lier la première fois que vous passez à un espace de travail d'un niveau d'étiquette plus élevé. Ce fichier est stocké dans votre répertoire personnel avec votre étiquette minimale. Le fichier `.link_files` est utile lorsqu'un fichier spécifique doit être disponible au niveau de plusieurs étiquettes, mais que le contenu doit être identique pour chaque étiquette.

Sécurité du mot de passe dans le SE Oracle Solaris

Les utilisateurs qui changent régulièrement de mot de passe réduisent les risques qu'un intrus n'utilise des mots de passe obtenus de manière illicite. Par conséquent, la stratégie de sécurité de votre site peut exiger que vous changiez régulièrement votre mot de passe. Le SE Oracle Solaris peut définir des exigences quant au contenu et à la réinitialisation des mots de passe. Les exigences concernant la réinitialisation peuvent être les suivantes :

- **Nombre minimum de jours entre les modifications :** empêche de modifier votre mot de passe pendant un nombre de jours défini.
- **Nombre maximum de jours entre les modifications :** exige la modification du mot de passe au bout d'un nombre de jours défini.
- **Nombre maximum de jours inactifs :** verrouille votre compte après le nombre de jours d'inactivité défini si le mot de passe n'a pas été modifié.
- **Date d'expiration :** oblige à modifier le mot de passe à une date spécifique.

Si votre administrateur a mis en oeuvre l'une des options qui précèdent, vous recevez un e-mail qui vous rappelle que vous devez changer votre mot de passe avant la date limite.

Des critères de contenu peuvent s'appliquer aux mots de passe. Dans le SE Oracle Solaris, les mots de passe doivent au minimum satisfaire les critères suivants :

- Le mot de passe doit comporter au moins huit caractères.
- Le mot de passe doit contenir au moins deux caractères alphabétiques et au moins un caractère numérique ou un caractère spécial.
- Le nouveau mot de passe doit être différent du mot de passe précédent. Vous ne pouvez pas utiliser le même mot de passe dans le désordre ou dans un ordre inversé. Pour cette comparaison, les lettres majuscules et minuscules sont considérées comme équivalentes.
- Le nouveau mot de passe doit comporter au moins trois caractères différents de l'ancien mot de passe. Pour cette comparaison, les lettres majuscules et minuscules sont considérées comme équivalentes.
- Le mot de passe doit être difficile à deviner. N'utilisez pas un mot courant ou un nom propre. Les programmes et les individus qui tentent de s'introduire dans un compte peuvent utiliser des listes pour essayer de deviner les mots de passe des utilisateurs.

Vous pouvez modifier votre mot de passe à l'aide de l'option de menu Change Password (Modifier le mot de passe) à partir du menu Trusted Path. Pour connaître la procédure à suivre, reportez-vous à la section "Procédure de modification du mot de passe dans Trusted Extensions" à la page 46.

Sécurité de l'espace de travail dans Trusted Extensions

Dans Trusted Extensions, les espaces de travail et les applications de bureau sont sensibles à l'étiquette. Les applications s'exécutent au niveau de l'étiquette de l'espace de travail actif et affichent uniquement des informations de même étiquette que la procédure qui a ouvert l'application.

Comportement et emplacement des fonctions de sécurité du bureau sécurisé :

- Le menu Trusted Path est accessible à partir de la bande de confiance.
- Le nom de l'étiquette d'une fenêtre dans la liste des tâches du tableau de bord s'affiche dans une info-bulle lorsque la souris passe sur la fenêtre. De même, le nom de l'étiquette d'un espace de travail dans la zone de commutation s'affiche dans l'info-bulle.
- Pour assumer un rôle, cliquez sur le nom du compte dans la bande de confiance et choisissez le rôle.
- Pour ajouter un espace de travail possédant une étiquette donnée, sélectionnez un espace de travail existant et modifiez son étiquette.
- Le bureau est configuré de manière à ce que chaque espace de travail s'affiche dans la couleur de l'étiquette qui lui est associée. Les panneaux dans la bande inférieure affichent également la couleur de l'étiquette.

Glossaire

administrateur de sécurité Sur un système configuré avec Trusted Extensions, rôle qui est affecté à l'utilisateur ou aux utilisateurs chargé(s) de définir et d'appliquer la stratégie de sécurité. L'administrateur de sécurité peut travailler au niveau de n'importe quelle étiquette dans la plage d'accréditations du système, et peut éventuellement accéder à toutes les informations du site. L'administrateur de sécurité configure les attributs de sécurité pour tous les utilisateurs et équipements. Voir également fichier de codage des étiquettes.

administrateur système Fonction de sécurité du SE Oracle Solaris. Le rôle d'administrateur système peut être affecté à l'utilisateur ou aux utilisateurs chargé(s) de réaliser des tâches standard d'administration du système telles que la configuration des éléments non liés à la sécurité des comptes utilisateur. Voir également administrateur de sécurité.

affichage des étiquettes Fonction de sécurité qui affiche les étiquettes d'administration ou les remplace par des éléments de substitution non classifiés. Par exemple, si la stratégie de sécurité interdit d'exposer les étiquettes `ADMIN_HIGH` et `ADMIN_LOW` , les étiquettes `RESTRICTED` et `PUBLIC` peuvent leur être substituées.

allocation de périphériques Fonction de sécurité du SE Oracle Solaris. L'allocation de périphériques est un mécanisme destiné à protéger les informations d'un périphérique affectable en empêchant toute personne autre que l'utilisateur qui affecte le périphérique d'y accéder. Lorsque le périphérique est libéré, des scripts de nettoyage du périphérique sont exécutés pour supprimer les informations du périphérique avant que celui-ci ne soit à nouveau accessible pour un autre utilisateur. Dans Trusted Extensions, l'allocation de périphériques est gérée par le gestionnaire de périphériques (Device Manager).

application sécurisée Application qui a reçu un ou plusieurs privilèges.

attributs de sécurité Fonction de sécurité du SE Oracle Solaris. Propriétés d'une entité liée à la sécurité telle qu'un processus, une zone, un utilisateur ou un périphérique. Les attributs de sécurité comprennent les valeurs d'identification comme ID utilisateur (UID) and ID de groupe (GID). Les attributs qui sont spécifiques à Trusted Extensions incluent les étiquettes et la plage d'étiquettes. Notez que certains attributs de sécurité seulement s'appliquent à un type d'entité particulier.

audit Fonction de sécurité du SE Oracle Solaris. L'audit est un processus permettant de capturer l'activité de l'utilisateur et d'autres événements survenant sur le système, puis de stocker ces informations dans un ensemble de fichiers appelé *piste d'audit*. L'audit génère des rapports d'activité du système dans le cadre de la stratégie de sécurité du site.

autorisation Fonction de sécurité du SE Oracle Solaris. Une autorisation permet à un utilisateur d'exécuter une action qui serait par ailleurs interdite par la stratégie de sécurité. L'administrateur de sécurité affecte les autorisations à un profil de droits. Les profils de droits sont ensuite assignés à des comptes utilisateur ou des rôles. Certaines commandes et actions ne fonctionnent pas parfaitement si l'utilisateur ne dispose pas des autorisations nécessaires. Voir également privilège.

autorisation de session autorisation définie lors de la connexion, qui indique la limite supérieure des étiquettes pour une session Trusted Extensions. Si l'utilisateur est autorisé à définir l'autorisation de session, il peut spécifier toute valeur figurant dans la plage d'étiquettes du compte de l'utilisateur. Si le compte de l'utilisateur est configuré de manière à ne permettre que des sessions à niveau unique, l'autorisation de session est définie sur la valeur par défaut indiquée par l'administrateur de sécurité. Voir également autorisation.

autorisation utilisateur Autorisation gérée par l'administrateur de sécurité. Une autorisation utilisateur définit la limite supérieure de la plage d'étiquettes du compte de l'utilisateur. L'autorisation utilisateur détermine l'étiquette la plus haute au niveau de laquelle l'utilisateur est autorisé à travailler. Voir également autorisation et autorisation de session.

autorisation étiquette définissant la limite supérieure de la plage d'étiquettes. Une autorisation comprend deux composants : une classification et aucun, un ou plusieurs compartiments. Une autorisation n'a pas besoin d'être une étiquette bien formée. Une autorisation définit une limite théorique et pas nécessairement une étiquette réelle. Voir également autorisation utilisateur, autorisation de session et fichier de codage des étiquettes.

bande de confiance Zone graphique rectangulaire plein écran apparaissant dans une zone réservée de l'écran. La bande de confiance s'affiche dans toutes les sessions Trusted Extensions pour confirmer qu'il s'agit de sessions Trusted Extensions valides. La bande de confiance dispose de deux composants : (1) un symbole de confiance obligatoire qui indique l'interaction avec la base informatique sécurisée (TCB, Trusted Computing Base) et (2) une étiquette qui indique l'étiquette active de la fenêtre ou de l'espace de travail actif.

base informatique sécurisée (TCB, Trusted Computing Base) Partie d'un système configuré avec Trusted Extensions qui a une incidence sur la sécurité. La TCB englobe les logiciels, le matériel, les microprogrammes, la documentation et les procédures administratives. Les utilitaires et applications pouvant accéder aux fichiers liés à la sécurité font partie de la base informatique sécurisée.

canal caché Canal de communication qui n'est normalement pas destiné à la communication de données. Un canal caché autorise un processus à transférer indirectement des informations d'une manière qui va à l'encontre de la stratégie de sécurité.

chemin de confiance Fait référence au mécanisme permettant d'accéder à des actions et des commandes autorisées à interagir avec la base informatique sécurisée (TCB, Trusted Computing Base). Voir également Menu Trusted Path (Chemin de confiance), symbole de confiance et bande de confiance.

classification Composant d'une autorisation ou d'une étiquette. Une classification indique un niveau de sécurité hiérarchique, par exemple `TOP SECRET` ou `UNCLASSIFIED`.

compartiment Composant non hiérarchique d'une étiquette utilisé avec le composant classification pour former une autorisation ou une étiquette. Un compartiment représente un groupe d'utilisateurs qui pourraient avoir besoin d'accéder à des informations, par exemple un département ingénierie ou une équipe de projet pluridisciplinaire.

compartmented mode workstation (CMW) Système informatique répondant aux exigences du gouvernement américain en termes de sécurité des stations de travail telles que spécifiées à la section *Security Requirements for System High and Compartmented Mode Workstations* du document DDS-2600-5502-87 de la DIA. Plus précisément, ce document définit un système d'exploitation sécurisé basé sur un système Window X pour les stations de travail UNIX.

configuration à niveau unique Compte utilisateur configuré pour être utilisé avec une étiquette unique. Egalement appelée configuration à niveau unique.

configuration étendue Système informatique qui n'est plus une configuration évaluable en raison de modifications qui ont enfreint la stratégie de sécurité.

configuration évaluable Système informatique répondant aux exigences de sécurité standard définies par le gouvernement. Voir également configuration étendue.

contrôle d'accès discrétionnaire (DAC, Discretionary Access Control) Mécanisme de contrôle d'accès qui permet au propriétaire d'un fichier ou d'un répertoire d'accorder ou de refuser l'accès à d'autres utilisateurs. Le propriétaire affecte des permissions en lecture, écriture et exécution au propriétaire, au groupe d'utilisateurs auquel appartient le propriétaire et à une catégorie appelée autres, qui fait référence à tous les autres utilisateurs non spécifiés. Le propriétaire peut également spécifier une liste de contrôle d'accès (ACL, Access Control List) . Une ACL permet au propriétaire d'attribuer des permissions spécifiques à d'autres utilisateurs et à d'autres groupes. Contraire de contrôle d'accès obligatoire (MAC, Mandatory Access Control).

contrôle d'accès obligatoire (MAC, Mandatory Access Control) Mécanisme de contrôle d'accès appliqué par le système qui utilise des autorisations et des étiquettes pour appliquer la stratégie de sécurité. Une autorisation ou une étiquette est un niveau de sécurité. MAC associe les programmes qu'un utilisateur exécute au niveau de sécurité auquel l'utilisateur choisit de travailler dans la session. MAC autorise uniquement l'accès aux informations, aux programmes et aux périphériques correspondant au même niveau ou à un niveau inférieur. MAC empêche également les utilisateurs d'écrire dans des fichiers de niveau inférieur. MAC ne peut pas être contourné sans une autorisation ou un privilège spécial. Contraire de contrôle d'accès discrétionnaire (DAC, Discretionary Access Control).

device Voir périphérique affectable.

domination stricte Voir également étiquette dominante.

droit d'accès Fonction de sécurité présente sur la plupart des systèmes informatiques. Les droits d'accès donnent à l'utilisateur l'autorisation de lire, d'écrire, d'exécuter ou d'afficher le nom d'un fichier ou d'un répertoire. Voir également contrôle d'accès discrétionnaire (DAC, Discretionary Access Control) et contrôle d'accès obligatoire (MAC, Mandatory Access Control).

espace de travail Voir espace de travail étiqueté.

espace de travail étiqueté Espace de travail associé à une étiquette. Un espace de travail étiqueté étiquette chaque activité qui y est lancée avec l'étiquette de l'espace de travail. Lorsque les utilisateurs déplacent une fenêtre dans un espace de travail correspondant à une autre étiquette, la fenêtre déplacée conserve son étiquette d'origine. Chaque espace de travail d'un bureau sécurisé est étiqueté. Deux espaces de travail peuvent être associés à la même étiquette.

étiquette Egalement appelée étiquette de sensibilité. Une étiquette indique le niveau de sécurité d'une entité. Une entité est un fichier, un répertoire, un processus, un périphérique ou une interface réseau. L'étiquette d'une entité permet de déterminer si l'accès doit être autorisé dans une transaction particulière. Les étiquettes comprennent deux composants : une classification qui indique le niveau hiérarchique de sécurité et aucun, un ou plusieurs compartiments permettant de définir qui peut accéder à une entité d'une classification donnée. Voir également fichier de codage des étiquettes.

étiquette bien formée étiquette pouvant être incluse dans une plage, car elle est autorisée par toutes les règles applicables dans le fichier de codage des étiquettes.

étiquette de sensibilité Voir étiquette.

étiquette déclassée étiquette d'un objet qui a été modifiée et remplacée par une valeur qui n'est pas dominante par rapport à la valeur précédente de l'étiquette.

étiquette disjointe Voir également étiquette dominante.

étiquette dominante Lors de la comparaison de deux étiquettes, étiquette dont le composant classification est supérieur ou égal à la classification de la deuxième étiquette et dont les composants compartiment comprennent tous les composants compartiment de la deuxième étiquette. Si les composants sont les mêmes, les étiquettes sont dites dominantes et sont *égales*. Si une étiquette domine l'autre et les étiquettes ne sont donc pas égales, la première étiquette est dite *strictement dominante* par rapport à l'autre. Deux étiquettes sont *disjointes* si elles ne sont pas égales et qu'aucune étiquette n'est dominante.

étiquette minimale étiquette affectée à un utilisateur en tant que limite inférieure de l'ensemble d'étiquettes dans lequel cet utilisateur peut travailler. La première fois qu'un utilisateur ouvre une session Trusted Extensions, l'étiquette minimum est l'étiquette par défaut de l'utilisateur. Au moment de la connexion, l'utilisateur peut choisir une autre étiquette comme étiquette initiale.

Désigne aussi l'étiquette la plus basse autorisée pour tout utilisateur non administratif. L'étiquette minimum est affectée par l'administrateur de sécurité et définit la limite inférieure de la plage d'accréditations de l'utilisateur.

étiquette surclassée étiquette d'un objet ayant été modifiée et remplacée par une valeur qui est dominante par rapport à la valeur précédente de l'étiquette.

étiquettes d'administration Deux étiquettes spéciales prévues pour les fichiers d'administration uniquement : `ADMIN_LOW` et `ADMIN_HIGH`. `ADMIN_LOW` est l'étiquette la plus basse dans le système sans catégories. Cette étiquette est strictement dominée par toutes les étiquettes du système. Les informations de niveau `ADMIN_LOW` sont lisibles par tous, mais peuvent uniquement être écrites par un utilisateur occupant un rôle qui travaille au niveau de l'étiquette `ADMIN_LOW`. `ADMIN_HIGH` est l'étiquette la plus haute dans le système sans catégories. Cette étiquette domine strictement toutes les étiquettes du système. Les informations de niveau `ADMIN_HIGH` ne sont lisibles que par les utilisateurs occupant un rôle opérant au niveau `ADMIN_HIGH`. Les étiquettes d'administration sont utilisées comme des étiquettes ou des autorisations pour les rôles et les systèmes. Voir également étiquette dominante.

fichier de codage des étiquettes Fichier géré par l'administrateur de sécurité. Le fichier de codage contient les définitions de toutes les autorisations et étiquettes valides. Il définit également la plage d'accréditations du système et la plage d'accréditations de l'utilisateur et définit les informations de sécurité des impressions sur le site.

générateur d'étiquettes (label builder) Application sécurisée de Trusted Extensions. Cette interface graphique permet aux utilisateurs de choisir des autorisations pour la session ou une étiquette de session. L'autorisation ou l'étiquette doit être comprise dans la plage d'étiquettes du compte que l'administrateur de sécurité a affectée à l'utilisateur.

gestion des installations sécurisées Toutes les activités associées à l'administration du système dans un système UNIX classique, plus toutes les activités d'administration nécessaires au maintien de la sécurité d'un système distribué et des données qu'il contient.

gestionnaire de périphériques (Device Manager) Application sécurisée de Trusted Extensions. Cette interface graphique est utilisée pour configurer, allouer et libérer des périphériques. La configuration des périphériques inclut l'ajout d'exigences relatives à l'autorisation à un périphérique.

Gestionnaire de sélection (Selection Manager) Application sécurisée de Trusted Extensions. Cette interface graphique s'affiche lorsque des utilisateurs autorisés tentent d'augmenter ou de réduire le niveau de sécurité d'informations.

hôte Ordinateur connecté à un réseau.

ID de contrôle (AUID, Audit ID) Fonction de sécurité du SE Oracle Solaris. Un ID de contrôle représente l'utilisateur connecté. L'AUID n'est plus modifié une fois que l'utilisateur assume un rôle, de sorte qu'il est utilisé pour identifier l'utilisateur à des fins d'audit. L'ID d'audit représente toujours l'utilisateur objet du contrôle, même lorsque celui-ci acquiert des UID/GID effectifs. Voir également ID utilisateur (UID).

ID de groupe (GID) Fonction de sécurité du SE Oracle Solaris. Un ID de groupe est un nombre entier qui identifie un groupe d'utilisateurs partageant des droits d'accès communs. Voir également contrôle d'accès discrétionnaire (DAC, Discretionary Access Control).

ID utilisateur (UID) Fonction de sécurité du SE Oracle Solaris. Un UID identifie un utilisateur à des fins de contrôle d'accès discrétionnaire (DAC, Discretionary Access Control), de contrôle d'accès obligatoire (MAC, Mandatory Access Control) et d'audit. Voir également droit d'accès.

lecture Aptitude d'un sujet à visualiser un objet dont l'étiquette est dominée par le sujet. La stratégie de sécurité autorise généralement la lecture. Par exemple, un éditeur de texte qui s'exécute en tant que `Secret` peut lire les données `Unclassified`. Voir également contrôle d'accès obligatoire (MAC, Mandatory Access Control).

liste de contrôle d'accès (ACL, Access Control List) Fonction de sécurité du SE Oracle Solaris. Une ACL étend le contrôle d'accès discrétionnaire (DAC, Discretionary Access Control) à l'utilisation d'une liste de spécifications de permission (entrées ACL) qui s'appliquent à des utilisateurs et des groupes spécifiques. Une ACL permet un contrôle plus précis que celui que fourni par les permissions UNIX standard.

mécanisme de secours Méthode de raccourci permettant de spécifier des adresse IP dans la base de données `tnrhtp`. Pour les adresses IPv4, le mécanisme de secours reconnaît le `0` comme un caractère générique pour un sous-réseau.

Menu Trusted Path (Chemin de confiance) Menu des opérations Trusted Extensions qui s'affiche lorsque vous maintenez le bouton 3 de la souris enfoncé sur la zone de commutation du tableau de bord. Les sélections de menu se répartissent en trois catégories : sélections orientées espace de travail, sélections d'adoption de rôle et tâches liées à la sécurité.

modèle d'hôte Enregistrement dans la base de données `tnrhtp` qui définit les attributs de sécurité d'une classe d'hôtes pouvant accéder au réseau Trusted Extensions.

moindre privilège Voir principe du moindre privilège.

objet Entité passive contenant ou recevant des données, par exemple un fichier de données, un répertoire, une imprimante ou un autre périphérique. Un objet fait généralement l'objet d'interventions de la part de sujets. Dans certains cas, un processus peut être un objet, par exemple lorsque vous envoyez un signal à un processus.

opérateur rôle pouvant être affecté à l'utilisateur ou aux utilisateurs chargés de la sauvegarde des systèmes.

passerelle Hôte qui possède plusieurs interfaces réseau. Un tel hôte peut être utilisé pour relier deux ou plusieurs réseaux. Lorsque la passerelle est un hôte Trusted Extensions, elle peut restreindre le trafic à une étiquette donnée.

périphérique affectable Fonction de sécurité du SE Oracle Solaris. Un périphérique affectable peut être utilisé par un seul utilisateur à la fois et est en mesure d'importer ou d'exporter des données à partir du système. L'administrateur de sécurité détermine les utilisateurs autorisés à accéder à des périphériques affectables précis. Les périphériques affectables incluent les lecteurs de bande, les lecteurs de disquette, les périphériques audio et les lecteurs de CD-ROM. Voir également allocation de périphériques.

périphérique libéré Fonction de sécurité du SE Oracle Solaris. Un périphérique libéré n'est plus alloué exclusivement à un utilisateur. Voir également allocation de périphériques.

permissions Ensemble de codes qui indiquent quels utilisateurs sont autorisés à lire, écrire ou exécuter le fichier ou répertoire (dossier). Les utilisateurs sont classés dans les catégories suivantes : propriétaire, groupe (groupe du propriétaire) et autres (tous les autres). L'autorisation de lecture, indiquée par la lettre *r*, permet à l'utilisateur de lire le contenu d'un fichier ou, s'il s'agit d'un répertoire, d'afficher la liste des fichiers présents dans le dossier. La permission d'écriture, indiquée par la lettre *w*, permet à l'utilisateur d'apporter des modifications à un fichier ou, dans le cas d'un dossier, d'ajouter ou de supprimer des fichiers. Le droit d'exécution, indiqué par la lettre *e*, permet à l'utilisateur d'exécuter le fichier s'il s'agit d'un fichier exécutable. Si le fichier est un répertoire, le droit d'exécution permet à l'utilisateur de lire les fichiers dans le répertoire ou d'y effectuer une recherche. On parle également d'autorisations UNIX ou de bits d'autorisation.

plage d'accréditations Ensemble d'étiquettes approuvées pour une classe d'utilisateurs ou de ressources. Voir également plage d'accréditations du système, plage d'accréditations de l'utilisateur, fichier de codage des étiquettes et plage d'accréditations réseau.

plage d'accréditations de l'utilisateur Plus vaste ensemble d'étiquettes que l'administrateur de sécurité puisse potentiellement affecter à un utilisateur d'un site spécifique. La plage d'accréditations de l'utilisateur exclut les étiquettes d'administration et toute combinaison d'étiquettes uniquement disponible aux administrateurs. La plage d'accréditations de l'utilisateur est définie dans le fichier de codage des étiquettes.

plage d'accréditations du système Ensemble de toutes les étiquettes valides pour un site. Cet ensemble comprend les étiquettes d'administration disponibles pour l'administrateur de sécurité et l'administrateur système du site. La plage d'accréditations du système est définie dans le fichier de codage des étiquettes.

plage d'accréditations réseau Ensemble d'étiquettes au sein duquel les hôtes Trusted Extensions sont autorisés à communiquer sur un réseau. Cet ensemble peut être une liste de quatre étiquettes discrètes.

plage d'étiquettes N'importe quel ensemble d'étiquettes limité au niveau supérieur par une autorisation ou étiquette maximale, au niveau inférieur par une étiquette minimale et se composant d'étiquettes bien formées. Les plages d'étiquettes sont utilisées pour appliquer le contrôle d'accès obligatoire (MAC, Mandatory Access Control). Voir également fichier de codage des étiquettes, plage d'étiquettes du compte, plage d'accréditations, plage d'accréditations réseau, plage de session, plage d'accréditations du système et plage d'accréditations de l'utilisateur.

plage d'étiquettes du compte Ensemble d'étiquettes affecté par l'administrateur de sécurité à un utilisateur ou un rôle pour travailler sur un système configuré avec Trusted Extensions. Une plage d'étiquettes est définie au niveau supérieur par l'autorisation utilisateur et au niveau inférieur par l'étiquette minimale de l'utilisateur. Chaque étiquette de l'ensemble doit être bien formée.

plage de session Ensemble des étiquettes disponibles pour un utilisateur pendant une session Trusted Extensions. La plage de session est limitée au niveau supérieur par l'autorisation de session de l'utilisateur et au niveau inférieur par l'étiquette minimale.

principe du moindre privilège Principe de sécurité qui limite les utilisateurs aux seules fonctions nécessaires à leur travail. Ce principe est appliqué dans le SE Oracle Solaris en mettant les privilèges à la disposition des programmes en fonction des besoins. Les privilèges sont disponibles en fonction des besoins, à des fins spécifiques uniquement.

privilège Fonction de sécurité du SE Oracle Solaris. Un privilège est une autorisation accordée à un programme par l'administrateur de sécurité. Un privilège peut être requis pour passer outre à certains aspects de la stratégie de sécurité. Voir également autorisation.

processus Programme en cours d'exécution. Les processus Trusted Extensions disposent d'attributs de sécurité Oracle Solaris, tels que l'ID utilisateur (UID), l'ID de groupe (GID), l'ID de contrôle (AUID, Audit ID) de l'utilisateur et des privilèges. Trusted Extensions ajoute une étiquette à chaque processus.

processus privilégié Fonction de sécurité du SE Oracle Solaris. Un processus privilégié est exécuté par un utilisateur disposant de privilèges.

profil Voir profil de droits.

profil de droits Fonction de sécurité du SE Oracle Solaris. Un profil de droits permet à l'administrateur de sécurité d'un site de regrouper les commandes et les attributs de sécurité. Les attributs, tels que les autorisations et les privilèges de l'utilisateur, permettent aux commandes d'aboutir. Un profil de droits contient généralement des tâches connexes. Un profil peut être affecté à des utilisateurs et à des rôles.

rôle Fonction de sécurité du SE Oracle Solaris. Un rôle est un compte spécial qui donne à l'utilisateur qui assume le rôle accès à certaines applications avec les attributs de sécurité nécessaires à l'exécution de tâches spécifiques.

session Intervalle de temps qui s'écoule entre la connexion à l'hôte Trusted Extensions et la déconnexion de l'hôte. La bande de confiance apparaît lors de toutes les sessions Trusted Extensions pour confirmer que les utilisateurs ne sont pas victimes d'une usurpation par un système contrefait.

shell de profil Fonction de sécurité du SE Oracle Solaris. Une version du shell Bourne qui permet à un utilisateur d'exécuter des programmes avec des attributs de sécurité.

stratégie de sécurité Ensemble des règles DAC, MAC et d'étiquettes qui définissent la manière dont les informations peuvent être consultées et par qui. Sur le site d'un client, ensemble de règles qui définit la sensibilité des informations traitées au niveau de ce site. La stratégie comprend les mesures utilisées pour protéger les informations contre tout accès non autorisé.

sujet Entité active, généralement un processus qui s'exécute au nom d'un utilisateur ou d'un rôle. Un sujet fait circuler les informations entre les objets ou modifie l'état du système.

symbole de confiance Symbole qui s'affiche à gauche de la zone bande de confiance. Le symbole s'affiche chaque fois que l'utilisateur accède à une partie de la base informatique sécurisée (TCB, Trusted Computing Base).

Trusted GNOME Bureau graphique étiqueté incluant un gestionnaire de sessions, un gestionnaire de fenêtres et différents outils du bureau. Le bureau est entièrement accessible.

type d'hôte Classification d'un hôte. La classification est utilisée pour les communications réseau. Les définitions des types d'hôtes sont stockées dans la base de données `tnrhtp`. Le type d'hôte détermine si le protocole réseau CIPSO est utilisé pour communiquer avec d'autres hôtes sur le réseau. L'expression *protocole réseau* se rapporte aux règles d'empaquetage des informations de communication.

UID/GID effectif Fonction de sécurité du SE Oracle Solaris. Les ID effectifs remplacent le véritable ID lorsque cela est nécessaire pour exécuter un programme particulier ou une option d'un programme. L'administrateur de sécurité affecte un UID effectif à une commande ou une action ou dans un profil de droits lorsque cette commande ou action doit être exécutée par un utilisateur spécifique, le plus souvent lorsque la commande doit être exécutée en tant que root. Les ID de groupe effectifs sont utilisés de la même manière. Notez que l'utilisation de la commande `setuid` comme dans les systèmes UNIX classiques risque de ne pas fonctionner en raison des privilèges nécessaires.

usurpation Acte consistant à contrefaire un programme logiciel afin d'accéder de manière illicite aux informations présentes sur un système.

utilisateur standard Utilisateur qui ne détient aucune autorisation spéciale permettant des exceptions par rapport aux stratégies de sécurité standard du système. En général, un utilisateur standard ne peut pas assumer de rôle d'administration.

Index

C

D

E

F

G

I

L

M

N

O

P

R

S

T

U

V

Z