Procédures de l'administrateur Oracle® Solaris Trusted Extensions

Référence : E22290
Août 2011

111013@25097

Table des matières

Liste des figures

Liste des tableaux

Préface

Le guide *Procédures de l'administrateur Oracle Solaris Trusted Extensions* décrit les procédures de configuration de Trusted Extensions sur le Système d'exploitation Solaris. Ce guide décrit également des procédures de gestion des utilisateurs, zones, périphériques et hôtes étiquetés à l'aide du logiciel Trusted Extensions.

Remarque – Cette version d'Oracle Solaris prend en charge les systèmes utilisant les architectures de processeur SPARC et x86. Les systèmes pris en charge sont répertoriés dans les listes de la page Oracle Solaris OS: Hardware Compatibility Lists (`http://www.oracle.com/webfolder/technetwork/hcl/index.html`). Ce document présente les différences d'implémentation en fonction des divers types de plates-formes.

Dans ce document, les termes relatifs à x86 suivants ont la signification suivante :

- x86 désigne la famille des produits compatibles x86 64 bits.
- x64 concerne spécifiquement les UC compatibles x86 64 bits.

Pour connaître les systèmes pris en charge, reportez-vous aux *Oracle Solaris OS: Hardware Compatibility Lists*.

Utilisateurs de ce guide

Ce guide est destiné aux administrateurs système expérimentés et aux administrateurs de sécurité chargés de configurer et d'administrer le logiciel Trusted Extensions. Le niveau de confiance requis par votre stratégie de sécurité du site et votre niveau d'expertise déterminent les personnes habilitées à exécuter les tâches de configuration.

Les administrateurs doivent être familiarisés avec l'administration Oracle Solaris. En outre, il est important que les administrateurs connaissent les éléments suivants :

- Les fonctions de sécurité de Trusted Extensions et la stratégie de sécurité de votre site
- Les concepts de base et les procédures d'utilisation d'un hôte configuré avec Trusted Extensions, comme décrit dans le *Guide de l'utilisateur Oracle Solaris Trusted Extensions*
- La manière dont les tâches d'administration sont réparties entre les rôles de votre site

Organisation des guides Trusted Extensions

Le tableau suivant énumère les sujets abordés dans les guides Trusted Extensions et le public visé par chaque guide.

Titre du guide	Sujets	Public visé
Solaris Trusted Extensions Transition Guide	Obsolète. Fournit un aperçu des différences entre les logiciels Trusted Solaris 8, Solaris10 et Trusted Extensions. Pour cette version, le document *Nouveautés* pour le SE Oracle Solaris fournit un aperçu des modifications apportées à Trusted Extensions.	Tous
Solaris Trusted Extensions Reference Manual	Obsolète. Fournit les pages de manuel Trusted Extensions pour les versions Solaris 10 11/06 et Solaris 10 8/07 de Trusted Extensions. Pour cette version, les pages de manuel Trusted Extensions sont incluses dans les pages de manuel Solaris. Pour localiser les pages de manuel spécifiques, reportez-vous aux Annexe B, “Liste des pages de manuel Trusted Extensions”.	Tous
Guide de l'utilisateur Oracle Solaris Trusted Extensions	Décrit les fonctions de base de Trusted Extensions. Ce guide contient un glossaire.	Utilisateurs, administrateurs, développeurs
Solaris Trusted Extensions Installation and Configuration for Solaris 10 11/06 and Solaris 10 8/07 Releases	Obsolète. Décrit la planification, l'installation et la configuration de Trusted Extensions pour les versions Solaris 10 11/06 et Solaris 10 8/07 de Trusted Extensions.	Administrateurs, développeurs
Guide de configuration d'Oracle Solaris Trusted Extensions	À partir de la version Solaris 10 5/08, décrit l'activation et la configuration initiale de Trusted Extensions. Remplace *Solaris Trusted Extensions Installation and Configuration*.	Administrateurs, développeurs
Procédures de l'administrateur Oracle Solaris Trusted Extensions	Indique comment effectuer des tâches d'administration spécifiques.	Administrateurs, développeurs
Oracle Solaris Trusted Extensions Developer's Guide	Décrit le développement d'applications avec Trusted Extensions.	Développeurs, administrateurs
Oracle Solaris 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

Guides d'administration du système connexes

Les guides suivants contiennent des informations utiles pour la préparation et l'exécution du logiciel Trusted Extensions.

Titre du manuel	Sujets
System Administration Guide: Basic Administration	Comptes utilisateur et groupes, prise en charge serveur et client, arrêt et démarrage d'un système, gestion des services et des logiciels (packages et patchs)
Guide d'administration système : Administration avancée	Terminaux et modems, ressources système (quotas d'utilisation de disque, comptabilisation et crontabs), processus système et résolution des problèmes du logiciel Solaris
System Administration Guide: Devices and File Systems	Médias amovibles, disques et périphériques, systèmes de fichiers, et sauvegarde et restauration des données
Guide d'administration système : services IP	Administration de réseau TCP/IP, administration d'adresses IPv4 et IPv6, DHCP, IPsec, IKE, filtre IP Solaris, IP mobile, multiacheminement sur réseau IP (IPMP) et IPQoS
Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)	Services d'annuaire et d'attribution de noms DNS, NIS et LDAP, et transition de NIS à LDAP et de NIS+ à LDAP
Guide d'administration système : Services réseau	Serveurs cache Web, services à facteur temps, systèmes de fichiers de réseau (NFS et Autofs), mail, SLP et PPP
System Administration Guide: Security Services	Audit, gestion de périphérique, sécurité des fichiers, BART, services Kerberos, PAM, structure cryptographique Solaris, privilèges, RBAC, SASL et shell sécurisé Solaris
Guide d'administration système : Gestion des ressources des conteneurs et des zones Oracle Solaris	Gestion des ressources pour les projets et les tâches, comptabilisation étendue, contrôles de ressources, ordonnanceur FSS, contrôle de la mémoire physique à l'aide du démon d'allocation restrictive des ressources (rcapd) et pools de ressources ; virtualisation au moyen de la technologie de partitionnement du logiciel Solaris Zones et des zones marquées `lx`
Guide d'administration Oracle Solaris ZFS	Création et gestion de pools de stockage et de systèmes de fichiers ZFS, instantanés, clones, sauvegardes à l'aide de listes de contrôle d'accès (ACL) pour protéger les fichiers ZFS, utilisation de Solaris ZFS sur un système Solaris avec des zones installées, volumes émulés et dépannage et récupération de données
System Administration Guide: Printing	Tâches et sections relatives à l'impression Solaris, utilisation des services, outils, protocoles et technologies permettant de configurer et de gérer les imprimantes et services d'impression

Références connexes

Votre document de stratégie de sécurité du site : décrit la stratégie de sécurité et les procédures de sécurité de votre site.

Solaris CDE - Guide avancé de l'utilisateur et de l'administrateur système : décrit l'environnement CDE (Common Desktop Environment).

Guide de l'administrateur du système d'exploitation actuellement installé : décrit le processus de sauvegarde des fichiers système.

Références connexes aux sites Web de logiciels tiers

Des URL tiers pointant vers des informations complémentaires sont cités dans ce document.

Remarque – Oracle ne saurait être tenu responsable de la disponibilité des sites Web tiers mentionnés dans ce guide. Oracle décline toute responsabilité quant au contenu, à la publicité, aux produits et autres documents disponibles sur ces sites ou dans ces ressources, ou accessibles par leur intermédiaire, et ne saurait en être tenu pour responsable. Oracle ne saurait en aucun cas être tenu pour responsable de toute perte ou dommage, réel(le) ou prétendu(e), causé(e) ou prétendument causé(e) par l'utilisation desdits contenus, biens ou services disponibles sur ou par le biais de ces sites et ressources.

Documentation et support

Pour obtenir des ressources supplémentaires, reportez-vous aux sites Web suivants :

- Documentation (`http://www.oracle.com/technetwork/indexes/documentation/index.html`)
- Assistance (`http://www.oracle.com/us/support/systems/index.html`)

Ressources logicielles Oracle

Le site Réseau technologie d'Oracle (`http://www.oracle.com/technetwork/index.html`) propose un éventail de ressources liées aux logiciels Oracle :

- Discutez de problèmes techniques et trouvez des solutions sur les forums de discussion (`http://forums.oracle.com`).
- Passez à la pratique grâce aux didacticiels étape par étape avec Oracle By Example (`http://www.oracle.com/technetwork/tutorials/index.html`).

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` *nom_fichier*.
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%`

TABLEAU P–2 Invites de shell *(Suite)*

Shell	Invite
C shell pour superutilisateur	`nom_machine#`

◆ ◆ ◆ CHAPITRE 1

Concepts d'administration de Trusted Extensions

Ce chapitre vous initie à l'administration d'un système configuré avec le logiciel Solaris Trusted Extensions.

Le logiciel Trusted Extensions et le SE Oracle Solaris

Le logiciel Trusted Extensions ajoute des étiquettes à un système qui exécute le système d'exploitation Solaris (SE Oracle Solaris). Les étiquettes appliquent un *contrôle d'accès obligatoire* (MAC, Mandatory access control). Le MAC et le contrôle d'accès discrétionnaire (DAC, Discretionary access control) protègent les sujets (processus) et les objets (données) du système. Le logiciel Trusted Extensions fournit des interfaces pour gérer la configuration et l'assignation des étiquettes, ainsi que la stratégie les concernant.

Similarités entre Trusted Extensions et le SE Oracle Solaris

Le logiciel Trusted Extensions utilise des profils de droits, des rôles, l'audit, les privilèges et d'autres fonctions de sécurité du SE Oracle Solaris. Vous pouvez utiliser le shell sécurisé Oracle Solaris (SSH), BART, la structure cryptographique d'Oracle Solaris ainsi qu'IPsec et IP filter avec Trusted Extensions.

- Comme dans le SE Oracle Solaris, les utilisateurs peuvent être limités à l'utilisation des applications nécessaires pour exécuter leurs tâches. D'autres utilisateurs peuvent être autorisés à effectuer davantage de tâches.
- Comme dans le SE Oracle Solaris, les fonctions qui étaient autrefois assignées au superutilisateur sont assignées à des "rôles" distincts et discrets.

- Comme dans le SE Oracle Solaris, des privilèges protègent les processus. Des zones sont également utilisées pour séparer les processus.
- Comme dans le SE Oracle Solaris, les événements du système peuvent être audités.
- Trusted Extensions utilise les fichiers de configuration système du SE Oracle Solaris tels que `policy.conf` et `exec_attr`.

Différences entre Trusted Extensions et le SE Oracle Solaris

Le logiciel Trusted Extensions étend le SE Oracle Solaris. La liste suivante offre une vue d'ensemble. Pour une référence rapide, reportez-vous à Annexe A, “Guide de référence rapide pour l'administration de Trusted Extensions”.

- Trusted Extensions contrôle l'accès aux données à l'aide de balises de sécurité spéciales nommées *étiquettes*. Les étiquettes assurent un *contrôle d'accès obligatoire* (MAC). La protection MAC s'ajoute aux autorisations des fichiers UNIX, ou contrôle d'accès discrétionnaire (DAC). Les étiquettes sont directement assignées aux utilisateurs, aux zones, aux périphériques, aux fenêtres et aux extrémités de réseaux. Les étiquettes sont assignées implicitement à des processus, des fichiers et à d'autres objets système.

  Les utilisateurs standard ne peuvent pas passer outre au MAC. Dans Trusted Extensions les utilisateurs standard doivent travailler dans des zones étiquetées. Par défaut, aucun utilisateur ou processus de zone étiquetée ne peut passer outre au MAC.

  Comme dans le SE Oracle Solaris, la possibilité de passer outre à la stratégie de sécurité peut être assignée à des processus ou à des utilisateurs spécifiques lorsque le MAC peut être ignoré. Par exemple, des utilisateurs peuvent être autorisés à modifier l'étiquette d'un fichier. Cette opération permet de mettre à niveau ou de rétrograder des informations de ce fichier.
- Trusted Extensions ajoute des fichiers et des commandes à la configuration existante. Par exemple, Trusted Extensions ajoute des événements d'audit, des autorisations, des privilèges et des profils de droits.
- Certaines fonctions facultatives sur un système Oracle Solaris sont obligatoires sur un système Trusted Extensions. Par exemple, les zones et les rôles sont obligatoires sur un système configuré avec Trusted Extensions.
- Certaines fonctions facultatives sur un système Oracle Solaris sont recommandées sur un système Trusted Extensions. Par exemple, dans Trusted Extensions, il est recommandé de transformer l'utilisateur `root` en un rôle `root`.
- Trusted Extensions peut modifier le comportement par défaut du SE Oracle Solaris. Par exemple, sur un système configuré avec Trusted Extensions, l'audit est activé par défaut. En outre, l'allocation de périphériques est obligatoire.

- Trusted Extensions peut restreindre les options disponibles dans le SE Oracle Solaris. Par exemple, sur un système configuré avec Trusted Extensions, le service de nommage NIS+ n'est pas pris en charge. En outre, toutes les zones sont étiquetées dans Trusted Extensions. À la différence du SE Oracle Solaris, les zones étiquetées doivent utiliser le même pool d'ID utilisateur et d'ID de groupe. En outre, dans Trusted Extensions, les zones étiquetées peuvent partager une même adresse IP.
- Trusted Extensions fournit des versions sécurisées de deux bureaux. Pour travailler dans un environnement étiqueté, les utilisateurs de bureau de Trusted Extensions doivent utiliser l'un des bureaux suivants :
  - **Solaris Trusted Extensions (CDE)**, la version de confiance de Common Desktop Environment (CDE). Le nom peut être abrégé en Trusted CDE.
  - **Solaris Trusted Extensions (JDS)**, la version de confiance de Java Desktop System, version *number*. Le nom peut être abrégé en Trusted JDS.
- Trusted Extensions fournit d'autres interfaces utilisateur graphiques (GUI, Graphical user interfaces) et interfaces de ligne de commande (CLI, Command line interfaces). Par exemple, Trusted Extensions fournit le Device Allocation Manager (Gestionnaire d'allocation de périphériques) pour administrer les périphériques. En outre, la commande `updatehome` permet de placer les fichiers de démarrage dans le répertoire personnel d'un utilisateur standard à chaque étiquette.
- Trusted Extensions requiert l'utilisation d'interfaces utilisateur graphiques spécifiques pour l'administration. Par exemple, sur un système est configuré avec Trusted Extensions, la Console de gestion Solaris est utilisée pour administrer les utilisateurs, les rôles et le réseau. De même, dans Trusted CDE, l'action Admin Editor permet de modifier les fichiers système.
- Trusted Extensions limite les données lisibles par les utilisateurs. Par exemple, un périphérique qui ne peut pas être alloué par un utilisateur n'est pas visible pour cet utilisateur.
- Trusted Extensions limite les options de bureau des utilisateurs. Par exemple, le temps d'inactivité avant verrouillage de l'écran des utilisateurs est limité.

Systèmes multiécran et le bureau Trusted Extensions

Lorsque les écrans d'un système Trusted Extensions multiécran sont configurés horizontalement, une bande de confiance s'étend sur tous les écrans. Lorsque les moniteurs sont configurés verticalement, la bande de confiance s'affiche dans l'écran le plus bas.

Lorsque plusieurs espaces de travail sont affichés sur les moniteurs d'un système multiécran, Trusted CDE et Trusted JDS effectuent différemment le rendu de la bande de confiance.

- Sur un bureau Trusted JDS chaque moniteur affiche une bande de confiance.
- Sur un bureau Trusted CDE, une bande de confiance s'affiche sur l'écran principal.

Attention – Si une deuxième bande de confiance s'affiche sur un système multiécran Trusted CDE, celle-ci 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 la bande de confiance appropriée, reportez-vous à la section "Reprise du contrôle du focus actuel du bureau" à la page 74.

Concepts de base de Trusted Extensions

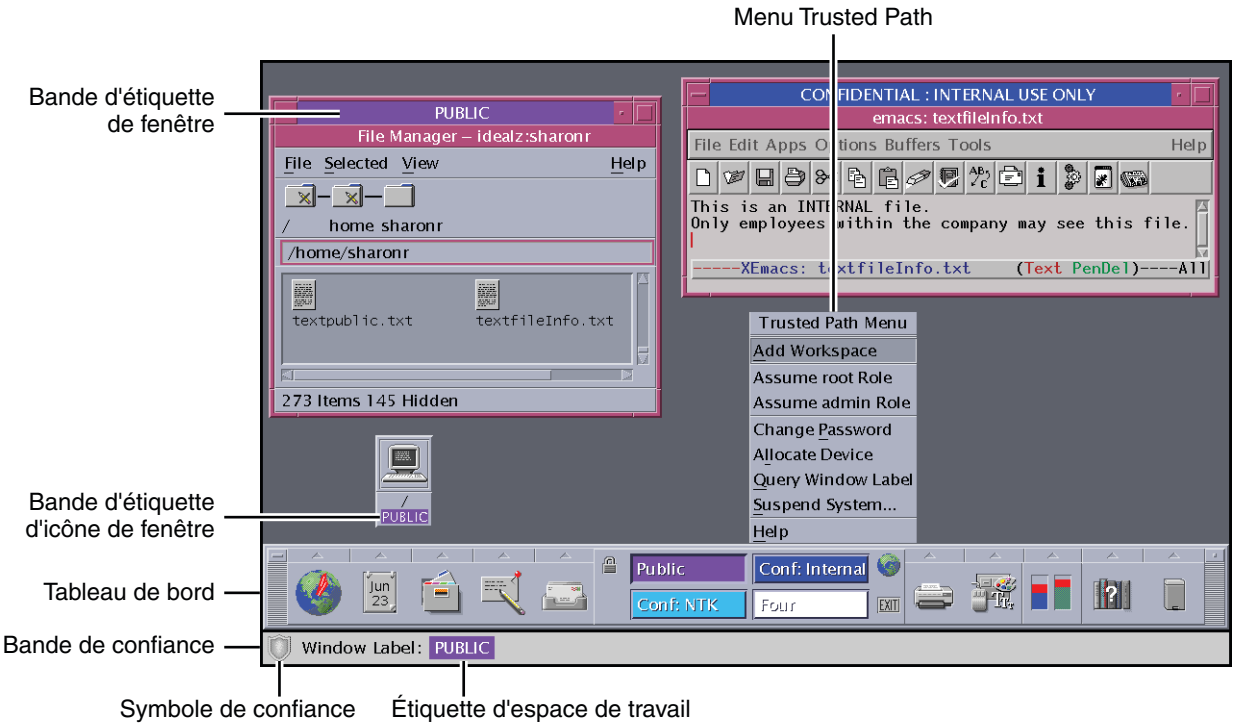
Le logiciel Trusted Extensions ajoute des étiquettes à un système Oracle Solaris. Des bureaux étiquetés et des applications sécurisées comme le générateur d'étiquettes (Label Builder) et le gestionnaire d'allocation de périphériques (Device Allocation Manager) sont également ajoutés. Les concepts présentés dans cette section sont nécessaires pour comprendre Trusted Extensions, aussi bien pour les utilisateurs que pour les administrateurs. Ces concepts sont présentés aux utilisateurs dans la section *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

Protections Trusted Extensions

Le logiciel Trusted Extensions renforce la protection du SE Oracle Solaris. Le SE Oracle Solaris protège l'accès au système à l'aide de comptes utilisateur nécessitant des mots de passe. Vous pouvez exiger que ces mots de passe soient modifiés régulièrement, qu'ils aient une longueur déterminée, etc. Les rôles requièrent des mots de passe supplémentaires pour effectuer des tâches d'administration. Une authentification supplémentaire limite les risques de voir un intrus ayant deviné le mot de passe root causer des dommages, car les rôles ne peuvent pas être utilisés en tant que comptes de connexion. Le logiciel Trusted Extensions va plus loin en restreignant les utilisateurs et les rôles à une plage d'étiquettes approuvée. Cette plage d'étiquettes limite les informations auxquelles les utilisateurs et les rôles peuvent accéder.

Le logiciel Trusted Extensions affiche le symbole Trusted Path (Chemin de confiance), une emblème d'inviolabilité sans équivoque qui s'affiche à gauche de la bande de confiance. Dans Trusted CDE, la bande apparaît en bas de l'écran. DansTrusted JDS, la bande apparaît en haut de l'écran. Le symbole du chemin de confiance indique que des utilisateurs utilisent des zones du système liées à la sécurité. Si ce symbole n'apparaît pas lorsque l'utilisateur exécute une application de confiance, l'authenticité de cette version de l'application doit être immédiatement vérifiée. Si la bande de confiance ne s'affiche pas, le bureau n'est pas digne de confiance. Pour un exemple d'affichage du bureau, reportez-vous à la Figure 1–1.

FIGURE 1–1 Bureau CDE multiniveau Trusted Extensions



Le logiciel au cœur même de la sécurité, la base informatique de confiance (TCB, Trusted Computing Base), s'exécute dans la zone globale. Les utilisateurs standard ne peuvent pas accéder à la zone globale ni consulter ses ressources. Les utilisateurs interagissent avec la TCB, par exemple lorsqu'ils modifient leur mot de passe. Le symbole du chemin de confiance s'affiche chaque fois que l'utilisateur interagit avec la TCB.

Trusted Extensions et contrôle d'accès

Le logiciel Trusted Extensions protège les informations et autres ressources à l'aide du contrôle d'accès discrétionnaire (DAC) et du contrôle d'accès obligatoire (MAC). Le contrôle d'accès discrétionnaire correspond aux listes de contrôle d'accès et aux bits d'autorisation UNIX définis par le propriétaire. Le MAC est un mécanisme appliqué automatiquement par le système. Le MAC contrôle toutes les transactions en vérifiant les étiquettes des processus et les données des transactions.

L'*étiquette* de l'utilisateur indique le niveau de sensibilité auquel l'utilisateur est autorisé à travailler et auquel il choisit de travailler. Les étiquettes `Secret` et `Public` sont des étiquettes usuelles. L'étiquette détermine les informations auxquelles l'utilisateur est autorisé à accéder.

Des autorisations spéciales incluses dans le SE Oracle Solaris permettent de passer outre au MAC et au DAC. Les *privilèges* sont des autorisations spéciales pouvant être accordées aux processus. Les *autorisations* sont des autorisations spéciales pouvant être attribuées par un administrateur à des rôles et des utilisateurs.

En tant qu'administrateur, vous devez former les utilisateurs aux procédures leur permettant de sécuriser leurs fichiers et répertoires, conformément à la stratégie de sécurité de votre site. En outre, vous devez indiquer à tous les utilisateurs autorisés à mettre à niveau ou à rétrograder des étiquettes dans quelles circonstances une telle modification est appropriée.

Rôles et Trusted Extensions

Sur un système exécutant le logiciel Oracle Solaris sans Trusted Extensions, les rôles sont facultatifs. Sur un système configuré avec Trusted Extensions, les rôles sont obligatoires. Le système est administré par le rôle d'administrateur système et le rôle d'administrateur de sécurité. Dans certains cas, le rôle `root` est utilisé.

Comme dans le SE Oracle Solaris, les profils de droits sont à l'origine des capacités d'un rôle. Trusted Extensions fournit deux profils de droits : Information Security (Sécurité des informations) et User Security (Sécurité de l'utilisateur). Ces deux profils définissent le rôle d'administrateur de la sécurité.

Les programmes disponibles pour un rôle dans Trusted Extensions ont une propriété spéciale, l'*attribut chemin de confiance*. Cet attribut indique que le programme fait partie de la TCB. L'attribut chemin de confiance est disponible lorsqu'un programme est lancé depuis la zone globale.

Pour plus d'informations sur les rôles, reportez-vous à la section Partie III, “Roles, Rights Profiles, and Privileges” du *System Administration Guide: Security Services*.

Étiquettes du logiciel Trusted Extensions

Les étiquettes et les autorisations sont au centre du contrôle d'accès obligatoire (MAC) dans Trusted Extensions. Elles permettent de déterminer quels utilisateurs peuvent accéder à quels programmes, fichiers et répertoires. Les étiquettes et les autorisations comprennent un composant de *classification* et aucun, un ou plusieurs composants de *compartiment*. Le composant de classification indique un niveau hiérarchique de sécurité tel que `TOP SECRET` ou `CONFIDENTIAL`. Le composant de compartiment représente un groupe d'utilisateurs pouvant avoir besoin d'accéder à un ensemble commun d'informations. Des exemples de compartiments classiques sont les projets, les services ou les emplacements physiques. Les étiquettes sont lisibles pour les utilisateurs autorisés, mais elles sont manipulées sous forme de nombres en interne. Les nombres et leurs versions lisibles sont définis dans le fichier `label_encodings`.

Trusted Extensions sert d'intermédiaire pour toutes les transactions tentées relevant de la sécurité. Le logiciel compare les étiquettes de l'entité demandant l'accès, généralement un processus, à celles de l'entité à laquelle l'accès est demandé, généralement un objet du système de fichiers. Ensuite, le logiciel autorise ou interdit la transaction en fonction de l'étiquette *dominante* . Les étiquettes sont également utilisées pour déterminer l'accès à d'autres ressources du système, telles que les périphériques, les réseaux, les mémoires graphiques et autres hôtes allouables.

Relations de domination entre les étiquettes

Une étiquette d'entité est dite *dominante* par rapport à une autre lorsque les deux conditions suivantes sont remplies :

- Le composant de classification de l'étiquette de la première entité est supérieur ou égal à la classification de la deuxième entité. L'administrateur de sécurité assigne des numéros aux classifications dans le fichier `label_encodings` . Le logiciel compare ces numéros pour déterminer la domination.
- Le jeu de compartiments de la première entité inclut tous les compartiments de la deuxième entité.

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

Si une étiquette a une classification plus élevée ou si elle a la même classification et que ses compartiments sont un sur-ensemble des compartiments de la deuxième étiquette ou des deux, la première étiquette est dite *strictement dominante* par rapport à la seconde.

Deux étiquettes sont considérées comme *disjointes* ou *non comparables* lorsqu'aucune étiquette ne domine l'autre.

Le tableau suivant présente des exemples de comparaisons d'étiquettes afin de déterminer la domination. Dans l'exemple, `NEED_TO_KNOW` est une classification supérieure à `INTERNAL`. Trois compartiments existent : Eng, Mkt et Fin.

TABLEAU 1–1 Exemples de relations d'étiquettes

Étiquette 1	Relation	Étiquette 2
`NEED_TO_KNOW Eng Mkt`	domine (strictement)	`INTERNAL Eng Mkt`
`NEED_TO_KNOW Eng Mkt`	domine (strictement)	`NEED_TO_KNOW Eng`
`NEED_TO_KNOW Eng Mkt`	domine (strictement)	`INTERNAL Eng`
`NEED_TO_KNOW Eng Mkt`	domine (est égal à)	`NEED_TO_KNOW Eng Mkt`
`NEED_TO_KNOW Eng Mkt`	est disjoint de	`NEED_TO_KNOW Eng Fin`

TABLEAU 1–1 Exemples de relations d'étiquettes *(Suite)*

Étiquette 1	Relation	Étiquette 2
`NEED_TO_KNOW Eng Mkt`	est disjoint de	`NEED_TO_KNOW Fin`
`NEED_TO_KNOW Eng Mkt`	est disjoint de	`INTERNAL Eng Mkt Fin`

Étiquettes d'administration

Trusted Extensions fournit deux étiquettes d'administration spéciales qui sont utilisées en tant qu'étiquettes ou autorisations : `ADMIN_HIGH` et `ADMIN_LOW`. Ces étiquettes sont utilisées pour protéger les ressources système et sont destinées aux administrateurs et non aux utilisateurs standard.

`ADMIN_HIGH` est l'étiquette la plus élevée. `ADMIN_HIGH` domine toutes les autres étiquettes du système et est utilisée pour empêcher que des données système, telles que les bases de données d'administration ou les pistes d'audit, ne soient lues. Pour lire les données associées à l'étiquette `ADMIN_HIGH`, vous devez vous trouver dans la zone globale.

`ADMIN_LOW` est l'étiquette la plus basse. `ADMIN_LOW` est dominée par toutes les autres étiquettes dans un système, notamment par celles des utilisateurs standard. Le contrôle d'accès obligatoire ne permet pas aux utilisateurs d'écrire des données dans des fichiers possédant des étiquettes inférieures à l'étiquette des utilisateurs. Par conséquent, un fichier possédant l'étiquette `ADMIN_LOW` peut être lu par les utilisateurs standard mais ne peut pas être modifié. `ADMIN_LOW` est généralement utilisé pour protéger les exécutables publics qui sont partagés, tels que les fichiers dans `/usr/bin`.

Fichier Label Encodings

Tous les composants de l'étiquette d'un système, c'est-à-dire les classifications, les compartiments et les règles associées sont stockés dans un fichier `ADMIN_HIGH`, le fichier `label_encodings`. Le fichier se trouve dans le répertoire `/etc/security/tsol`. L'administrateur de sécurité définit le fichier `label_encodings` pour le site. Un fichier de codage des étiquettes contient :

- **Définitions du composant** : définitions des classifications, compartiments, étiquettes et autorisations, y compris des règles pour les combinaisons et contraintes requises
- **Définitions des plages d'accréditations** : spécification des autorisations et des étiquettes minimales qui définissent les jeux d'étiquettes disponibles pour l'ensemble du système et les utilisateurs standard
- **Spécifications de l'impression** : informations d'identification et de gestion pour l'impression des pages de garde, des pages de fin, des en-têtes et pieds de page et autres fonctions de sécurité relatives aux sorties d'imprimante
- **Personnalisations** : définitions locales, notamment les codes de couleurs des étiquettes et d'autres paramètres par défaut

Pour plus d'informations, reportez-vous à la page de manuel `label_encodings(4)`. Des informations détaillées sont également disponibles dans les sections *Oracle Solaris Trusted Extensions Label Administration* et *Compartmented Mode Workstation Labeling: Encodings Format* .

Plages d'étiquettes

Une *plage d'étiquettes* représente l'ensemble des étiquettes potentiellement utilisables avec lesquelles les utilisateurs peuvent travailler. Les utilisateurs et les ressources possèdent des plages d'étiquettes. Les ressources pouvant être protégées à l'aide de plages d'étiquettes incluent les périphériques, les réseaux, les interfaces, les mémoires écran, les commandes et les actions attribuables. Une plage d'étiquettes est définie par une autorisation à l'extrémité supérieure de la plage et une étiquette minimale à l'extrémité inférieure.

Une plage n'inclut pas nécessairement toutes les combinaisons d'étiquettes comprises entre une étiquette maximale et une étiquette minimale. Les règles du fichier `label_encodings` peuvent exclure certaines combinaisons. Pour être incluse dans une plage, une étiquette doit être *bien formée*, c'est-à-dire, autorisée par toutes les règles applicables dans le fichier de codage.

Toutefois, une autorisation n'a pas besoin d'être bien formée. Supposons par exemple qu'un fichier `label_encodings` interdit toute combinaison des compartiments `Eng`, `Mkt` et `Fin` dans une étiquette. `INTERNAL Eng Mkt Fin` serait une autorisation valide mais pas une étiquette valide. En tant qu'autorisation, cette combinaison permettrait à l'utilisateur d'accéder à des fichiers incluant l'étiquette `INTERNAL Eng`, `INTERNAL Mkt` et `INTERNAL Fin`.

Plage d'étiquettes de compte

Lorsque vous assignez une autorisation et une étiquette minimale à un utilisateur, vous définissez les limites supérieures et inférieures de la *plage d'étiquettes du compte* dans laquelle cet utilisateur est autorisé à travailler. L'équation suivante décrit la plage d'étiquettes du compte, ≤ signifiant "dominée par ou identique à" :

étiquette minimale ≤ étiquette autorisée ≤ autorisation

Par conséquent, l'utilisateur est autorisé à travailler dans toute étiquette dominée par l'autorisation tant que celle-ci domine l'étiquette minimale. Lorsque l'autorisation ou l'étiquette minimale d'un utilisateur n'est pas expressément définie, les valeurs par défaut définies dans le fichier `label_encodings` s'appliquent.

Les utilisateurs peuvent se voir assigner une étiquette minimale et une autorisation leur permettant de travailler dans une ou plusieurs étiquettes. Lorsque l'autorisation et l'étiquette minimale d'un utilisateur sont égales, l'utilisateur peut travailler dans une étiquette unique.

Plage de session

Une *plage de session* est l'ensemble des étiquettes qui sont mises à la disposition d'un utilisateur au cours d'une session Trusted Extensions. La plage de session doit être comprise dans la plage d'étiquettes du compte de l'utilisateur et dans la plage d'étiquettes définie pour le système. Si l'utilisateur sélectionne le mode de session à étiquette unique au moment de la connexion, la plage de session est limitée à cette étiquette. Si l'utilisateur sélectionne le mode de session multiniveau, l'étiquette que l'utilisateur sélectionne devient l'autorisation de session. L'autorisation de session définit la limite supérieure de la plage de session. L'étiquette minimale de l'utilisateur définit la limite inférieure. L'utilisateur lance la session dans un espace de travail possédant l'étiquette minimale. Au cours de la session, l'utilisateur peut activer un espace de travail possédant n'importe quelle étiquette comprise dans la plage de session.

Où les étiquettes apparaissent-elles et que protègent-elles ?

Les étiquettes s'affichent sur le bureau et sur les sorties effectuées depuis ce bureau, telles que les sorties d'imprimante.

- **Applications** : les applications démarrent les processus. Ces processus sont exécutés sous l'étiquette de l'espace de travail où l'application est démarrée. Comme un fichier, une application se trouvant dans une zone étiquetée possède l'étiquette de la zone.
- **Périphériques** : le transfert des données via des périphériques est contrôlé par l'allocation de périphériques et par les plages d'étiquettes des périphériques. Pour utiliser un périphérique, les utilisateurs doivent être compris dans la plage d'étiquettes du périphérique et être autorisés à allouer le périphérique.
- **Points de montage du système de fichiers** : chaque point de montage possède une étiquette. L'étiquette est consultable à l'aide de la commande `getlabel`.
- **Interfaces réseau** : les adresses IP (hôtes) possèdent des modèles décrivant leur plage d'étiquettes. Les hôtes sans étiquette possèdent également une étiquette par défaut.
- **Imprimantes et impression** : les imprimantes possèdent des plages d'étiquettes. Les étiquettes sont imprimées sur les pages de corps de texte. Les étiquettes, la gestion des informations et d'autres informations de sécurité sont imprimées sur les pages de garde et de fin. Pour configurer l'impression dans Trusted Extensions, reportez-vous aux sections Chapitre 15, “Gestion de l'impression étiquetée (tâches)” et “Labels on Printed Output” du *Oracle Solaris Trusted Extensions Label Administration*.
- **Processus** : les processus sont étiquetés. Les processus s'exécutent sous l'étiquette de l'espace de travail où le processus débute. L'étiquette d'un processus s'affiche à l'aide de la commande `plabel`.
- **Utilisateurs** : les utilisateurs se voient assigner une étiquette par défaut et une plage d'étiquettes. L'étiquette de l'espace de travail d'un utilisateur indique l'étiquette des processus de cet utilisateur.

- **Fenêtres** : les étiquettes s'affichent dans la partie supérieure des fenêtres du bureau. L'étiquette du bureau est également indiquée par une couleur. La couleur s'affiche dans le commutateur du bureau et au-dessus des barres de titre de la fenêtre.

  Lorsqu'une fenêtre est déplacée vers un espace de travail étiqueté différemment, la fenêtre conserve son étiquette d'origine.
- **Zones** : chaque zone possède une étiquette unique. Les fichiers et répertoires possédés par une zone ont l'étiquette de la zone. Pour plus d'informations, reportez-vous à la page de manuel `getzonepath(1)`.

◆ ◆ ◆ CHAPITRE 2

Outils d'administration de Trusted Extensions

Ce chapitre décrit les outils disponibles dans Trusted Extensions, leur emplacement et les bases de données sur lesquelles ils fonctionnent.

Outils d'administration de Trusted Extensions

L'administration d'un système configuré avec Trusted Extensions s'effectue en grande partie avec les mêmes outils que dans le SE Oracle Solaris. Trusted Extensions offre également des outils à la sécurité améliorée. Les outils d'administration sont uniquement accessibles aux rôles dans un espace de travail de rôle.

Dans un espace de travail de rôle, vous pouvez accéder à des commandes, actions, applications et scripts sécurisés. Le tableau ci-dessous contient un récapitulatif de ces outils d'administration.

TABLEAU 2–1 Outils d'administration de Trusted Extensions

Outil	Description	Pour plus d'informations
`/usr/sbin/txzonemgr`	Fournit un assistant basé sur des menus pour la création, l'installation, l'initialisation et le démarrage des zones. Ce script remplace les actions Trusted CDE qui gèrent les zones. Le script fournit également des options de menu donnant accès à des options de réseau, des options de services de noms et pour rendre la zone globale cliente d'un serveur LDAP existant. `txzonemgr` utilise la commande `zenity`.	Reportez-vous à la section "Création de zones étiquetées" du *Guide de configuration d'Oracle Solaris Trusted Extensions* Consultez également la page de manuel `zenity`(1).
Dans Trusted CDE, actions dans le dossier Trusted_Extensions du dossier du gestionnaire d'applications (Application Manager)	Permettent de modifier des fichiers locaux que la Console de gestion Solaris ne gère pas, tels que `/etc/système`. Certaines actions exécutent des scripts, telles que l'action Install zone (Installer une zone).	Reportez-vous aux sections "Actions Trusted CDE" à la page 37 et "Démarrage d'actions d'administration CDE dans Trusted Extensions " à la page 58.
Dans Trusted CDE, gestionnaire d'allocation de périphériques (Device Allocation Manager) Dans Solaris Trusted Extensions (JDS), gestionnaire de périphériques (Device Manager)	Permet d'administrer les plages d'étiquettes des périphériques et d'allouer ou de libérer des périphériques.	Reportez-vous aux sections "Gestionnaire d'allocation de périphériques" à la page 39 et "Manipulation des périphériques dans Trusted Extensions (liste des tâches)" à la page 253.
Console de gestion Solaris	Permet de configurer des utilisateurs, des rôles, des droits, des hôtes, des zones et des réseaux. Cet outil peut mettre à jour les fichiers locaux ou les bases de données LDAP. Cet outil peut également lancer l'application existante `dtappsession`.	Pour connaître ses fonctionnalités de base, reportez-vous au Chapitre 2, "Working With the Solaris Management Console (Tasks)" du *System Administration Guide: Basic Administration*. Pour des informations spécifiques à Trusted Extensions, reportez-vous à la section "Outils de la Console de gestion Solaris" à la page 40.
Commandes de la Console de gestion Solaris, telles que `smuser` et `smtnzonecfg`	Constituent l'interface de ligne de commande de la Console de gestion Solaris.	Pour obtenir une liste, consultez le Tableau 2–4.
Générateur d'étiquettes (Label Builder)	Constitue également un outil utilisateur. Il s'affiche lorsqu'un programme vous demande de choisir une étiquette.	Pour obtenir un exemple, reportez-vous à la section "Procédure de modification de la plage d'étiquettes d'un utilisateur dans la Console de gestion Solaris " à la page 98.

TABLEAU 2–1 Outils d'administration de Trusted Extensions *(Suite)*

Outil	Description	Pour plus d'informations
Commandes de Trusted Extensions	Permettent d'effectuer des tâches qui ne sont pas couvertes par les outils de la Console de gestion Solaris ou des actions CDE.	Pour obtenir la liste des commandes d'administration, reportez-vous au Tableau 2–5.

Script `txzonemgr`

À partir de la version Solaris 10 5/08, le script `txzonemgr` est utilisé pour configurer des zones étiquetées. Ce script `zenity`(1) affiche une boîte de dialogue intitulée Labeled Zone Manager (Gestionnaire de zones étiquetées). Cette interface graphique présente un menu déterminé dynamiquement qui affiche uniquement les choix valides pour le statut de configuration en cours d'une zone étiquetée. Par exemple, si une zone est déjà étiquetée, l'option de menu Label (Étiquette) ne s'affiche pas.

Actions Trusted CDE

Les tableaux ci-dessous répertorient les actions CDE que les rôles de Trusted Extensions peuvent exécuter. Ces actions CDE sécurisées sont disponibles à partir du dossier Trusted_Extensions. Le dossier Trusted_Extensions est disponible à partir du dossier du gestionnaire d'applications (Application Manager) sur le bureau CDE.

TABLEAU 2–2 Actions d'administration dans Trusted CDE : objectifs et profils de droits associés

Nom de l'action	Objectif de l'action	Profil de droits par défaut
`Add Allocatable Device`	Permet de créer des périphériques en ajoutant des entrées à des bases de données de périphériques. Reportez-vous à `add_allocatable`(1M).	Device Security
`Admin Editor`	Permet de modifier le fichier spécifié. Reportez-vous à la section "Modification des fichiers d'administration dans Trusted Extensions" à la page 59.	Object Access Management
`Audit Classes`	Permet de modifier le fichier `audit_class`. Reportez-vous à `audit_class`(4).	Audit Control
`Audit Control`	Permet de modifier le fichier `audit_control`. Reportez-vous à `audit_control`(4).	Audit Control
`Audit Events`	Permet de modifier le fichier `audit_event`. Reportez-vous à `audit_event`(4).	Audit Control
`Audit Startup`	Permet de modifier le script `audit_startup.sh`. Reportez-vous à `audit_startup`(1M).	Audit Control

TABLEAU 2–2 Actions d'administration dans Trusted CDE : objectifs et profils de droits associés *(Suite)*

Nom de l'action	Objectif de l'action	Profil de droits par défaut
`Check Encodings`	Permet d'exécuter la commande `chk_encodings` sur un fichier de codage spécifié. Reportez-vous à `chk_encodings(1M)`.	Object Label Management
`Check TN Files`	Permet d'exécuter la commande `tnchkdb` sur les bases de données `tnrhdb`, `tnrhtp` et `tnzonecfg`. Reportez-vous à `tnchkdb(1M)`.	Network Management
`Configure Selection Confirmation`	Permet de modifier le fichier `/usr/dt/config/sel_config`. Reportez-vous à `sel_config(4)`.	Object Label Management
`Create LDAP Client`	Permet de faire de la zone globale un client LDAP d'un service d'annuaire LDAP.	Information Security
`Edit Encodings`	Permet de modifier le fichier `label_encodings` spécifié et d'exécuter la commande `chk_encodings`. Reportez-vous à `chk_encodings(1M)`.	Object Label Management
`Name Service Switch`	Permet de modifier le fichier `nsswitch.conf`. Reportez-vous à `nsswitch.conf(4)`.	Network Management
`Set DNS Servers`	Permet de modifier le fichier `resolv.conf`. Reportez-vous à `resolv.conf(4)`.	Network Management
`Set Daily Message`	Permet de modifier le fichier `/etc/motd`. Lors de la connexion, le contenu de ce fichier s'affiche dans la boîte de dialogue Last Login (Dernière connexion).	Network Management
`Set Default Routes`	Permet d'indiquer des routes statiques par défaut.	Network Management
`Share Filesystem`	Permet de modifier le fichier `dfstab`. Ne permet pas d'exécuter la commande `share`. Reportez-vous à `dfstab(4)`.	File System Management

Les actions suivantes sont utilisées par l'équipe de la configuration initiale lors de la création de zones. Certaines de ces actions peuvent être utilisées pour la maintenance et le dépannage.

TABLEAU 2–3 Actions d'installation dans Trusted CDE : objectifs et profils de droits associés

Nom de l'action	Objectif de l'action	Profil de droits par défaut
`Clone Zone`	Permet de créer une zone étiquetée à partir d'un instantané ZFS d'une zone existante.	Zone Management
`Copy Zone`	Permet de créer une zone étiquetée à partir d'une zone existante.	Zone Management
`Configure Zone`	Permet d'associer une étiquette à un nom de zone.	Zone Management
`Initialize Zone for LDAP`	Permet d'initialiser la zone pour la démarrer en tant que client LDAP.	Zone Management
`Install Zone`	Permet d'installer les fichiers système requis par une zone.	Zone Management

TABLEAU 2–3 Actions d'installation dans Trusted CDE : objectifs et profils de droits associés *(Suite)*

Nom de l'action	Objectif de l'action	Profil de droits par défaut
`Restart Zone`	Permet de redémarrer une zone qui a déjà été démarrée.	Zone Management
`Share Logical Interface`	Permet de configurer une interface pour la zone globale et une interface distincte destinée à être partagée par les zones étiquetées.	Network Management
`Share Physical Interface`	Permet de configurer une interface partagée par la zone globale et les zones étiquetées.	Network Management
`Shut Down Zone`	Permet d'arrêter une zone installée.	Zone Management
`Start Zone`	Permet de démarrer une zone installée et les services de cette zone.	Zone Management
`Zone Terminal Console`	Permet d'ouvrir une console pour afficher les processus d'une zone installée.	Zone Management

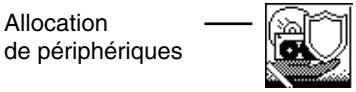
Gestionnaire d'allocation de périphériques

Le terme *périphérique* désigne soit un périphérique physique connecté à un ordinateur, soit un périphérique simulé par un logiciel et appelé *pseudopériphérique*. Pour assurer la protection correcte des données, les périphériques doivent être contrôlés car ils permettent l'importation et l'exportation de données depuis et vers un système. Trusted Extensions a recours à l'allocation de périphériques et aux plages d'étiquettes des périphériques pour contrôler les données transitant via des périphériques.

Disposent par exemple de plages d'étiquettes des périphériques tels que les mémoires graphiques, les lecteurs de bande, les unités de disquette et de CD-ROM, les imprimantes et les périphériques USB.

Les utilisateurs allouent des périphériques via le gestionnaire d'allocation de périphériques (Device Allocation Manager). Le gestionnaire d'allocation de périphériques monte le périphérique, exécute un script de nettoyage pour préparer le périphérique et effectue l'allocation. Lorsqu'il a terminé, l'utilisateur libère le périphérique par le biais du gestionnaire d'allocation de périphériques, lequel exécute un autre script de nettoyage, démonte et libère le périphérique.

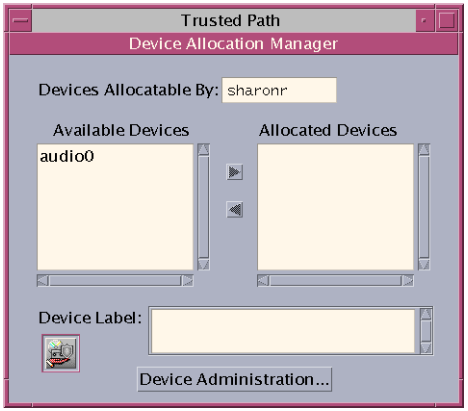
FIGURE 2–1 Icône du gestionnaire d'allocation de périphériques dans Trusted CDE



Vous pouvez gérer les périphériques à l'aide de l'outil Device Administration (Administration des périphériques) à partir du gestionnaire d'allocation de périphériques. Les utilisateurs standard ne peuvent pas accéder à l'outil Device Administration.

Remarque – Dans Solaris Trusted Extensions (JDS), cette interface graphique s'appelle Device Manager (Gestionnaire de périphériques), et le bouton Device Administration s'appelle Administration.

FIGURE 2–2 Interface graphique du gestionnaire d'allocation de périphériques



Pour plus d'informations à propos de la protection des périphériques dans Trusted Extensions, reportez-vous au Chapitre 17, “Gestion des périphériques pour Trusted Extensions (tâches) ”.

Outils de la Console de gestion Solaris

La Console de gestion Solaris donne accès aux boîtes à outils d'outils d'administration basés sur une interface graphique. Ces outils vous permettent de modifier des éléments dans différentes bases de données de configuration. Dans Trusted Extensions, la Console de gestion Solaris est l'interface d'administration pour les utilisateurs, les rôles et les bases de données du réseau de confiance.

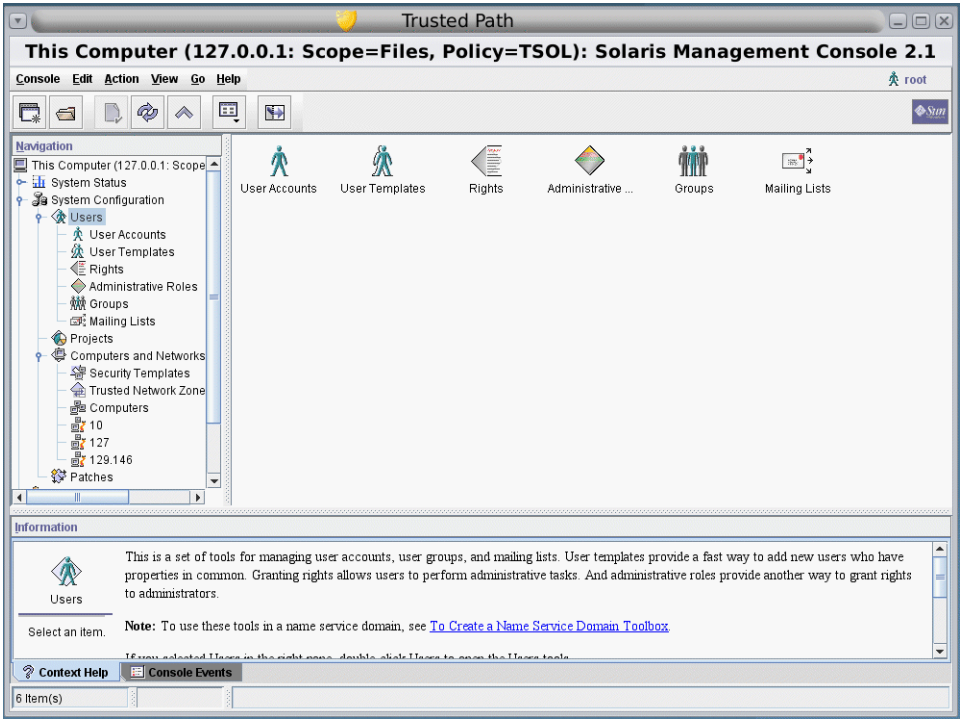
Trusted Extensions étend la Console de gestion Solaris :

- Trusted Extensions modifie l'ensemble d'outils Users (Utilisateurs) de la Console de gestion Solaris. Pour une présentation de cet ensemble d'outils, reportez-vous au Chapitre 2, “Working With the Solaris Management Console (Tasks)” du *System Administration Guide: Basic Administration*.
- Trusted Extensions ajoute l'outil Security Templates (Modèles de sécurité) et l'outil Trusted Network Zones (Zones de réseau de confiance) à l'ensemble d'outils Computers and Networks (Ordinateurs et réseaux).

Les outils de la Console de gestion Solaris sont rassemblés dans des *boîtes à outils* selon l'étendue et la stratégie de sécurité. Pour sa gestion, Trusted Extensions fournit des boîtes à outils dont la stratégie est `Policy=TSOL`. Vous pouvez accéder à des outils en fonction de l'étendue (Scope), c'est-à-dire en fonction du service de nommage. Les étendues disponibles sont l'hôte local et LDAP.

La Console de gestion Solaris est illustrée dans la figure ci-après. Une boîte à outils de Trusted Extensions `Scope=Files` est chargée, et l'ensemble d'outils Users (Utilisateurs) est ouvert.

FIGURE 2–3 Boîte à outils Trusted Extensions typique dans la Console de gestion Solaris



Outils de Trusted Extensions dans la Console de gestion Solaris

Trusted Extensions ajoute des attributs de sécurité configurables à trois outils :

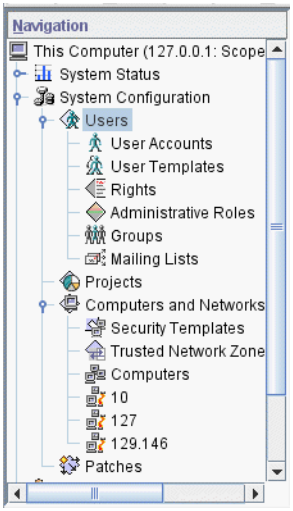
- **Outil User Accounts (Comptes utilisateur) :** interface d'administration permettant de modifier l'étiquette d'un utilisateur, de modifier la visibilité des étiquettes pour un utilisateur et de contrôler l'utilisation des comptes.
- **Outil Administrative Roles (Rôles d'administration) :** interface d'administration permettant de modifier la plage d'étiquettes d'un rôle et le comportement de verrouillage de l'écran en période d'inactivité.
- **Outil Rights (Droits) :** inclut des actions CDE qui peuvent être affectées à des profils de droits. Des attributs de sécurité peuvent être affectés à ces actions.

Trusted Extensions ajoute deux outils à l'ensemble d'outils Computers and Networks (Ordinateurs et réseaux) :

- **Outil Security Templates (Modèles de sécurité) :** interface d'administration permettant de gérer les aspects relatifs aux étiquettes des hôtes et des réseaux. Cet outil modifie les bases de données `tnrhtp` et `tnrhdb`,, applique la précision syntaxique et met à jour le noyau à l'aide des modifications.
- **Outil Trusted Network Zones (Zones de réseau de confiance) :** interface d'administration permettant de gérer les aspects relatifs aux étiquettes des zones. Cet outil modifie la base de données `tnzonecfg`, applique la précision syntaxique et met à jour le noyau avec les modifications.

La Figure 2–4 affiche la boîte à outils Files (Fichiers) avec l'ensemble d'outils Users mis en surbrillance. Les outils de Trusted Extensions s'affichent sous l'ensemble d'outils Computers and Networks.

FIGURE 2–4 Ensemble d'outils Computers and Networks dans la Console de gestion Solaris



Outil Security Templates

Un *modèle de sécurité* décrit un ensemble d'attributs de sécurité qui peuvent être affectés à un groupe d'hôtes. L'outil Security Templates (Modèles de sécurité) vous permet d'affecter facilement une combinaison spécifique d'attributs de sécurité à un groupe d'hôtes. Ces attributs contrôlent la façon dont les données sont regroupées, transmises et interprétées. Les hôtes assignés à un modèle ont les mêmes paramètres de sécurité.

Les hôtes sont définis dans l'outil Computers (Ordinateurs). Les attributs de sécurité des hôtes sont attribués dans l'outil Security Templates. La boîte de dialogue Modify Template (Modifier le modèle) contient deux onglets :

- **Onglet Général :** décrit le modèle. Indique son nom, type d'hôte, étiquette par défaut, domaine d'interprétation (DOI), plage d'accréditations et ensemble d'étiquettes de sensibilité discrètes.
- **Hôtes affectés à l'onglet Template (Modèle) :** répertorie tous les hôtes sur le réseau que vous avez affectés à ce modèle.

Le réseau de confiance et les modèles de sécurité sont décrits de manière plus détaillée au Chapitre 12, “Gestion de réseaux de confiance (présentation)”.

Outil Trusted Network Zones

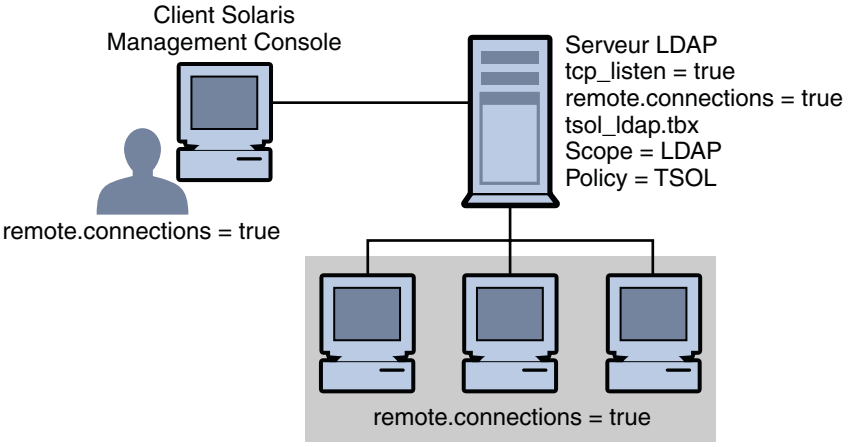
L'outil Trusted Network Zones (Zones de réseau de confiance) identifie les zones de votre système. Au départ, la zone globale est répertoriée. Lorsque vous ajoutez des zones et leurs étiquettes, les noms des zones s'affichent dans le volet. Les zones sont généralement créées lors de la configuration du système. L'assignation de l'étiquette, la configuration du port

multiniveau et la stratégie d'étiquette sont configurées dans cet outil. Pour plus d'informations, reportez-vous au Chapitre 10, “Gestion des zones dans Trusted Extensions (tâches)”.

Communication client-serveur avec la Console de gestion Solaris

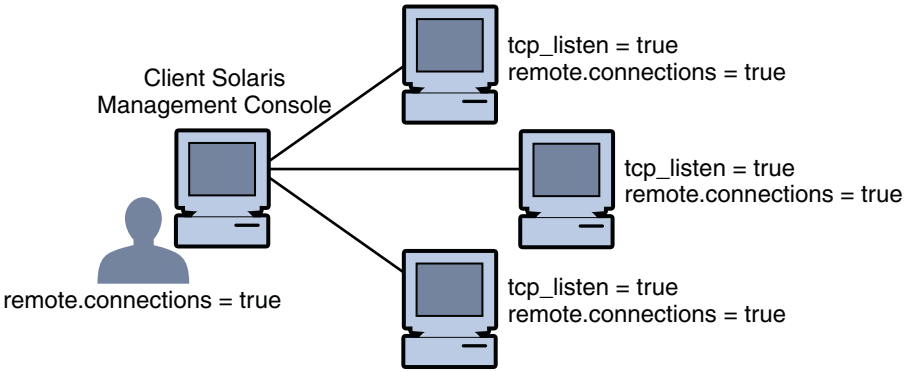
En règle générale, un client de la Console de gestion Solaris administre *à distance* les systèmes. Sur un réseau utilisant le protocole LDAP comme service de nommage, un client de la Console de gestion Solaris se connecte au serveur de la Console de gestion Solaris qui s'exécute sur le serveur LDAP. La figure suivante illustre cette configuration.

FIGURE 2–5 Client de la Console de gestion Solaris utilisant un serveur LDAP pour administrer le réseau



La Figure 2–6 présente un réseau non configuré avec un serveur LDAP. L'administrateur a configuré chaque système distant avec un serveur de la Console de gestion Solaris.

FIGURE 2–6 Client de la Console de gestion Solaris administrant des systèmes distants individuels sur un réseau

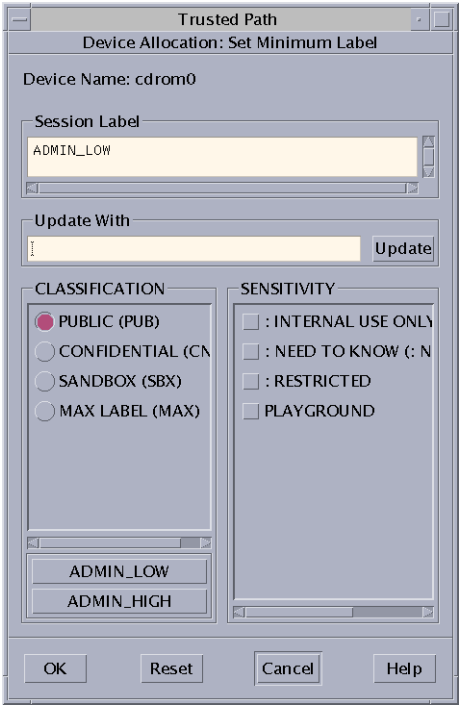


Documentation de la Console de gestion Solaris

La principale source de documentation pour la Console de gestion Solaris est son aide en ligne. Une aide contextuelle est liée à la fonction sélectionnée et s'affiche dans le volet d'informations. Des rubriques d'aide complètes sont disponibles à partir du menu Help (Aide) ou en cliquant sur les liens de l'aide contextuelle. Des informations supplémentaires sont fournies au Chapitre 2, "Working With the Solaris Management Console (Tasks)" du *System Administration Guide: Basic Administration*. Reportez-vous également à la section "Using the Solaris Management Tools With RBAC (Task Map)" du *System Administration Guide: Basic Administration*.

Générateur d'étiquettes dans Trusted Extensions

L'interface graphique du générateur d'étiquettes applique votre choix d'étiquette ou d'autorisation valide lorsqu'un programme vous demande d'affecter une étiquette. Par exemple, un générateur d'étiquettes s'affiche lors de la connexion (reportez-vous au Chapitre 2, "Connexion à Trusted Extensions (tâches)" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*). Le générateur d'étiquettes s'affiche également lorsque vous modifiez l'étiquette d'un espace de travail ou lorsque vous affectez une étiquette à un utilisateur, une zone, ou une interface réseau dans la Console de gestion Solaris. Le générateur d'étiquettes suivant s'affiche lorsque vous affectez une plage d'étiquettes à un nouveau périphérique.



Dans le générateur d'étiquettes, les noms de composant figurant dans la colonne Classification correspondent à la section `CLASSIFICATIONS` du fichier `label_encodings`. Les noms de composant figurant dans la colonne Sensitivity (Sensibilité) correspondent à la section `WORDS` (MOTS) du fichier `label_encodings`.

Outils de ligne de commande dans Trusted Extensions

Les commandes spécifiques à Trusted Extensions sont traitées dans le *manuel de référence de Trusted Extensions*. Les commandes d'Oracle Solaris modifiées par Trusted Extensions sont traitées dans le *manuel de référence d'Oracle Solaris*. La commande `man` permet d'afficher toutes les commandes.

Le tableau suivant répertorie les commandes spécifiques à Trusted Extensions. Elles sont répertoriées au format des pages de manuel.

TABLEAU 2–4 Commandes utilisateur et d'administration de Trusted Extensions

Page de manuel	Modification apportée par Trusted Extensions	Pour plus d'informations
`add_allocatable`(1M)	Permet à un périphérique d'être alloué par ajout du périphérique aux bases de données d'allocation de périphériques. Par défaut, les périphériques amovibles peuvent être alloués.	"Procédure de configuration d'un périphérique dans Trusted Extensions" à la page 255
`atohexlabel`(1M)	Convertit une étiquette au format hexadécimal.	"Obtention de l'équivalent hexadécimal d'une étiquette" à la page 75
`chk_encodings`(1M)	Vérifie l'intégrité du fichier `label_encodings`.	"How to Debug a label_encodings File" du *Oracle Solaris Trusted Extensions Label Administration*
`dtappsession`(1)	Ouvre une session Trusted CDE à distance à l'aide du gestionnaire d'applications (Application Manager).	Chapitre 8, "Administration à distance dans Trusted Extensions (tâches)"
`getlabel`(1)	Affiche l'étiquette des fichiers ou des répertoires sélectionnés.	"Procédure d'affichage des étiquettes de fichiers montés" à la page 137
`getzonepath`(1)	Affiche le chemin d'accès complet d'une zone donnée.	"Acquiring a Sensitivity Label" du *Oracle Solaris Trusted Extensions Developer's Guide*
`hextoalabel`(1M)	Convertit une étiquette hexadécimale en son équivalent lisible.	"Obtention d'une étiquette lisible à partir de sa forme hexadécimale " à la page 77
`plabel`(1)	Affiche l'étiquette du processus actuel.	Reportez-vous à la page de manuel.
`remove_allocatable`(1M)	Empêche l'allocation d'un périphérique en supprimant l'entrée correspondante dans les bases de données d'allocation de périphériques.	"Procédure de configuration d'un périphérique dans Trusted Extensions" à la page 255
`setlabel`(1)	Modifie l'étiquette de l'élément sélectionné. Requiert l'autorisation `solaris.label.file.downgrade` ou `solaris.label.file.upgrade`. Ces autorisations sont incluses dans le profil de droits Object Label Management.	Pour consulter la procédure d'interface graphique équivalente, reportez-vous à la section "Procédure de déplacement de fichiers entre les étiquettes dans Trusted CDE" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.
`smtnrhdb`(1M)	Gère les entrées de la base de données `tnrhdb` de manière locale ou dans une base de données de service de nommage.	Pour consulter des procédures équivalentes utilisant la Console de gestion Solaris, reportez-vous à la section "Configuration des bases de données réseau de confiance (liste des tâches)" à la page 186.
`smtnrhtp`(1M)	Gère les entrées dans la base de données `tnrhtp` de manière locale ou dans une base de données de service de nommage.	Reportez-vous à la page de manuel.

TABLEAU 2–4 Commandes utilisateur et d'administration de Trusted Extensions *(Suite)*

Page de manuel	Modification apportée par Trusted Extensions	Pour plus d'informations
smtnzonecfg(1M)	Gère les entrées de la base de données locale `tnzonecfg`.	Pour consulter une procédure équivalente utilisant la Console de gestion Solaris, reportez-vous à la section "Procédure de création d'un port multiniveau pour une zone" à la page 146.
tnchkdb(1M)	Vérifie l'intégrité des bases de données `tnrhdb` et `tnrhtp`.	"Procédure de vérification de la syntaxe des bases de données d'un réseau de confiance" à la page 202
tnctl(1M)	Met en cache les informations réseau dans le noyau.	"Procédure de synchronisation du cache du noyau avec les bases de données d'un réseau de confiance" à la page 204
tnd(1M)	Exécute le démon du réseau de confiance.	"Procédure de synchronisation du cache du noyau avec les bases de données d'un réseau de confiance" à la page 204
tninfo(1M)	Affiche les informations réseau au niveau du noyau et des statistiques.	"Procédure de comparaison des informations des base de données du réseau de confiance et du cache du noyau" à la page 203.
updatehome(1M)	Met à jour les fichiers `.copy_files` et `.link_files` de l'étiquette actuelle.	"Procédure de configuration des fichiers de démarrage pour les utilisateurs dans Trusted Extensions " à la page 92

Le tableau suivant répertorie les commandes d'Oracle Solaris qui sont modifiées ou étendues par Trusted Extensions. Elles sont répertoriées au format des pages de manuel.

TABLEAU 2–5 Commandes utilisateur et d'administration modifiées par Trusted Extensions

Page de manuel	Modification apportée par Trusted Extensions	Pour plus d'informations
allocate(1)	Ajoute des options pour nettoyer le périphérique alloué et allouer un périphérique à une zone donnée. Dans Trusted Extensions, les utilisateurs standard n'utilisent pas cette commande.	"Procédure d'allocation d'un périphérique dans Trusted Extensions" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*
deallocate(1)	Ajoute des options pour nettoyer le périphérique et libérer un périphérique depuis une zone donnée. Dans Trusted Extensions, les utilisateurs standard n'utilisent pas cette commande.	"Procédure d'allocation d'un périphérique dans Trusted Extensions" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*

TABLEAU 2–5 Commandes utilisateur et d'administration modifiées par Trusted Extensions *(Suite)*

Page de manuel	Modification apportée par Trusted Extensions	Pour plus d'informations
`list_devices(1)`	Ajoute l'option `-a` pour afficher les attributs des périphériques, tels que les autorisations et les étiquettes. Ajoute l'option `-d` pour afficher les attributs par défaut d'un type de périphérique alloué. Ajoute l'option `-z` pour afficher les périphériques disponibles qui peuvent être alloués à une zone étiquetée.	Reportez-vous à la page de manuel.
`tar(1)`	Ajoute l'option `-T` pour archiver et extraire les fichiers et répertoires étiquetés.	"Procédure de sauvegarde de fichiers dans Trusted Extensions" à la page 157 et "Procédure de restauration de fichiers dans Trusted Extensions" à la page 157
`auditconfig(1M)`	Ajoute les options de stratégie d'audit `windata_down` et `windata_up`.	"How to Configure Audit Policy" du *System Administration Guide: Security Services*
`auditreduce(1M)`	Ajoute l'option `-l` pour sélectionner les enregistrements d'audit par étiquette.	"How to Select Audit Events From the Audit Trail" du *System Administration Guide: Security Services*
`automount(1M)`	Modifie le nom et le contenu de cartes `auto_home` pour prendre en compte les noms de zones et la visibilité de zones d'étiquettes supérieures.	"Modifications apportées à l'automonteur dans Trusted Extensions" à la page 154
`ifconfig(1M)`	Ajoute l'option `all-zones` pour mettre une interface à la disposition de chaque zone sur le système.	"Procédure de vérification de l'état d'activité des interfaces d'un hôte" à la page 207
`netstat(1M)`	Ajoute l'option `-R` pour afficher les attributs de sécurité étendus pour les sockets et les entrées de table de routage.	"Débogage du réseau Trusted Extensions" à la page 208
`route(1M)`	Ajoute l'option `-secattr` pour afficher les attributs de sécurité de la route : `cipso`, `doi`, `max_sl` et `min_sl`.	"Procédure de configuration de routes à l'aide d'attributs de sécurité" à la page 201

Administration à distance dans Trusted Extensions

Vous pouvez administrer à distance un système configuré avec Trusted Extensions en utilisant la commande `ssh`, le programme `dtappsession` ou la Console de gestion Solaris. Si la stratégie de sécurité du site le permet, vous pouvez configurer un hôte de Trusted Extensions de manière à ce qu'il active la connexion à partir d'un hôte non-Trusted Extensions, bien que cette configuration soit moins sécurisée. Pour plus d'informations, reportez-vous au Chapitre 8, "Administration à distance dans Trusted Extensions (tâches)".

◆ ◆ ◆ CHAPITRE 3

Mise en route en tant qu'administrateur Trusted Extensions (tâches)

Ce chapitre vous initie à l'administration d'un système configuré avec Trusted Extensions.

Nouveautés de Trusted Extensions

Solaris 10 10/08 : dans cette version, Trusted Extensions fournit les fonctions suivantes :

- La pile IP partagée de Trusted Extensions permet aux routes par défaut d'isoler les zones étiquetées les unes des autres ainsi que de la zone globale.
- L'interface loopback `lo0` est une interface `all-zones`.
- La séparation des tâches peut être appliquée par rôle. Le rôle d'administrateur système crée des utilisateurs, mais ne peut pas affecter de mots de passe, tandis que le rôle d'administrateur de sécurité affecte des mots de passe, mais ne peut pas créer d'utilisateurs. Pour plus d'informations, reportez-vous à la section “Création de profils de droits permettant d’appliquer la séparation des tâches” du *Guide de configuration d’Oracle Solaris Trusted Extensions*.
- L'Annexe B, “Liste des pages de manuel Trusted Extensions” de ce guide contient une liste des pages de manuel de Trusted Extensions.

Solaris 10 5/08 : dans cette version, Trusted Extensions fournit les fonctions suivantes :

- L'utilitaire de gestion des services (SMF) gère Trusted Extensions en tant que service `svc:/system/labeld`. Par défaut, le service `labeld` est désactivé. Lorsque le service est activé, le système doit tout de même être configuré et redémarré pour appliquer les stratégies de sécurité de Trusted Extensions.
- Le numéro du domaine d'interprétation (DOI) CIPSO utilisé par votre système est configurable.

  - Pour plus d'informations sur le DOI, reportez-vous à la section “Attributs de sécurité réseau dans Trusted Extensions” à la page 172.
  - Pour spécifier un DOI différent du DOI par défaut, reportez-vous à la section “Configuration du domaine d’interprétation” du *Guide de configuration d’Oracle Solaris Trusted Extensions*.
- Trusted Extensions reconnaît les étiquettes CIPSO dans les systèmes de fichiers montés de la version 3 de NFS (NFSv3), ainsi que de la version 4 (NFSv4). Par conséquent, vous pouvez monter des systèmes de fichiers NFSv3 sur un système Trusted Extensions en tant que système de fichiers étiqueté. Pour utiliser udp en tant que protocole sous-jacent pour des montages multiniveau dans NFSv3, reportez-vous à la section “Procédure de configuration d'un port multiniveau pour NFSv3 sur udp” à la page 145.
- Le démon de cache de service de noms `nscd` peut être configuré pour s'exécuter dans chaque zone étiquetée sous l'étiquette de la zone.

Exigences de sécurité lors de l'administration de Trusted Extensions

Dans Trusted Extensions, le système est traditionnellement administré par le biais des rôles. En règle générale, le superutilisateur n'est pas utilisé. Les rôles sont créés de la même manière que dans le SE Oracle Solaris et la plupart des tâches sont effectuées par les rôles. Dans Trusted Extensions, l'utilisateur `root` n'est pas utilisé pour effectuer des tâches d'administration.

Les rôles suivants sont typiques d'un site Trusted Extensions :

- **Rôle**`root` : créé par l'équipe de configuration initiale
- **Rôle d'administrateur de sécurité** : créé pendant ou après la configuration initiale par l'équipe de configuration initiale
- **Rôle d'administrateur système** : créé par le rôle d'administrateur de sécurité

Comme dans le SE Oracle Solaris, vous pouvez également créer un rôle d'administrateur principal, un rôle d'opérateur, et ainsi de suite. À l'exception du rôle `root`, les rôles que vous créez peuvent être administrés dans un service de nommage.

Comme dans le SE Oracle Solaris, seuls les utilisateurs auxquels un rôle à été assigné peuvent jouer ce rôle. Dans Solaris Trusted Extensions (CDE), vous pouvez assumer un rôle à partir d'un menu du bureau appelé le menu Trusted Path (Chemin de confiance). Dans Solaris Trusted Extensions (JDS), vous pouvez assumer un rôle lorsque votre nom d'utilisateur s'affiche dans la bande de confiance. Les choix de rôle s'affichent lorsque vous cliquez sur votre nom d'utilisateur.

Création de rôles dans Trusted Extensions

Pour administrer Trusted Extensions, vous créez des rôles qui répartissent les fonctions système et les fonctions de sécurité. L'équipe de configuration initiale a créé le rôle d'administrateur de sécurité lors de la configuration. Pour plus d'informations, reportez-vous à la section "Création du rôle d'administrateur de sécurité dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.

Le processus de création d'un rôle dans Trusted Extensions est le même que dans le SE Oracle Solaris. Comme décrit au Chapitre 2, "Outils d'administration de Trusted Extensions", Console de gestion Solaris est l'interface graphique permettant de gérer les rôles dans Trusted Extensions.

- Pour une présentation de la création de rôles, reportez-vous au Chapitre 10, "Role-Based Access Control (Reference)" du *System Administration Guide: Security Services* et à la section "Using RBAC (Task Map)" du *System Administration Guide: Security Services*.
- Pour créer un rôle puissant équivalent au superutilisateur, reportez-vous à la section "Creating the Primary Administrator Role" du *System Administration Guide: Basic Administration*. Pour les sites qui utilisent Trusted Extensions, le rôle d'administrateur principal peut aller à l'encontre de la stratégie de sécurité. Ces sites doivent transformer `root` en un rôle et créer un rôle d'administrateur de sécurité.
- Pour créer le rôle `root`, reportez-vous à la section "How to Make root User Into a Role" du *System Administration Guide: Security Services*.
- Pour créer des rôles à l'aide de Console de gestion Solaris, reportez-vous à la section "How to Create and Assign a Role by Using the GUI" du *System Administration Guide: Security Services*.

Choix d'un rôle dans Trusted Extensions

À la différence du SE Oracle Solaris, Trusted Extensions fournit une option de menu Assume Role (Assumer le rôle) *nom du rôle* dans le menu Trusted Path. Après avoir confirmé le mot de passe du rôle, le logiciel active un espace de travail du rôle possédant l'attribut chemin de confiance. Les espaces de travail des rôles sont des espaces de travail d'administration. Ces espaces de travail se trouvent dans la zone globale.

Mise en route en tant qu'administrateur Trusted Extensions (liste des tâches)

Familiarisez-vous avec les procédures suivantes avant d'administrer Trusted Extensions.

Tâche	Description	Voir
Ouverture d'une session.	Vous permet de vous connecter en toute sécurité.	"Connexion à Trusted Extensions" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*
Réalisation de tâches utilisateur courantes sur un ordinateur de bureau.	Ces tâches comprennent : ■ la configuration de vos espaces de travail ; ■ l'utilisation d'espaces de travail à différentes étiquettes ; ■ l'accès aux pages de manuel de Trusted Extensions ; ■ l'accès à l'aide en ligne de Trusted Extensions.	"Travail sur un système étiqueté" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*
Réalisation de tâches nécessitant le chemin de confiance (trusted path).	Ces tâches comprennent : ■ l'allocation d'un périphérique ; ■ la modification de votre mot de passe ; ■ la modification de l'étiquette d'un espace de travail.	"Réalisation d'actions sécurisées" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*
Création de rôles utiles.	Crée des rôles d'administration pour votre site. La création de rôles dans LDAP ne doit être effectuée qu'une seule fois. Le rôle d'administrateur de sécurité est un rôle utile.	"Création de rôles dans Trusted Extensions " à la page 53 "Création du rôle d'administrateur de sécurité dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions*
(Facultatif) Création d'un rôle `root`.	Empêche la connexion anonyme par `root`. Cette tâche s'effectue une fois par système.	"How to Make root User Into a Role" du *System Administration Guide: Security Services*
Choix d'un rôle à assumer.	Accède à la zone globale dans un rôle. Toutes les tâches d'administration sont effectuées dans la zone globale.	"Accès à la zone globale dans Trusted Extensions " à la page 55
Sortie d'un espace de travail de rôle et transformation en utilisateur standard.	Quitte la zone globale.	"Sortie de la zone globale dans Trusted Extensions " à la page 56
Administration locale des utilisateurs, rôles, droits, zones et réseaux.	Gère le système distribué à l'aide de Console de gestion Solaris.	"Administration du système local avec Console de gestion Solaris " à la page 57
Administration du système au moyen d'actions Trusted CDE.	Utilise les actions d'administration du dossier Trusted_Extensions.	"Démarrage d'actions d'administration CDE dans Trusted Extensions " à la page 58
Modification d'un fichier d'administration.	Modifie des fichiers dans un éditeur de confiance.	"Modification des fichiers d'administration dans Trusted Extensions" à la page 59

Tâche	Description	Voir
Administration de l'allocation de périphériques.	Utilise le gestionnaire d'allocation de périphériques, l'interface graphique d'administration de périphériques.	"Gestion des périphériques dans Trusted Extensions (liste des tâches)" à la page 254

▼ Accès à la zone globale dans Trusted Extensions

En assumant un rôle, vous accédez à la zone globale dans Trusted Extensions. L'administration de l'intégralité du système n'est possible qu'à partir de la zone globale. Seul le superutilisateur ou un rôle peut accéder à la zone globale.

Une fois un rôle assumé, le rôle peut créer un espace de travail sous une étiquette utilisateur pour modifier des fichiers d'administration dans une zone étiquetée.

À des fins de dépannage, vous pouvez également accéder à la zone globale en démarrant une session de secours. Pour de plus amples d'informations, reportez-vous à la section "Procédure de connexion à une session de secours dans Trusted Extensions " à la page 97.

Avant de commencer Vous avez créé un ou plusieurs rôles, ou vous envisagez d'accéder à la zone globale en tant que superutilisateur. Pour les pointeurs, reportez-vous à la section "Création de rôles dans Trusted Extensions " à la page 53.

1 Utilisez une méthode sécurisée.

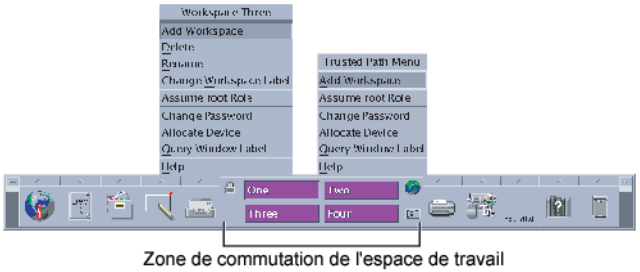
- **Dans Solaris Trusted Extensions (JDS), cliquez sur votre nom d'utilisateur dans la bande de confiance et choisissez un rôle.**

  Si un rôle vous a été affecté, les noms de rôles s'affichent dans une liste.

  Pour l'emplacement et la signification des fonctionnalités du bureau de Trusted Extensions, reportez-vous au Chapitre 4, "Éléments de Trusted Extensions (Référence)" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

- **Dans Solaris Trusted Extensions (CDE), ouvrez le menu Trusted Path (Chemin de confiance).**

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



  b. **Choisissez Assume Role (Assumer le rôle)** *nom du rôle* **à partir du menu Trusted Path.**

2 **À l'invite, saisissez le mot de passe du rôle.**

Dans Trusted CDE, un nouvel espace de travail de rôle est créé, le bouton de commutation de l'espace de travail s'affiche dans la couleur du bureau du rôle et la barre de titre située au-dessus de chaque fenêtre affiche `Trusted Path`. Dans Trusted JDS, l'espace de travail actif et remplacé par l'espace de travail du rôle.

Dans Trusted CDE, vous quittez un espace de travail de rôle en choisissant un espace de travail d'utilisateur standard à l'aide de la souris. Vous pouvez également quitter un rôle en supprimant le dernier espace de travail de rôle. Dans Trusted JDS, cliquez sur le nom du rôle sur la bande de confiance et sélectionnez un rôle ou un utilisateur différent dans le menu. L'espace de travail actif est alors remplacé par le processus du nouveau rôle ou du nouvel utilisateur.

▼ Sortie de la zone globale dans Trusted Extensions

Les menus permettant de quitter un rôle sont situés à des emplacements différents dans Trusted JDS et Trusted CDE.

Avant de commencer Vous vous trouvez dans la zone globale.

- **Sur les deux bureaux, vous pouvez cliquer sur un espace de travail d'utilisateur dans la zone de commutation de l'espace de travail.**

  Vous pouvez également quitter l'espace de travail d'un rôle, et par conséquent la zone globale, en procédant de l'une des manières suivantes :

  - **Dans Trusted JDS, cliquez sur votre nom de rôle dans la bande de confiance.**

    Lorsque vous cliquez sur le nom du rôle, votre nom d'utilisateur et une liste des rôles que vous pouvez assumer s'affichent. Lorsque vous sélectionnez votre nom d'utilisateur, toutes

les fenêtres suivantes que vous créez dans cet espace de travail sont créées par le nom sélectionné. Les fenêtres que vous avez précédemment créées sur le bureau actuel continuent de s'afficher au niveau du nom et de l'étiquette de ce rôle.

Si vous choisissez un autre nom de rôle, vous restez dans la zone globale en assumant un rôle différent.

- **Dans Trusted CDE, supprimez l'espace de travail du rôle.**

  Cliquez avec le bouton 3 de la souris sur le bouton de l'espace de travail et sélectionnez Supprimer. Vous retournez dans le dernier espace de travail que vous avez occupé.

▼ Administration du système local avec Console de gestion Solaris

La première fois que vous lancez Console de gestion Solaris, vous devez patienter un peu pendant l'enregistrement des outils et la création de différents répertoires. Ce délai est normal lors de la configuration du système. Pour de plus amples d'informations sur cette procédure, reportez-vous à la section "Initialisation du serveur Console de gestion Solaris dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.

Pour l'administration d'un système distant, reportez-vous à la section "Administration à distance de Trusted Extensions (liste des tâches)" à la page 112.

Avant de commencer Vous devez avoir assumé un rôle. Pour plus d'informations, reportez-vous à la section "Accès à la zone globale dans Trusted Extensions " à la page 55.

1. **Démarrez Console de gestion Solaris.**

   Dans Solaris Trusted Extensions (JDS), utilisez la ligne de commande.

   ```
   $ /usr/sbin/smc &
   ```

   Dans Trusted CDE, vous avez trois possibilités.

   - **Utilisez la commande `smc` dans une fenêtre de terminal.**
   - **À partir du menu déroulant Tools du tableau de bord, cliquez sur l'icône de Console de gestion Solaris.**
   - **Dans le dossier Trusted_Extensions, cliquez deux fois sur l'icône de Console de gestion Solaris.**

2. **Choisissez Console -> Open Toolbox (Ouvrir une boîte à outils).**

3 **Dans la liste, sélectionnez une boîte à outils Trusted Extensions de l'étendue appropriée.**

Le nom d'une boîte à outils d'Trusted Extensions contient `Policy=TSOL`. L'étendue des fichiers met à jour des fichiers locaux sur le système actuel. L'étendue LDAP met à jour des annuaires LDAP sur l'Oracle Directory Server Enterprise Edition. Les noms des boîtes à outils se présentent de la manière suivante :

```
Cet ordinateur (this-host : Scope=Files, Policy=TSOL)
Cet ordinateur (ldap-server : Scope=LDAP, Policy=TSOL)
```

4 **Accédez à l'outil de Console de gestion Solaris souhaité.**

L'invite de mot de passe s'affiche.

Pour les outils modifiés par Trusted Extensions, cliquez sur Configuration du système.

5 **Tapez le mot de passe**

Reportez-vous à l'aide en ligne pour plus d'informations sur les outils de Console de gestion Solaris. Pour une introduction aux outils modifiés par Trusted Extensions, reportez-vous à la section "Outils de la Console de gestion Solaris" à la page 40.

6 **Pour fermer l'interface graphique, choisissez Exit (Quitter) dans le menu de la console.**

▼ Démarrage d'actions d'administration CDE dans Trusted Extensions

1 **Assumez un rôle.**

Pour plus d'informations, reportez-vous à la section "Accès à la zone globale dans Trusted Extensions " à la page 55.

2 **Dans Trusted CDE, affichez le gestionnaire d'applications (Application Manager).**

a. **Cliquez avec le bouton 3 de la souris sur l'arrière-plan pour faire apparaître le menu de l'espace de travail.**

b. Cliquez sur Applications, puis cliquez sur l'option de menu Application Manager (Gestionnaire d'applications).

Le dossier Trusted_Extensions se trouve dans le gestionnaire d'applications.

3 Ouvrez le dossier Trusted_Extensions.

4 Double-cliquez sur l'icône appropriée.

Pour obtenir une liste des actions d'administration, reportez-vous à la section "Actions Trusted CDE" à la page 37.

▼ Modification des fichiers d'administration dans Trusted Extensions

Les fichiers d'administration sont modifiés à l'aide d'un éditeur de confiance qui procède également à un audit. Cet éditeur empêche également l'utilisateur d'exécuter des commandes shell et d'enregistrer un fichier sous un nom différent de son nom d'origine.

1 Assumez un rôle.

Pour plus d'informations, reportez-vous à la section "Accès à la zone globale dans Trusted Extensions " à la page 55.

2. **Ouvrez un éditeur de confiance.**

   - **Dans Solaris Trusted Extensions (CDE), procédez comme suit :**

     a. **Pour afficher l'éditeur, cliquez avec bouton 3 de la souris sur l'arrière-plan pour faire apparaître le menu de l'espace de travail.**

     b. **Cliquez sur Applications, puis sur l'option de menu Application Manager (Gestionnaire d'applications).**

        Le dossier Trusted_Extensions se trouve dans le gestionnaire d'applications.

     c. **Ouvrez le dossier Trusted_Extensions.**

     d. **Double-cliquez sur l'action Admin Editor.**

        Vous êtes invité à entrer un nom de fichier. Pour le format, reportez-vous à l'Étape 3 et l'Étape 4.

   - **Dans Solaris Trusted Extensions (JDS), procédez comme suit :**

     - **(Facultatif) Pour utiliser `gedit` comme éditeur de confiance, modifiez la variable `EDITOR`.**

       Pour plus d'informations, reportez-vous à la section "Affectation de l'éditeur de votre choix en tant qu'éditeur de confiance" à la page 72.

     - **Utilisez la ligne de commande pour afficher l'éditeur de confiance.**

       ```
       # /usr/dt/bin/trusted_edit filename
       ```

       Vous devez fournir un argument *filename*.

3. **Pour créer un nouveau fichier, saisissez son chemin d'accès complet.**

   Lorsque vous enregistrez le fichier, l'éditeur crée un fichier temporaire.

4. **Pour modifier un fichier existant, saisissez son chemin d'accès complet.**

   Remarque – Si votre éditeur fournit une option Enregistrer sous, ne l'utilisez pas. Utilisez l'option Enregistrer de l'éditeur pour enregistrer le fichier.

5. **Pour enregistrer le fichier dans le chemin d'accès spécifié, fermez l'éditeur.**

◆ ◆ ◆ CHAPITRE 4

Exigences de sécurité sur un système Trusted Extensions (présentation)

Ce chapitre décrit les fonctions de sécurité configurables sur un système configuré avec Trusted Extensions.

Fonctions de sécurité configurables d'Oracle Solaris

Trusted Extensions offre les mêmes fonctions de sécurité que celles fournies par le SE Oracle Solaris, ainsi que quelques fonctions supplémentaires. Par exemple, le SE Oracle Solaris fournit une protection `eeprom`, exige des mots de passe en ayant recours à des algorithmes de mot de passe puissants, assure une protection du système par exclusion d'utilisateur ainsi qu'une protection contre le blocage du clavier.

Toutefois, les procédures permettant de modifier ces paramètres de sécurité par défaut sont différentes dans Trusted Extensions et dans le SE Oracle Solaris. Dans Trusted Extensions, vous administrez généralement des systèmes en assumant un rôle. Les paramètres locaux sont modifiés à l'aide de l'éditeur de confiance. Les modifications qui touchent le réseau d'utilisateurs, les rôles et les hôtes sont apportées dans Console de gestion Solaris.

Interfaces de Trusted Extensions pour la configuration des fonctions de sécurité

Ce manuel décrit les procédures de modification des paramètres de sécurité requérant une interface particulière dans Trusted Extensions, lorsque l'interface concernée est facultative dans le SE Oracle Solaris. Ne figurent pas dans ce manuel les procédures pour lesquelles Trusted Extensions nécessite l'éditeur de confiance afin de modifier des fichiers locaux. Par exemple, la

procédure "Procédure de désactivation du verrouillage du compte pour certains utilisateurs " à la page 103 décrit la mise à jour du compte d'un utilisateur à l'aide de Console de gestion Solaris pour empêcher le verrouillage du compte. En revanche, la procédure de définition d'une stratégie de verrouillage de mot de passe à l'échelle du système n'est pas fournie dans ce manuel. Vous devez suivre les instructions d'Oracle Solaris, à la différence près que dans Trusted Extensions, vous utilisez l'éditeur de confiance pour modifier le fichier système.

Extension des mécanismes de sécurité d'Oracle Solaris par Trusted Extensions

Les mécanismes de sécurité d'Oracle Solaris suivants sont extensibles dans Trusted Extensions ainsi que dans le SE Oracle Solaris :

- **Événements et classes d'audit :** l'ajout d'événements et de classes d'audit est décrit au Chapitre 30, "Managing Oracle Solaris Auditing (Tasks)" du *System Administration Guide: Security Services*.
- **Profils de droits :** l'ajout de profils de droits est décrit dans la Partie III, "Roles, Rights Profiles, and Privileges" du *System Administration Guide: Security Services*.
- **Rôles :** l'ajout de rôles est décrit dans la Partie III, "Roles, Rights Profiles, and Privileges" du *System Administration Guide: Security Services*.
- **Autorisations :** pour un exemple d'ajout d'une nouvelle autorisation, reportez-vous à la section "Personnalisation des autorisations de périphériques dans Trusted Extensions (liste des tâches)" à la page 264.

Comme dans le SE Oracle Solaris, les privilèges ne peuvent pas être étendus.

Fonctions de sécurité de Trusted Extensions

Trusted Extensions fournit les fonctions de sécurité uniques suivantes :

- **Étiquettes :** les sujets et les objets sont étiquetés. Les processus sont étiquetés. Les zones et le réseau sont étiquetés.
- **Gestionnaire d'allocation de périphériques :** par défaut, les périphériques sont protégés par des conditions d'allocation. L'interface graphique du Gestionnaire d'allocation de périphériques est l'interface destinée aux administrateurs et aux utilisateurs standard.
- **Option de menu Change Password (Modifier le mot de passe) :** le menu Trusted Path vous permet de modifier votre mot de passe utilisateur et le mot de passe du rôle que vous avez assumé.

Application des exigences de sécurité

Pour s'assurer que la sécurité du système n'est pas compromise, les administrateurs doivent protéger les mots de passe, les fichiers et les données d'audit. Les utilisateurs doivent être formés pour effectuer les tâches qui leur incombent. Pour respecter les exigences d'une configuration évaluée, suivez les instructions fournies dans cette section.

Exigences de sécurité et utilisateurs

Chaque administrateur de sécurité de site s'assure que les utilisateurs sont formés aux procédures de sécurité. L'administrateur de sécurité doit communiquer les règles ci-après aux nouveaux employés et faire des rappels réguliers pour les employés existants :

- Ne divulguez pas votre mot de passe.

  Toute personne qui connaît votre mot de passe peut accéder aux mêmes informations que vous sans être identifiée et donc sans être responsable.
- Ne notez pas votre mot de passe et ne l'incluez pas dans un e-mail.
- Choisissez des mots de passe difficiles à deviner.
- N'envoyez à personne votre mot de passe par e-mail.
- Ne laissez pas votre ordinateur sans surveillance sans verrouiller l'écran ou vous déconnecter.
- N'oubliez pas que les administrateurs ne recourent pas à des e-mails pour envoyer des instructions aux utilisateurs. Ne suivez jamais des instructions envoyées par e-mail par un administrateur sans lui demander confirmation au préalable.

  Sachez que les informations concernant l'expéditeur d'un e-mail peuvent être falsifiées.
- Vous êtes responsable des autorisations d'accès aux fichiers et aux répertoires que vous créez, c'est pourquoi vous devez vous assurer qu'elles sont correctement définies. Ne permettez pas à des utilisateurs non autorisés de lire ou de modifier un fichier, de lister le contenu d'un répertoire ou d'y ajouter des éléments.

Votre site peut souhaiter fournir des suggestions supplémentaires.

Utilisation d'e-mails

Utiliser des e-mails pour communiquer des instructions aux utilisateurs est une pratique dangereuse.

Indiquez aux utilisateurs qu'il ne faut pas faire confiance aux e-mails contenant des instructions prétendument envoyés par un administrateur. Vous évitez ainsi le risque que de faux e-mails les invitant à changer leur mot de passe en une valeur imposée ou à communiquer leur mot de passe ne soient envoyés aux utilisateurs, ces informations pouvant ensuite être utilisées pour ouvrir une session et compromettre le système.

Application d'un mot de passe

L'administrateur système doit spécifier un nom et un ID d'utilisateur uniques lors de la création d'un nouveau compte. Lors du choix du nom et de l'ID d'un nouveau compte, l'administrateur doit s'assurer que ce nom et l'ID associé ne sont dupliqués nulle part sur le réseau et n'ont pas été précédemment utilisés.

L'administrateur de sécurité est chargé d'indiquer le mot de passe d'origine de chaque compte et de communiquer les mots de passe aux utilisateurs de nouveaux comptes. Vous devez prendre en compte les informations suivantes lorsque vous administrez les mots de passe :

- Assurez-vous que les comptes des utilisateurs qui ont la possibilité d'assumer le rôle d'administrateur de sécurité sont configurés de manière à ne pas pouvoir être verrouillés. Ceci vous permet de garantir qu'il existe toujours au moins un compte capable de se connecter et d'assumer le rôle d'administrateur de sécurité afin de rouvrir les autres comptes, dans l'hypothèse où tous les autres comptes seraient verrouillés.
- Communiquez le mot de passe à l'utilisateur d'un nouveau compte de telle façon que le mot de passe ne puisse pas être récupéré par une autre personne.
- Modifiez un mot de passe de compte si vous suspectez qu'il a été découvert par quelqu'un qui ne doit pas le connaître.
- Ne réutilisez jamais les noms ou les ID d'utilisateur pendant la durée de vie d'un système.

  En vous assurant que les noms et les ID d'utilisateur ne sont pas réutilisés, vous évitez toute confusion en ce qui concerne :

  - l'identité des utilisateurs ayant réalisé les actions (lors de l'analyse d'enregistrements d'audit) ;
  - l'identité du propriétaire des fichiers lorsque des fichiers archivés sont restaurés

Protection de l'information

En tant qu'administrateur, vous êtes responsable de la configuration et de la mise à jour correctes de la protection DAC (Discretionary Access Control, contrôle d'accès discrétionnaire) et de la protection MAC (Mandatory Access Control) pour les fichiers critiques. Sont notamment critiques les fichiers suivants :

- **Fichier** `shadow` : contient des mots de passe chiffrés. Reportez-vous à `shadow(4)`.
- **Base de données** `prof_attr` : contient les définitions des profils de droits. Reportez-vous à `prof_attr(4)`.
- **Base de données** `exec_attr` : contient des commandes et des actions qui font partie des profils de droits. Reportez-vous à `exec_attr(4)`.
- **Fichier** `user_attr` : contient les profils de droits, les privilèges et les autorisations affectés aux utilisateurs locaux. Reportez-vous à `user_attr(4)`.

- **Analyse rétrospective** : contient les enregistrements d'audit collectés par le service d'audit. Reportez-vous à `audit.log(4)`

Attention – Les entrées LDAP par défaut ne doivent pas être étendues et leurs règles d'accès ne doivent pas être modifiées car les mécanismes de protection des entrées LDAP ne sont pas soumises à la stratégie de contrôle d'accès appliquée par Trusted Extensions.

Protection par mot de passe

Dans les fichiers locaux, les mots de passe sont protégés de l'affichage par DAC et des modifications apportées par DAC et MAC. Les mots de passe pour les comptes locaux sont conservés dans le fichier `/etc/shadow`, qui est uniquement lisible par le superutilisateur. Pour de plus amples d'informations, reportez-vous à la page de manuel `shadow(4)`.

Administration de groupes

L'administrateur système doit vérifier sur le système local et sur le réseau que tous les groupes possèdent un ID de groupe (GID) unique.

Lorsqu'un groupe local est supprimé du système, l'administrateur système doit s'assurer de ce qui suit :

- Tous les objets possédant le GID du groupe supprimé doivent être supprimés ou affectés à un autre groupe.
- Tous les utilisateurs ayant pour groupe principal le groupe supprimé doivent être réaffectés à un autre groupe principal.

Pratiques de suppression d'un utilisateur

Lorsqu'un compte est supprimé du système, l'administrateur système et l'administrateur de sécurité doivent prendre les mesures suivantes :

- Supprimer les répertoires personnels du compte dans chaque zone.
- Supprimer tout processus ou travail détenu par le compte supprimé :
  - supprimer tous les objets qui sont détenus par le compte ou affecter la propriété à un autre utilisateur ;
  - supprimer tout travail `et` ou `batch` programmé pour le compte de l'utilisateur. Pour plus d'informations, reportez-vous aux pages de manuel `at(1)` et `crontab(1)`.
- Ne jamais réutiliser le nom (compte) d'utilisateur ou l'ID d'utilisateur.

Règles lors de la modification du niveau de sécurité des données

Par défaut, les utilisateurs standard peuvent effectuer des opérations de couper-coller, copier-coller, et glisser-déposer sur les fichiers et les sélections. La source et la cible doivent être à la même étiquette.

La modification d'étiquettes de fichiers ou d'informations dans les fichiers nécessite une autorisation. Lorsque les utilisateurs sont autorisés à modifier le niveau de sécurité de données, l'application gestionnaire de sélection sert d'intermédiaire pour le transfert. Dans Trusted CDE, le fichier `/usr/dt/config/sel_config` contrôle les actions de modification de l'étiquette de fichiers et les opérations de couper-copier d'informations vers une autre étiquette. Dans Trusted JDS, le fichier `/usr/share/gnome/sel_config` contrôle ces transferts. Dans Trusted CDE, l'application `/usr/dt/bin/sel_mgr` contrôle les opérations de glisser-déposer entre les fenêtres. Comme les tableaux suivants l'illustrent, la modification de l'étiquette d'une sélection est plus restrictive que celle d'un fichier.

Le tableau suivant récapitule les règles régissant la modification de l'étiquette de fichiers. Les règles s'appliquent aux opérations de couper-coller, copier-coller et glisser-déposer.

TABLEAU 4–1 Conditions pour le nouvel étiquetage de fichiers

Description de l'opération	Relation étiquette	Relation propriétaire	Autorisation requise
Opérations de copier-coller, couper-coller ou glisser-déposer de fichiers entre gestionnaires de fichiers	Même étiquette	ID utilisateur identique	Aucune
	Rétrogradation	ID utilisateur identique	`solaris.label.file.downgrade`
	Mise à niveau	ID utilisateur identique	`solaris.label.file.upgrade`
	Rétrogradation	ID utilisateur différents	`solaris.label.file.downgrade`
	Mise à niveau	ID utilisateur différents	`solaris.label.file.upgrade`

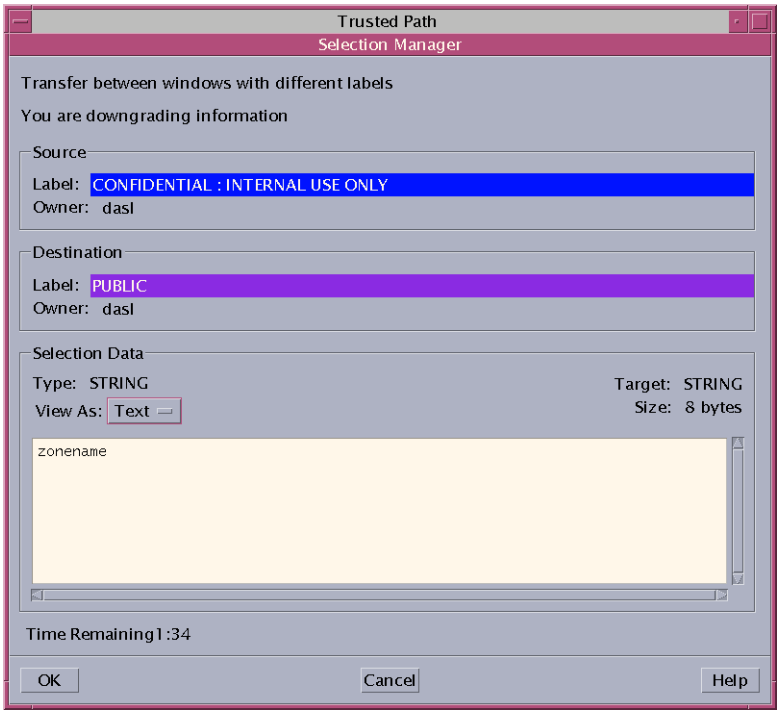
Des règles différentes s'appliquent aux sélections dans une fenêtre ou un fichier. L'opération de glisser-déposer de *sélections* nécessite toujours des étiquettes et des propriétaires identiques. L'opération de glisser-déposer entre les fenêtres est effectuée par le biais de l'application gestionnaire de sélection, et non pas par le fichier `sel_config`.

Les règles applicables à la modification de l'étiquette de sélections sont résumées dans le tableau ci-dessous.

TABLEAU 4–2 Conditions pour le nouvel étiquetage de sélections

Description de l'opération	Relation étiquette	Relation propriétaire	Autorisation requise
Opérations de copier-coller ou couper-coller de sélections entre fenêtres	Même étiquette	ID utilisateur identique	Aucune
	Rétrogradation	ID utilisateur identique	`solaris.label.win.downgrade`
	Mise à niveau	ID utilisateur identique	`solaris.label.win.upgrade`
	Rétrogradation	ID utilisateur différents	`solaris.label.win.downgrade`
	Mise à niveau	ID utilisateur différents	`solaris.label.win.upgrade`
Opérations de glisser-déposer de sélections entre fenêtres	Même étiquette	ID utilisateur identique	Aucune autorisation applicable

Trusted Extensions prévoit une confirmation de la sélection pour les modifications d'étiquette. Cette fenêtre s'affiche lorsqu'un utilisateur autorisé tente de modifier l'étiquette d'un fichier ou d'une sélection. L'utilisateur dispose de 120 secondes pour confirmer l'opération. La modification du niveau de sécurité des données sans cette fenêtre nécessite l'autorisation `solaris.label.win.noview`, en plus des autorisations de modification de l'étiquette. L'illustration suivante montre une sélection, `zonename`, dans la fenêtre.



Par défaut, le fenêtre de confirmation de sélection s'affiche lorsque les données sont transférées vers une autre étiquette. Si une sélection nécessite plusieurs décisions de transfert, le mécanisme de réponse automatique permet de répondre une seule fois pour plusieurs transferts. Pour plus d'informations, reportez-vous à la page de manuel `sel_config(4)` et à la section suivante.

Fichier `sel_config`

Le fichier `sel_config` est vérifié pour déterminer le comportement de la fenêtre de confirmation de sélection d'une opération de mise à niveau ou de rétrogradation d'une étiquette.

Le fichier `sel_config` définit :

- les types de sélections auxquelles une réponse automatique est donnée ;
- si certains types d'opérations peuvent être automatiquement confirmés ;
- si la boîte de dialogue de confirmation de sélection s'affiche.

Dans Trusted CDE, l'administrateur de sécurité peut modifier les valeurs par défaut à l'aide de l'action Configure Section Confirmation (Configurer la confirmation de sélection) dans le dossier Trusted_Extensions. Les nouveaux paramètres prennent effet lors de l'ouverture de

session suivante. Dans Solaris Trusted Extensions (JDS), l'action CDE n'est pas disponible. Pour modifier les valeurs par défaut, modifiez le fichier `/usr/share/gnome/sel_config` dans un éditeur de texte.

Personnalisation de Solaris Trusted Extensions (CDE)

Dans Solaris Trusted Extensions (CDE), les utilisateurs peuvent ajouter des actions au tableau de bord et personnaliser le menu de l'espace de travail. Trusted Extensions limite la capacité des utilisateurs à ajouter des programmes et des commandes à CDE.

Personnalisation du tableau de bord

N'importe quel utilisateur peut glisser-déposer une action préexistante du gestionnaire d'applications sur le tableau de bord, tant que le compte qui effectue la modification dispose de l'action dans son profil. Les actions du répertoire `/usr/dt/` ou `/etc/dt/` peuvent être ajoutées au tableau de bord, mais les applications du répertoire `$HOME/.dt/appconfig` répertoire ne le peuvent pas. Les utilisateurs peuvent utiliser l'action Create Action (Créer l'action), mais ils ne peuvent écrire dans aucun des répertoires dans lesquels les actions à l'échelle du système sont stockées. Par conséquent, les utilisateurs standard ne peuvent pas créer d'actions utilisables.

Dans Trusted Extensions, le chemin de recherche des actions a été modifié. Les actions placées dans le répertoire personnel d'un utilisateur sont traitées en dernier au lieu de l'être en premier. Par conséquent, personne ne peut personnaliser les actions existantes.

L'action Admin Editor est assignée au rôle d'administrateur de sécurité et ce dernier peut donc apporter toutes les modifications nécessaires au fichier `/usr/dt/appconfig/types/C/dtwm.fp` et aux autres fichiers de configuration des panneaux secondaires du tableau de bord.

Personnalisation du menu de l'espace de travail

Le menu de l'espace de travail est le menu qui s'affiche lorsque vous cliquez avec le bouton 3 de la souris sur l'arrière-plan de l'espace de travail. Les utilisateurs standard peuvent personnaliser le menu et y ajouter des options.

Les conditions suivantes s'appliquent lorsqu'un utilisateur est autorisé à travailler sous plusieurs étiquettes :

- L'utilisateur doit disposer d'un répertoire personnel dans la zone globale.

  Pour enregistrer les personnalisations, les processus de la zone globale doivent être en mesure d'écrire dans le répertoire personnel de l'utilisateur sous l'étiquette appropriée. Le chemin d'accès à la zone du répertoire personnel d'un l'utilisateur qui est accessible en écriture par les processus de la zone globale est de la forme :

`/zone/`*zone-name*`/home/`*username*

- L'utilisateur doit utiliser les options Customize Menu (Personnaliser le menu) et Add Item (Ajouter l'élément) au menu dans un espace de travail d'utilisateur standard. L'utilisateur peut créer une personnalisation différente pour chaque étiquette.
- Lorsque l'utilisateur assume un rôle, les modifications apportées au menu de l'espace de travail subsistent.
- Les modifications apportées au menu de l'espace de travail sont stockées dans le répertoire personnel de l'utilisateur sous l'étiquette en cours. Le fichier du menu personnalisé est `.dt/wsmenu`.
- Le profil des droits de l'utilisateur doit permettre à ce dernier d'exécuter l'action souhaitée.

  Toute action ajoutée au menu de l'espace de travail doit être traitée par l'un des profils de droits de l'utilisateur. Dans le cas contraire, l'action échoue lorsqu'elle est appelée et un message d'erreur s'affiche.

  Par exemple, toute personne à laquelle l'action Run (Exécuter) a été assignée peut double-cliquer sur l'icône de tout fichier exécutable et l'exécuter, même si l'action ou une commande que l'action appelle n'est pas inclus dans l'un des profils de droits du compte. Par défaut, l'action Run n'est pas affectée aux rôles. Par conséquent, toute option de menu qui requiert l'action Run échoue lorsqu'elle est exécutée par un rôle.

◆ ◆ ◆ CHAPITRE 5

Administration des exigences de sécurité dans Trusted Extensions (tâches)

Ce chapitre décrit des tâches fréquemment effectuées sur un système configuré avec Trusted Extensions.

Tâches courantes dans Trusted Extensions (liste des tâches)

La liste des tâches ci-dessous décrit des procédures permettant de configurer un environnement de travail pour les administrateurs de Trusted Extensions.

Tâche	Description	Voir
Modification du programme utilisé comme éditeur de confiance.	Spécifiez l'éditeur utilisé pour les fichiers d'administration.	"Affectation de l'éditeur de votre choix en tant qu'éditeur de confiance" à la page 72
Modification du mot de passe de root.	Spécifiez un nouveau mot de passe pour l'utilisateur `root` ou pour le rôle `root`.	"Modification du mot de passe de `root`" à la page 73
Modification du mot de passe d'un rôle.	Spécifiez un nouveau mot de passe pour votre rôle actuel.	Exemple 5–2
Utilisation de la combinaison de touches de sécurité (Secure Attention).	Permet d'obtenir le contrôle de la souris ou du clavier. Permet par ailleurs de vérifier si la souris ou le clavier est de confiance.	"Reprise du contrôle du focus actuel du bureau" à la page 74
Détermination du nombre hexadécimal d'une étiquette.	Permet d'afficher la représentation interne d'une étiquette textuelle.	"Obtention de l'équivalent hexadécimal d'une étiquette" à la page 75
Détermination de la représentation textuelle d'une étiquette.	Permet d'afficher la représentation textuelle d'une étiquette hexadécimale.	"Obtention d'une étiquette lisible à partir de sa forme hexadécimale " à la page 77

Tâche	Description	Voir
Modification des fichiers système.	Permet de modifier en toute sécurité des fichiers système d'Oracle Solaris ou de Trusted Extensions.	"Procédure de modification des paramètres de sécurité par défaut dans des fichiers système" à la page 77
Allocation d'un périphérique.	Permet d'utiliser un périphérique pour ajouter ou supprimer des informations du système.	"Procédure d'allocation d'un périphérique dans Trusted Extensions" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*
Administration d'un hôte à distance.	Permet d'administrer des hôtes d'Oracle Solaris ou de Trusted Extensions à partir d'un hôte distant.	Chapitre 8, "Administration à distance dans Trusted Extensions (tâches)"

▼ Affectation de l'éditeur de votre choix en tant qu'éditeur de confiance

L'éditeur de confiance utilise comme éditeur la valeur de la variable d'environnement `$EDITOR`.

Avant de commencer Vous devez être dans un rôle dans la zone globale.

1 Déterminez la valeur de la variable `$EDITOR`.

```
# echo $EDITOR
```

Les valeurs suivantes constituent des possibilités. La variable `$EDITOR` peut également ne pas être définie.

- `/usr/dt/bin/dtpad` : correspond à l'éditeur fourni par CDE.
- `/usr/bin/gedit` : correspond à l'éditeur fourni par Java Desktop System, version *number*. Solaris Trusted Extensions (JDS) est la version de confiance de ce bureau.
- `/usr/bin/vi` : correspond à l'éditeur visuel.

2 Définissez la valeur de la variable `$EDITOR`.

- **Pour définir la valeur définitivement, modifiez la valeur dans le fichier d'initialisation du shell du rôle.**

  Par exemple, dans le répertoire personnel du rôle, modifiez le fichier `.kshrc` pour un shell Korn et le fichier `.cshrc` pour un shell C.

- **Pour définir la valeur du shell actuel, définissez la valeur dans la fenêtre de terminal.**

  Par exemple, dans un shell Korn, utilisez les commandes suivantes :

  ```
  # setenv EDITOR=pathname-of-editor
  # export $EDITOR
  ```

Dans un shell C, utilisez la commande suivante :

```
# setenv EDITOR=pathname-of-editor
```

Dans un shell Bourne, utilisez les commandes suivantes :

```
# EDITOR=pathname-of-editor
# export EDITOR
```

Exemple 5–1 Spécification de l'éditeur pour l'éditeur de confiance

Le rôle d'administrateur de sécurité veut utiliser `vi` lors de la modification de fichiers système. Un utilisateur qui a assumé ce rôle modifie le fichier d'initialisation `.kshrc` dans le répertoire personnel du rôle.

```
$ cd /home/secadmin
$ vi .kshrc

## Interactive shell
set -o vi
...
export EDITOR=vi
```

La prochaine fois qu'un utilisateur assumera le rôle d'administrateur de la sécurité, `vi` sera l'éditeur de confiance.

▼ Modification du mot de passe de `root`

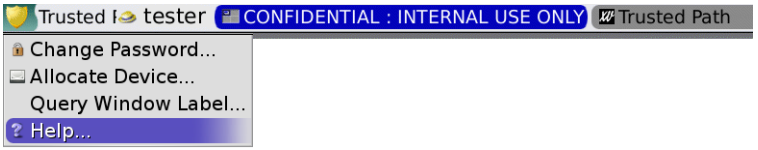
Le rôle d'administrateur de sécurité est habilité à modifier le mot de passe de n'importe quel compte à tout moment à l'aide de la Console de gestion Solaris. Cependant, la Console de gestion Solaris n'est pas en mesure de modifier le mot de passe d'un compte système. Un *compte système* est un compte dont l'UID est inférieur à 100. `root` est un compte système car son UID est 0.

1 Prenez le rôle de superutilisateur.

Si votre site a fait du superutilisateur le rôle `root`, assumez le rôle `root`.

2 **Choisissez l'option Change Password (Modifier le mot de passe) dans le menu Trusted Path (Chemin de confiance).**

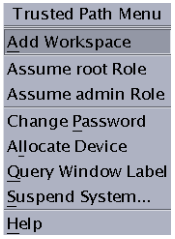
- **Dans Trusted JDS, cliquez sur le symbole de confiance dans la bande de confiance.**
  Dans le menu Trusted Path, sélectionnez Change Password.



- **Dans Solaris Trusted Extensions (CDE), ouvrez le menu Trusted Path.**

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

  b. **Choisissez l'option Change Password dans le menu Trusted Path.**



3 **Modifiez le mot de passe et confirmez la modification.**

Exemple 5–2 Modification du mot de passe d'un rôle

Tout utilisateur qui peut assumer un rôle défini dans le protocole LDAP peut modifier le mot de passe du rôle par le biais du menu Trusted Path. Le mot de passe est ensuite modifié dans le protocole LDAP pour tous les utilisateurs qui tentent d'assumer le rôle.

Comme dans le SE Oracle Solaris, le rôle d'administrateur principal peut modifier le mot de passe d'un rôle à l'aide de la Console de gestion Solaris. Dans Trusted Extensions, le rôle d'administrateur de sécurité peut modifier le mot de passe d'un autre rôle en utilisant la Console de gestion Solaris.

▼ Reprise du contrôle du focus actuel du bureau

La combinaison de touches de sécurité "Secure Attention" permet d'annuler la préhension d'un pointeur ou d'un clavier par une application non sécurisée. Elle permet également de vérifier si

un pointeur ou un clavier a été capté par une application de confiance. Sur un système multiécran victime d'une usurpation et affichant plusieurs bandes de confiance, cette combinaison de touches aligne le pointeur sur la bande de confiance autorisée.

1 **Pour reprendre le contrôle d'un clavier Sun, utilisez la combinaison de touches suivante.**

Appuyez sur les touches simultanément pour reprendre le contrôle du focus du bureau actuel. Sur le clavier Sun, la touche Meta est le losange.

```
<Meta> <Stop>
```

Si la préhension, un pointeur par exemple, n'est pas de confiance, le pointeur se déplace vers la bande. Un pointeur de confiance ne se déplace pas vers la bande de confiance.

2 **Si vous n'utilisez pas un clavier Sun, utilisez la combinaison de touches suivante.**

```
<Alt> <Break>
```

Appuyez sur les touches simultanément pour reprendre le contrôle du focus du bureau actuel de votre ordinateur portable.

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

Sur un système x86 utilisant un clavier Sun, l'utilisateur a été invité à saisir un mot de passe. Le curseur a été capté et se trouve 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> <Stop> . Si le pointeur reste dans la boîte de dialogue, l'utilisateur sait que l'invite de mot de passe est de confiance.

Si le pointeur se déplace vers la bande de confiance, l'utilisateur sait que l'invite de mot de passe n'est pas de confiance et il contacte l'administrateur.

Exemple 5–4 Forcer le pointeur à se déplacer 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 placer le pointeur au centre de la bande de confiance, l'utilisateur appuie simultanément sur les touches <Meta> <Stop>.

▼ Obtention de l'équivalent hexadécimal d'une étiquette

Cette procédure fournit une représentation hexadécimale interne d'une étiquette. Cette représentation est sûre et permet le stockage dans un annuaire public. Pour plus d'informations, reportez-vous à la page de manuel `atohexlabel(1M)`.

Avant de commencer Vous devez être administrateur de sécurité dans la zone globale. Pour plus d'informations, reportez-vous à la section "Accès à la zone globale dans Trusted Extensions " à la page 55.

- **Pour obtenir la valeur hexadécimale d'une étiquette, effectuez l'une des opérations suivantes.**

  - **Pour obtenir la valeur hexadécimale d'une étiquette de sensibilité, transmettez l'étiquette à la commande.**

    ```
    $ atohexlabel "CONFIDENTIAL : NEED TO KNOW"
    0x0004-08-68
    ```

  - **Pour obtenir la valeur hexadécimale d'une autorisation, utilisez l'option `-c`.**

    ```
    $ atohexlabel -c "CONFIDENTIAL NEED TO KNOW"
    0x0004-08-68
    ```

    Remarque – Les étiquettes de sensibilité lisibles par l'utilisateur et les étiquettes d'autorisation sont formées conformément aux règles du fichier `label_encodings`. Chaque type d'étiquette utilise les règles d'une section distincte de ce fichier. Lorsqu'une étiquette de sensibilité et une étiquette d'autorisation expriment toutes les deux le même niveau de sensibilité sous-jacent, leurs formes hexadécimales sont identiques. Toutefois, leurs formes lisibles par l'utilisateur peuvent être différentes. Les interfaces système qui acceptent les étiquettes lisibles par l'utilisateur en tant qu'entrées s'attendent à un type d'étiquette donné. Si les chaînes textuelles des types d'étiquette diffèrent, ces chaînes textuelles ne peuvent pas être utilisées de façon interchangeable.

    Dans le fichier par défaut `label_encodings`, le texte équivalent à une étiquette d'autorisation n'inclut pas les deux points (:).

Exemple 5–5 Utilisation de la commande `atohexlabel`

Lorsque vous transmettez une étiquette valide au format hexadécimal, la commande renvoie l'argument.

```
$ atohexlabel 0x0004-08-68
0x0004-08-68
```

Lorsque vous transmettez une étiquette d'administration, la commande renvoie l'argument.

```
$ atohexlabel admin_high
ADMIN_HIGH
atohexlabel admin_low
ADMIN_LOW
```

Erreurs fréquentes Le message d'erreur `atohexlabel parsing error found in <string> at position 0` indique que l'argument `<string>` que vous avez transmis à la commande `atohexlabel` n'était ni une étiquette valide, ni une autorisation. Vérifiez votre saisie et vérifiez que l'étiquette existe dans votre fichier `label_encodings` installé.

▼ Obtention d'une étiquette lisible à partir de sa forme hexadécimale

Cette procédure constitue un moyen de réparer des étiquettes stockées dans des bases de données internes. Pour plus d'informations, reportez-vous à la page de manuel `hextoalabel(1M)`.

Avant de commencer Vous devez être administrateur de sécurité dans la zone globale.

- **Pour obtenir l'équivalent textuel d'une représentation interne d'une étiquette, effectuez l'une des opérations suivantes.**

  - **Pour obtenir l'équivalent textuel d'une étiquette de sensibilité, transmettez la forme hexadécimale de l'étiquette.**

    ```
    $ hextoalabel 0x0004-08-68
    CONFIDENTIAL : NEED TO KNOW
    ```

  - **Pour obtenir l'équivalent textuel d'une autorisation, utilisez l'option `-c`.**

    ```
    $ hextoalabel -c 0x0004-08-68
    CONFIDENTIAL NEED TO KNOW
    ```

▼ Procédure de modification des paramètres de sécurité par défaut dans des fichiers système

Dans Trusted Extensions, c'est l'administrateur de sécurité qui modifie ou accède aux paramètres de sécurité par défaut sur un système.

Les fichiers des répertoires `/etc/security` et `/etc/default` contiennent des paramètres de sécurité. Sur un système Oracle Solaris, le superutilisateur peut modifier ces fichiers. Pour obtenir des informations sur la sécurité d'Oracle Solaris, reportez-vous au Chapitre 3, “Controlling Access to Systems (Tasks)” du *System Administration Guide: Security Services*.

Attention – Assouplissez uniquement les paramètres de sécurité par défaut du système si la stratégie de sécurité du site vous le permet.

Avant de commencer Vous devez être administrateur de sécurité dans la zone globale.

- **Utilisez l'éditeur de confiance pour modifier le fichier système.**

  Pour plus d'informations, reportez-vous à la section “Modification des fichiers d'administration dans Trusted Extensions” à la page 59.

Le tableau ci-dessous répertorie les fichiers de sécurité et les paramètres de sécurité pouvant être modifiés dans ces fichiers.

Fichier	Tâche	Pour plus d'informations
`/etc/default/login`	Réduire le nombre autorisé de tentatives de saisie de mot de passe.	Reportez-vous à l'exemple sous "How to Monitor All Failed Login Attempts" du *System Administration Guide: Security Services*. Page de manuel `passwd(1)`
`etc/default/kbd`	Désactiver l'arrêt du clavier	"How to Disable a System's Abort Sequence" du *System Administration Guide: Security Services* **Remarque –** Sur les hôtes qui sont utilisés par les administrateurs pour le débogage, le paramètre par défaut pour `KEYBOARD_ABORT` permet d'accéder au débogueur de noyau `kadb`. Pour plus d'informations sur le débogueur, reportez-vous à la page de manuel `kadb(1M)`.
`/etc/security/policy.conf`	Exiger un algorithme plus puissant pour les mots de passe utilisateur. Supprimer un privilège de base pour tous les utilisateurs de cet hôte. Limiter les utilisateurs de cet hôte aux autorisations utilisateur Solaris de base.	Page de manuel `policy.conf(4)`
`/etc/default/passwd`	Exiger des utilisateurs qu'ils modifient fréquemment leur mot de passe. Exiger des utilisateurs qu'ils créent des mots de passe les plus différents possibles. Exiger des mots de passe utilisateur plus longs. Exiger des mots de passe introuvables dans votre dictionnaire.	Page de manuel `passwd(1)`

◆ ◆ ◆ CHAPITRE 6

Utilisateurs, droits et rôles dans Trusted Extensions (présentation)

Ce chapitre décrit les décisions essentielles que vous devez prendre avant de créer des utilisateurs standard, et fournit des informations générales complémentaires sur la gestion des comptes utilisateur. Ce chapitre considère que l'équipe de configuration initiale a configuré des rôles et un nombre limité de comptes utilisateur. Ces utilisateurs peuvent assumer les rôles qui sont utilisés pour configurer et administrer Trusted Extensions. Pour plus d'informations, reportez-vous à la section "Création de rôles et d'utilisateurs dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.

Fonctions de sécurité des utilisateurs dans Trusted Extensions

Le logiciel Trusted Extensions permet d'ajouter les fonctions de sécurité suivantes aux utilisateurs, aux rôles ou aux profils de droits :

- Un utilisateur dispose d'une plage d'étiquettes à l'intérieur de laquelle il peut utiliser le système.
- Un rôle dispose d'une plage d'étiquettes à l'intérieur de laquelle il peut être utilisé pour effectuer des tâches d'administration.
- Un profil de droits de Trusted Extensions peut inclure des actions d'administration CDE. Comme les commandes, les actions peuvent disposer d'attributs de sécurité.
- Dans un profil de droits de Trusted Extensions, les commandes et les actions disposent d'un attribut d'étiquette. La commande ou l'action doit être effectuée dans une plage d'étiquettes ou dans une étiquette donnée.

- Le logiciel de Trusted Extensions permet d'ajouter des privilèges et des autorisations à l'ensemble de privilèges et d'autorisations défini par le SE Oracle Solaris.

Responsabilités des administrateurs concernant les utilisateurs

Le rôle d'administrateur système crée des comptes utilisateur. Le rôle d'administrateur de sécurité configure les aspects de sécurité d'un compte.

Si vous utilisez l'Oracle Directory Server Enterprise Edition pour le service de nommage LDAP, vérifiez que l'équipe de configuration initiale a configuré la boîte à outils `tsol_ldap.tbx`. Pour connaître la procédure, reportez-vous à la section "Configuration de la Console de gestion Solaris pour LDAP (liste des tâches)" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.

Pour plus d'informations sur le paramétrage des utilisateurs et des rôles, reportez-vous aux sections suivantes :

- "How to Create the First Role (Primary Administrator)" du *System Administration Guide: Basic Administration*
- "Setting Up User Accounts (Task Map)" du *System Administration Guide: Basic Administration*
- Partie III, "Roles, Rights Profiles, and Privileges" du *System Administration Guide: Security Services*

Responsabilités de l'administrateur système concernant les utilisateurs

Dans Trusted Extensions, le rôle d'administrateur système est chargé de déterminer qui peut accéder au système. L'administrateur système est responsable de l'exécution des tâches suivantes :

- l'ajout et la suppression d'utilisateurs ;
- l'ajout et la suppression de rôles ;
- la modification des configurations des utilisateurs et des rôles, à l'exception des attributs de sécurité.

Responsabilités de l'administrateur de sécurité concernant les utilisateurs

Dans Trusted Extensions, le rôle d'administrateur de sécurité est responsable de tous les attributs de sécurité d'un utilisateur ou d'un rôle. L'administrateur de sécurité est responsable de l'exécution des tâches suivantes :

- l'affectation et la modification des attributs de sécurité d'un utilisateur, d'un rôle ou d'un profil de droits ;
- la création et la modification des profils de droits ;
- l'affectation de profils de droits aux utilisateurs ou aux rôles
- l'affectation de privilèges aux utilisateurs, rôles ou profils de droits ;
- l'affectation d'autorisations aux utilisateurs, rôles ou profils de droits ;
- la suppression des privilèges d'un utilisateur, d'un rôle ou d'un profil de droits ;
- la suppression des autorisations d'un utilisateur, d'un rôle ou d'un profil de droits.

En général, le rôle d'administrateur de sécurité permet de créer des profils de droits. Toutefois, si un profil a besoin de capacités que le rôle d'administrateur de sécurité ne peut pas octroyer, le superutilisateur ou le rôle d'administrateur principal peut alors créer le profil.

Avant de créer un profil de droits, l'administrateur de sécurité doit analyser si des commandes ou actions du nouveau profil ont besoin de privilèges ou d'autorisations pour réussir. Les pages de manuel des commandes individuelles répertorient les privilèges et les autorisations qui peuvent être nécessaires. Pour des exemples d'actions qui nécessitent des privilèges et des autorisations, reportez-vous à la base de données `exec_attr`.

Décisions à prendre avant de créer des utilisateurs dans Trusted Extensions

Les décisions suivantes ont une incidence sur ce que les utilisateurs sont autorisés à faire dans Trusted Extensions et sur l'effort requis. Certaines décisions sont identiques aux décisions que vous prendriez lors de l'installation du SE Oracle Solaris. Toutefois, les décisions propres à Trusted Extensions peuvent avoir une incidence sur la sécurité du site et la simplicité d'utilisation.

- Décidez si vous voulez modifier les attributs de sécurité utilisateur par défaut dans le fichier `policy.conf`. Les valeurs utilisateur par défaut dans le fichier `label_encodings` ont été configurées par l'équipe de configuration initiale. Pour une description de ces valeurs par défaut, reportez-vous à la section "Attributs de sécurité utilisateur par défaut dans Trusted Extensions" à la page 82.

- Le cas échéant, choisissez les fichiers de démarrage à copier ou à lier du répertoire personnel de l'étiquette minimale de chaque utilisateur au répertoire personnel de niveau supérieur de chaque utilisateur. Pour plus d'informations sur cette procédure, reportez-vous à la section “Procédure de configuration des fichiers de démarrage pour les utilisateurs dans Trusted Extensions ” à la page 92.
- Décidez si les utilisateurs peuvent accéder aux périphériques, tels que le microphone, l'unité de CD-ROM et le lecteur JAZ.

  Si certains utilisateurs sont autorisés à y accéder, choisissez si votre site nécessite ou non des autorisations supplémentaires pour satisfaire la sécurité du site. Pour la liste par défaut des autorisations relatives aux périphériques, reportez-vous à la section “Procédure d'assignation d'autorisations de périphériques” à la page 268. Pour un ensemble plus détaillé d'autorisations de périphériques, reportez-vous à la section “Personnalisation des autorisations de périphériques dans Trusted Extensions (liste des tâches)” à la page 264.

Attributs de sécurité utilisateur par défaut dans Trusted Extensions

Les paramètres dans les fichiers `label_encodings` et `policy.conf` définissent les attributs de sécurité par défaut des comptes utilisateur. Les valeurs que vous avez explicitement définies pour un utilisateur remplacent ces valeurs du système. Certaines des valeurs qui sont définies dans ces fichiers s'appliquent également aux comptes de rôles. Pour les attributs de sécurité que vous pouvez définir explicitement, reportez-vous à la section “Attributs de l'utilisateur configurables dans Trusted Extensions” à la page 83.

Valeurs par défaut du fichier `label_encodings`

Le fichier `label_encodings` définit l'étiquette minimale, l'autorisation et l'affichage des étiquettes par défaut d'un utilisateur. Pour plus d'informations sur ce fichier, reportez-vous à la page de manuel `label_encodings(4)`. Le fichier `label_encodings` de votre site a été installé par votre équipe de configuration initiale. Leurs décisions se sont basées sur la section “Élaboration d’une stratégie d’étiquetage” du *Guide de configuration d’Oracle Solaris Trusted Extensions* et sur des exemples de la section *Oracle Solaris Trusted Extensions Label Administration* .

Les valeurs d'étiquette que l'administrateur de sécurité définit explicitement pour les utilisateurs individuels dans la Console de gestion Solaris sont dérivées du fichier `label_encodings`. Les valeurs définies explicitement remplacent les valeurs dans le fichier `label_encodings`.

Valeurs par défaut du fichier `policy.conf` dans Trusted Extensions

Le fichier `/etc/security/policy.conf` d'Oracle Solaris contient les paramètres de sécurité par défaut du système. Trusted Extensions permet d'ajouter deux mots-clés à ce fichier. Vous pouvez ajouter ces paires mot-clé=valeur au fichier si vous souhaitez modifier la valeur à l'échelle du système. Ces mots-clés sont appliqués par Trusted Extensions. Le tableau ci-dessous présente les valeurs possibles de ces paramètres de sécurité et leurs valeurs par défaut.

TABLEAU 6–1 Paramètres de sécurité Trusted Extensions par défaut dans le fichier `policy.conf`

Mot-clé	Valeur par défaut	Valeurs possibles	Remarques
IDLECMD	LOCK	LOCK | LOGOUT	Ne s'applique pas aux rôles.
IDLETIME	30	0 à 120 minutes	Ne s'applique pas aux rôles.

Les autorisations et les profils de droits qui sont définis dans le fichier `policy.conf` *s'ajoutent* à toutes les autorisations et tous les profils qui sont affectés à des comptes individuels. Pour les autres champs, la valeur de l'utilisateur individuel remplace la valeur du système.

La section "Planification de la sécurité de l'utilisateur dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions* comprend une tableau répertoriant chaque mot-clé `policy.conf`. Reportez-vous également à la page de manuel `policy.conf(4)`.

Attributs de l'utilisateur configurables dans Trusted Extensions

La Console de gestion Solaris 2.1 est l'outil qui vous permet de créer et modifier des comptes utilisateur. Pour les utilisateurs qui peuvent se connecter à plus d'une étiquette, vous pouvez également souhaiter paramétrer les fichiers `.copy_files` et `.link_files` dans le répertoire personnel de l'étiquette minimale de chaque utilisateur.

L'outil des comptes utilisateur dans la Console de gestion Solaris fonctionne comme dans le SE Oracle Solaris, à deux exceptions près :

- Trusted Extensions ajoute des attributs à des comptes utilisateur.
- L'accès au serveur d'annuaire personnel requiert une intervention d'administration dans Trusted Extensions.
  - Vous créez l'entrée du serveur d'annuaire personnel comme vous le feriez sur un système Oracle Solaris.
  - L'utilisateur et vous effectuez ensuite des opérations supplémentaires pour monter le répertoire personnel sous l'étiquette de chaque utilisateur.

Comme décrit à la section "How to Add a User With the Solaris Management Console's Users Tool" du *System Administration Guide: Basic Administration*, un assistant vous permet de créer des comptes utilisateur rapidement. Après avoir utilisé l'assistant, vous pouvez modifier les attributs Trusted Extensions par défaut de l'utilisateur.

Pour plus d'informations sur les fichiers `.copy_files` et `.link_files`, reportez-vous à la section "Fichiers `.copy_files` et `.link_files`" à la page 86.

Attributs de sécurité devant être affectés aux utilisateurs

Le rôle de l'administrateur de sécurité doit indiquer certains attributs de sécurité pour les nouveaux utilisateurs, comme indiqué dans le tableau suivant. Pour plus d'informations sur les fichiers qui contiennent des valeurs par défaut, reportez-vous à la section "Attributs de sécurité utilisateur par défaut dans Trusted Extensions" à la page 82. Le tableau suivant présente les attributs de sécurité pouvant être affectés aux utilisateurs et les effets de chaque affectation.

TABLEAU 6–2 Attributs de sécurité affectés après la création d'un utilisateur

Attribut de l'utilisateur	Emplacement de la valeur par défaut	Action requise ?	Effet de l'action
Mot de passe	Aucun	Requise	L'utilisateur dispose d'un mot de passe
Rôles	Aucun	Facultative	L'utilisateur peut assumer un rôle
Autorisations	Fichier `policy.conf`	Facultative	L'utilisateur dispose d'autorisations supplémentaires
Profils de droits	Fichier `policy.conf`	Facultative	L'utilisateur dispose de profils de droits supplémentaires
Étiquettes	Fichier `label_encodings`	Facultative	L'utilisateur dispose d'une étiquette ou d'une plage d'accréditations par défaut différente.
Privilèges	Fichier `policy.conf`	Facultative	L'utilisateur dispose d'un ensemble de privilèges différent
Utilisation du compte	Fichier `policy.conf`	Facultative	L'utilisateur dispose d'un paramétrage différent pour l'ordinateur lorsque ce dernier est inactif
Audit	Fichier `audit_control`	Facultative	L'audit auquel est soumis l'utilisateur n'est pas le même que celui prévu par les paramètres d'audit du système.

Affectation d'attributs de sécurité aux utilisateurs dans Trusted Extensions

Une fois que les comptes utilisateur ont été créés, le rôle d'administrateur de sécurité affecte des attributs de sécurité aux utilisateurs dans la Console de gestion Solaris. Si vous avez défini des valeurs par défaut correctes, l'étape suivante consiste à affecter des attributs de sécurité aux utilisateurs qui ont besoin d'exceptions aux valeurs par défaut.

Lorsqu'il affecte des attributs de sécurité aux utilisateurs, l'administrateur de sécurité prend en compte les informations suivantes :

Affectation de mots de passe
Le rôle d'administrateur de sécurité affecte des mots de passe aux comptes utilisateur une fois que les comptes ont été créés. Après cette première affectation, les utilisateurs peuvent modifier leurs mots de passe.

Comme dans le SE Oracle Solaris, les utilisateurs peuvent être obligés de modifier leurs mots de passe à intervalles réguliers. Les options de vieillissement du mot de passe limitent la durée pendant laquelle un intrus qui aurait deviné ou usurpé un mot de passe peut accéder au système. En outre, l'instauration d'un délai minimal avant que la modification d'un mot de passe ne soit autorisée permet d'empêcher qu'un utilisateur disposant d'un nouveau mot de passe ne rétablisse immédiatement son ancien mot de passe. Pour plus d'informations, reportez-vous à la page de manuel `passwd(1)`.

Remarque – Les mots de passe des utilisateurs qui peuvent assumer des rôles ne doivent être soumis à aucune contrainte de vieillissement du mot de passe.

Affectation de rôles
L'adoption d'un rôle n'est pas obligatoire pour les utilisateurs. Plusieurs rôles peuvent être affectés à un seul utilisateur si cela est cohérent avec la stratégie de sécurité de votre site.

Affectation d'autorisations
Comme dans le SE Oracle Solaris, l'affectation d'autorisations directement à un utilisateur ajoute ces autorisations aux autorisations existantes. Dans Trusted Extensions, vous ajoutez les autorisations à un profil de droits, puis vous affectez le profil à l'utilisateur.

Affectation de profils de droits
Comme dans le SE Oracle Solaris, l'ordre des profils est important. Le mécanisme des profils utilise la première instance de la commande ou de l'action dans l'ensemble de profils d'un compte.

Vous pouvez utiliser l'ordre de tri de profils à votre avantage. Si vous souhaitez qu'une commande s'exécute en utilisant d'autres attributs de sécurité que ceux qui sont définis pour elle dans un profil existant, créez un nouveau profil avec les affectations souhaitées pour la commande. Ensuite, insérez ce nouveau profil avant le profil existant.

Remarque – N'affectez pas de profils de droits incluant des actions ou des commandes d'administration à un utilisateur standard. En effet, le profil ne fonctionnera pas car un utilisateur standard ne peut pas accéder à la zone globale.

Modification de la valeur par défaut des privilèges
L'ensemble de privilèges par défaut peut être trop souple pour un grand nombre de sites. Pour limiter l'ensemble de privilèges de tous les utilisateurs standard sur un système, modifiez le paramètre du fichier `policy.conf`. Pour modifier l'ensemble de privilèges d'utilisateurs particuliers, utilisez la Console de gestion Solaris. Pour obtenir un exemple, reportez-vous à la section "Procédure de limitation du jeu de privilèges d'un utilisateur" à la page 101.

Modification des valeurs d'étiquette par défaut
La modification des valeurs d'étiquette par défaut d'un utilisateur crée une exception pour les valeurs par défaut de l'utilisateur dans le fichier `label_encodings`.

Modification des valeurs par défaut de l'audit
Comme dans le SE Oracle Solaris, l'assignation de classes d'audit à un utilisateur crée des exceptions pour les classes d'audit qui sont affectées dans le fichier `/etc/security/audit_control` sur le système. Pour plus d'informations sur l'audit, reportez-vous au Chapitre 18, "Audit de Trusted Extensions (présentation) ".

Fichiers `.copy_files` et `.link_files`

Dans Trusted Extensions, les fichiers sont automatiquement copiés du répertoire squelette dans la zone qui contient l'étiquette minimale du compte, et *uniquement* à cet endroit. Pour permettre l'utilisation des fichiers de démarrage par les zones d'étiquette supérieure, l'utilisateur ou l'administrateur doit créer les fichiers `.copy_files` et `.link_files`.

Les fichiers `.copy_files` et `.link_files` de Trusted Extensions facilitent l'automatisation de la copie ou de la liaison de fichiers de démarrage dans chaque étiquette du répertoire personnel d'un compte. Chaque fois qu'un utilisateur crée un espace de travail sous une nouvelle étiquette, la commande `updatehome` lit le contenu des fichiers `.copy_files` et `.link_files` placés sous l'étiquette minimale du compte. La commande copie ou lie alors chaque fichier répertorié dans ou à l'espace de travail d'étiquette supérieure.

Le fichier `.copy_files` est utile lorsqu'un utilisateur souhaite utiliser un fichier de démarrage légèrement différent pour chaque étiquette. La copie est préférable, par exemple, lorsque les utilisateurs utilisent différents alias de messagerie pour les différentes étiquettes. Le fichier `.link-files` est utile lorsqu'un fichier de démarrage doit être identique pour toutes les étiquettes appelées. La liaison est préférable, par exemple, lorsqu'une même imprimante est utilisée pour tous les travaux d'impression étiquetés. Pour obtenir des exemples de fichiers, reportez-vous à la section "Procédure de configuration des fichiers de démarrage pour les utilisateurs dans Trusted Extensions " à la page 92.

Vous trouverez ci-dessous une liste de fichiers de démarrage qu'il peut être souhaitable que les utilisateurs puissent lier à des étiquettes supérieures ou copier vers des étiquettes supérieures :

- `.acrorc`
- `.aliases`
- `.cshrc`
- `.dtprofile`
- `.emacs`
- `.login`
- `.mailrc`
- `.mime_types`
- `.newsrc`
- `.profile`
- `.signature`
- `.soffice`
- `.Xdefaults`
- `.Xdefaults-`*`hostname`*

◆ ◆ ◆ CHAPITRE 7

Gestion des utilisateurs, des droits et des rôles dans Trusted Extensions (tâches)

Ce chapitre décrit les procédures Trusted Extensions de configuration et de gestion des utilisateurs, des comptes utilisateur et des profils de droits.

Personnalisation de l'environnement de l'utilisateur pour en assurer la sécurité (liste des tâches)

La liste des tâches ci-dessous décrit les tâches courantes que vous pouvez effectuer lorsque vous personnalisez un système pour tous les utilisateurs ou lorsque vous personnalisez un compte utilisateur.

Tâche	Description	Voir
Modification des attributs d'étiquette.	Modifiez les attributs d'étiquette, tels que l'étiquette minimale et la visibilité par défaut des étiquettes, pour un compte utilisateur.	"Procédure de modification des attributs d'étiquette par défaut des utilisateurs" à la page 90

Tâche	Description	Voir
Modification de la stratégie Trusted Extensions pour tous les utilisateurs d'un système.	Modifie le fichier `policy.conf`.	"Procédure de modification des valeurs par défaut de `policy.conf`" à la page 91
	Active l'économiseur d'écran après une durée définie. Déconnecte l'utilisateur après une durée d'inactivité du système définie.	Exemple 7–1
	Supprime les privilèges inutiles de tous les utilisateurs ordinaires d'un système.	Exemple 7–2
	Supprime les étiquettes des sorties étiquetées dans un kiosque public.	Exemple 7–3
Configuration de fichiers d'initialisation pour les utilisateurs.	Configure les fichiers de démarrage, tels que `.cshrc`, `.copy_files` et `.soffice` pour tous les utilisateurs.	"Procédure de configuration des fichiers de démarrage pour les utilisateurs dans Trusted Extensions " à la page 92
Prolongation du délai d'attente pour la modification de l'étiquette de fichiers.	Configure certaines applications de manière à ce qu'elles permettent à des utilisateurs autorisés de modifier l'étiquette de fichiers.	"Procédure d'allongement du délai d'attente lors de la modification de l'étiquette d'informations" à la page 95
Connexion à une session de secours.	Répare les fichiers d'initialisation défectueux d'un utilisateur .	"Procédure de connexion à une session de secours dans Trusted Extensions " à la page 97

▼ Procédure de modification des attributs d'étiquette par défaut des utilisateurs

Vous pouvez modifier les attributs d'étiquette par défaut des utilisateurs lors de la configuration du premier système. Les modifications doivent être copiées sur chaque hôte de Trusted Extensions.

Avant de commencer Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale. Pour plus d'informations, reportez-vous à la section "Accès à la zone globale dans Trusted Extensions " à la page 55.

1 Vérifiez les paramètres des attributs par défaut des utilisateurs dans le fichier `/etc/security/tsol/label_encodings`.

Pour les valeurs par défaut, reportez-vous à "Valeurs par défaut du fichier `label_encodings`" à la page 82.

2. **Modifiez les paramètres des attributs des utilisateurs dans le fichier `label_encodings`.**

   Utilisez l'éditeur de confiance. Pour plus d'informations, reportez-vous à la section"Modification des fichiers d'administration dans Trusted Extensions" à la page 59. Dans Trusted CDE, vous pouvez également utiliser l'action Edit Label Encodings (Modifier le codage des étiquettes). Pour plus d'informations, reportez-vous à la section "Démarrage d'actions d'administration CDE dans Trusted Extensions " à la page 58.

   Le fichier `label_encodings` doit être identique sur tous les hôtes.

3. **Transmettez une copie du fichier à chaque hôte Trusted Extensions.**

▼ Procédure de modification des valeurs par défaut de `policy.conf`

La modification des valeurs par défaut du fichier `policy.conf` dans Trusted Extensions est similaire à la modification de tout fichier système lié à la sécurité dans le SE Oracle Solaris. Dans Trusted Extensions, vous utilisez un éditeur de confiance pour modifier les fichiers système.

Avant de commencer Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale. Pour plus d'informations, reportez-vous à la section "Accès à la zone globale dans Trusted Extensions " à la page 55.

1. **Contrôlez les paramètres par défaut dans le fichier `/etc/security/policy.conf`.**

   Pour les mots-clés de Trusted Extensions, reportez-vous au Tableau 6–1.

2. **Modifiez les paramètres.**

   Servez-vous de l'éditeur de confiance pour modifier le fichier système. Pour plus d'informations, reportez-vous à la section "Modification des fichiers d'administration dans Trusted Extensions" à la page 59.

Exemple 7–1 Modification des paramètres d'inactivité du système

Dans cet exemple, l'administrateur de sécurité souhaite que les systèmes inactifs reviennent à l'écran de connexion. Par défaut, un système inactif est verrouillé. Le rôle de l'administrateur de sécurité ajoute donc le couple mot-clé `IDLECMD`=valeur au fichier `/etc/security/policy.conf` comme suit :

```
IDLECMD=LOGOUT
```

L'administrateur veut également réduire la durée d'inactivité des systèmes avant la déconnexion. Le rôle d'administrateur de sécurité ajoute donc le couple mot-clé `IDLETIME`=valeur au fichier `policy.conf` comme suit :

```
IDLETIME=10
```

Le système déconnecte désormais l'utilisateur après 10 minutes d'inactivité du système.

Exemple 7–2 Modification du jeu de privilèges de base de chaque utilisateur

Dans cet exemple, l'administrateur de sécurité d'une installation Sun Ray ne souhaite pas que les utilisateurs standard puissent voir les processus d'autres utilisateurs Sun Ray. Par conséquent, sur chaque système configuré avec Trusted Extensions, l'administrateur supprime `proc_info` du jeu de privilèges de base. Le paramètre `PRIV_DEFAULT` dans le fichier `/etc/policy.conf` est modifié comme suit :

```
PRIV_DEFAULT=basic,!proc_info
```

Exemple 7–3 Affectation d'autorisations liées à l'impression à tous les utilisateurs d'un système

Dans cet exemple, l'administrateur de sécurité permet à un kiosque public d'imprimer sans étiquettes en saisissant la ligne suivante dans le fichier `/etc/security/policy.conf` de l'ordinateur. Au prochain démarrage, les travaux d'impression de tous les utilisateurs de ce kiosque seront imprimés sans étiquettes de pages.

```
AUTHS_GRANTED= solaris.print.unlabeled
```

Ensuite, l'administrateur décide d'économiser du papier en supprimant les pages de garde et de fin. Il s'assure tout d'abord que la case Always Print Banners (Toujours imprimer les bannières) n'est pas cochée dans le gestionnaire d'impression. Il modifie ensuite l'entrée `policy.conf` pour lire les informations suivantes et redémarre. Désormais, tous les travaux d'impression sont sans étiquette et n'ont ni page de garde, ni page de fin.

```
AUTHS_GRANTED= solaris.print.unlabeled,solaris.print.nobanner
```

▼ Procédure de configuration des fichiers de démarrage pour les utilisateurs dans Trusted Extensions

Les utilisateurs peuvent placer un fichier `.copy_files` et un fichier `.link_files` dans leur répertoire personnel sous l'étiquette correspondant à leur étiquette de sensibilité minimale. Les utilisateurs peuvent également modifier les fichiers `.copy_files` et `.link_files` existants sous l'étiquette minimale des utilisateurs. Cette procédure permet au rôle d'administrateur d'automatiser la configuration pour un site.

Avant de commencer Vous devez être dans le rôle d'administrateur système dans la zone globale. Pour plus d'informations, reportez-vous à la section “Accès à la zone globale dans Trusted Extensions ” à la page 55.

1. **Créez deux fichiers de démarrage Trusted Extensions.**

   Vous allez ajouter `.copy_files` et `.link_files` à votre liste de fichiers de démarrage.

   ```
   # cd /etc/skel
   # touch .copy_files .link_files
   ```

2. **Personnalisez le fichier `.copy_files`.**

   a. **Démarrez l'éditeur de confiance.**

      Pour plus d'informations, reportez-vous à la section "Modification des fichiers d'administration dans Trusted Extensions" à la page 59.

   b. **Saisissez le chemin d'accès complet du fichier `.copy_files`.**

      ```
      /etc/skel/.copy_files
      ```

   c. **Saisissez dans `.copy_files`, à raison d'un fichier par ligne, les fichiers à copier dans le répertoire personnel de l'utilisateur à toutes les étiquettes.**

      Reportez-vous à la section "Fichiers `.copy_files` et `.link_files`" à la page 86 si vous avez besoin de suggestions. Pour des exemples de fichiers, reportez-vous à l'Exemple 7–4.

3. **Personnalisez le fichier `.link_files`.**

   a. **Saisissez le chemin d'accès complet du fichier `.link_files` dans l'éditeur de confiance.**

      ```
      /etc/skel/.link_files
      ```

   b. **Saisissez dans `.link_files`, à raison d'un fichier par ligne, les fichiers à lier au répertoire personnel de l'utilisateur à toutes les étiquettes.**

4. **Personnalisez les autres fichiers de démarrage pour vos utilisateurs.**

   - Pour une description des éléments à inclure dans les fichiers de démarrage, reportez-vous à la section "Customizing a User's Work Environment" du *System Administration Guide: Basic Administration*.
   - Pour plus d'informations, reportez-vous à la section "How to Customize User Initialization Files" du *System Administration Guide: Basic Administration*.
   - Pour un exemple, reportez-vous à l'Exemple 7–4.

5. **(Facultatif) Créez un sous-répertoire `skeIP` pour les utilisateurs dont le shell par défaut est un shell de profil.**

   Le caractère `P` représente le shell de profil.

6. **Copiez les fichiers de démarrage personnalisés dans le répertoire squelette approprié.**

7 **Utilisez le chemin d'accès `skel`*X* approprié lorsque vous créez l'utilisateur.**

Le caractère *X* représente la première lettre du nom du shell, tel que `B` pour Bourne, `K` pour Korn, `C` pour un shell C et `P` pour un shell de profil.

Exemple 7–4 Personnalisation des fichiers de démarrage pour les utilisateurs

Dans cet exemple, l'administrateur de sécurité configure des fichiers pour le répertoire personnel de chaque utilisateur. Les fichiers sont en place avant la connexion du premier utilisateur. Les fichiers sont sous l'étiquette minimale de l'utilisateur. Sur ce site, le shell par défaut des utilisateurs est le shell C.

L'administrateur de sécurité crée un fichier `.copy_files` et un fichier `.link_files` dans l'éditeur de confiance avec le contenu suivant :

```
## .copy_files for regular users
## Copy these files to my home directory in every zone
.mailrc
.mozilla
.soffice
:wq

## .link_files for regular users with C shells
## Link these files to my home directory in every zone
.cshrc
.login
.Xdefaults
.Xdefaults-hostname
:wq

## .link_files for regular users with Korn shells
# Link these files to my home directory in every zone
.ksh
.profile
.Xdefaults
.Xdefaults-hostname
:wq
```

Dans les fichiers d'initialisation du shell, l'administrateur s'assure que les travaux d'impression des utilisateurs sont envoyés vers une imprimante étiquetée.

```
## .cshrc file
setenv PRINTER conf-printer1
setenv LPDEST  conf-printer1

## .ksh file
export PRINTER conf-printer1
export LPDEST  conf-printer1
```

L'administrateur modifie le fichier `.Xdefaults-`*home-directory-server* pour forcer la commande `dtterm` à utiliser le fichier `.profile` en tant que source pour un nouveau terminal.

```
## Xdefaults-HDserver
Dtterm*LoginShell: true
```

Les fichiers personnalisés sont copiés dans le répertoire squelette approprié.

```
$ cp .copy_files .link_files .cshrc .login .profile \
.mailrc .Xdefaults .Xdefaults-home-directory-server \
/etc/skelC
$ cp .copy_files .link_files .ksh .profile \
.mailrc .Xdefaults .Xdefaults-home-directory-server \
/etc/skelK
```

Erreurs fréquentes

Si vous créez un fichier `.copy_files` à votre étiquette la plus basse, que vous vous connectez ensuite à une zone supérieure afin d'exécuter la commande `updatehome` et que l'exécution de cette commande échoue avec une erreur d'accès, vérifiez les points suivants :

- Vérifiez que vous pouvez visualiser le répertoire de niveau inférieur à partir de la zone supérieure.

  ```
  higher-level zone# ls /zone/lower-level-zone/home/username
  ACCESS ERROR: there are no files under that directory
  ```

- Si vous ne pouvez pas visualiser le répertoire, redémarrez le service de montage automatique dans la zone de niveau supérieur :

  ```
  higher-level zone# svcadm restart autofs
  ```

À moins que vous n'utilisiez des montages NFS pour les répertoires personnels, le montage automatique dans la zone supérieure doit être en loopback de `/zone/`*lower-level-zone*`/export/home/`*username* à `/zone/`*lower-level-zone*`/home/`*username*.

▼ Procédure d'allongement du délai d'attente lors de la modification de l'étiquette d'informations

Dans Trusted Extensions, le gestionnaire de sélection sert d'intermédiaire pour le transfert d'informations entre des étiquettes. Le gestionnaire de sélection s'affiche pour les opérations de glisser-déposer et pour les opérations de couper-coller. Certaines applications nécessitent que vous définissiez un délai d'attente adéquat pour que le gestionnaire de sélection ait le temps d'intervenir. Une valeur de deux minutes est suffisante.

Attention – Ne modifiez pas la valeur de temps d'attente par défaut sur un système sans étiquette. Avec une valeur de délai d'attente plus longue, les opérations échouent.

Avant de commencer

Vous devez être dans le rôle d'administrateur système dans la zone globale. Pour plus d'informations, reportez-vous à la section “Accès à la zone globale dans Trusted Extensions ” à la page 55.

1 **Pour l'application StarOffice, effectuez les opérations suivantes :**

   a. **Accédez au fichier** *office-install-directory*`/VCL.xcu`**.**

      où *office-install-directory* est le répertoire d'installation de StarOffice, par exemple :

      office-top-dir`/share/registry/data/org/staroffice`

   b. **Modifiez la valeur de la propriété `SelectionTimeout` sur 120.**

      Utilisez l'éditeur de confiance. Pour plus d'informations, reportez-vous à la section "Modification des fichiers d'administration dans Trusted Extensions" à la page 59.

      La valeur par défaut est de trois secondes. Une valeur de 120 définit le délai d'attente sur deux minutes.

2 **Pour les utilisateurs d'applications qui s'appuient sur la bibliothèque GNOME ToolKit (GTK), modifiez la valeur de la propriété à deux minutes.**

Remarque – Vous pouvez aussi faire en sorte que chaque utilisateur change lui-même la valeur de la propriété.

La plupart des applications Sun Java Desktop System utilisent la bibliothèque GTK. Les navigateurs Web tels que Mozilla, Firefox et Thunderbird utilisent la bibliothèque GTK.

Par défaut, la valeur du délai d'attente est de 300, ou 5 secondes. Une valeur de 7 200 définit le délai d'attente sur deux minutes.

   a. **Créez un fichier de démarrage GTK.**

      Nommez le fichier `.gtkrc-mine`. Le fichier `.gtkrc-mine` se trouve dans le répertoire personnel de l'utilisateur sous l'étiquette minimale.

   b. **Ajoutez la valeur de délai d'attente au fichier.**

```
## $HOME/.gtkrc-mine file
*gtk-selection-timeout: 7200
```

      Comme dans le SE Oracle Solaris, la commande `gnome-settings-daemon` lit ce fichier au démarrage.

3 **(Facultatif) Ajoutez le fichier `.gtkrc-mine` à la liste du fichier `.link_files` de chaque utilisateur.**

Pour plus d'information, reportez-vous à la section "Procédure de configuration des fichiers de démarrage pour les utilisateurs dans Trusted Extensions " à la page 92.

▼ Procédure de connexion à une session de secours dans Trusted Extensions

Dans Trusted Extensions, la connexion de secours est protégée. Si un utilisateur standard a des fichiers d'initialisation du shell personnalisés et ne peut pas se connecter, vous pouvez utiliser la connexion de secours pour corriger les fichiers de l'utilisateur.

Avant de commencer Vous devez connaître le mot de passe `root`.

1. **Comme dans le SE Oracle Solaris, choisissez Options -> Failsafe Session (Session de secours) dans l'écran de connexion.**
2. **À l'invite, demandez à l'utilisateur de fournir le nom d'utilisateur et le mot de passe.**
3. **À l'invite pour le mot de passe `root`, fournissez le mot de passe pour `root`.**

   Vous pouvez ensuite déboguer les fichiers d'initialisation de l'utilisateur.

Gestion des utilisateurs et des droits à l'aide de la Console de gestion Solaris (liste des tâches)

Dans Trusted Extensions, vous devez utiliser la Console de gestion Solaris pour administrer les utilisateurs, les autorisations, les droits et les rôles. Pour gérer les utilisateurs et leurs attributs de sécurité, prenez le rôle d'administrateur de sécurité. La liste des tâches ci-dessous décrit des tâches courantes que vous effectuez pour des utilisateurs travaillant dans un environnement étiqueté.

Tâche	Description	Voir
Modification de la plage d'étiquettes d'un utilisateur.	Modifie les étiquettes sous lesquelles un utilisateur peut travailler. Les modifications peuvent limiter ou étendre la plage autorisée par le fichier `label_encodings`.	"Procédure de modification de la plage d'étiquettes d'un utilisateur dans la Console de gestion Solaris " à la page 98
Création d'un profil de droits pour des autorisations commodes.	Il existe plusieurs autorisations qui peuvent s'avérer utiles pour des utilisateurs standard. Crée un profil pour des utilisateurs considérés aptes à recevoir ces autorisations.	"Procédure de création d'un profil de droits pour des autorisations commodes" à la page 99
Modification du jeu de privilèges par défaut d'un utilisateur.	Supprime un privilège du jeu de privilèges par défaut de l'utilisateur.	"Procédure de limitation du jeu de privilèges d'un utilisateur" à la page 101

Tâche	Description	Voir
Désactivation du verrouillage du compte pour des utilisateurs particuliers.	Le verrouillage du compte des utilisateurs pouvant assumer un rôle doit être désactivé.	"Procédure de désactivation du verrouillage du compte pour certains utilisateurs " à la page 103
Octroi de l'autorisation de modifier l'étiquette de données à un utilisateur.	Autorise un utilisateur à mettre à niveau ou rétrograder des informations.	"Procédure d'octroi de l'autorisation de modifier le niveau de sécurité de données à un utilisateur" à la page 104
Suppression d'un utilisateur du système.	Supprime complètement un utilisateur et ses processus.	"Procédure de suppression d'un compte utilisateur d'un système Trusted Extensions" à la page 105
Gestion d'autres tâches.	Utilise la Console de gestion Solaris pour gérer des tâches qui ne sont pas spécifiques à Trusted Extensions.	"Gestion d'autres tâches dans la Console de gestion Solaris (liste des tâches) " à la page 106

▼ Procédure de modification de la plage d'étiquettes d'un utilisateur dans la Console de gestion Solaris

Vous pouvez souhaiter étendre la plage d'étiquettes d'un utilisateur pour lui donner les autorisations en lecture à une application d'administration. Par exemple, un utilisateur qui peut se connecter à la zone globale pourrait ensuite exécuter la Console de gestion Solaris. L'utilisateur pourrait visualiser le contenu mais pas le modifier.

Vous pouvez aussi souhaiter réduire la plage d'étiquettes de l'utilisateur. Par exemple, un utilisateur invité peut être limité à une étiquette.

Avant de commencer Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

1. **Ouvrez une boîte à outils Trusted Extensions dans la Console de gestion Solaris.**

   Utilisez une boîte à outils de portée adéquate. Pour plus d'informations, reportez-vous à la section "Initialisation du serveur Console de gestion Solaris dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.

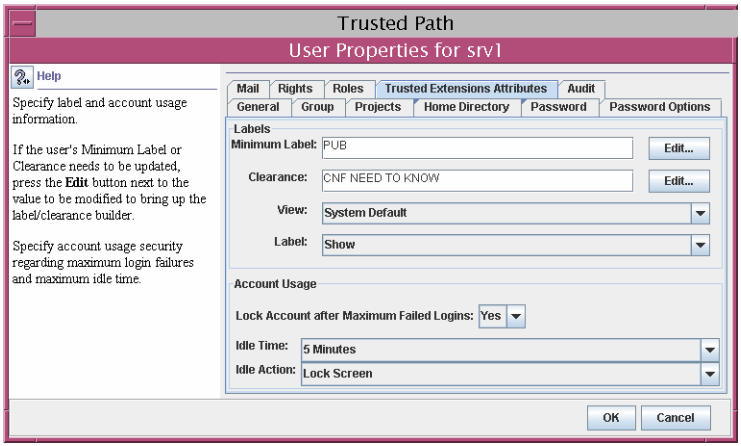
2. **Sous System Configuration (Configuration système), allez à User Accounts (Comptes utilisateur).**

   Une invite de mot de passe est susceptible de s'afficher.

3. **Saisissez le mot de passe du rôle.**

4. **Sélectionnez l'utilisateur individuel dans User Accounts**

5 **Cliquez sur l'onglet Attributes (Attributs) de Trusted Extensions.**



- **Pour étendre la plage d'étiquettes de l'utilisateur, choisissez une autorisation supérieure.**

  Vous pouvez également réduire l'étiquette minimale.

- **Pour limiter la plage d'étiquettes à une seule étiquette, l'autorisation doit être égale à l'étiquette minimale.**

6 **Pour enregistrer les modifications, cliquez sur OK.**

▼ Procédure de création d'un profil de droits pour des autorisations commodes

Lorsque la stratégie de sécurité du site le permet, vous pouvez souhaiter créer un profil de droits contenant des autorisations destinées à des utilisateurs habilités à effectuer des tâches nécessitant une autorisation. Pour permettre à tous les utilisateurs d'un système particulier d'être autorisés, reportez-vous à la section "Procédure de modification des valeurs par défaut de `policy.conf`" à la page 91.

Avant de commencer Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

1 **Ouvrez une boîte à outils Trusted Extensions dans la Console de gestion Solaris.**

Utilisez une boîte à outils de portée adéquate. Pour plus d'informations, reportez-vous à la section "Initialisation du serveur Console de gestion Solaris dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.

2 **Dans System Configuration (Configuration système), allez à Rights (Droits).**

Une invite de mot de passe est susceptible de s'afficher.

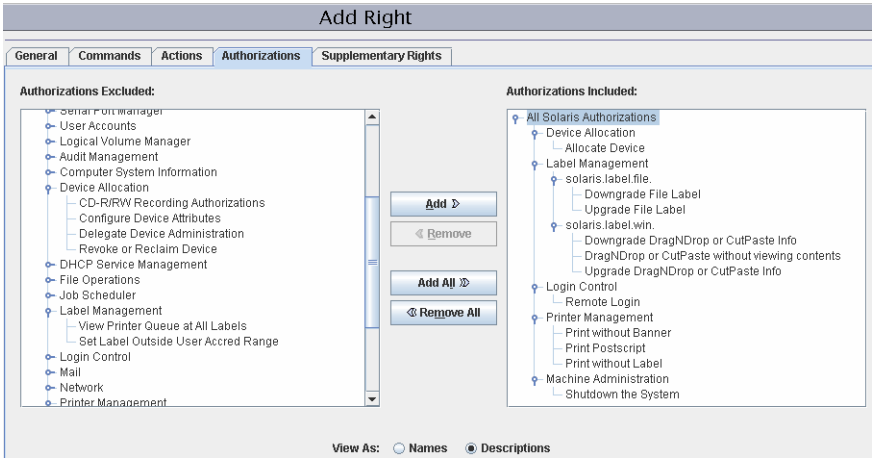
3 **Saisissez le mot de passe du rôle.**

4 **Pour ajouter un profil de droits, cliquez sur Action -> Add Right (Ajouter un droit).**

5 **Créez un profil de droits contenant une ou plusieurs des autorisations suivantes.**

Pour la procédure étape par étape, reportez-vous à la section "How to Create or Change a Rights Profile" du *System Administration Guide: Security Services*.

Dans l'image ci-dessous, la fenêtre Authorizations Included (Autorisations incluses) affiche les autorisations pouvant être utiles pour les utilisateurs.



- Allocate Device (Allouer un périphérique) : autorise un utilisateur à allouer un périphérique, tel qu'un microphone.

  Par défaut, les utilisateurs d'Oracle Solaris peuvent lire et écrire sur un CD-ROM. Toutefois, dans Trusted Extensions, seuls les utilisateurs qui peuvent allouer un périphérique peuvent accéder à l'unité de CD-ROM. L'allocation du disque nécessite une autorisation. Par conséquent, pour lire et écrire sur un CD-ROM dans Trusted Extensions, un utilisateur a besoin de l'autorisation Allocate Device.
- Downgrade DragNDrop or CutPaste Info (Rétrograder des informations par glisser-déposer ou copier-coller) : autorise un utilisateur à sélectionner les informations d'un fichier de niveau supérieur et à les placer dans un fichier de niveau inférieur.
- Downgrade File Label (Rétrograder l'étiquette d'un fichier) : autorise un utilisateur à réduire le niveau de sécurité d'un fichier

- DragNDrop or CutPaste without viewing contents (Glisser-déposer ou couper-coller sans visualiser le contenu) : autorise un utilisateur à déplacer des informations sans visualiser les informations déplacées.
- Print PostScript (Imprimer Postscript) : autorise un utilisateur à imprimer des fichiers PostScript.
- Print without Banner (Imprimer sans page de garde) : autorise un utilisateur à imprimer sur papier sans page de garde.
- Print without Label (Imprimer sans étiquette) : autorise un utilisateur à imprimer sur papier sans étiquette.
- Remote Login (Connexion à distance) : autorise un utilisateur à se connecter à distance.
- Shutdown the System (Arrêter le système) : autorise un utilisateur à arrêter le système et à arrêter une zone.
- Upgrade DragNDrop or CutPaste Info (Mettre à niveau des informations par glisser-déposer ou couper-coller) : autorise un utilisateur à sélectionner les informations d'un fichier de niveau inférieur et à les placer dans un fichier de niveau supérieur.
- Upgrade File Label (Mettre à niveau l'étiquette d'un fichier) : autorise un utilisateur à renforcer le niveau de sécurité d'un fichier.

6 **Attribuez le profil de droits à un utilisateur ou à un rôle.**

Pour obtenir de l'aide, reportez-vous à l'aide en ligne. Pour la procédure étape par étape, reportez-vous à la section "How to Change the RBAC Properties of a User" du *System Administration Guide: Security Services*.

Exemple 7–5 Attribution d'une autorisation liée à l'impression à un rôle

Dans l'exemple suivant, l'administrateur de sécurité permet à un rôle d'imprimer des travaux sans étiquettes sur les pages de corps de texte.

Dans la Console de gestion Solaris, l'administrateur de sécurité accède à Administrative Roles (Rôles d'administration). Il consulte les profils de droits qui sont inclus dans un rôle particulier, puis s'assure que les autorisations liées à l'impression sont contenues dans l'un des profils de droits du rôle.

▼ Procédure de limitation du jeu de privilèges d'un utilisateur

La sécurité du site peut exiger que les utilisateurs aient moins de privilèges que ceux qui leur sont assignés par défaut. Par exemple, sur un site qui utilise Trusted Extensions sur des systèmes Sun Ray, vous voudrez peut-être empêcher les utilisateurs de visualiser les processus des autres utilisateurs sur le serveur Sun Ray.

Avant de commencer Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

1. **Ouvrez une boîte à outils Trusted Extensions dans la Console de gestion Solaris.**

   Utilisez une boîte à outils de portée adéquate. Pour plus d'informations, reportez-vous à la section "Initialisation du serveur Console de gestion Solaris dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.

2. **Sous System Configuration (Configuration système), allez à User Accounts (Comptes utilisateur).**

   Une invite de mot de passe est susceptible de s'afficher.

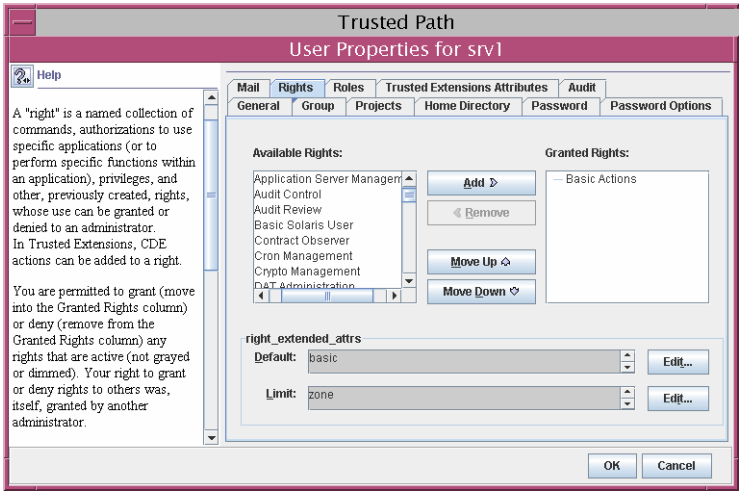
3. **Saisissez le mot de passe du rôle.**

4. **Double-cliquez sur l'icône correspondant à l'utilisateur.**

5. **Supprimez un ou plusieurs privilèges dans le jeu `basic`.**

   a. **Double-cliquez sur l'icône correspondant à l'utilisateur.**

   b. **Cliquez sur l'onglet Rights (Droits).**

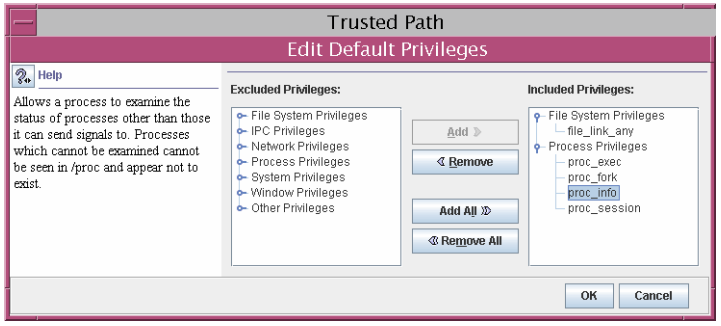


   c. **Cliquez sur le bouton Edit (Modifier) placé à droite du jeu `basic` dans le champ `right_extended_attr`.**

d. Supprimez `proc_session` ou `file_link_any`.

En supprimant le privilège `proc_session`, vous empêchez l'utilisateur d'examiner les processus externes à la session en cours de l'utilisateur. En supprimant le privilège `file_link_any`, vous empêchez l'utilisateur de créer des liens physiques vers des fichiers dont il n'est pas le propriétaire.

Attention – Ne supprimez pas le privilège `proc_fork` ou le privilège `proc_exec`. Sans ces privilèges, l'utilisateur ne peut pas utiliser le système.



6 Pour enregistrer les modifications, cliquez sur OK.

▼ Procédure de désactivation du verrouillage du compte pour certains utilisateurs

Trusted Extensions étend les fonctionnalités de sécurité de l'utilisateur dans la Console de gestion Solaris et y ajoute le verrouillage du compte. Désactivez le verrouillage du compte pour les utilisateurs qui peuvent assumer un rôle.

Avant de commencer Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

1 Démarrez la Console de gestion Solaris.

Utilisez une boîte à outils de portée adéquate. Pour plus d'informations, reportez-vous à la section "Initialisation du serveur Console de gestion Solaris dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.

2 Sous System Configuration (Configuration système), allez à User Accounts (Comptes utilisateur).

Une invite de mot de passe est susceptible de s'afficher.

3 **Saisissez le mot de passe du rôle.**

4 **Double-cliquez sur l'icône correspondant à l'utilisateur.**

5 **Cliquez sur l'onglet Attributes (Attributs) de Trusted Extensions.**

6 **Dans la section Account Usage (Utilisation du compte), choisissez `No` (Non) dans le menu déroulant en regard de `Lock account after maximum failed logins` (Verrouiller le compte après le nombre maximal d'échecs de connexion).**

7 **Pour enregistrer les modifications, cliquez sur OK.**

▼ Procédure d'octroi de l'autorisation de modifier le niveau de sécurité de données à un utilisateur

Un utilisateur standard ou un rôle peut être autorisé à modifier le niveau de sécurité ou les étiquettes de fichiers et de répertoires. L'utilisateur ou le rôle, en plus d'avoir l'autorisation, doit être configuré pour pouvoir travailler à plus d'une étiquette. Aussi, les zones étiquetées doivent être configurées de façon à autoriser la modification de leur étiquette. Pour plus d'informations sur cette procédure, reportez-vous à la section "Procédure d'octroi de l'autorisation de modifier l'étiquette de fichiers à un utilisateur" à la page 143.

Attention – La modification du niveau de sécurité des données est une opération qui nécessite des privilèges. Cette tâche ne peut être effectuée que par des utilisateurs dignes de confiance.

Avant de commencer Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

1 **Suivez la procédure décrite dans la section"Procédure de création d'un profil de droits pour des autorisations commodes" à la page 99 pour créer un profil de droits.**

Les autorisations suivantes permettent à un utilisateur de modifier l'étiquette d'un fichier :

- Downgrade File Label (Rétrograder l'étiquette d'un fichier)
- Upgrade File Label (Mettre à niveau l'étiquette d'un fichier)

Les autorisations suivantes permettent à un utilisateur de modifier l'étiquette d'informations contenues dans un fichier :

- Downgrade DragNDrop or CutPaste Info (Rétrograder des informations par glisser-déposer ou couper-coller)
- DragNDrop or CutPaste Info Without Viewing (Glisser-déposer ou couper-coller sans visualiser le contenu)

- Upgrade DragNDrop or CutPaste Info (Mettre à niveau des informations par glisser-déposer ou couper-coller)

2 **Utilisez la Console de gestion Solaris pour attribuer le profil aux utilisateurs et aux rôles appropriés.**

Pour obtenir de l'aide, utilisez l'aide en ligne. Pour une procédure pas à pas, reportez-vous à la section "How to Change the RBAC Properties of a User" du *System Administration Guide: Security Services*.

▼ Procédure de suppression d'un compte utilisateur d'un système Trusted Extensions

Lorsqu'un utilisateur est supprimé du système, vous devez vous assurer que le répertoire personnel de l'utilisateur et tous les objets qui lui appartiennent sont également supprimés. Comme alternative à la suppression d'objets appartenant à l'utilisateur, vous pouvez transférer la propriété de ces objets à un utilisateur valide.

Vous devez aussi vous assurer que tous les traitements par lots associés à l'utilisateur sont également supprimés. Aucun objet ou processus appartenant à un utilisateur supprimé ne peut rester sur le système.

Avant de commencer Vous devez être dans le rôle d'administrateur système.

1 **Archivez le répertoire personnel de l'utilisateur sur chaque étiquette.**

2 **Archivez les fichiers courrier de l'utilisateur sur chaque étiquette.**

3 **Dans la Console de gestion Solaris, supprimez le compte utilisateur.**

a. **Ouvrez une boîte à outils Trusted Extensions dans la Console de gestion Solaris.**

Utilisez une boîte à outils de portée adéquate. Pour plus d'informations, reportez-vous à la section "Initialisation du serveur Console de gestion Solaris dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.

b. **Sous System Configuration (Configuration système), allez à User Accounts (Comptes utilisateur).**

Une invite de mot de passe est susceptible de s'afficher.

c. **Saisissez le mot de passe du rôle.**

d. Sélectionnez le compte utilisateur à supprimer, puis cliquez sur le bouton Supprimer.

Vous êtes invité à supprimer le répertoire personnel de l'utilisateur ainsi que ses fichiers courrier. Lorsque vous acceptez l'invite, le répertoire personnel de l'utilisateur et ses fichiers courrier sont uniquement supprimés dans la zone globale.

4 Dans chaque zone étiquetée, supprimez manuellement les répertoires et fichiers courrier de l'utilisateur.

Remarque – Vous êtes chargé de rechercher et supprimer les fichiers temporaires de l'utilisateur à toutes les étiquettes, tels que les fichiers dans les répertoires `/tmp`.

Gestion d'autres tâches dans la Console de gestion Solaris (liste des tâches)

Suivez les procédures Oracle Solaris pour gérer les tâches dans la Console de gestion Solaris. Vous devez être superutilisateur ou dans un rôle dans la zone globale. La liste des tâches suivante fait référence à des tâches de base de la Console de gestion Solaris.

Tâche	Voir
Réalisation de tâches d'administration à l'aide de la Console de gestion Solaris.	Chapitre 2, "Working With the Solaris Management Console (Tasks)" du *System Administration Guide: Basic Administration*
Création d'utilisateurs.	"Using the Solaris Management Tools With RBAC (Task Map)" du *System Administration Guide: Basic Administration*
Création de rôles.	"How to Create and Assign a Role by Using the GUI" du *System Administration Guide: Security Services*
Modification de rôles.	"How to Change the Properties of a Role" du *System Administration Guide: Security Services*
Création ou modification d'un profil de droits.	"How to Create or Change a Rights Profile" du *System Administration Guide: Security Services*
Modification d'autres attributs de sécurité d'un utilisateur.	"How to Change the RBAC Properties of a User" du *System Administration Guide: Security Services*
Contrôle des actions d'un rôle.	"How to Audit Roles" du *System Administration Guide: Security Services*
Lister les profils de droits à l'aide de `smprofile list -D`*name-service-type*`:/`*server-name*`/`*domain-name*	*Chapitre 9, "Using Role-Based Access Control (Tasks)" du System Administration Guide: Security Services* ou la page de manuel`smprofile(1M)`

◆ ◆ ◆ CHAPITRE 8

Administration à distance dans Trusted Extensions (tâches)

Ce chapitre décrit l'utilisation des outils d'administration de Trusted Extensions pour administrer un système à distance.

Administration à distance sécurisée dans Trusted Extensions

Par défaut, Trusted Extensions n'autorise pas l'administration à distance. L'administration à distance présenterait un risque important pour la sécurité si des utilisateurs de systèmes distants non sécurisés pouvaient administrer des systèmes configurés avec Trusted Extensions. Par conséquent, les systèmes sont installés sans l'option d'administration à distance dans un premier temps.

Tant que le réseau n'est pas configuré, le modèle de sécurité `admin_low` est assigné à tous les hôtes distants. C'est pourquoi le protocole CIPSO n'est ni utilisé, ni accepté pour aucune connexion. Dans cet état d'origine, les systèmes sont protégés contre les attaques à distance par plusieurs mécanismes. Ces mécanismes incluent les paramètres `netservices`, la stratégie de connexion par défaut et la stratégie PAM.

- Lorsque le SMF (Service Management Facility, utilitaire de gestion de service) `netservices` est défini sur `limited`, aucun service distant, à l'exception du shell sécurisé, n'est activé. Toutefois, le service `ssh` ne peut pas être utilisé pour établir des connexions distantes en raison de la stratégie de connexion et de la stratégie PAM.
- Le compte `root` ne peut pas être utilisé pour établir des connexions distantes car la stratégie par défaut pour `CONSOLE` dans le fichier `/etc/default/login` empêche les connexions distantes par `root`.
- Deux paramètres PAM ont également une incidence sur les connexions à distance.

Le module `pam_roles` rejette systématiquement les connexions locales à partir des comptes de type `role`. Par défaut, ce module rejette également les connexions distantes. Cependant, vous pouvez configurer le système afin qu'il accepte les connexions à distance en spécifiant `allow_remote` dans l'entrée `pam.conf` du système.

En outre, le module `pam_tsol_account` renvoie les connexions distantes vers la zone globale, sauf lorsque le protocole CIPSO est utilisé. L'objectif de cette stratégie est de permettre l'administration à distance par un autre système Trusted Extensions.

Pour activer la fonctionnalité de connexion à distance, les deux systèmes doivent assigner leur homologue à un modèle de sécurité CIPSO. Si cette approche n'est pas pratique, la stratégie de protocole réseau peut être assouplie en spécifiant l'option `allow_unlabeled` dans le fichier `pam.conf`. Si l'une ou l'autre des stratégies est assouplie, le modèle de réseau par défaut doit être modifié afin que des machines quelconques ne puissent pas accéder à la zone globale. Le modèle `admin_low` doit être utilisé avec parcimonie et la base de données `tnrhdb` doit être modifiée afin que l'adresse générique `0.0.0.0` ne soit pas par défaut associée à l'étiquette `ADMIN_LOW`. Pour plus d'informations, reportez-vous aux sections "Administration à distance de Trusted Extensions (liste des tâches)" à la page 112 et "Procédure de limitation des hôtes pouvant être contactés sur le réseau de confiance" à la page 196.

Méthodes d'administration de systèmes distants dans Trusted Extensions

En général, les administrateurs utilisent les commandes `rlogin` et `ssh` pour administrer les systèmes distants à partir de la ligne de commande. La Console de gestion Solaris peut également être utilisée. Dans Trusted CDE, le programme `dtappsession` permet de lancer des actions Trusted CDE à distance. À partir de la version Solaris 10 5/09, un VNC peut être utilisé pour afficher un bureau multiniveau à distance.

Les méthodes d'administration à distance suivantes sont disponibles dans Trusted Extensions:

- L'utilisateur root peut se connecter à un hôte distant à partir d'un terminal. Reportez-vous à la section "Procédure de connexion à distance à partir de la ligne de commande dans Trusted Extensions" à la page 113. Cette méthode fonctionne de la même manière que sur un système Oracle Solaris. Cette méthode n'est pas sécurisée.
- Un rôle peut se connecter à un hôte distant à partir d'un terminal dans l'espace de travail du rôle. Reportez-vous à la section "Procédure de connexion à distance à partir de la ligne de commande dans Trusted Extensions" à la page 113.
- Les administrateurs peuvent démarrer un serveur Console de gestion Solaris en cours d'exécution sur un système distant. Reportez-vous à la section "Procédure d'administration à distance des systèmes à l'aide de la Console de gestion Solaris dans un système Trusted Extensions" à la page 115.

- Les actions du dossier Trusted_Extensions peuvent être démarrées à distance à l'aide de la commande `dtappsession`. Reportez-vous à la section "Procédure d'administration à distance de Trusted Extensions avec `dtappsession`" à la page 114.
- Un utilisateur peut se connecter à un bureau multiniveau distant à l'aide d'un programme client VNC afin d'accéder au serveur Xvnc sur un système Trusted Extensions. Reportez-vous à la section "Procédure d'utilisation de Xvnc afin d'accéder à distance à un système Trusted Extensions" à la page 120.

Connexion à distance par un rôle dans Trusted Extensions

Comme dans le SE Oracle Solaris, un paramètre du fichier `/etc/default/login` de chaque hôte doit être modifié pour permettre les connexions à distance. En outre, la modification du fichier `pam.conf` peut être nécessaire. Dans Trusted Extensions, l'administrateur de sécurité est responsable des modifications. Pour connaître les procédures à suivre, reportez-vous aux sections "Activation de la connexion à distance par l'utilisateur root dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions* et "Activation de la connexion à distance par un rôle dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.

Sur les hôtes Trusted Extensions comme sur les hôtes Oracle Solaris, les connexions à distance peuvent ou non requérir des autorisations. La section "Gestion des connexions à distance dans Trusted Extensions" à la page 112 décrit les types de connexions nécessitant une autorisation et les conditions. Par défaut, les rôles disposent de l'autorisation de connexion à distance.

Administration basée sur des rôles distants à partir d'hôtes sans étiquettes

Dans Trusted Extensions, les utilisateurs assument des rôles via le menu Trusted Path (Chemin de confiance). Les rôles fonctionnent ensuite dans des espaces de travail sécurisés. Par défaut, il n'est pas possible d'assumer un rôle en dehors du chemin de confiance. Si la stratégie du site le permet, l'administrateur de sécurité peut modifier la stratégie par défaut. Les administrateurs d'hôtes sans étiquette qui exécutent le logiciel client Console de gestion Solaris 2.1 peuvent alors administrer des hôtes de confiance.

- Pour modifier la stratégie par défaut, reportez-vous à la section "Activation de la connexion à distance par un rôle dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.
- Pour administrer des systèmes à distance, reportez-vous à la section "Procédure de connexion à distance à partir de la ligne de commande dans Trusted Extensions" à la page 113.

Cette modification de la stratégie s'applique uniquement lorsque l'utilisateur du système sans étiquette distant possède un compte utilisateur sur l'hôte Trusted Extensions. L'utilisateur

Trusted Extensions doit pouvoir assumer un rôle d'administration. Le rôle peut alors utiliser la Console de gestion Solaris pour administrer le système distant.

Attention – Si l'administration à distance est activée à partir d'un hôte autre que Trusted Extensions, l'environnement d'administration est moins protégé qu'un espace de travail d'administration Trusted Extensions. Soyez prudent lorsque vous saisissez des mots de passe et autres données sécurisées. Par mesure de précaution, arrêtez toutes les applications qui ne sont pas de confiance avant le démarrage de la Console de gestion Solaris.

Gestion des connexions à distance dans Trusted Extensions

Une connexion à distance entre deux hôtes Trusted Extensions est considérée comme une extension de la session de connexion en cours.

Aucune autorisation n'est nécessaire lorsque la commande `rlogin` ne vous invite pas à saisir un mot de passe. Si un fichier `/etc/hosts.equiv` ou `.rhosts` placé dans le répertoire personnel de l'utilisateur situé sur l'hôte distant contient le nom d'utilisateur ou l'hôte à partir duquel la connexion à distance est tentée, aucun mot de passe n'est nécessaire. Pour plus d'informations, reportez-vous aux pages de manuel `rhosts(4)` et `rlogin(1)`.

Pour toutes les autres connexions à distance, y compris les connexions effectuées à l'aide de la commande `ftp`, l'autorisation de connexion à distance est requise.

Pour créer un profil de droits incluant l'autorisation de connexion à distance, reportez-vous à la section “Gestion des utilisateurs et des droits à l'aide de la Console de gestion Solaris (liste des tâches) ” à la page 97.

Administration à distance de Trusted Extensions (liste des tâches)

La liste ci-dessous décrit les tâches utilisées pour administrer un système Trusted Extensions à distance.

Tâche	Description	Voir
Permettre à l'utilisateur `root` de se connecter à distance au système Trusted Extensions.	Permet à l'utilisateur `root` de travailler à distance depuis un système étiqueté.	“Activation de la connexion à distance par l'utilisateur root dans Trusted Extensions” du *Guide de configuration d'Oracle Solaris Trusted Extensions*

Tâche	Description	Voir
Permettre à un rôle de se connecter à distance au système Trusted Extensions.	Permet à n'importe quel rôle ou utilisateur de travailler à distance à partir d'un système étiqueté.	"Activation de la connexion à distance par un rôle dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions*
Permettre la connexion à distance à un système Trusted Extensions à partir d'un système sans étiquette.	Permet à n'importe quel utilisateur ou rôle de travailler à distance à partir d'un système sans étiquette.	"Activation de la connexion à distance à partir d'un système sans étiquette" du *Guide de configuration d'Oracle Solaris Trusted Extensions*
Connexion à distance à un système Trusted Extensions.	Permet de se connecter en tant que rôle à un système Trusted Extensions.	"Procédure de connexion à distance à partir de la ligne de commande dans Trusted Extensions" à la page 113
Administration à distance d'un système.	Utilise la commande `dtappsession` pour administrer le système distant à l'aide d'actions Trusted_Extensions.	"Procédure d'administration à distance de Trusted Extensions avec `dtappsession`" à la page 114
	Sur un système Trusted Extensions utilise la Console de gestion Solaris pour administrer l'hôte distant.	"Procédure d'administration à distance des systèmes à l'aide de la Console de gestion Solaris dans un système Trusted Extensions" à la page 115
	Sur un système sans étiquette, utilise la Console de gestion Solaris pour administrer les hôtes Trusted Extensions distants.	"Procédure d'administration à distance des systèmes à l'aide de la Console de gestion Solaris depuis un système sans étiquette" à la page 117
Administration et utilisation d'un système distant.	À partir de n'importe quel client, utilise le serveur Xvnc du système Trusted Extensions distant pour afficher une session multiniveau sur le client.	"Procédure d'utilisation de Xvnc afin d'accéder à distance à un système Trusted Extensions" à la page 120
Permettre à des utilisateurs spécifiques de se connecter à la zone globale.	Utilise des outils utilisateur et réseau de la Console de gestion Solaris pour autoriser des utilisateurs spécifiques à accéder à la zone globale.	"Procédure d'octroi à des utilisateurs spécifiques de l'autorisation de se connecter à distance à la zone globale dans Trusted Extensions" à la page 119

▼ Procédure de connexion à distance à partir de la ligne de commande dans Trusted Extensions

Remarque – La commande `telnet` ne peut pas être utilisée pour assumer un rôle à distance car la commande n'est pas capable de transmettre les identités primaire et de rôle au module `pam_roles`.

Avant de commencer

L'utilisateur et le rôle doivent être définis de façon identique sur le système local et le système distant.

Le rôle doit disposer de l'autorisation Remote Login (connexion à distance). Par défaut, cette autorisation se trouve dans les profils de droits Remote Administration (Administration à distance) et Maintenance and Repair (Maintenance et réparations).

L'administrateur de sécurité a effectué la procédure "Activation de la connexion à distance par un rôle dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions* sur tous les systèmes pouvant être administrés à distance. Lorsque le système peut être administré à partir d'un système sans étiquette, la procédure "Activation de la connexion à distance à partir d'un système sans étiquette" du *Guide de configuration d'Oracle Solaris Trusted Extensions* est également effectuée.

- **Dans l'espace de travail d'un utilisateur capable d'assumer un rôle, connectez-vous à l'hôte distant.**

  Utilisez la commande `rlogin`, `ssh` ou `ftp`.

  - Si vous utilisez la commande `rlogin -l` ou `ssh` pour vous connecter, toutes les commandes qui se trouvent dans les profils de droits du rôle sont disponibles.
  - Si vous utilisez la commande `ftp`, reportez-vous à page de manuel `ftp(1)` pour connaître les commandes disponibles.

▼ Procédure d'administration à distance de Trusted Extensions avec `dtappsession`

Le programme `dtappsession` permet à un administrateur d'administrer un système distant exécutant CDE.

`dtappsession` est utile lorsqu'un système distant ne possède pas d'écran. Par exemple, `dtappsession` est souvent utilisé pour administrer les domaines sur des serveurs de grande capacité. Pour plus d'informations, reportez-vous à la page de manuel `dtappsession(1)`.

Avant de commencer

Sur un système étiqueté, vous devez être dans un rôle d'administration dans la zone globale. Sur un système sans étiquette, vous devez assumer un rôle défini sur le système distant. Vous devez ensuite exécuter la connexion à distance à partir du shell du profil du rôle.

1. **(Facultatif) Créez un espace de travail dédié à la session distante.**

   Afin d'éviter toute confusion entre les applications CDE distantes et les applications locales, dédiez un espace de travail de rôle d'administration à cette procédure. Pour plus d'informations, reportez-vous à la section "Procédure d'ajout d'un espace de travail possédant une étiquette particulière" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

2 **Connectez-vous à l'hôte distant.**

Vous pouvez utiliser la commande `rlogin` ou la commande `ssh`.

```
$ ssh remote-host
```

3 **Démarrez l'administration à distance.**

Dans la fenêtre de terminal, saisissez la commande `dtappsession` suivie du nom de l'hôte local.

```
$ /usr/dt/bin/dtappsession local-host
```

Le gestionnaire d'applications (Application Manager) en cours d'exécution sur l'hôte distant s'affiche sur l'hôte local. Une boîte de dialogue Exit (Quitter) s'affiche également.

4 **Administrez l'hôte distant.**

Si vous avez appelé la session à distance à partir de Trusted CDE, vous pouvez utiliser des actions du dossier Trusted_Extensions.

5 **Lorsque vous avez terminé, cliquez sur Exit (Quitter).**

Attention – La fermeture du gestionnaire d'applications ne met pas fin à la session de connexion et sa fermeture est déconseillée.

6 **Dans la fenêtre de terminal, quittez la session de connexion à distance.**

Utilisez ensuite la commande `hostname` pour vérifier que vous vous trouvez bien sur votre hôte local.

```
$ exit
$ hostname
local-host
```

▼ Procédure d'administration à distance des systèmes à l'aide de la Console de gestion Solaris dans un système Trusted Extensions

La Console de gestion Solaris fournit une interface d'administration à distance pour la gestion des utilisateurs, des droits, des rôles et du réseau. Pour l'utiliser, vous devez assumer un rôle. Durant cette procédure, vous devez lancer la console sur le système local et indiquer le système distant comme serveur.

Avant de commencer

Vous avez effectué les procédures suivantes :

- Sur les deux systèmes : "Initialisation du serveur Console de gestion Solaris dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions*
- Sur le système distant : "Activation de la connexion à distance par un rôle dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions* et "Activation de la Console de gestion Solaris afin qu'elle accepte les communications réseau" du *Guide de configuration d'Oracle Solaris Trusted Extensions*
- Sur le système distant utilisé en tant que serveur LDAP : "Configuration de la Console de gestion Solaris pour LDAP (liste des tâches)" du *Guide de configuration d'Oracle Solaris Trusted Extensions*

1. **Connectez-vous au système local à l'aide du rôle de l'utilisateur défini de façon identique sur le système distant.**

2. **Assumez le rôle que vous avez l'intention d'utiliser pour administrer le système.**

3. **Dans le rôle, démarrez la Console de gestion Solaris.**

   Pour plus d'informations, reportez-vous à la section "Initialisation du serveur Console de gestion Solaris dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.

   a. **Dans la boîte de dialogue Server (Serveur), saisissez le nom du serveur distant.**

      - **Si vous utilisez LDAP comme service de nommage, saisissez le nom du serveur LDAP.**

        Choisissez ensuite l'une des étendues suivantes.

        - **Pour administrer les bases de données dans le service de nommage, choisissez la boîte à outils `Scope=LDAP`.**

          `Cet ordinateur (`*ldap-server* `: Scope=LDAP, Policy=TSOL)`

        - **Pour administrer les fichiers locaux sur le serveur LDAP, choisissez la boîte à outils `Scope=Files`.**

          `Cet ordinateur (`*ldap-server* `: Scope=Files, Policy=TSOL)`

      - **Si vous n'utilisez pas LDAP en tant que service de nommage, saisissez le nom du système distant que vous souhaitez administrer.**

        Choisissez ensuite la boîte à outils `Scope=Files`.

        `Cet ordinateur (`*remote-system* `: Scope=Files, Policy=TSOL)`

4 **Sélectionnez un outil sous System Configuration (Configuration du système).**

Lorsque vous sélectionnez un outil tel que User (Utilisateur), une boîte de dialogue affiche le nom de serveur de la Console de gestion Solaris, votre nom d'utilisateur, votre nom de rôle ainsi qu'un espace pour la saisie du mot de passe du rôle. Assurez-vous que les entrées sont correctes.

5 **Connectez-vous au serveur de la Console de gestion Solaris à l'aide du rôle défini de façon identique sur le système local et le système distant.**

Saisissez le mot de passe du rôle, puis appuyez sur Login as Role (Connexion à l'aide d'un rôle). Vous pouvez maintenant utiliser la Console de gestion Solaris pour gérer le système.

Remarque – Bien qu'il soit possible d'utiliser la Console de gestion Solaris pour exécuter `dtappsession`, le moyen le plus simple d'utiliser `dtappsession` est décrit dans la section "Procédure d'administration à distance de Trusted Extensions avec `dtappsession`" à la page 114.

▼ Procédure d'administration à distance des systèmes à l'aide de la Console de gestion Solaris depuis un système sans étiquette

Dans le cadre de cette procédure, vous exécutez le client et le serveur de la Console de gestion Solaris sur le système distant et vous affichez la console sur le système local.

Avant de commencer

Le système Trusted Extensions doit avoir assigné l'étiquette `ADMIN_LOW` au système local.

Remarque – Un système qui n'exécute pas le protocole CIPSO, tel qu'un système Trusted Solaris, est considéré comme un système sans étiquette pour le système Trusted Extensions.

Le serveur de la Console de gestion Solaris du système distant doit être configuré pour accepter la connexion à distance. Pour connaître la procédure, reportez-vous à la section "Activation de la Console de gestion Solaris afin qu'elle accepte les communications réseau" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.

Les deux systèmes doivent avoir le même utilisateur, auquel le même rôle permettant d'utiliser la Console de gestion Solaris doit être assigné. La plage d'étiquettes de l'utilisateur peut être celle d'un utilisateur standard mais son rôle doit posséder la plage allant de `ADMIN_LOW` à `ADMIN_HIGH`.

Vous devez être dans un rôle d'administration dans la zone globale.

1. **Activez le serveur X local pour afficher la Console de gestion Solaris distante.**

   ```
   # xhost + TX-SMC-Server
   # echo $DISPLAY
   :n.n
   ```

2. **Sur le système local, devenez l'utilisateur autorisé à assumer un rôle pour la Console de gestion Solaris.**

   ```
   # su - same-username-on-both-systems
   ```

3. **Sous l'identité de cet utilisateur, connectez-vous au serveur distant en tant que rôle.**

   ```
   $ rlogin -l same-rolename-on-both-systems TX-SMC-Server
   ```

4. **Assurez-vous que les valeurs des variables d'environnement utilisées par la Console de gestion Solaris sont correctes.**

   a. **Définissez la valeur de la variable `DISPLAY`.**

      ```
      $ DISPLAY=local:n.n
      $ export DISPLAY=local:n.n
      ```

   b. **Définissez la valeur de la variable `LOGNAME` sur le nom d'utilisateur.**

      ```
      $ LOGNAME=same-username-on-both-systems
      $ export LOGNAME=same-username-on-both-systems
      ```

   c. **Définissez la valeur de la variable `USER` sur le nom du rôle.**

      ```
      $ USER=same-rolename-on-both-systems
      $ export USER=same-rolename-on-both-systems
      ```

5. **Dans le rôle, démarrez la Console de gestion Solaris à partir de la ligne de commande.**

   ```
   $ /usr/sbin/smc &
   ```

6. **Sélectionnez un outil sous System Configuration (Configuration du système).**

   Lorsque vous sélectionnez un outil tel que User (Utilisateur), une boîte de dialogue affiche le nom de serveur de la Console de gestion Solaris, votre nom d'utilisateur, votre nom de rôle ainsi qu'un espace pour la saisie du mot de passe du rôle. Assurez-vous que les entrées sont correctes.

7. **Connectez-vous au serveur à l'aide du rôle.**

   Saisissez le mot de passe du rôle, puis appuyez sur Login as Role (Connexion à l'aide d'un rôle). Vous pouvez maintenant utiliser la Console de gestion Solaris pour gérer le système.

Remarque – Lorsque vous tentez d'accéder à des informations de base de données réseau à partir d'un système autre que le serveur LDAP, l'opération échoue. La console vous permet de vous connecter à l'hôte distant et d'ouvrir la boîte à outils. Cependant, lorsque vous tentez d'accéder aux informations ou de les modifier, le message d'erreur suivant indique que vous avez sélectionné `Scope=LDAP` sur un système qui n'est pas le serveur LDAP :

```
Management server cannot perform the operation requested.
...
Error extracting the value-from-tool.
The keys received from the client were machine, domain, Scope.
Problem with Scope.
```

▼ Procédure d'octroi à des utilisateurs spécifiques de l'autorisation de se connecter à distance à la zone globale dans Trusted Extensions

La plage d'étiquettes par défaut de l'utilisateur et le comportement par défaut de la zone sont modifiés pour permettre la connexion à distance d'un utilisateur sans rôle. Vous pouvez être amené à effectuer cette procédure pour un testeur utilisant un système étiqueté distant. Pour des raisons de sécurité, le système du testeur doit exécuter une étiquette disjointe de celle des autres utilisateurs.

Avant de commencer

Vous devez avoir une très bonne raison de laisser cet utilisateur se connecter à la zone globale.

Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

1. **Pour permettre à des utilisateurs spécifiques de se connecter à la zone globale, assignez-leur une plage d'étiquettes d'administration.**

   Utilisez la Console de gestion Solaris pour assigner une autorisation `ADMIN_HIGH` et une étiquette minimale de `ADMIN_LOW` à chaque utilisateur. Pour plus d'informations, reportez-vous à la section "Procédure de modification de la plage d'étiquettes d'un utilisateur dans la Console de gestion Solaris " à la page 98.

   Les zones étiquetées de l'utilisateur doivent elles aussi permettre la connexion.

2. **Pour autoriser la connexion à distance dans la zone globale à partir d'une zone étiquetée, procédez comme suit :**

   a. **Ajoutez un port multiniveau pour la connexion à distance à la zone globale.**

      Utilisez la Console de gestion Solaris. Le port 513 sur le protocole TCP permet la connexion à distance. Pour un exemple, reportez-vous à la section "Procédure de création d'un port multiniveau pour une zone" à la page 146.

b. Intégrez les modifications `tnzonecfg` dans le noyau.

```
# tnctl -fz /etc/security/tsol/tnzonecfg
```

c. Redémarrez le service de connexion à distance.

```
# svcadm restart svc:/network/login:rlogin
```

▼ Procédure d'utilisation de Xvnc afin d'accéder à distance à un système Trusted Extensions

La technologie VNC (Virtual Network Computing) connecte un client à un serveur distant et affiche le bureau du serveur distant dans une fenêtre sur le client. Xvnc est la version UNIX de VNC, laquelle est basée sur un serveur X standard. Trusted Extensions, permet aux clients de n'importe quelle plate-forme de se connecter à un programme Xvnc exécutant le logiciel Trusted Extensions d'accéder au serveur Xvnc et de visualiser et travailler dans un bureau multiniveau.

Avant de commencer

Vous avez installé et configuré le logiciel Trusted Extensions sur le système qui sera utilisé en tant que serveur Xvnc. Vous avez créé et initialisé les zones étiquetées. Votre serveur Xvnc reconnaît les clients VNC par nom d'hôte ou adresse IP.

Vous êtes superutilisateur dans la zone globale du système qui sera utilisé en tant que serveur Xvnc.

1 Configurez le serveur Xvnc.

Pour plus d'informations, reportez-vous aux pages de manuel `Xvnc`(1) et `vncconfig`(1).

Attention – Si vous exécutez la version Solaris 10 10/08 ou Solaris 10 5/08, vous devez mettre à niveau votre système avant de configurer le serveur. Pour un système SPARC, installez la dernière version du patch 125719. Pour un système x86, installez la dernière version du patch 125720.

a. Créez le répertoire de configuration Xservers.

```
# mkdir -p /etc/dt/config
```

b. Copiez le fichier `/usr/dt/config/Xservers` dans le répertoire `/etc/dt/config`.

```
# cp /usr/dt/config/Xservers /etc/dt/config/Xservers
```

c. Modifiez le fichier `/etc/dt/config/Xservers` pour démarrer le programme Xvnc plutôt que Xserver ou Xorg.

Dans cet exemple, l'entrée est configurée pour permettre la connexion au serveur sans mot de passe. Pour réussir à se connecter au bureau, l'UID local doit être `none` au lieu de `console`.

L'entrée est fractionnée pour permettre son affichage. L'entrée doit être sur une seule ligne.

```
#   :0  Local local_uid@console root /usr/X11/bin/Xserver :0 -nobanner
  :0  Local local_uid@none root /usr/X11/bin/Xvnc :0 -nobanner
  -AlwaysShared -SecurityTypes None -geometry 1024x768x24 -depth 24
```

Remarque – Une configuration plus sûre consiste à exiger un mot de passe à l'aide du paramètre `-SecurityTypes VncAuth`. La page de manuel `Xvnc(1)` décrit les exigences de mot de passe.

---

d. Redémarrez le serveur ou démarrez le serveur Xvnc.

```
# reboot
```

Après le redémarrage, assurez-vous que le programme Xvnc est en cours d'exécution.

```
# ps -ef | grep Xvnc
  root  2145  932  0  Jan 18 ?  6:15 /usr/X11/bin/Xvnc :0 -nobanner
  -AlwaysShared -SecurityTypes None -geometry 1024
```

2 Sur chaque client VNC du serveur Xvnc de Trusted Extensions, installez le logiciel client VNC.

Pour le système client, vous disposez d'un choix de logiciels. Cet exemple utilise le logiciel Sun VNC.

```
# cd SUNW-pkg-directory
# pkgadd -d . SUNWvncviewer
```

3 Dans une fenêtre de terminal sur un client VNC, connectez-vous au serveur.

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

4 Dans la fenêtre qui s'affiche, saisissez votre nom et votre mot de passe.

Poursuivez la procédure de connexion. Pour une description des étapes restantes, reportez-vous à la section "Connexion à Trusted Extensions" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

Si vous vous êtes connecté au serveur en tant que superutilisateur, vous pouvez l'administrer directement. Si vous vous êtes connecté au serveur en tant qu'utilisateur, vous devez assumer un rôle pour administrer le système.

◆ ◆ ◆ CHAPITRE 9

Trusted Extensions et LDAP (présentation)

Ce chapitre décrit l'utilisation d'Oracle Directory Server Enterprise Edition (serveur d'annuaire) pour un système configuré avec Trusted Extensions.

Utilisation d'un service de nommage dans Trusted Extensions

Pour uniformiser les attributs d'utilisateur, d'hôte et de réseau au sein d'un domaine de sécurité comprenant plusieurs systèmes Trusted Extensions, un service de nommage est utilisé pour distribuer la plupart des informations de configuration. LDAP est un exemple de service de nommage. Le fichier `nsswitch.conf` détermine le service de nommage utilisé. Dans Trusted Extensions, le service de nommage recommandé est LDAP

Le serveur d'annuaire peut fournir le service de nommage LDAP pour les clients Trusted Extensions et Oracle Solaris. Le serveur doit inclure les bases de données réseau Trusted Extensions et les clients Trusted Extensions doivent se connecter au serveur par l'intermédiaire d'un port multiniveau. L'administrateur de sécurité indique le port multiniveau lors de la configuration de Trusted Extensions.

Trusted Extensions ajoute deux bases de données réseau de confiance au serveur LDAP : `tnrhdb` et `tnrhtp`. Ces bases de données sont administrées à l'aide de l'outil Security Templates (Modèles de sécurité) de la Console de gestion Solaris. Une boîte à outils de `Scope=LDAP, Policy=TSOL` enregistre les modifications de configuration sur le serveur d'annuaire.

- Pour plus d'informations sur l'utilisation du service de nommage LDAP dans le SE Oracle Solaris, reportez-vous au *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*.
- La configuration du serveur d'annuaire pour les clients Trusted Extensions est décrite dans le *Guide de configuration d'Oracle Solaris Trusted Extensions*. Les systèmes Trusted Extensions peuvent être clients d'un serveur LDAP Oracle Solaris s'ils utilisent un serveur proxy LDAP configuré à l'aide de Trusted Extensions.

Remarque – Les systèmes configurés à l'aide de Trusted Extensions ne peuvent pas être des clients de serveurs maître NIS ou NIS+.

Systèmes Trusted Extensions sans réseau

Lorsqu'aucun service de nommage n'est pas utilisé sur un site, les administrateurs doivent s'assurer que les informations de configuration des utilisateurs, des hôtes et des réseaux sont identiques sur tous les hôtes. Lorsqu'une modification est effectuée sur un hôte, elle doit être effectuée sur tous les hôtes.

Sur un système Trusted Extensions sans réseau, les informations de configuration sont conservées dans les répertoires `/etc`, `/etc/security` et `/etc/security/tsol`. Les actions contenues dans le dossier Trusted_Extensions vous permettent de modifier certaines informations de configuration. L'outil Security Templates (Modèles de sécurité) de la Console de gestion Solaris vous permet de modifier les paramètres de la base de données réseau. Les utilisateurs, les rôles et les droits sont modifiés dans les outils User Accounts (Comptes utilisateur), Administrative Roles (Rôles administratifs) et Rights (Droits). Une boîte à outils sur le poste de travail avec `Scope=Files, Policy=TSOL` enregistre les modifications de configuration en local.

Bases de données LDAP Trusted Extensions

Trusted Extensions étend le schéma du serveur d'annuaire pour inclure les bases de données `tnrhdb` et `tnrhtp`. Trusted Extensions définit deux nouveaux attributs : `iptnetnumber` et `iptnettemplatename` , et deux nouvelles classes d'objets : `iptnettemplate` et `iptnethost`.

Les définitions d'attributs se présentent comme suit :

```
ipTnetNumber
   ( 1.3.6.1.1.1.1.34 NAME 'ipTnetNumber'
     DESC 'Trusted network host or subnet address'
```

```
     EQUALITY caseExactIA5Match
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
     SINGLE-VALUE )

ipTnetTemplateName
   ( 1.3.6.1.1.1.1.35 NAME 'ipTnetTemplateName'
     DESC 'Trusted network template name'
     EQUALITY caseExactIA5Match
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
     SINGLE-VALUE )
```

Les définitions de classes d'objets se présentent comme suit :

```
ipTnetTemplate
   ( 1.3.6.1.1.1.2.18 NAME 'ipTnetTemplate' SUP top STRUCTURAL
     DESC 'Object class for Trusted network host templates'
     MUST ( ipTnetTemplateName )
     MAY ( SolarisAttrKeyValue ) )

ipTnetHost
   ( 1.3.6.1.1.1.2.19 NAME 'ipTnetHost' SUP top AUXILIARY
     DESC 'Object class for Trusted network host/subnet address
           to template mapping'
     MUST ( ipTnetNumber $ ipTnetTemplateName ) )
```

La définition du modèle `cipso` dans LDAP se présente comme suit :

```
ou=ipTnet,dc=example,dc=example1,dc=exampleco,dc=com
 objectClass=top
 objectClass=organizationalUnit
 ou=ipTnet

 ipTnetTemplateName=cipso,ou=ipTnet,dc=example,dc=example1,dc=exampleco,dc=com
 objectClass=top
 objectClass=ipTnetTemplate
 ipTnetTemplateName=cipso
 SolarisAttrKeyValue=host_type=cipso;doi=1;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH;

 ipTnetNumber=0.0.0.0,ou=ipTnet,dc=example,dc=example1,dc=exampleco,dc=com
 objectClass=top
 objectClass=ipTnetTemplate
 objectClass=ipTnetHost
 ipTnetNumber=0.0.0.0
 ipTnetTemplateName=internal
```

Utilisation du service de nommage LDAP dans Trusted Extensions

Le service de nommage LDAP est géré dans Trusted Extensions de la même manière que dans le SE Oracle Solaris. L'exemple ci-dessous illustre les commandes utiles et contient des références à des informations plus détaillées.

- Pour connaître les stratégies de résolution des problèmes de configuration LDAP, reportez-vous au Chapitre 13, "LDAP Troubleshooting (Reference)" du *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.
- Pour dépanner les problèmes de connexion LDAP du client au serveur causés par des étiquettes, reportez-vous à la section "Procédure de débogage d'une connexion client au serveur LDAP" à la page 211.
- Pour dépanner les problèmes de connexion LDAP du client au serveur, reportez-vous au Chapitre 13, "LDAP Troubleshooting (Reference)" du *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.
- Pour afficher des entrées LDAP à partir d'un client LDAP, saisissez :

```
$ ldaplist -l
$ ldap_cachemgr -g
```

- Pour afficher des entrées LDAP à partir d'un serveur LDAP, saisissez :

```
$ ldap_cachemgr -g
$ idsconfig -v
```

- Pour afficher la liste des hôtes gérés par LDAP, saisissez :

```
$ ldaplist -l hosts      Long listing
$ ldaplist hosts         One-line listing
```

- Pour afficher la liste des informations dans l'arborescence des informations d'annuaire (DIT, Directory Information Tree) sur LDAP, saisissez :

```
$ ldaplist -l services | more
dn: cn=apocd+ipServiceProtocol=udp,ou=Services,dc=exampleco,dc=com
  objectClass: ipService
  objectClass: top
  cn: apocd
  ipServicePort: 38900
  ipServiceProtocol: udp

...
$ ldaplist services name
dn=cn=name+ipServiceProtocol=udp,ou=Services,dc=exampleco,dc=com
```

- Pour afficher l'état du service LDAP sur le client, saisissez :

```
# svcs -xv network/ldap/client
svc:/network/ldap/client:default (LDAP client)
 State: online since date
   See: man -M /usr/share/man -s 1M ldap_cachemgr
   See: /var/svc/log/network-ldap-client:default.log
Impact: None.
```

- Pour démarrer et arrêter le client LDAP, saisissez :

  ```
  # svcadm enable network/ldap/client
  ```

  ```
  # svcadm disable network/ldap/client
  ```

- Pour démarrer et arrêter le serveur LDAP dans la version 5.2 du logiciel Oracle Directory Server Enterprise Edition, saisissez :

  ```
  # installation-directory/slap-LDAP-server-hostname/start-slapd
  # installation-directory/slap-LDAP-server-hostname/stop-slapd
  ```

- Pour démarrer et arrêter le serveur LDAP dans la version 6 du logiciel Oracle Directory Server Enterprise Edition, saisissez :

  ```
  # dsadm start /export/home/ds/instances/your-instance
  # dsadm stop /export/home/ds/instances/your-instance
  ```

- Pour démarrer et arrêter un serveur proxy LDAP dans la version 6 du logiciel Oracle Directory Server Enterprise Edition, saisissez :

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

◆ ◆ ◆ CHAPITRE 10

Gestion des zones dans Trusted Extensions (tâches)

Ce chapitre décrit le fonctionnement des zones non globales sur un système configuré avec Trusted Extensions. Les procédures spécifiques aux zones de Trusted Extensions y sont également décrites.

Zones dans Trusted Extensions

Un système Trusted Extensions correctement configuré comprend une zone globale, qui correspond à l'instance du système d'exploitation, et une ou plusieurs zones étiquetées non globales. Lors de la configuration, Trusted Extensions joint une étiquette unique à chaque zone et crée ainsi des zones étiquetées. Les étiquettes proviennent du fichier `label_encodings`. Les administrateurs peuvent créer une zone pour chaque étiquette, mais cela n'est pas obligatoire. Un système peut comporter plus d'étiquettes que de zones étiquetées. Il n'est pas possible d'avoir plus de zones étiquetées que d'étiquettes.

Sur un système Trusted Extensions, les systèmes de fichiers d'une zone sont généralement montés en tant que systèmes de fichiers en loopback (LOFS). Tous les fichiers et répertoires accessibles en écriture d'une zone étiquetée ont l'étiquette de la zone. Par défaut, un utilisateur peut visualiser les fichiers appartenant à une zone dont le niveau d'étiquette est inférieur à celui de l'étiquette actuelle de l'utilisateur. Cette configuration permet aux utilisateurs de visualiser leurs répertoires personnels correspondant à des étiquettes de niveau inférieur par rapport à celle de l'espace de travail actuel. Bien que les utilisateurs puissent visualiser les fichiers correspondant à un niveau inférieur, ils ne peuvent pas les modifier. Les utilisateurs peuvent uniquement modifier les fichiers à partir d'un processus de même étiquette que les fichiers concernés.

Dans Trusted Extensions, la zone globale est une zone d'administration. Les zones étiquetées sont destinées aux utilisateurs standard. Les utilisateurs peuvent travailler dans une zone dont l'étiquette est comprise dans la plage d'accréditations de l'utilisateur.

Chaque zone est associée à une adresse IP et à des attributs de sécurité. Une zone peut être configurée avec des ports multiniveau (les MLP). En outre, une zone peut être configurée avec une stratégie relative aux diffusions ICMP (Internet Control Message Protocol), telles que `ping`.

Pour plus d'informations sur le partage de répertoires d'une zone étiquetée et sur le montage à distance de répertoires depuis des zones étiquetées, reportez-vous au Chapitre 11, “Gestion et montage de fichiers dans Trusted Extensions (tâches)”.

Les zones de Trusted Extensions sont basées sur le produit de zones d'Oracle Solaris. Pour plus d'informations, reportez-vous à la section Partie II, “Zones” du *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*. Trusted Extensions est notamment concerné par les problèmes liés à l'installation de packages et de correctifs. Pour plus d'informations, reportez-vous à la section Chapitre 25, “About Packages and Patches on a Solaris System With Zones Installed (Overview)” du *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones* et au Chapitre 30, “Troubleshooting Miscellaneous Solaris Zones Problems” du *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*.

Zones et adresses IP dans Trusted Extensions

Votre équipe de configuration initiale a assigné des adresses IP à la zone globale et aux zones étiquetées. Trois types de configurations sont décrits à la section “Création de zones étiquetées” du *Guide de configuration d'Oracle Solaris Trusted Extensions* :

- Le système dispose d'une adresse IP pour la zone globale et toutes les zones étiquetées.

  Cette configuration est utile sur un système qui utilise le logiciel DHCP pour déterminer son adresse IP. Un serveur LDAP peut avoir cette configuration si aucun utilisateur ne doit s'y connecte.

- Le système dispose d'une adresse IP pour la zone globale et d'une adresse IP partagée par toutes les zones, y compris par la zone globale. N'importe quelle zone peut combiner une adresse unique et une adresse partagée.

  Cette configuration est utile sur des systèmes auxquels des utilisateurs standard se connectent. Elle peut également être utilisée pour une imprimante ou un serveur NFS. Cette configuration conserve les adresses IP.

- Le système dispose d'une adresse IP pour la zone globale et chaque zone étiquetée possède une adresse IP unique.

  Cette configuration est utile pour permettre l'accès à des réseaux physiques distincts sur des systèmes à niveau unique. En règle générale, chaque zone possède une adresse IP sur un réseau physique distinct de celui des autres zones étiquetées. Dans la mesure où cette

configuration est mise en œuvre avec une instance IP unique, la zone globale contrôle les interfaces physiques et gère les ressources globales, telles que la table de routage.

Avec l'introduction d'instances IP exclusives pour une zone non globale, un quatrième type de configuration est disponible dans le SE Oracle Solaris. À partir de la version Solaris 10 8/07 une zone non globale peut se voir attribuer sa propre instance IP et gérer ses propres interfaces physiques. Dans cette configuration, chaque zone fonctionne comme si elle constituait un système distinct. Pour plus d'informations, reportez-vous à la section "Zone Network Interfaces" du *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*.

Cependant, dans une telle configuration, chaque zone étiquetée fonctionne comme si elle constituait un système à étiquette unique distinct. Les fonctions de mise en réseau multiniveau de Trusted Extensions s'appuient sur les fonctions d'une pile IP partagée. Les procédures d'administration dans Trusted Extensions supposent que la gestion de réseaux soit entièrement contrôlée par la zone globale. Par conséquent, si votre équipe de configuration initiale a installé des zones étiquetées avec des instances IP exclusives, vous devez fournir ou vous reporter à la documentation spécifique du site.

Zones et ports multiniveau

Par défaut, une zone ne peut pas envoyer ni recevoir des paquet vers ni depuis une autre zone. Les ports multiniveau (les MLP) permettent à certains services particuliers sur un port d'accepter des demandes correspondant à une plage d'étiquettes ou à un jeu d'étiquettes donné. Ces services privilégiés peuvent répondre sous l'étiquette de la demande. Vous pouvez par exemple souhaiter créer un port de navigateur Web privilégié capable d'écouter sur toutes les étiquettes, mais dont les réponses sont limitées en fonction de l'étiquette. Par défaut, les zones étiquetées n'ont pas de MLP.

La plage d'étiquettes ou l'ensemble d'étiquettes qui limite les paquets pouvant être acceptés par le MLP dépend de l'adresse IP de la zone. Un modèle d'hôte distant est assigné à l'adresse IP dans la base de données `tnrhdb`. La plage d'étiquettes ou l'ensemble d'étiquettes du modèle d'hôte distant limite les paquets que le MLP peut accepter.

- Les contraintes qui s'appliquent aux MPL pour les différentes configurations d'adresse IP sont les suivantes :
- Sur un système sur lequel la zone globale a une adresse IP et chacune des zones étiquetées une adresse IP unique, un MLP pour un service particulier peut être ajouté à chaque zone. Par exemple, le système peut être configuré de manière à ce que le service `ssh` soit, par le biais du port TCP 22, un MLP dans la zone globale et dans chaque zone étiquetée.
- Dans une configuration standard, une adresse IP est attribuée à la zone globale et les zones étiquetées partagent une seconde adresse IP avec la zone globale. Lorsqu'un MLP est ajouté à une interface partagée, le paquet du service est acheminé vers la zone étiquetée où le MLP est défini. Le paquet n'est accepté que si le modèle de l'hôte distant pour la zone étiquetée

inclut l'étiquette du paquet. Lorsque la plage est comprise entre `ADMIN_LOW` et `ADMIN_HIGH`, tous les paquets sont acceptés. Lorsque la plage d'étiquettes est plus restreinte, les paquets dont l'étiquette n'est pas comprise dans la plage sont rejetés.

Au mieux, une zone peut définir un port particulier en tant que MLP sur une interface partagée. Dans le scénario précédent, où le port `ssh` était configuré en tant que MLP partagé dans une zone non globale, aucune autre zone ne peut recevoir de connexions `ssh` sur l'adresse partagée. Toutefois, la zone globale pourrait définir le port `ssh` en tant que MLP privé pour la réception de connexions sur son adresse spécifique de zone.

- Sur un système où la zone globale et les zones étiquetées partagent une adresse IP, un MLP pour le service `ssh` pourrait être ajouté à une zone. Si le programme MLP pour `ssh` est ajouté à la zone globale, aucune zone étiquetée ne peut ajouter de MLP pour le service `ssh`. De même, si le MLP du service `ssh` est ajouté à une zone étiquetée, la zone globale ne peut pas être configurée avec un MLP `ssh`.

Pour voir un exemple d'ajout de MLP aux zones étiquetées, consultez l'Exemple 13–16.

Zones et ICMP dans Trusted Extensions

Les réseaux transmettent des messages de diffusion et envoient des paquets ICMP aux systèmes du réseau. Sur un système multiniveau, ces transmissions risquent d'inonder le système sous chaque étiquette. Par défaut, la stratégie réseau des zones étiquetées exige que les paquets ICMP soient uniquement reçus sous l'étiquette correspondante.

Processus de zone globale et zones étiquetées

Dans Trusted Extensions, la stratégie MAC s'applique à tous les processus, y compris aux processus de la zone globale. Les processus de la zone globale s'exécutent sous l'étiquette `ADMIN_HIGH`. Lorsque des fichiers provenant d'une zone globale sont partagés, ils sont partagés avec l'étiquette `ADMIN_LOW`. Par conséquent, étant donné que MAC empêche le processus d'une étiquette de niveau supérieur de modifier un objet de niveau inférieur, la zone globale ne peut généralement pas écrire sur un système monté via NFS.

Toutefois, dans certains cas limités, des actions effectuées dans une zone étiquetée peuvent nécessiter qu'un processus de la zone globale modifie un fichier de la zone concernée.

Pour permettre à un processus de la zone globale de monter un système de fichiers distant avec des autorisations de lecture/écriture, le montage doit être placé sous le chemin de zone de la zone dont l'étiquette correspond à celle du système de fichiers distant. Toutefois, il ne doit pas être monté sous le chemin racine de la zone concernée.

- Le système effectuant le montage doit comporter une zone possédant la même étiquette que le système de fichiers distant.

- Le système doit monter le système de fichiers distant sous le chemin de zone de la zone étiquetée possédant la même étiquette.

  Le système *ne doit pas* monter le système de fichiers distant sous le *chemin racine de zone* de la zone étiquetée possédant la même étiquette.

Prenons l'exemple d'une zone nommée `publique` possédant l'étiquette `PUBLIC`. Le *chemin de la zone* est `/zone/public/`. Tous les répertoires placés sous le chemin de la zone ont l'étiquette `PUBLIC`, comme dans :

```
/zone/public/dev
/zone/public/etc
/zone/public/home/username
/zone/public/root
/zone/public/usr
```

Parmi les fichiers placés dans les répertoires qui se trouvent sous le chemin de zone, seuls les fichiers subordonnés à `/zone/public/root` sont visibles depuis la zone publique. Les autres fichiers et répertoires d'étiquette `PUBLIC` sont uniquement accessibles à partir de la zone globale. Le chemin `/zone/public/root` est le *chemin racine de la zone*.

Pour l'administrateur de la zone publique, le chemin racine de la zone est identifié par `/`. De même, l'administrateur de la zone publique ne peut pas accéder au répertoire personnel d'un utilisateur dans le chemin de la zone, répertoire `/zone/public/home/`*nom de l'utilisateur*. Ce répertoire est uniquement visible depuis la zone globale. La zone publique monte ce répertoire dans le chemin racine de la zone en tant que `/home/`*nom de l'utilisateur*. Depuis la zone globale, ce montage est visible sous la forme `/zone/public/root/home/`*nom de l'utilisateur*.

L'administrateur de la zone publique peut modifier `/home/`*nom de l'utilisateur*. Lorsque les fichiers du répertoire personnel d'un utilisateur doivent être modifiés, un processus de zone globale n'utilise pas le chemin cité ci-dessus. La zone globale utilise le répertoire personnel de l'utilisateur, dans le chemin de la zone, `/zone/public/Home/`*nom de l'utilisateur*.

- Les fichiers et répertoires qui se trouvent sous le chemin de la zone, `/zone/`*nom de zone*`/`, mais pas sous le chemin racine de la zone, le répertoire `/zone/`*nom de la zone*`/root` , peuvent être modifiés par un processus de la zone globale qui s'exécute sous l'étiquette `ADMIN_HIGH`.
- Les fichiers et répertoires qui se trouvent sous le chemin racine de la zone, `/zone/public/root`, peuvent être modifiés par l'administrateur de la zone étiquetée.

Par exemple, lorsqu'un utilisateur alloue un périphérique dans la zone publique, un processus de la zone globale exécuté sous l'étiquette `ADMIN_HIGH` modifie le répertoire `dev` dans le chemin de la zone, `/zone/public/dev`. De même, lorsqu'un utilisateur enregistre une configuration du bureau, le fichier de configuration du bureau est modifié par un processus de la zone globale dans `/zone/public/Home/`*nom de l'utilisateur*. Enfin, pour partager des fichiers provenant d'une zone étiquetée, l'administrateur de la zone globale crée le fichier de configuration `dfstab` dans le chemin de la zone `/zone/public/etc/dfs/dfstab`. L'administrateur d'une zone étiquetée ne peut pas accéder à ce fichier ni partager des fichiers provenant de la zone étiquetée.

Pour partager un répertoire étiqueté, reportez-vous à la section "Procédure de partage de répertoires à partir d'une zone étiquetée" à la page 157.

Utilitaires d'administration des zones dans Trusted Extensions

Certaines tâches d'administration des zones peuvent être exécutées à partir de la ligne de commande. Cependant, la méthode d'administration des zones la plus simple consiste à utiliser les interfaces graphiques fournies dans Trusted Extensions :

- La configuration des attributs de sécurité des zones s'effectue à l'aide de l'outil Trusted Network Zones (Zones de réseau de confiance) de la Console de gestion Solaris. Pour une description de l'outil, reportez-vous à la section "Outil Trusted Network Zones" à la page 43. Pour des exemples de création et de configuration de zones, reportez-vous au Chapitre 4, "Configuration de Trusted Extensions (tâches)" du *Guide de configuration d'Oracle Solaris Trusted Extensions* et à la section "Procédure de création d'un port multiniveau pour une zone" à la page 146.
- Le script shell, `/usr/sbin/txzonemgr`, fournit un assistant basé sur les menus pour la création, l'installation et l'initialisation et le démarrage des zones. Si vous administrez les zones à partir de Solaris Trusted Extensions (JDS), utilisez le script `txzonemgr` plutôt que les actions Trusted CDE. `txzonemgr` utilise la commande `zenity`. Pour plus d'informations, reportez-vous à la page de manuel `zenity`(1).
- Dans Trusted CDE, la configuration et la création de zones peut être effectuée à l'aide des actions du dossier Trusted_Extensions. Pour une description des actions, reportez-vous à la section "Actions Trusted CDE" à la page 37. Pour connaître les procédures qui utilisent les actions, reportez-vous à la section "Démarrage d'actions d'administration CDE dans Trusted Extensions " à la page 58.

Gestion des zones (liste des tâches)

La liste ci-dessous décrit les tâches de gestion des zones qui sont spécifiques à Trusted Extensions. Elle contient également des liens vers des procédures courantes qui s'effectuent de la même manière dans Trusted Extensions que sur un système Oracle Solaris.

Tâche	Description	Voir
Visualisation de toutes les zones.	À n'importe quelle étiquette, affiche les zones dominées par la zone en cours.	"Procédure d'affichage des zones prêtes ou en cours d'exécution" à la page 136
Visualisation des répertoires montés.	À n'importe quelle étiquette, affiche les répertoires dominés par l'étiquette en cours.	"Procédure d'affichage des étiquettes de fichiers montés" à la page 137

Tâche	Description	Voir
Activation de la visualisation d'un fichier `/etc` pour des utilisateurs standard.	Monte en loopback à partir de la zone globale un répertoire ou un fichier qui n'est pas visible par défaut dans une zone globale.	"Procédure de montage en loopback d'un fichier qui n'est généralement pas visible dans une zone étiquetée" à la page 139
Désactivation de la visualisation par les utilisateurs standard d'un répertoire personnel de niveau inférieur à partir d'une étiquette supérieure.	Par défaut, les répertoires de niveau inférieur sont visibles depuis les zones de niveau supérieur. Lorsque vous désactivez le montage d'une zone de niveau inférieur, vous désactivez tous les montages des zones de niveau inférieur.	"Procédure de désactivation du montage pour les fichiers de niveau inférieur " à la page 140
Configuration d'une zone de manière à permettre la modification des étiquettes des fichiers.	Les zones étiquetées disposent de privilèges limités. Par défaut, les zones étiquetées ne disposent pas du privilège permettant à un utilisateur autorisé de modifier l'étiquette d'un fichier. Vous modifiez la configuration de la zone pour ajouter ce privilège.	"Procédure d'octroi de l'autorisation de modifier l'étiquette de fichiers à un utilisateur" à la page 143
Déplacement d'un fichier ou d'un répertoire à l'intérieur ou à l'extérieur d'une zone étiquetée.	Modifie le niveau de sécurité d'un fichier ou d'un répertoire en modifiant son étiquette.	"Procédure de déplacement de fichiers entre les étiquettes dans Trusted CDE" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*
Ajout d'un ensemble de données ZFS dans une zone étiquetée et partage de l'ensemble.	Monte un ensemble de données ZFS avec autorisations de lecture/écriture dans une zone étiquetée et partage l'ensemble de données en lecture seule avec une zone de niveau supérieur.	"Procédure de partage d'un ensemble de données ZFS à partir d'une zone étiquetée" à la page 141.
Configuration d'une nouvelle zone.	Crée une zone sous une étiquette qui n'est pas en cours d'utilisation pour permettre l'étiquetage d'une zone de ce système.	Reportez-vous à la section "Attribution de nom et étiquetage de la zone" du *Guide de configuration d'Oracle Solaris Trusted Extensions*. Suivez ensuite la procédure que l'équipe de configuration initiale a utilisée pour créer les autres zones. Pour connaître les étapes, reportez-vous à la section "Création de zones étiquetées" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.
Création d'un port multiniveau pour une application.	Les ports multiniveau sont utiles pour les programmes qui nécessitent un flux multiniveau vers la zone étiquetée.	"Procédure de configuration d'un port multiniveau pour NFSv3 sur `udp`" à la page 145 "Procédure de création d'un port multiniveau pour une zone" à la page 146

Tâche	Description	Voir
Dépannage du montage NFS et des problèmes d'accès.	Débogue les problèmes généraux d'accès pour les montages, et éventuellement les zones.	"Dépannage des échecs de montage dans Trusted Extensions" à la page 165
Suppression d'une zone étiquetée.	Supprime complètement une zone étiquetée du système.	"How to Remove a Non-Global Zone" du *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*

▼ Procédure d'affichage des zones prêtes ou en cours d'exécution

Cette procédure crée un script de shell qui affiche les étiquettes de la zone active et toutes les zones qu'elle domine.

Avant de commencer Vous devez être dans le rôle d'administrateur système dans la zone globale.

1 Servez-vous de l'éditeur de confiance pour créer le script `getzonelabels`.

Pour plus d'informations, reportez-vous à la section "Modification des fichiers d'administration dans Trusted Extensions" à la page 59.

Indiquez le nom du chemin d'accès du script, par exemple : `/usr/local/scripts/getzonelabels`.

2 Ajoutez le contenu suivant, puis enregistrez le fichier :

```
#!/bin/sh
#
echo "NAME\t\tSTATUS\t\tLABEL"
echo "====\t\t======\t\t====="
myzone=‘zonename‘
for i in ‘/usr/sbin/zoneadm list -p‘ ; do
        zone=‘echo $i | cut -d ":" -f2‘
        status=‘echo $i | cut -d ":" -f3‘
        path=‘echo $i | cut -d ":" -f4‘
        if [ $zone != global ]; then
                if [ $myzone = global ]; then
                        path=$path/root/tmp
                else
                        path=$path/export/home
                fi
        fi
        label=‘/usr/bin/getlabel -s $path |cut -d ":" -f2-9‘
        if [ ‘echo $zone|wc -m‘ -lt 8 ]; then
                echo "$zone\t\t$status\t$label"
        else
                echo "$zone\t$status\t$label"
        fi
done
```

3 **Testez le script dans la zone globale.**

```
# getzonelabels
NAME            STATUS          LABEL
====            ======          =====
global          running         ADMIN_HIGH
needtoknow      running         CONFIDENTIAL : NEED TO KNOW
restricted      ready           CONFIDENTIAL : RESTRICTED
internal        running         CONFIDENTIAL : INTERNAL
public          running         PUBLIC
```

Lorsqu'il est exécuté à partir de la zone globale, le script affiche les étiquettes de toutes les zones prêtes ou en cours d'exécution. Vous trouverez ci-dessous le résultat fourni par le script depuis la zone globale pour les zones créées à partir du fichier `label_encodings` par défaut :

Exemple 10–1 Affichage des étiquettes de toutes les zones prêtes ou en cours d'exécution

Dans l'exemple suivant, un utilisateur exécute le script `getzonelabels` dans la zone `internal`.

```
# getzonelabels
NAME            STATUS          LABEL
====            ======          =====
internal        running         CONFIDENTIAL : INTERNAL
public          running         PUBLIC
```

▼ Procédure d'affichage des étiquettes de fichiers montés

Cette procédure crée un script shell qui affiche les systèmes de fichiers montés de la zone active. Lorsqu'il est exécuté à partir de la zone globale, le script affiche les étiquettes de tous les systèmes de fichiers montés dans chaque zone.

Avant de commencer Vous devez être dans le rôle d'administrateur système dans la zone globale.

1 **Servez-vous de l'éditeur de confiance pour créer le script `getmounts`.**

Pour plus d'informations, reportez-vous à la section "Modification des fichiers d'administration dans Trusted Extensions" à la page 59.

Indiquez le chemin d'accès du script, par exemple `/usr/local/scripts/getmounts`.

2 **Ajoutez le contenu suivant et enregistrez le fichier :**

```
#!/bin/sh
#
for i in `/usr/sbin/mount -p | cut -d " " -f3` ; do
        /usr/bin/getlabel $i
done
```

3 Testez le script dans la zone globale.

```
# /usr/local/scripts/getmounts
/:      ADMIN_LOW
/dev:   ADMIN_LOW
/kernel:        ADMIN_LOW
/lib:   ADMIN_LOW
/opt:   ADMIN_LOW
/platform:      ADMIN_LOW
/sbin:  ADMIN_LOW
/usr:   ADMIN_LOW
/var/tsol/doors:        ADMIN_LOW
/zone/needtoknow/export/home:   CONFIDENTIAL : NEED TO KNOW
/zone/internal/export/home:     CONFIDENTIAL : INTERNAL USE ONLY
/zone/restricted/export/home:   CONFIDENTIAL : RESTRICTED
/proc:  ADMIN_LOW
/system/contract:       ADMIN_LOW
/etc/svc/volatile:      ADMIN_LOW
/etc/mnttab:    ADMIN_LOW
/dev/fd:        ADMIN_LOW
/tmp:           ADMIN_LOW
/var/run:       ADMIN_LOW
/zone/public/export/home:  PUBLIC
/root:          ADMIN_LOW
```

Exemple 10–2 Affichage des étiquettes de systèmes de fichiers dans la zone `restricted`

Lorsqu'il est exécuté à partir d'une zone étiquetée par un utilisateur standard, le script `getmounts` affiche les étiquettes de tous les systèmes de fichiers montés dans cette zone. Sur un système où des zones sont créées pour chaque étiquette du fichier `label_encodings` par défaut, le résultat de la zone `restricted` se présente comme suit :

```
# /usr/local/scripts/getmounts
/:      CONFIDENTIAL : RESTRICTED
/dev:   CONFIDENTIAL : RESTRICTED
/kernel:        ADMIN_LOW
/lib:   ADMIN_LOW
/opt:   ADMIN_LOW
/platform:      ADMIN_LOW
/sbin:  ADMIN_LOW
/usr:   ADMIN_LOW
/var/tsol/doors:        ADMIN_LOW
/zone/needtoknow/export/home:   CONFIDENTIAL : NEED TO KNOW
/zone/internal/export/home:     CONFIDENTIAL : INTERNAL USE ONLY
/proc:  CONFIDENTIAL : RESTRICTED
/system/contract:       CONFIDENTIAL : RESTRICTED
/etc/svc/volatile:      CONFIDENTIAL : RESTRICTED
/etc/mnttab:    CONFIDENTIAL : RESTRICTED
/dev/fd:        CONFIDENTIAL : RESTRICTED
/tmp:   CONFIDENTIAL : RESTRICTED
/var/run:       CONFIDENTIAL : RESTRICTED
/zone/public/export/home:       PUBLIC
/home/gfaden:   CONFIDENTIAL : RESTRICTED
```

▼ Procédure de montage en loopback d'un fichier qui n'est généralement pas visible dans une zone étiquetée

Cette procédure permet à un utilisateur dans une zone étiquetée spécifiée de visualiser des fichiers qui, par défaut, ne sont pas exportés depuis la zone globale.

Avant de commencer Vous devez être dans le rôle d'administrateur système dans la zone globale.

1 Arrêtez la zone dont vous souhaitez modifier la configuration.

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

2 Montez un fichier ou un répertoire en loopback.

Par exemple, autorisez les utilisateurs ordinaires à afficher un fichier dans le répertoire `/etc`.

```
# zonecfg -z zone-name
 add filesystem
 set special=/etc/filename
 set directory=/etc/filename
 set type=lofs
 add options [ro,nodevices,nosetuid]
 end
 exit
```

Remarque – Certains fichiers ne sont pas utilisés par le système, leur montage en loopback est donc sans effet. Par exemple, le fichier `/etc/dfs/dfstab` d'une zone étiquetée n'est pas contrôlé par le logiciel Trusted Extensions. Pour plus d'informations, reportez-vous à la section "Partage de fichiers à partir d'une zone étiquetée" à la page 151.

3 Démarrez la zone.

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

Exemple 10–3 Montage en loopback du fichier `/etc/passwd`

Dans cet exemple, l'administrateur de sécurité souhaite permettre aux testeurs et aux programmeurs de vérifier que leurs mots de passe locaux sont définis. Une fois qu'elle a été arrêtée, la zone `sandbox` est configurée de manière à monter en loopback le fichier `passwd`. Ensuite, la zone est redémarrée.

```
# zoneadm -z sandbox halt
# zonecfg -z sandbox
 add filesystem
    set special=/etc/passwd
    set directory=/etc/passwd
    set type=lofs
```

```
    add options [ro,nodevices,nosetuid]
 end
 exit
# zoneadm -z sandbox boot
```

▼ Procédure de désactivation du montage pour les fichiers de niveau inférieur

Par défaut, les utilisateurs peuvent visualiser les fichiers de niveau inférieur. Supprimez le privilège `net_mac_aware` pour empêcher l'affichage de tous les fichiers de niveau inférieur depuis une zone particulière. Pour une description du privilège `net_mac_aware`, reportez-vous à la page de manuel `privileges(5)`.

Avant de commencer Vous devez être dans le rôle d'administrateur système dans la zone globale.

1 Arrêtez la zone dont vous souhaitez modifier la configuration.

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

2 Configurez la zone de manière à empêcher la visualisation des fichiers de niveau inférieur.

Supprimez le privilège `net_mac_aware` de la zone.

```
# zonecfg -z zone-name
 set limitpriv=default,!net_mac_aware
 exit
```

3 Redémarrez la zone.

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

Exemple 10–4 Désactivation de la visualisation par les utilisateurs des fichiers de niveau inférieur

Dans cet exemple, l'administrateur de sécurité souhaite éviter toute confusion aux utilisateurs d'un système. Les utilisateurs ne doivent donc pouvoir visualiser que les fichiers correspondant à l'étiquette à laquelle ils travaillent. Pour ce faire, l'administrateur de sécurité empêche la visualisation de tous les fichiers de niveau inférieur. Sur ce système, les utilisateurs ne peuvent pas voir les fichiers mis à la disposition du public, à moins qu'ils ne travaillent sous l'étiquette `PUBLIC`. En outre, les utilisateurs peuvent uniquement monter des fichiers via NFS sous l'étiquette des zones.

```
# zoneadm -z restricted halt
# zonecfg -z restricted
 set limitpriv=default,!net_mac_aware
 exit
# zoneadm -z restricted boot

# zoneadm -z needtoknow halt
# zonecfg -z needtoknow
```

```
 set limitpriv=default,!net_mac_aware
 exit
# zoneadm -z needtoknow boot

# zoneadm -z internal halt
# zonecfg -z internal
 set limitpriv=default,!net_mac_aware
 exit
# zoneadm -z internal boot
```

Étant donné que PUBLIC est l'étiquette la plus basse, l'administrateur de sécurité n'exécute pas les commandes pour la zone PUBLIC.

▼ Procédure de partage d'un ensemble de données ZFS à partir d'une zone étiquetée

Dans le cadre de cette procédure, vous montez un ensemble de données ZFS avec autorisations en lecture/écriture dans une zone étiquetée. Toutes les commandes étant exécutées dans la zone globale, l'administrateur de la zone globale contrôle l'ajout d'ensembles de données ZFS à des zones étiquetées.

L'état de la zone étiquetée doit être au minimum prêt pour qu'elle puisse partager un ensemble de données. L'état de la zone peut être en cours d'exécution.

Avant de commencer Pour configurer la zone avec l'ensemble de données, vous devez d'abord arrêter la zone.

1 Créez l'ensemble de données ZFS

```
# zfs create datasetdir/subdir
```

Le nom de l'ensemble de données peut inclure un répertoire, par exemple zone/data.

2 Dans la zone globale, arrêtez la zone étiquetée.

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

3 Définissez le point de montage de l'ensemble de données.

```
# zfs set mountpoint=legacy datasetdir/subdir
```

Le paramétrage de la propriété mountpoint ZFS définit l'étiquette du point de montage lorsque celui-ci correspond à une zone étiquetée.

4 Ajoutez l'ensemble de données à la zone en tant que système de fichiers.

```
# zonecfg -z labeled-zone-name
# zonecfg:labeled-zone-name> add fs
# zonecfg:labeled-zone-name:dataset> set dir=/subdir
# zonecfg:labeled-zone-name:dataset> set special=datasetdir/subdir
# zonecfg:labeled-zone-name:dataset> set type=zfs
# zonecfg:labeled-zone-name:dataset> end
# zonecfg:labeled-zone-name> exit
```

Lorsque vous ajoutez l'ensemble de données en tant que système de fichiers, l'ensemble de données est monté dans la zone au niveau `/data`, avant que le fichier `dfstab` ne soit interprété. Cette étape permet de s'assurer que l'ensemble de données n'est pas monté avant que la zone ne soit démarrée. Plus précisément, la zone est démarrée, l'ensemble de données est monté, puis le fichier `dfstab` est interprété.

5 Partagez l'ensemble de données.

Ajoutez une entrée au système de fichiers de l'ensemble de données dans le fichier `/zone/`*labeled-zone-name*`/etc/dfs/dfstab`. Cette entrée utilise également le nom de chemin */subdir*.

```
share  -F nfs  -d "dataset-comment"  /subdir
```

6 Démarrez la zone étiquetée.

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

Lorsque la zone est démarrée, l'ensemble de données est automatiquement monté en tant que point de montage en lecture/écriture dans la zone *labeled-zone-name* avec l'étiquette de la zone *labeled-zone-name*.

Exemple 10–5 Partage et montage d'un ensemble de données ZFS à partir de zones étiquetées

Dans cet exemple, l'administrateur ajoute un ensemble de données ZFS à la zone `needtoknow` et partage l'ensemble de données. L'ensemble de données, `zone/data` est actuellement assigné au point de montage `/mnt`. Les utilisateurs de la zone `restricted` peuvent consulter l'ensemble de données.

Tout d'abord, l'administrateur arrête la zone.

```
# zoneadm -z needtoknow halt
```

Étant donné que l'ensemble de données est actuellement assigné à un autre point de montage, l'administrateur supprime l'assignation précédente, puis définit le nouveau point de montage.

```
# zfs set zoned=off zone/data
# zfs set mountpoint=legacy zone/data
```

Puis, dans les interfaces interactives `zonecfg`, l'administrateur ajoute explicitement l'ensemble de données à la zone `needtoknow`.

```
# zonecfg -z needtoknow
# zonecfg:needtoknow> add fs
# zonecfg:needtoknow:dataset> set dir=/data
# zonecfg:needtoknow:dataset> set special=zone/data
# zonecfg:needtoknow:dataset> set type=zfs
# zonecfg:needtoknow:dataset> end
# zonecfg:needtoknow> exit
```

Il modifie ensuite le fichier `/zone/needtoknow/etc/dfs/dfstab` afin de partager l'ensemble de données et démarre la zone `needtoknow`.

```
## Global zone dfstab file for needtoknow zone
share  -F nfs  -d "App Data on ZFS"  /data

# zoneadm -z needtoknow boot
```

L'ensemble de données est désormais accessible.

Les utilisateurs de la zone `restricted` qui domine la zone `needtoknow` peuvent afficher l'ensemble de données monté en basculant dans le répertoire `/data`. Du point de vue de la zone globale, ils utilisent le chemin complet de l'ensemble de données monté. Dans cet exemple, `machine1` est le nom d'hôte du système qui inclut la zone étiquetée. L'administrateur a assigné ce nom d'hôte à une adresse IP non partagée.

```
# cd /net/machine1/zone/needtoknow/root/data
```

Erreurs fréquentes Si la tentative d'accès à l'ensemble de données depuis l'étiquette de niveau supérieur renvoie l'erreur `not found` (introuvable) ou `No such file or directory` (Fichier ou répertoire introuvable), l'administrateur doit redémarrer le service de montage automatique à l'aide de la commande `svcadm restart autofs`.

▼ Procédure d'octroi de l'autorisation de modifier l'étiquette de fichiers à un utilisateur

Cette procédure est indispensable pour permettre à un utilisateur de modifier l'étiquette de fichiers.

Avant de commencer Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

1. **Arrêtez la zone dont vous souhaitez modifier la configuration.**

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

2. **Configurez la zone afin de permettre la modification de l'étiquette.**

   Ajoutez les privilèges appropriés à la zone. Les privilèges windows permettent aux utilisateurs d'effectuer des opérations de glisser-déposer et de couper-coller.

   - **Pour autoriser la rétrogradation, ajoutez le privilège `file_downgrade_sl` à la zone.**

     ```
     # zonecfg -z zone-name
      set limitpriv=default,win_dac_read,win_mac_read,win_dac_write,
      win_mac_write,win_selection,file_downgrade_sl
      exit
     ```

- **Pour autoriser la mise à niveau, ajoutez les privilèges `sys_trans_label` et `file_upgrade_sl` à la zone.**

  ```
  # zonecfg -z zone-name
   set limitpriv=default,win_dac_read,win_mac_read,win_dac_write,
   win_mac_write,win_selection,sys_trans_label,file_upgrade_sl
   exit
  ```

- **Pour autoriser à la fois la mise à niveau et la rétrogradation, ajoutez les trois privilèges à la zone.**

  ```
  # zonecfg -z zone-name
   set limitpriv=default,win_dac_read,win_mac_read,win_dac_write,
   win_mac_write,win_selection,sys_trans_label,file_downgrade_sl,
   file_upgrade_sl
   exit
  ```

3 **Redémarrez la zone.**

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

Pour connaître les conditions à remplir par l'utilisateur et les processus, reportez-vous à la page de manuel `setflabel`(3TSOL). Pour autoriser un utilisateur à modifier l'étiquette de fichiers, reportez-vous à la section "Procédure d'octroi de l'autorisation de modifier le niveau de sécurité de données à un utilisateur" à la page 104.

Exemple 10–6 Octroi de l'autorisation de mettre à niveau à partir de la zone `internal`

Dans cet exemple, l'administrateur de sécurité souhaite permettre aux utilisateurs autorisés d'un système de mettre à niveau des fichiers. En permettant aux utilisateurs de mettre à niveau des informations, l'administrateur leur permet de protéger les informations à l'aide d'un niveau de sécurité plus élevé. Dans la zone globale, l'administrateur exécute les commandes d'administration de zone suivantes.

```
# zoneadm -z internal halt
# zonecfg -z internal
 set limitpriv=default,sys_trans_label,file_upgrade_sl
 exit
# zoneadm -z internal boot
```

Les utilisateurs autorisés peuvent à présent mettre à niveau des informations `internal` en `restricted` à partir de la zone `internal`.

Exemple 10–7 Octroi de l'autorisation de rétrograder à partir de la zone `restricted`

Dans cet exemple, l'administrateur de sécurité souhaite permettre aux utilisateurs autorisés d'un système de rétrograder des fichiers. Étant donné que l'administrateur n'ajoute pas de privilèges windows à la zone, les utilisateurs autorisés ne peuvent pas utiliser le gestionnaire de fichiers (File Manager) pour modifier l'étiquette de fichiers. Pour modifier l'étiquette de fichiers, les utilisateurs utilisent la commande `setlabel`.

En permettant aux utilisateurs de rétrograder des informations, l'administrateur autorise les utilisateurs dont le niveau de sécurité est inférieur à accéder aux fichiers. Dans la zone globale, l'administrateur exécute les commandes d'administration de zone suivantes.

```
# zoneadm -z restricted halt
# zonecfg -z restricted
 set limitpriv=default,file_downgrade_sl
 exit
# zoneadm -z restricted boot
```

Les utilisateurs autorisés peuvent à présent rétrograder des informations `restricted` en `internal` ou `public` à l'aide de la commande `setlabel` à partir de la zone `restricted`.

▼ Procédure de configuration d'un port multiniveau pour NFSv3 sur udp

Cette procédure est utilisée pour activer les montages "read-down" NFSv3 sur `udp`. Le MLP est ajouté à l'aide de la Console de gestion Solaris.

Avant de commencer Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

1. **Démarrez la Console de gestion Solaris.**

   Pour plus d'informations, reportez-vous à la section “Administration du système local avec Console de gestion Solaris ” à la page 57.

2. **Choisissez la boîte à outils Fichiers.**

   Le titre de la boîte à outils inclut `Scope=Files, Policy=TSOL`.

3. **Configurez la zone et le MLP.**

   a. **Accédez à l'outil Trusted Network Zones (Zones de réseau de confiance).**

   b. **Double-cliquez sur la zone globale.**

   c. **Ajoutez un port multiniveau pour le protocole UDP :**

      i. **Cliquez sur Add (Ajouter) pour Multilevel Ports for Zone's IP Addresses (Ports multiniveau pour adresses IP de la zone).**

      ii. **Saisissez 2049 pour le numéro de port, puis cliquez sur OK.**

   d. **Cliquez sur OK pour enregistrer les paramètres.**

4. **Fermez la Console de gestion Solaris.**

5 **Mettez à jour le noyau.**

```
# tnctl -fz /etc/security/tsol/tnzonecfg
```

▼ Procédure de création d'un port multiniveau pour une zone

Cette procédure est utilisée lorsqu'une application exécutée dans une zone étiquetée nécessite un port multiniveau (MLP) pour communiquer avec la zone. Dans cette procédure, un proxy Web communique avec la zone. Le MLP est ajouté à l'aide de la Console de gestion Solaris.

Avant de commencer Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale. La zone étiquetée doit exister. Pour plus d'informations, reportez-vous à la section "Création de zones étiquetées" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.

1 **Démarrez la Console de gestion Solaris.**

Pour plus d'informations, reportez-vous à la section " Administration du système local avec Console de gestion Solaris " à la page 57.

2 **Choisissez la boîte à outils Fichiers.**

Le titre de la boîte à outils inclut `Scope=Files, Policy=TSOL`.

3 **Ajoutez l'hôte proxy et l'hôte de services Web à la liste des ordinateurs.**

a. **Dans System Configuration (Configuration système), accédez à l'outil Computers and Networks (Ordinateurs et réseaux).**

b. **Dans l'outil Computers (Ordinateurs), cliquez sur le menu Action et choisissez Add Computer (Ajouter un ordinateur).**

c. **Ajoutez le nom d'hôte et l'adresse IP de l'hôte proxy.**

d. **Enregistrez les modifications.**

e. **Ajoutez le nom d'hôte et l'adresse IP de l'hôte du service Web.**

f. **Enregistrez les modifications.**

4 **Configurez la zone et le MLP.**

a. **Accédez à l'outil Trusted Network Zones (Zones de réseau de confiance).**

b. **Sélectionnez la zone étiquetée.**

c. Dans la section MLP Configuration for Local IP Addresses (Configuration MLP pour adresses IP locales), indiquez le champ de port/protocole approprié.

d. Enregistrez les modifications.

5 Pour la zone, personnalisez un modèle en effectuant les étapes suivantes :

a. Accédez à l'outil Security Templates (Modèles de sécurité).

Cliquez sur le menu Action et sélectionnez Add Template (Ajouter un modèle).

b. Utilisez le nom d'hôte comme nom du modèle.

c. Spécifiez CIPSO pour le type d'hôte.

d. Utilisez l'étiquette de la zone en tant qu'étiquette minimale et maximale.

e. Assignez l'étiquette de zone à l'ensemble d'étiquettes de sécurité.

f. Sélectionnez l'onglet Hosts Explicitly Assigned (Hôtes assignés de façon explicite).

g. Dans la section Add an Entry (Ajouter une entrée), ajoutez l'adresse IP associée à la zone.

h. Enregistrez les modifications.

6 Fermez la Console de gestion Solaris.

7 Démarrez les zones.

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

8 Dans la zone globale, ajoutez des routes pour les nouvelles adresses.

Par exemple, si les zones ont une adresse IP partagée, effectuez les opérations suivantes :

```
# route add proxy labeled-zones-IP-address
# route add webservice labeled-zones-IP-address
```

◆ ◆ ◆ CHAPITRE 11

Gestion et montage de fichiers dans Trusted Extensions (tâches)

Ce chapitre décrit le fonctionnement des montages LOFS et NFS sur un système configuré avec Trusted Extensions. Ce chapitre traite également de la sauvegarde et de la restauration de fichiers.

Partage et montage de fichiers dans Trusted Extensions

Le logiciel Trusted Extensions prend en charge les mêmes systèmes de fichiers et les mêmes commandes de gestion de systèmes de fichiers que le SE Oracle Solaris. Trusted Extensions ajoute la possibilité pour une zone non globale de partager des fichiers. En outre, Trusted Extensions joint une étiquette unique à chaque zone non globale. Tous les fichiers et répertoires appartenant à cette zone sont montés sous l'étiquette de la zone. Tous les systèmes de fichiers partagés qui appartiennent à d'autres zones ou à des serveurs NFS sont montés sous l'étiquette du propriétaire. Trusted Extensions empêche tout montage qui irait à l'encontre des stratégies de contrôle d'accès obligatoire (MAC) pour l'étiquetage. Par exemple, l'étiquette d'une zone doit dominer toutes les étiquettes de son système de fichiers montés, et seuls les systèmes de fichiers possédant des étiquettes égales peuvent être montés avec des autorisations en lecture/écriture.

Montages NFS dans Trusted Extensions

Les montages NFS dans Trusted Extensions sont similaires aux montages d'Oracle Solaris. Ils ne présentent de différences qu'au niveau de l'utilisation du nom de chemin racine de zone lors du montage d'une zone étiquetée dans Trusted Extensions et de l'application de la stratégie MAC.

Les partages NFS dans Trusted Extensions sont similaires aux partages d'Oracle Solaris dans une zone globale. Cependant, le partage des fichiers d'une zone étiquetée sur un système multiniveau est propre à Trusted Extensions :

- **Partages et montages dans la zone globale** : les procédures de partage et de montage de fichiers dans la zone globale d'un système Trusted Extensions sont presque identiques aux procédures correspondantes dans le SE Oracle Solaris. Le montage de fichiers peut être effectué à l'aide de l'automonteur, du fichier `vfstab` ou de la commande `mount`. Le partage de fichiers est réalisé à l'aide du fichier `dfstab`.
- **Montages dans des zones étiquetées** : le montage de fichiers dans des zones étiquetées de Trusted Extensions est presque identique au montage de fichiers dans des zones non globales du SE Oracle Solaris. Le montage de fichiers peut être effectué à l'aide de l'automonteur, du fichier `vfstab` ou de la commande `mount`. Dans Trusted Extensions, un fichier de configuration `automount_home_`*étiquette* spécifique existe pour chaque zone étiquetée.
- **Partages dans des zones étiquetées** : les fichiers d'une zone étiquetée peuvent être partagés sous l'étiquette de la zone à l'aide d'un fichier `dfstab` ; ce fichier se trouve sous l'étiquette de la zone, mais est uniquement visible depuis la zone globale. Par conséquent, c'est l'administrateur de la zone globale qui, dans la zone globale, configure une zone étiquetée de manière à ce qu'elle partage ses fichiers. Ce fichier de configuration n'est pas visible depuis la zone étiquetée correspondante. Pour plus d'informations, reportez-vous à la section “Processus de zone globale et zones étiquetées” à la page 132.

Les étiquettes déterminent quels fichiers peuvent être montés. Les fichiers sont partagés et montés sous une étiquette particulière. Pour qu'un client Trusted Extensions écrive dans un fichier qui est monté via NFS, le fichier doit être monté avec des autorisations en lecture/écriture *et* doit posséder la même étiquette que le client. Si vous montez un fichier entre deux hôtes de Trusted Extensions, le serveur et le client doivent disposer de modèles d'hôte distant de type `cipso` compatibles. Si vous montez un fichier entre un hôte de Trusted Extensions et un hôte sans étiquette, les fichiers possédant l'étiquette unique spécifiée pour l'hôte sans étiquette dans le fichier `tnrhdb` peuvent être montés. Les fichiers qui sont montés avec LOFS peuvent être visualisés, mais ne peuvent pas être modifiés. Pour plus d'informations sur les montages NFS, reportez-vous à la section “Accès aux répertoires montés via NFS dans Trusted Extensions” à la page 152.

Les étiquettes déterminent également quels répertoires et fichiers peuvent être affichés. Par défaut, les objets de niveau inférieur sont disponibles dans l'environnement d'un utilisateur. Par conséquent, dans la configuration par défaut, un utilisateur standard peut visualiser les fichiers

appartenant à une zone de niveau inférieur au niveau actuel de l'utilisateur. Par exemple, les utilisateurs peuvent visualiser leurs répertoires personnels de niveau inférieur à partir d'une étiquette supérieure. Pour plus d'informations, reportez-vous à la section "Création de répertoires personnels dans Trusted Extensions" à la page 153.

Si la sécurité du site interdit l'affichage des objets de niveau inférieur, vous pouvez rendre les répertoires de niveau inférieur invisibles pour l'utilisateur. Pour plus d'informations, reportez-vous à la section "Procédure de désactivation du montage pour les fichiers de niveau inférieur " à la page 140.

La stratégie de montage dans Trusted Extensions n'offre pas de possibilité de contourner le MAC. Les fichiers montés visibles depuis une étiquette inférieure ne peuvent jamais être modifiés par un processus d'étiquette supérieure. Cette stratégie MAC s'applique également dans la zone globale. Un processus de zone globale `ADMIN_HIGH` ne peut pas modifier un fichier monté via NFS d'étiquette inférieure, tel qu'un fichier `PUBLIC` ou un fichier `ADMIN_LOW`. Les stratégies MAC appliquent la configuration par défaut et sont invisibles pour les utilisateurs standard. Les utilisateurs standard ne peuvent pas visualiser d'objets, à moins qu'ils ne disposent d'un accès MAC à ces derniers.

Partage de fichiers à partir d'une zone étiquetée

Dans le SE Oracle Solaris, une zone non globale ne peut pas partager de répertoires. Toutefois, dans Trusted Extensions, une zone étiquetée peut partager des répertoires. Les répertoires d'une zone étiquetée pouvant être partagés sont spécifiés dans la zone globale à l'aide d'un répertoire n'appartenant pas au chemin `root` de la zone. Pour plus d'informations, reportez-vous à la section "Processus de zone globale et zones étiquetées" à la page 132.

`/zone/`*labeled-zone*`/`*répertoires*	Également appelé le chemin d'accès de la zone. C'est le chemin d'accès de la zone globale à la zone étiquetée. Chaque répertoire sous *labeled-zone* possède la même étiquette que la zone.
`/zone/`*labeled-zone*`/root/`*répertoires*	Également appelé le chemin racine de la zone. C'est le chemin `root` d'une zone étiquetée du point de vue de la zone globale. Du point de vue de la zone étiquetée, il s'agit de la racine de la zone, le répertoire `/`. Ce chemin d'accès n'est pas utilisé par la zone globale pour l'administration de la zone.

Pour partager des répertoires à partir d'une zone étiquetée, l'administrateur de la zone globale crée et modifie le fichier `dfstab` dans le répertoire `/etc` du chemin d'accès de la zone :

`/zone/`*labeled-zone*`/etc/dfs/dfstab`

Ce répertoire `/etc` n'est pas visible à partir de la zone étiquetée. Ce répertoire est distinct du répertoire `/etc` visible à partir de la zone :

```
Global zone view: /zone/labeled-zone/root/etc
Labeled zone view of the same directory: /etc
```

Un fichier `dfstab` placé dans ce chemin d'accès ne permet pas le partage de répertoires étiquetés.

Lorsque l'état de la zone étiquetée est `ready` (prêt) ou `running` (en cours d'exécution), les fichiers qui sont répertoriés dans le fichier `/zone/`*labeled-zone*`/etc/dfs/dfstab` sont partagés sous l'étiquette de la zone. Pour plus d'informations sur cette procédure, reportez-vous à la section "Procédure de partage de répertoires à partir d'une zone étiquetée" à la page 157.

Accès aux répertoires montés via NFS dans Trusted Extensions

Par défaut, les systèmes de fichiers montés via NFS sont visibles sous l'étiquette du système de fichiers exporté. Si le système de fichiers est exporté avec des autorisations en lecture/écriture, les utilisateurs travaillant sous cette étiquette peuvent accéder en écriture aux fichiers. Les montages NFS possédant une étiquette inférieure à celle de la session actuelle de l'utilisateur peuvent être visualisés par l'utilisateur, mais celui-ci ne peut pas y accéder en écriture. Même si un système de fichiers est partagé avec des autorisations en lecture/écriture, le système de montage peut uniquement y accéder en écriture sous l'étiquette du montage.

Pour rendre des répertoires de niveau inférieur montés via NFS visibles pour les utilisateurs se trouvant dans une zone de niveau supérieur, l'administrateur de la zone globale sur le serveur NFS doit exporter le répertoire parent. Le répertoire parent est exporté sous son étiquette. Du côté client, chaque zone doit posséder le privilège `net_mac_aware`. Par défaut, les zones étiquetées incluent le privilège `net_mac_aware` dans leur ensemble `limitpriv`.

- **Configuration de serveur** : sur le serveur NFS, vous exportez le répertoire parent dans un fichier `dfstab`. Si le répertoire parent se trouve dans une zone étiquetée, le fichier `dfstab` doit être modifié dans la zone étiquetée du répertoire parent. Le fichier `dfstab` d'une zone étiquetée n'est visible qu'à partir de la zone globale. Pour plus d'informations sur cette procédure, reportez-vous à la section "Procédure de partage de répertoires à partir d'une zone étiquetée" à la page 157.
- **Configuration client** : le privilège `net_mac_aware` doit être spécifié dans le fichier de configuration de zone utilisé lors de la configuration initiale de la zone. Ainsi, un utilisateur autorisé à visualiser tous les répertoires personnels de niveau inférieur doit disposer du privilège `net_mac_aware` dans chaque zone, à l'exception de la zone la plus basse. Pour voir un exemple, reportez-vous à la section "Procédure de montage NFS de fichiers dans une zone étiquetée" à la page 159.

EXEMPLE 11–1 Fourniture d'accès à des répertoires personnels de niveau inférieur

Sur le serveur d'annuaire personnel, l'administrateur crée et modifie le fichier `/zone/`*labeled-zone*`/etc/dfs/dfstab` dans chaque zone étiquetée. Le fichier `dfstab` exporte le

EXEMPLE 11–1 Fourniture d'accès à des répertoires personnels de niveau inférieur *(Suite)*

répertoire `/export/home` avec des autorisations en lecture/écriture. Par conséquent, lorsque le répertoire est monté à la même étiquette, le répertoire personnel est accessible en écriture. Pour exporter le répertoire `/export/home` de `PUBLIC`, l'administrateur crée un espace de travail sous l'étiquette `PUBLIC` sur le serveur d'annuaire personnel et, à partir de la zone globale, il modifie le fichier `/zone/public/etc/dfs/dfstab`.

Sur le client, l'administrateur de la zone globale vérifie que chaque zone étiquetée, à l'exception de l'étiquette la plus basse, dispose du privilège `net_mac_aware`. Ce privilège permet le montage. Ce privilège peut être spécifié à l'aide de la commande `zonecfg` au cours de la configuration de la zone. Le répertoire personnel de niveau inférieur peut uniquement être visualisé. MAC protège les fichiers du répertoire contre toute tentative de modification.

Création de répertoires personnels dans Trusted Extensions

Les répertoires personnels constituent un cas particulier dans Trusted Extensions. Vous devez vous assurer que les répertoires personnels sont créés dans chaque zone pouvant être utilisée par un utilisateur. En outre, les points de montage du répertoire personnel doivent être créés dans les zones du système de l'utilisateur. Pour que les répertoires personnels montés via NFS fonctionnent correctement, l'emplacement habituel des répertoires, `/export/Home`, doit être utilisé. Dans Trusted Extensions, l'automonteur a été modifié afin de gérer les répertoires personnels dans chaque zone, c'est-à-dire sous chaque étiquette. Pour plus d'informations, reportez-vous à la section "Modifications apportées à l'automonteur dans Trusted Extensions" à la page 154.

Les répertoires personnels sont créés au moment de la création des utilisateurs. Dans Trusted Extensions, les utilisateurs sont créés à l'aide de Console de gestion Solaris (console) ; c'est donc elle qui crée les répertoires personnels. Toutefois, la console crée les répertoires personnels dans la zone globale du serveur d'annuaire personnel. Sur ce serveur, les répertoires sont montés par LOFS. Les répertoires personnels sont automatiquement créés par l'automonteur s'ils sont définis comme montages LOFS.

Remarque – Lorsque vous supprimez un utilisateur à l'aide de la console, seul le répertoire personnel de l'utilisateur dans la zone globale est supprimé. Les répertoires personnels de l'utilisateur dans les zones étiquetées ne sont pas supprimés. Vous êtes responsable de l'archivage et de la suppression des répertoires personnels dans les zones étiquetées. Pour connaître la procédure, reportez-vous à la section "Procédure de suppression d'un compte utilisateur d'un système Trusted Extensions" à la page 105.

Cependant, l'automonteur ne peut pas créer de manière automatique des répertoires personnels sur des serveurs NFS distants. L'utilisateur doit d'abord se connecter au serveur NFS ou l'intervention d'un l'administrateur est requise. Pour créer des répertoires personnels pour les utilisateurs, reportez-vous à la section "Activation de l'accès des utilisateurs à leurs répertoires personnels dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.

Modifications apportées à l'automonteur dans Trusted Extensions

Dans Trusted Extensions, chaque étiquette requiert un montage de répertoire personnel distinct. La commande `automount` a été modifiée pour gérer ces montages automatiques étiquetés. Pour chaque zone, l'automonteur `autofs` monte un fichier `auto_home_` *zone-name*. Par exemple, l'entrée suivante est l'entrée de la zone globale dans le fichier `auto_home_global` :

```
+auto_home_global
*       -fstype=lofs    :/export/home/&
```

Lorsqu'une zone qui autorise le montage des zones de niveau inférieur est démarrée, les opérations suivantes se produisent. Les répertoires personnels des zones de niveau inférieur sont montés en lecture seule sous `/zone/<`*zone-name*`>/export/home` . La carte `auto_home_<`*zone-name*`>` spécifie le chemin `/zone` comme répertoire source pour un remontage `lofs` sur `/zone/<` *zone-name*`>/home/<`*username*`>`.

Par exemple, l'entrée suivante est une entrée `auto_home_public` dans une carte `auto_home_`*zone-at-higher-label* qui est générée à partir d'une zone de niveau supérieur :

```
+auto_home_public
*       -fstype=lofs    :/zone/public/export/home/&
```

L'entrée suivante est l'entrée correspondante dans la zone publique :

```
auto_home_public
*       -fstype=lofs    :/export/home/&
```

Lorsqu'un répertoire personnel est référencé et que le nom ne correspond à aucune entrée de la carte `auto_home_<`*zone-name*`>`, cette dernière tente de trouver une correspondance pour cette spécification de montage en loopback. Le logiciel crée le répertoire personnel lorsque les deux conditions suivantes sont réunies :

1. La carte trouve la correspondance de la spécification de montage en loopback
2. Le nom du répertoire personnel correspond à un utilisateur correct dont le répertoire personnel n'existe pas encore dans *zone-name*

Pour plus d'informations sur les modifications apportées à l'automonteur, reportez-vous à la page de manuel `automount(1M)`.

Logiciel Trusted Extensions et versions du protocole NFS

Dans les versions Solaris 10 11/06 et Solaris 10 8/07, Trusted Extensions reconnaît plusieurs étiquettes uniquement sur NFS version 4 (NFSv4). À partir de la version Solaris 10 5/08, le logiciel Trusted Extensions reconnaît les étiquettes sur NFS version 3 (NFSv3) et NFSv4. Vous pouvez utiliser l'un des ensembles d'options de montage suivants :

```
vers=4 proto=tcp
vers=3 proto=tcp
vers=3 proto=udp
```

Trusted Extensions n'a pas de restrictions concernant les montages à l'aide du protocole `tcp`. Dans NFSv3 et NFSv4, le protocole `tcp` peut être utilisé pour les montages à étiquette identique et les montages "read down". Les montages "read down" requièrent un port multiniveau (MLP).

Pour NFSv3, Trusted Extensions se comporte comme le SE Oracle Solaris. Le protocole `udp` est la valeur par défaut pour NFSv3, mais `udp` est uniquement utilisé pour l'opération de montage initiale. Lors d'opérations NFS ultérieures, le système utilise `tcp`. Par conséquent, les montages "read down" fonctionnent avec NFSv3 dans la configuration par défaut.

Dans les rares cas où vous avez limité les montages NFSv3 à l'utilisation du protocole udp pour les opérations NFS initiales et ultérieures, vous devez créer un MLP pour les opérations NFS qui utilisent le protocole `udp`. Pour connaître la procédure, reportez-vous à la section “Procédure de configuration d'un port multiniveau pour NFSv3 sur `udp`” à la page 145.

Un hôte configuré avec Trusted Extensions peut également partager ses propres systèmes de fichiers avec des hôtes sans étiquette. Un fichier ou un répertoire exporté vers un hôte sans étiquette est *inscriptible* si son étiquette est égale à l'étiquette associée à l'hôte distant dans les entrées de base de données du réseau de confiance. Un fichier ou un répertoire exporté vers un hôte sans étiquette est uniquement *lisible* si son étiquette est dominée par l'étiquette associée à l'hôte distant.

Les communications avec des systèmes qui exécutent une version du logiciel Trusted Solaris ne sont possibles que sous une seule étiquette. Le système Trusted Extensions et le système Trusted Solaris doivent affecter à l'autre système un modèle avec le type d'hôte sans étiquette. Les types d'hôtes sans étiquette doivent indiquer la même étiquette unique. En tant que client NFS d'un serveur de Trusted Solaris, l'étiquette du client ne peut pas être `ADMIN_LOW`.

Le protocole NFS utilisé est indépendant du type de système de fichiers local, mais dépend du type de système d'exploitation de l'ordinateur hébergeant le partage. Le type de système de fichiers spécifié pour la commande `mount` ou dans le fichier `vfstab` pour les systèmes de fichiers distants est toujours NFS.

Sauvegarde, partage et montage de fichiers étiquetés (liste des tâches)

La liste des tâches ci-dessous décrit des tâches courantes permettant d'effectuer la sauvegarde et la restauration de données de systèmes de fichiers étiquetés, ainsi que le partage et le montage de répertoires et de fichiers étiquetés.

Tâche	Description	Voir
Sauvegarde de fichiers.	Permet de protéger vos données en les sauvegardant.	"Procédure de sauvegarde de fichiers dans Trusted Extensions" à la page 157
Restauration de données.	Permet de restaurer des données à partir d'une sauvegarde.	"Procédure de restauration de fichiers dans Trusted Extensions" à la page 157
Partage du contenu d'un répertoire à partir d'une zone étiquetée.	Permet au contenu d'un répertoire étiqueté d'être partagé entre les utilisateurs.	"Procédure de partage de répertoires à partir d'une zone étiquetée" à la page 157
Montage du contenu d'un répertoire qui a été partagé par une zone étiquetée.	Permet au contenu d'un répertoire d'être monté dans une zone à la même étiquette pour la lecture/l'écriture. Lorsqu'une zone de niveau supérieur monte le répertoire partagé, le répertoire est monté en lecture seule.	"Procédure de montage NFS de fichiers dans une zone étiquetée" à la page 159
Création de points de montage de répertoire personnel.	Permet de créer les points de montage pour chaque utilisateur à chaque étiquette. Cette tâche permet aux utilisateurs d'accéder à leur répertoire personnel sur un système qui n'est pas le serveur d'annuaire personnel NFS.	"Activation de l'accès des utilisateurs à leurs répertoires personnels dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions*
Masquage des informations de niveau inférieur pour un utilisateur travaillant à une étiquette de niveau supérieur.	Permet d'empêcher l'affichage des informations de niveau inférieur à partir d'une fenêtre de niveau supérieur.	"Procédure de désactivation du montage pour les fichiers de niveau inférieur " à la page 140
Dépannage des problèmes de montage de systèmes de fichiers.	Permet de résoudre les problèmes de montage d'un système de fichiers.	"Dépannage des échecs de montage dans Trusted Extensions" à la page 165

▼ Procédure de sauvegarde de fichiers dans Trusted Extensions

1 **Prenez le rôle d'opérateur.**

Ce rôle inclut le profil de droits Media Backup (Sauvegarde de supports).

2 **Choisissez l'une des méthodes de sauvegarde suivantes :**

- `/usr/lib/fs/ufs/ufsdump` pour les sauvegardes importantes
- `/usr/sbin/tar cT` pour les petites sauvegardes
- Un script appelant l'une ou l'autre de ces commandes

  Par exemple, l'application de sauvegarde Budtool appelle la commande `ufsdump`. Reportez-vous à la page de manuel `ufsdump(1M)`. Pour plus d'informations sur l'option `T` de la commande `tar`, reportez-vous à la page de manuel `tar(1)`.

▼ Procédure de restauration de fichiers dans Trusted Extensions

1 **Connectez-vous en tant qu'utilisateur root.**

2 **Utilisez l'une des méthodes suivantes :**

- `/usr/lib/fs/ufs/ufsrestore` pour les restaurations importantes
- `/usr/sbin/tar xT` pour les petites restaurations
- Un script appelant l'une ou l'autre de ces commandes

Pour plus d'informations sur l'option `T` de la commande `tar`, reportez-vous à la page de manuel `tar(1)`.

Attention – Seules ces commandes préservent les étiquettes.

▼ Procédure de partage de répertoires à partir d'une zone étiquetée

Comme dans le SE Oracle Solaris, l'outil Mounts and Shares (Montages et partages) dans la Console de gestion Solaris est utilisé pour le partage et le montage de fichiers à partir de la zone

globale. L'outil ne peut pas être utilisé pour monter ou partager des répertoires qui proviennent de zones étiquetées. Créez un fichier `dfstab` sous l'étiquette de la zone, puis redémarrez la zone pour partager les répertoires étiquetés.

Attention – N'utilisez pas de noms propriétaires pour les systèmes de fichiers partagés. Les noms des systèmes de fichiers partagés sont visibles pour tous les utilisateurs.

Avant de commencer Vous devez être le superutilisateur ou être dans le rôle d'administrateur système dans la zone globale sur le serveur de fichiers.

1 Créez un espace de travail sous l'étiquette du répertoire qui va être partagé.

Pour plus d'informations, reportez-vous à la section "Procédure d'ajout d'un espace de travail possédant une étiquette particulière" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

2 Créez un fichier `dfstab` sous l'étiquette de cette zone.

Pour chaque zone qui partage un répertoire, répétez les étapes suivantes :

a. Créez le répertoire `/etc/dfs` dans la zone.

```
# mkdir -p /zone/zone-name/etc/dfs
```

b. Ouvrez l'éditeur de confiance.

Pour plus d'informations, reportez-vous à la section "Modification des fichiers d'administration dans Trusted Extensions" à la page 59.

c. Saisissez le nom du chemin d'accès complet du fichier `dfstab` dans l'éditeur.

```
# /zone/zone-name/etc/dfs/dfstab
```

d. Ajoutez une entrée pour partager un répertoire à partir de cette zone.

L'entrée décrit le répertoire du point de vue du chemin racine de la zone. Par exemple, l'entrée suivante partage les fichiers d'une application sous l'étiquette de la zone qui les contient :

```
share -F nfs -o ro /viewdir/viewfiles
```

3 Pour chaque zone, partagez les répertoires en démarrant la zone.

Dans la zone globale, exécutez l'une des commandes suivantes pour chaque zone. Chaque zone peut partager ses répertoires de n'importe laquelle des manières décrites. Le partage devient effectif lorsque chaque zone passe à l'état `ready` (prêt) ou `running` (en cours d'exécution).

- **Si la zone n'est pas dans l'état running et que vous ne souhaitez pas que les utilisateurs se connectent au serveur sous l'étiquette de la zone, définissez l'état de la zone sur `ready`.**

  ```
  # zoneadm -z zone-name ready
  ```

- **Si la zone n'est pas dans l'état running et si les utilisateurs sont autorisés à se connecter au serveur sous l'étiquette de la zone, démarrez la zone.**

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

- **Si la zone est déjà en cours d'exécution, redémarrez la zone.**

  ```
  # zoneadm -z zone-name reboot
  ```

4. **Affichez les répertoires qui sont partagés à partir de votre système.**

   ```
   # showmount -e
   ```

5. **Pour permettre au client de monter les fichiers exportés, reportez-vous à la section "Procédure de montage NFS de fichiers dans une zone étiquetée" à la page 159.**

Exemple 11–2 Partage du répertoire `/export/share` sous l'étiquette `PUBLIC`

Pour les applications qui s'exécutent sous l'étiquette `PUBLIC`, l'administrateur système autorise les utilisateurs à lire la documentation se trouvant dans le répertoire `/export/share` de la zone `public`. La zone nommée `public` s'exécute sous l'étiquette `PUBLIC`.

Tout d'abord, l'administrateur crée un espace de travail `public` et modifie le fichier `dfstab`.

```
# mkdir -p /zone/public/etc/dfs
# /usr/dt/bin/trusted_edit /zone/public/etc/dfs/dfstab
```

Dans le fichier, l'administrateur ajoute l'entrée suivante :

```
## Sharing PUBLIC user manuals
share -F nfs -o ro /export/appdocs
```

L'administrateur quitte l'espace de travail `public` et retourne dans l'espace de travail Trusted Path (Chemin de confiance). Les utilisateurs n'étant pas autorisés à se connecter à ce système, l'administrateur partage les fichiers en plaçant la zone dans l'état ready :

```
# zoneadm -z public ready
```

Les utilisateurs peuvent accéder aux répertoires partagés une fois que ces derniers sont montés sur les systèmes des utilisateurs.

▼ Procédure de montage NFS de fichiers dans une zone étiquetée

Dans Trusted Extensions, une zone étiquetée gère le montage de fichiers dans sa zone.

Les fichiers d'hôtes étiquetés et d'hôtes sans étiquette peuvent être montés sur un hôte étiqueté Trusted Extensions.

- Pour monter les fichiers en lecture/écriture à partir d'un hôte à étiquette unique, l'étiquette assignée à l'hôte distant doit être identique à celle de la zone dans laquelle le fichier est monté.
- Les fichiers qui sont montés par une zone de niveau supérieur sont en lecture seule.
- Dans Trusted Extensions, le fichier de configuration `auto_home` est personnalisé pour chaque zone. Le nom de la zone est repris dans le nom du fichier. Par exemple, un système comportant une zone globale et une zone publique dispose de deux fichiers `auto_home`, `auto_home_global` et `auto_home_public`.

Trusted Extensions utilise les mêmes interfaces de montage que le SE Oracle Solaris :

- Pour monter des fichiers lors du démarrage, utilisez le fichier `/etc/vfstab` dans la zone étiquetée.
- Pour monter des fichiers dynamiquement, utilisez la commande `mount` dans la zone étiquetée.
- Pour monter automatiquement des répertoires personnels, utilisez les fichiers `auto_home_`*zone-name*.
- Pour monter automatiquement d'autres répertoires, utilisez les cartes de montage automatique standard. Si les cartes de montage automatique sont dans le protocole LDAP, utilisez les commandes LDAP pour les gérer.

Avant de commencer Vous devez être sur le système client, dans la zone possédant l'étiquette des fichiers que vous souhaitez monter. Si vous n'utilisez pas l'automonteur, vous devez être connecté en tant que superutilisateur ou être dans le rôle d'administrateur système. Pour effectuer des montages à partir de serveurs de niveau inférieur, la zone doit être configurée avec le privilège `net_mac_aware`.

- **Pour effectuer un montage NFS de fichiers dans une zone étiquetée, utilisez les procédures suivantes.**

  La plupart des procédures impliquent la création d'un espace de travail à une étiquette particulière. Pour créer un espace de travail, reportez-vous à la section "Procédure d'ajout d'un espace de travail possédant une étiquette particulière" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

  - **Montage dynamique de fichiers.**

    Dans la zone étiquetée, utilisez la commande `mount`. Pour voir un exemple de montage dynamique de fichiers, reportez-vous à l'Exemple 11–3.

  - **Montage de fichiers lors du démarrage de la zone**

    Dans la zone étiquetée, ajoutez les montages au fichier `vfstab`.

Pour voir des exemples de montages de fichiers lors du démarrage d'une zone étiquetée, reportez-vous à l'Exemple 11–4 et à l'Exemple 11–5.

- **Montage de répertoires personnels pour des systèmes administrés à l'aide du protocole LDAP.**

  a. **À chaque étiquette, ajoutez les spécifications de l'utilisateur pour les fichiers `auto_home`_*zone-name*.**

  b. **Utilisez ensuite ces fichiers pour remplir la base de données `auto_home`_*zone-name* sur le serveur LDAP.**

  Pour voir un exemple, reportez-vous à l'Exemple 11–6.

- **Montage de répertoires personnels pour des systèmes administrés à l'aide de fichiers.**

  a. **Créez et remplissez un fichier `/export/home/auto_home`_*lowest-labeled-zone-name*.**

  b. **Modifiez le fichier `/etc/auto_home`_*lowest-labeled-zone-name* afin qu'il désigne le fichier qui vient d'être rempli.**

  c. **Modifiez le fichier `/etc/auto_home`_*lowest-labeled-zone-name* dans chaque zone de niveau supérieur afin qu'il désigne le fichier que vous avez créé à l'Étape a.**

  Pour voir un exemple, reportez-vous à l'Exemple 11–7.

Exemple 11–3 Montage de fichiers dans une zone étiquetée en utilisant la commande `mount`

Dans cet exemple, l'administrateur système monte un système de fichiers distant à partir d'une zone publique. La zone publique se trouve sur un serveur multiniveau.

Après avoir assumé le rôle d'administrateur système, l'administrateur crée un espace de travail sous l'étiquette `PUBLIC`. Dans cet espace de travail, l'administrateur exécute la commande `mount`.

```
# zonename
public
# mount -F nfs remote-sys:/zone/public/root/opt/docs  /opt/docs
```

Un serveur de fichiers à étiquette unique possédant l'étiquette `PUBLIC` contient également des documents à monter :

```
# mount -F nfs public-sys:/publicdocs  /opt/publicdocs
```

Lorsque la zone publique du serveur de fichiers `remote-sys` est dans l'état `ready` (prêt) ou `running` (en cours d'exécution), les fichiers `remote-sys` sont montés avec succès sur ce système. Lorsque le serveur de fichiers `public-sys` est en cours d'exécution, les fichiers sont montés avec succès.

Exemple 11–4 Montage de fichiers en lecture/écriture dans une zone étiquetée en modifiant le fichier `vfstab`

Dans cet exemple, l'administrateur système monte deux systèmes de fichiers distants sous l'étiquette `PUBLIC` dans la zone publique du système local lorsque la zone publique démarre. Un montage de système de fichiers provient d'un système multiniveau, et l'autre provient d'un système à étiquette unique.

Après avoir assumé le rôle d'administrateur système, l'administrateur crée un espace de travail sous l'étiquette `PUBLIC`. Dans cet espace de travail, l'administrateur modifie le fichier `vfstab` de cette zone.

```
## Writable books directories at PUBLIC
remote-sys:/zone/public/root/opt/docs  - /opt/docs  nfs  no  yes  rw
public-sys:/publicdocs    - /opt/publicdocs  nfs no yes rw
```

Pour accéder aux fichiers de la zone étiquetée distante du système multiniveau, l'entrée `vfstab` utilise le chemin racine de la zone publique du système distant, `/zone/public/root`, comme chemin d'accès des répertoires à monter. Le chemin d'accès au système à étiquette unique est identique au chemin d'accès qui serait utilisé sur un système Oracle Solaris.

Dans une fenêtre de terminal sous l'étiquette `PUBLIC`, l'administrateur monte les fichiers.

```
# mountall
```

Exemple 11–5 Montage de fichiers de niveau inférieur dans une zone étiquetée en modifiant le fichier `vfstab`

Dans cet exemple, l'administrateur système monte un système de fichiers distant à partir d'une zone publique dans la zone internal du système local. Après avoir assumé le rôle d'administrateur système, l'administrateur crée un espace de travail sous l'étiquette `INTERNAL`, puis modifie le fichier `vfstab` dans cette zone.

```
## Readable books directory at PUBLIC
## ro entry indicates that PUBLIC docs can never be mounted rw in internal zone
remote-sys:/zone/public/root/opt/docs  - /opt/docs  nfs  no  yes  ro
```

Pour accéder aux fichiers de la zone étiquetée distante, l'entrée `vfstab` utilise le chemin racine de la zone publique du système distant, `/zone/public/root`, comme chemin d'accès des répertoires à monter.

Du point de vue d'un utilisateur dans la zone internal, les fichiers sont accessibles dans `/opt/docs`.

Dans une fenêtre de terminal sous l'étiquette `INTERNAL`, l'administrateur monte les fichiers.

```
# mountall
```

Exemple 11–6 Montage de répertoires personnels étiquetés dans un réseau administré à l'aide du protocole LDAP

Dans cet exemple, l'administrateur système permet à un nouvel utilisateur, `ikuk`, d'accéder à son répertoire personnel à chaque étiquette. Ce site utilise deux serveurs d'annuaire personnel et est géré à l'aide du protocole LDAP. Le second serveur contient les répertoires personnels des utilisateurs `jdoe` et `pkai`. Le nouvel utilisateur est ajouté à cette liste.

Après avoir assumé le rôle d'administrateur système, l'administrateur modifie tout d'abord les fichiers `auto_home_`*zone-name* dans le répertoire `/etc` de la zone globale pour inclure le nouvel utilisateur sur le second serveur d'annuaire personnel.

```
## auto_home_global file
jdoe   homedir2-server:/export/home/jdoe
pkai   homedir2-server:/export/home/pkai
ikuk   homedir2-server:/export/home/ikuk
*      homedir-server:/export/home/&

## auto_home_internal file
## Mount the home directory from the internal zone of the NFS server
jdoe   homedir2-server:/export/home/jdoe
pkai   homedir2-server:/export/home/pkai
ikuk   homedir2-server:/export/home/ikuk
*      homedir-server:/export/home/&

## auto_home_public
## Mount the home directory from the public zone of the NFS server
jdoe   homedir2-server:/export/home/jdoe
pkai   homedir2-server:/export/home/pkai
ikuk   homedir2-server:/export/home/ikuk
*      homedir-server:/export/home/&
```

Ensuite, pour permettre aux utilisateurs de se connecter à toutes les étiquettes, l'administrateur répète ces modifications pour les fichiers `auto_home_`*zone-name* à chaque étiquette.

Enfin, après avoir modifié chaque fichier `auto_home_`*zone-name* sur ce système, l'administrateur utilise ces fichiers pour ajouter des entrées à la base de données LDAP.

Comme dans le SE Oracle Solaris, l'entrée `+auto_home_public` des fichiers `/etc/auto_home_`*zone-name* dirige l'automonteur vers les entrées LDAP. Les fichiers `auto_home_`*zone-name* sur d'autres systèmes du réseau sont mis à jour à partir de la base de données LDAP.

Exemple 11–7 Montage d'un répertoire personnel de niveau inférieur sur un système administré à l'aide de fichiers

Dans cet exemple, l'administrateur système permet aux utilisateurs d'accéder à leurs répertoires personnels à chaque étiquette. Les étiquettes utilisées sur le site sont `PUBLIC`, `INTERNAL` et `NEEDTOKNOW`. Ce site a recours à deux serveurs d'annuaire personnel et est administré à l'aide de fichiers. Le second serveur contient les répertoires personnels des utilisateurs `jdoe` et `pkai`.

Pour accomplir cette tâche, l'administrateur système définit les répertoires personnels NFS de la zone publique dans cette dernière, et partage cette configuration avec les zones internal et needtoknow.

Après avoir assumé le rôle d'administrateur système, l'administrateur crée tout d'abord un espace de travail sous l'étiquette `PUBLIC`. Dans cet espace de travail, l'administrateur crée un nouveau fichier, `/export/home/auto_home_public`. Ce fichier contient toutes les entrées de spécifications NFS par utilisateur personnalisées.

```
## /export/home/auto_home_public file at PUBLIC label
jdoe   homedir2-server:/export/home/jdoe
pkai   homedir2-server:/export/home/pkai
*      homedir-server:/export/home/&
```

Ensuite, l'administrateur modifie le fichier `/etc/auto_home_public` afin qu'il désigne ce nouveau fichier.

```
## /etc/auto_home_public file in the public zone
## Use /export/home/auto_home_public for the user entries
## +auto_home_public
+ /export/home/auto_home_public
```

Cette entrée indique à l'automonteur d'utiliser le contenu du fichier local.

Enfin, l'administrateur modifie de la même façon le fichier `/etc/auto_home_public` dans les zones internal et needtoknow. L'administrateur utilise le nom du chemin d'accès à la zone publique qui est visible pour les zones internal et needtoknow.

```
## /etc/auto_home_public file in the internal zone
## Use /zone/public/export/home/auto_home_public for PUBLIC user home dirs
## +auto_home_public
+ /zone/public/export/home/auto_home_public

## /etc/auto_home_public file in the needtoknow zone
## Use /zone/public/export/home/auto_home_public for PUBLIC user home dirs
## +auto_home_public
+ /zone/public/export/home/auto_home_public
```

Lorsque l'administrateur ajoute le nouvel utilisateur `ikuk`, l'ajout est effectué dans le fichier `/export/home/auto_home_public` sous l'étiquette `PUBLIC`.

```
## /export/home/auto_home_public file at PUBLIC label
jdoe   homedir2-server:/export/home/jdoe
pkai   homedir2-server:/export/home/pkai
ikuk   homedir2-server:/export/home/ikuk
*      homedir-server:/export/home/&
```

Les zones de niveau supérieur lisent vers le bas afin d'obtenir les répertoires personnels par utilisateur de la zone publique de niveau inférieur.

▼ Dépannage des échecs de montage dans Trusted Extensions

Avant de commencer Vous devez être dans la zone possédant l'étiquette des fichiers que vous souhaitez monter. Vous devez être connecté en tant que superutilisateur ou être dans le rôle d'administrateur système.

1 Vérifiez les attributs de sécurité du serveur NFS.

Utilisez l'outil Security Templates (Modèles de sécurité) dans la Console de gestion Solaris à l'étendue appropriée. Pour plus d'informations, reportez-vous à la section "Initialisation du serveur Console de gestion Solaris dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.

a. Vérifiez que l'adresse IP du serveur NFS est un hôte assigné dans l'un des modèles de sécurité.

L'adresse peut être assignée directement, ou indirectement par le biais d'un mécanisme de caractère générique. L'adresse peut être dans un modèle étiqueté ou sans étiquette.

b. Vérifiez l'étiquette que le modèle assigne au serveur NFS.

L'étiquette doit être compatible avec l'étiquette à laquelle vous essayez de monter les fichiers.

2 Vérifiez l'étiquette de la zone actuelle.

Si l'étiquette est plus élevée que l'étiquette du système de fichiers montés, vous ne pouvez pas effectuer d'opération d'écriture dans le montage même si le système de fichiers distant est exporté avec des autorisations en lecture/écriture. Vous pouvez uniquement effectuer des opérations d'écriture sur le système de fichiers monté sous l'étiquette du montage.

3 Pour monter des systèmes de fichiers à partir d'un serveur NFS qui exécute des versions antérieures du logiciel Trusted Solaris, procédez comme suit :

- **Pour un serveur NFS Trusted Solaris 1, utilisez les options `vers=2` et `proto=udp` pour la commande `mount`.**
- **Pour un serveur NFS Trusted Solaris 2.5.1, utilisez les options `vers=2` et `proto=udp` pour la commande `mount`.**
- **Pour un serveur NFS Trusted Solaris 8, utilisez les options `vers=3` et `proto=udp` pour la commande `mount`.**

Pour monter des systèmes de fichiers à partir d'un de ces serveurs, le serveur doit être assigné à un modèle sans étiquette.

◆ ◆ ◆ CHAPITRE 12

Gestion de réseaux de confiance (présentation)

Ce chapitre décrit les concepts et les mécanismes de gestion de réseaux de confiance dans Trusted Extensions.

Le réseau de confiance

Trusted Extensions assigne des attributs de sécurité à des zones, des hôtes et des réseaux. Ces attributs garantissent que les fonctions de sécurité suivantes sont appliquées sur le réseau :

- Les données sont correctement étiquetées dans les communications réseau.
- Les règles du contrôle d'accès obligatoire (MAC, Mandatory Access Control) sont appliquées lorsque les données sont envoyées ou reçues par le biais d'un réseau local et lorsque des systèmes de fichiers sont montés.
- Les règles MAC sont appliquées lorsque des données sont acheminées vers des réseaux distants.
- Les règles MAC sont appliquées lorsque des données sont acheminées vers des zones.

Dans Trusted Extensions, les paquets réseau sont protégés par le MAC. Les étiquettes sont utilisées pour les décisions MAC. Les données sont étiquetées explicitement ou implicitement à l'aide d'une étiquette de sensibilité. Une étiquette contient un champ ID, un champ classification ou "niveau" et un champ compartiment ou "catégorie". Les données sont soumises à un contrôle d'accréditation. Ce contrôle permet de déterminer si l'étiquette est bien formée et si elle est comprise dans la plage d'accréditations de l'hôte récepteur. L'accès est accordé aux paquets bien formés compris dans la plage d'accréditations de l'hôte récepteur.

Les paquets IP échangés entre des systèmes de confiance peuvent être étiquetés. Trusted Extensions prend en charge les étiquettes CIPSO (Commercial IP Security Option, option de sécurité IP commerciale). L'étiquetage CIPSO d'un paquet permet de classer, de séparer et d'acheminer des paquets IP. Les décisions de routage comparent l'étiquette de sensibilité des données et l'étiquette de la destination.

Sur un réseau de confiance, l'étiquette est, en règle générale, générée par un hôte émetteur et traitée par l'hôte récepteur. Cependant, un routeur de confiance est également susceptible d'ajouter ou de retirer des étiquettes lors du transfert de paquets au sein d'un réseau de confiance. Une étiquette de sensibilité est mappée vers une étiquette CIPSO avant la transmission. L'étiquette CIPSO est incorporée dans le paquet IP. En règle générale, l'expéditeur et le destinataire d'un paquet opèrent à la même étiquette.

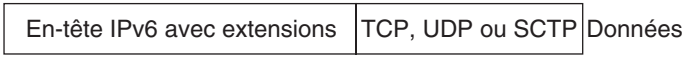
Le logiciel de gestion de réseaux de confiance veille à ce que la stratégie de sécurité de Trusted Extensions soit appliquée même lorsque les sujets (processus) et les objets (données) se trouvent sur des hôtes différents. La gestion de réseaux Trusted Extensions assure le respect du MAC dans des applications distribuées.

Paquets de données Trusted Extensions

Les paquets de données Trusted Extensions incluent une option d'étiquetage CIPSO. Les paquets de données peuvent être envoyés sur des réseaux IPv4 ou IPv6.

Dans le format IPv4 standard, l'en-tête IPv4 avec options est suivi d'un en-tête TCP, UDP ou SCTP, puis des données effectives. La version Trusted Extensions d'un paquet IPv4 utilise l'option CIPSO de l'en-tête IP pour les attributs de sécurité.

Dans le format IPv6 standard, un en-tête IPv6 avec extensions est suivi d'un en-tête TCP, UDP ou SCTP, puis des données effectives. Le paquet IPv6 de Trusted Extensions inclut une option de sécurité multiniveau dans l'en-tête avec extensions.



Communications sur le réseau de confiance

Trusted Extensions prend en charge les hôtes étiquetés et sans étiquette sur un réseau de confiance. LDAP est un service de nommage entièrement pris en charge. Plusieurs commandes et interfaces graphiques permettent d'administrer le réseau.

Les systèmes qui exécutent le logiciel Trusted Extensions prennent en charge les communications réseau entre les hôtes Trusted Extensions et n'importe lequel des types de systèmes suivants :

- D'autres systèmes qui exécutent Trusted Extensions
- Des systèmes exécutant des systèmes d'exploitation qui ne reconnaissent pas les attributs de sécurité, mais qui prennent en charge le protocole TCP/IP, tels que les systèmes Oracle Solaris, d'autres systèmes UNIX et les systèmes d'exploitation Microsoft Windows et Macintosh
- Les systèmes exécutant d'autres systèmes d'exploitation de confiance qui reconnaissent les étiquettes CIPSO

Comme dans le SE Oracle Solaris, les communications et services réseau Trusted Extensions peuvent être gérés par un service de nommage. Trusted Extensions ajoute les interfaces suivantes aux interfaces réseau Oracle Solaris :

- Trusted Extensions ajoute trois bases de données de configuration réseau, `tnzonecfg`, `tnrhdb` et `tnrhtp`. Pour plus d'informations, reportez-vous à la section "Bases de données de configuration réseau dans Trusted Extensions" à la page 170.
- La version Trusted Extensions du fichier du commutateur du service de nommage, `nsswitch.conf`, inclut des entrées pour les bases de données `tnrhtp` et `tnrhdb`. Ces entrées peuvent être modifiées afin de s'adapter à chaque configuration de site.

  Trusted Extensions utilise le service de nommage LDAP pour gérer de manière centralisée les fichiers de configuration qui définissent les hôtes, les réseaux et les utilisateurs. Les entrées `nsswitch.conf` par défaut des bases de données du réseau de confiance pour le service de nommage LDAP sont les suivantes :

  ```
  # Trusted Extensions
  tnrhtp: files ldap
  tnrhdb: files ldap
  ```

  Le service de nommage LDAP sur un Oracle Directory Server Enterprise Edition est le seul service de nommage entièrement pris en charge dans Trusted Extensions. Pour plus d'informations sur l'utilisation du service LDAP sur un système configuré avec Trusted Extensions, reportez-vous à la section Chapitre 9, "Trusted Extensions et LDAP (présentation)".
- Trusted Extensions ajoute des outils à la Console de gestion Solaris. La console est utilisée pour gérer les zones, les hôtes et les réseaux de manière centralisée. Les outils réseau sont décrits dans "Outils de la Console de gestion Solaris" à la page 40.

Le *Guide de configuration d'Oracle Solaris Trusted Extensions* indique comment définir les zones et les hôtes lors de la configuration du réseau. Pour plus d'informations, reportez-vous à la section Chapitre 13, "Gestion des réseaux dans Trusted Extensions (tâches) ".

- Trusted Extensions ajoute des commandes permettant d'administrer la gestion de réseaux de confiance. Le logiciel ajoute également des options aux commandes réseau Oracle Solaris. Pour une description de ces commandes, reportez-vous à la section "Commandes réseau dans Trusted Extensions" à la page 171.

Bases de données de configuration réseau dans Trusted Extensions

Trusted Extensions charge trois bases de données de configuration réseau dans le noyau. Ces bases de données sont utilisées lors des contrôles d'accréditation lorsque les données sont transmises à partir d'un hôte vers un autre hôte.

- `tnzonecfg` : cette base de données locale enregistre les attributs liés à la sécurité des zones. Pour chaque zone, les attributs spécifient l'étiquette de la zone ainsi l'accès de la zone à des ports à niveau unique et multiniveau. Un autre attribut gère les réponses aux messages de contrôle, tels que `ping`. Les étiquettes des zones sont définies dans le fichier `label_encodings`. Pour plus d'informations, reportez-vous aux pages de manuel `label_encodings(4)` et `smtnzonecfg(1M)`. Pour une description des ports multiniveau, reportez-vous à la section "Zones et ports multiniveau" à la page 131.
- `tnrhtp` : cette base de données stocke des modèles qui décrivent les attributs de sécurité d'hôtes et de passerelles. `tnrhtp` peut être une base de données locale ou être enregistrée sur le serveur LDAP. Les hôtes et les passerelles utilisent les attributs de l'hôte de destination et de la passerelle du prochain saut pour appliquer le MAC lors de l'envoi de trafic. À réception de trafic, les hôtes et les passerelles utilisent les attributs de l'expéditeur. Pour plus d'informations sur les attributs de sécurité, reportez-vous à la section "Attributs de sécurité du réseau de confiance" à la page 172. Pour plus d'informations, reportez-vous à la page de manuel `smtnrhtp(1M)`.
- `tnrhdb` : cette base de données contient les adresses IP et les préfixes de réseau (mécanisme de secours) correspondant à chacun des hôtes autorisés à communiquer. `tnrhdb` peut être une base de données locale ou être enregistré sur le serveur LDAP. Chaque hôte ou préfixe du réseau est assigné à un modèle de sécurité à partir de la base de données `tnrhtp`. Les attributs du modèle définissent les attributs de l'hôte assigné. Pour plus d'informations, reportez-vous à la page de manuel `smtnrhdb(1M)`.

Dans Trusted Extensions, la Console de gestion Solaris a été étendue afin de gérer ces bases de données. Pour plus d'informations, reportez-vous à la section "Outils de la Console de gestion Solaris" à la page 40.

Commandes réseau dans Trusted Extensions

Trusted Extensions ajoute les commandes suivantes pour administrer la gestion de réseaux de confiance :

- `tnchkdb` : cette commande permet de vérifier que les bases de données du réseau de confiance sont correctes. La commande `tnchkdb` est utilisée chaque fois que vous modifiez un modèle de sécurité (`tnrhtp`), une assignation de modèle de sécurité (`tnrhdb`) ou la configuration d'une zone (`tnzonecfg`). Les outils de la Console de gestion Solaris exécutent automatiquement cette commande lorsqu'une base de données est modifiée. Pour plus d'informations, reportez-vous à la page de manuel `tnchkdb(1M)`.
- `tnctl` : cette commande peut être utilisée pour mettre à jour les informations du réseau de confiance dans le noyau. `tnctl` est également un service système. Le redémarrage à l'aide de la commande `svcadm restart /network/tnctl` actualise le cache du noyau à partir des bases de données du réseau de confiance sur le système local. Les outils de la Console de gestion Solaris exécutent automatiquement cette commande lorsqu'une base de données est modifiée dans l'étendue Files (Fichiers). Pour plus d'informations, reportez-vous à la page de manuel `tnctl(1M)`.
- `tnd` : ce démon extrait les informations de `tnrhdb` et `tnrhtp` du répertoire LDAP et des fichiers locaux. Les informations issues du service de nommage sont chargées en fonction de leur ordre dans le fichier `nsswitch.conf`. Le démon `tnd` est démarré par le service `svc:/network/tnd` pendant le démarrage. Ce service dépend de `svc:/network/ldap/client`.

  La commande `tnd` permet également de déboguer et de modifier l'intervalle d'interrogation. Pour plus d'informations, reportez-vous à la page de manuel `tnd(1M)`.
- `tninfo` : cette commande affiche les informations sur l'état actuel du cache du noyau dans le réseau de confiance. La sortie peut être filtrée par nom d'hôte, par zone ou par modèle de sécurité. Pour plus d'informations, reportez-vous à la page de manuel `tninfo(1M)`.

Trusted Extensions ajoute des options aux commandes réseau Oracle Solaris suivantes :

- `ifconfig` : l'indicateur d'interface `all-zones` pour cette commande rend l'interface spécifiée disponible pour toutes les zones du système. L'étiquette associée aux données permet de déterminer la zone de distribution appropriée des données. Pour plus d'informations, reportez-vous à la page de manuel `ifconfig(1M)`.
- `netstat` : l'option `-R` étend l'utilisation d'Oracle Solaris `netstat` afin de permettre l'affichage des informations spécifiques à Trusted Extensions telles que les attributs de sécurité pour les sockets multiniveau et les entrées de table de routage. Les attributs de sécurité étendus incluent l'étiquette de l'homologue et indiquent si le socket est spécifique à une zone ou disponible pour plusieurs zones. Pour plus d'informations, reportez-vous à la page de manuel `netstat(1M)`.
- `route` : l'option `-secattr` étend l'utilisation de `route`d'Oracle Solaris afin de permettre l'affichage des attributs de sécurité de la route. La valeur de l'option a le format suivant :

`min_sl=`*label*`,max_sl=`*label*`,doi=`*integer*`,cipso`

Le mot-clé `cipso` est facultatif et défini par défaut. Pour plus d'informations, reportez-vous à la page de manuel `route(1M)`.

- `snoop` : comme dans le SE Oracle Solaris, l'option `-v` permet d'afficher les détails des en-têtes IP. Dans Trusted Extensions, les en-têtes contiennent les informations d'étiquette.

Attributs de sécurité du réseau de confiance

L'administration réseau dans Trusted Extensions repose sur des modèles de sécurité. Un modèle de sécurité décrit un ensemble d'hôtes ayant des protocoles communs et des attributs de sécurité identiques.

Les attributs de sécurité sont assignés aux systèmes (hôtes et routeurs) par le biais de modèles. L'administrateur de sécurité administre des modèles et les assigne à des systèmes. La communication avec un système auquel aucun modèle de sécurité n'est assigné n'est pas autorisée.

Chaque modèle est nommé et inclut les éléments suivants :

- Un hôte de type sans étiquette ou CIPSO. Le protocole utilisé pour les communications réseau est déterminé par le type d'hôte du modèle.

  Le type d'hôte permet de déterminer si des options CIPSO doivent être utilisées et a une incidence sur le MAC. Reportez-vous à la section “Type d'hôte et nom du modèle dans les modèles de sécurité” à la page 174.
- Un ensemble d'attributs de sécurité appliqués à chaque type d'hôte.

Pour plus d'informations sur les types d'hôtes et les attributs de sécurité, reportez-vous à la section “Attributs de sécurité réseau dans Trusted Extensions” à la page 172

Attributs de sécurité réseau dans Trusted Extensions

Trusted Extensions est installé avec un ensemble de modèles de sécurité par défaut. Lorsqu'un modèle est assigné à un hôte, les valeurs de sécurité du modèle sont appliquées à l'hôte. Dans Trusted Extensions, les hôtes étiquetés et les hôtes sans étiquette se trouvant sur le réseau se voient assigner des attributs de sécurité par le biais d'un modèle. Les hôtes auxquels aucun modèle de sécurité ne peuvent pas être atteints. Les modèles peuvent être stockés localement ou dans le service de nommage LDAP du Oracle Directory Server Enterprise Edition.

Les modèles peuvent être assignés à un hôte directement ou indirectement. L'assignation directe assigne un modèle à une adresse IP donnée. L'assignation indirecte assigne un modèle à une adresse réseau incluant l'hôte. Les hôtes sans modèle de sécurité ne peuvent pas communiquer avec les hôtes configurés à l'aide de Trusted Extensions. Pour plus d'informations sur l'assignation directe et indirecte, reportez-vous à la section “Mécanisme de secours du réseau de confiance” à la page 176.

Les modèles sont modifiés ou créés à l'aide de l'outil Modèles de sécurité dans la Console de gestion Solaris. L'outil Modèles de sécurité impose le renseignement des champs obligatoires dans les modèles. Le caractère obligatoire d'un champ dépend du type d'hôte.

Chaque type d'hôte possède son propre ensemble d'attributs de sécurité obligatoires et facultatifs supplémentaires. Les attributs de sécurité suivants sont spécifiés dans les modèles de sécurité :

- **Type d'hôte** : détermine si les paquets contiennent des étiquettes de sécurité CIPSO ou s'ils sont sans étiquette.
- **Étiquette par défaut** : détermine le niveau de fiabilité de l'hôte sans étiquette. Les paquets envoyés par un hôte sans étiquette sont lus sous cette étiquette par l'hôte ou la passerelle Trusted Extensions destinataire.

  L'attribut Étiquette par défaut est spécifique au type d'hôte sans étiquette. Pour plus d'informations, reportez-vous à la page de manuel `smtnrhtp(1M)` et aux sections suivantes.
- **DOI** : nombre entier, non nul et positif identifiant le domaine d'interprétation. Le DOI est utilisé pour indiquer quel ensemble de codages d'étiquettes s'applique à une communication réseau ou une entité réseau. Les étiquettes possédant des DOI différents sont disjointes, et ce même si elles sont identiques par ailleurs. Pour les hôtes sans étiquette, le DOI s'applique à l'étiquette par défaut. Dans Trusted Extensions, la valeur par défaut est 1.
- **Étiquette minimale** : définit l'étiquette la plus basse de la plage d'accréditations d'étiquettes. Les hôtes et les passerelles du prochain saut ne reçoivent pas les paquets dont l'étiquette est inférieure à l'étiquette minimale spécifiée dans leur modèle.
- **Étiquette maximale** : définit l'étiquette maximale de la page d'accréditations d'étiquettes. Les hôtes et les passerelles du prochain saut ne reçoivent pas les paquets dont l'étiquette est supérieure à l'étiquette maximale spécifiée dans leur modèle.
- **Ensemble d'étiquettes de sécurité** : facultatif. Spécifie un ensemble discret d'étiquettes de sécurité pour un modèle de sécurité. En plus de leur plage d'accréditations qui est déterminée par l'étiquette maximale et minimale, les hôtes assignés à un modèle incluant un ensemble d'étiquettes de sécurité peuvent envoyer et recevoir des paquets correspondant à n'importe quelle étiquette de cet ensemble d'étiquettes. Le nombre maximal d'étiquettes pouvant être spécifié est de 4.

Type d'hôte et nom du modèle dans les modèles de sécurité

Trusted Extensions prend en charge deux types d'hôtes dans les bases de données du réseau de confiance et fournit deux modèles par défaut :

- **Type d'hôte CIPSO** : destiné aux hôtes exécutant des systèmes d'exploitation de confiance. Trusted Extensions fournit le modèle nommé `cipso` pour ce type d'hôte.

  Le protocole CIPSO (Common IP Security Option, option de sécurité IP commune) indique les étiquettes de sécurité transmises au champ des options d'IP. Les étiquettes CIPSO sont automatiquement déduites de l'étiquette des données. Le type de balise 1 permet de transmettre l'étiquette de sécurité CIPSO. Cette étiquette est ensuite utilisée pour effectuer des contrôles de sécurité au niveau de l'IP et pour étiqueter les données dans le paquet réseau.
- **Type d'hôte sans étiquette** : destiné aux hôtes utilisant des protocoles de gestion de réseaux standard mais ne prenant pas en charge les options CIPSO. Trusted Extensions fournit le modèle nommé `admin_low` pour ce type d'hôte.

  Ce type d'hôte est assigné aux hôtes exécutant le SE Oracle Solaris ou d'autres systèmes d'exploitation sans étiquette. Ce type d'hôte fournit une étiquette et une autorisation par défaut s'appliquant aux communications avec l'hôte sans étiquette. En outre, une plage d'étiquettes ou un ensemble d'étiquettes discrètes peuvent être spécifiées pour permettre l'envoi de paquets à une passerelle sans étiquette chargée d'en assurer le transfert.

Attention – Le modèle `admin_low` fournit un exemple pour la construction de modèles pour hôtes sans étiquettes à l'aide d'étiquettes spécifiques à un site. Le modèle `admin_low` est obligatoire pour installer Trusted Extensions, mais les paramètres de sécurité peuvent ne pas être appropriés pour les opérations courantes du système. Conservez les modèles fournis sans modification en vue de la maintenance du système et pour les besoins de l'assistance.

Étiquette par défaut dans les modèles de sécurité

Les modèles destinés aux types d'hôtes sans étiquette spécifient une étiquette par défaut. Cette étiquette permet de contrôler les communications avec les hôtes dont le système d'exploitation ne prennent pas en compte les étiquettes, par exemple, les systèmes Oracle Solaris. L'étiquette par défaut qui est assignée reflète le niveau de confiance approprié pour l'hôte et ses utilisateurs.

Étant donné que les communications avec les hôtes sans étiquette sont essentiellement limitées à l'étiquette par défaut, ces hôtes sont également appelés *hôtes à étiquette unique*.

Domaine d'interprétation dans les modèles de sécurité

Les organisations qui utilisent le même domaine d'interprétation (DOI) s'accordent entre elles pour interpréter de façon identique les informations d'étiquette et les autres attributs de sécurité. Lorsque Trusted Extensions effectue une comparaison d'étiquettes, un contrôle vérifie que les DOI sont identiques.

Un système Trusted Extensions applique sa stratégie concernant les étiquettes à une valeur de DOI. Toutes les zones d'un système Trusted Extensions doivent utiliser le même DOI. Un système Trusted Extensions ne fournit pas de gestion des exceptions sur les paquets reçus d'un système utilisant un autre DOI.

Si votre site utilise une valeur DOI différente de la valeur par défaut, vous devez ajouter cette valeur au fichier `/etc/system` et modifier la valeur dans chaque modèle de sécurité. Pour connaître la procédure initiale, reportez-vous à la section "Configuration du domaine d'interprétation" du *Guide de configuration d'Oracle Solaris Trusted Extensions*. Pour configurer le DOI dans chaque modèle de sécurité, consultez l'Exemple 13–1.

Plage d'étiquettes dans les modèles de sécurité

Les attributs d'étiquette minimale et maximale sont utilisés pour définir la plage d'étiquettes des hôtes étiquetés et sans étiquette. Ces attributs sont utilisés pour effectuer les opérations suivantes :

- Définition de la plage d'étiquettes pouvant être utilisée lors de la communication avec un hôte CIPSO distant

  Pour qu'un paquet puisse être envoyé à un hôte de destination, il faut que son étiquette soit comprise dans la plage d'étiquettes assignée à l'hôte de destination dans le modèle de sécurité de cet hôte.
- Définition d'une plage d'étiquettes pour les paquets transférés par le biais d'une passerelle CIPSO ou d'une passerelle sans étiquette

  La plage d'étiquettes peut être spécifiée dans le modèle destiné au type d'hôte sans étiquette. La plage d'étiquettes permet à l'hôte de transférer des paquets qui ne correspondent pas nécessairement à sa propre étiquette, mais dont l'étiquette est comprise dans une plage d'étiquettes spécifiée.

Ensemble d'étiquettes de sécurité dans les modèles de sécurité

L'ensemble d'étiquettes de sécurité, qui comprend quatre étiquettes discrètes au maximum, définit les étiquettes sous lesquelles l'hôte distant peut accepter, transférer ou envoyer des paquets. Cet attribut est facultatif. Par défaut, aucun ensemble d'étiquettes de sécurité n'est défini.

Mécanisme de secours du réseau de confiance

La base de données `tnrhdb` peut assigner un modèle de sécurité à un hôte particulier de façon directe ou indirecte. L'assignation directe assigne un modèle à l'adresse IP d'un hôte. L'assignation indirecte est gérée par un mécanisme de secours. Le logiciel du réseau de confiance recherche d'abord une entrée qui assigne spécifiquement l'adresse IP de l'hôte à un modèle. Si le logiciel ne trouve pas d'entrée spécifique pour l'hôte, il recherche le "préfixe de bits correspondants le plus long". Vous pouvez attribuer indirectement un hôte à un modèle de sécurité lorsque l'adresse IP de l'hôte est comprise dans le "préfixe de bits correspondants le plus long" d'une adresse IP dont la longueur du préfixe est prédéfinie.

Dans IPv4, vous pouvez effectuer une assignation indirecte via un sous-réseau. Lorsque vous créez une assignation indirecte en utilisant 4, 3, 2 ou 1 zéro final (0) octets, le logiciel calcule respectivement des longueurs de préfixe de 0, 8, 16 ou 24. Les entrées 3 à 6 du Tableau 12–1 illustrent ce mécanisme de secours.

Vous pouvez également définir une longueur de préfixe fixe en ajoutant une barre oblique (/) suivie du nombre de bits fixes. La longueur de préfixe des adresses réseau IPv4 peut être comprise entre 1 et 32. La longueur de préfixe des adresses réseau IPv6 peut être comprise entre 1 et 128.

Le tableau qui suit fournit des exemples d'adresses de secours et d'adresses d'hôtes. Si une adresse d'un ensemble d'adresses de secours est assignée directement, le mécanisme de secours n'est pas utilisé pour cette adresse.

TABLEAU 12–1 Entrées du mécanisme de secours et de l'adresse hôte `tnrhdb`

Version IP	Entrée `tnrhdb`	Adresses couvertes
IPv4	`192.168.118.57:cipso`	`192.168.118.57`
	`192.168.118.57/32:cipso`	`/32` définit une longueur de préfixe fixe de 32 bits.
	`192.168.118.128/26:cipso`	De `192.168.118.0` à `192.168.118.63`
	`192.168.118.0:cipso`	Toutes les adresses du réseau `192.168.118.`
	`192.168.118.0/24:cipso`	
	`192.168.0.0/24:cipso`	Toutes les adresses du réseau `192.168.0.`.
	`192.168.0.0:cipso`	Toutes les adresses du réseau `192.168.`
	`192.168.0.0/16:cipso`	
	`192.0.0.0:cipso`	Toutes les adresses du réseau `192.`
	`192.0.0.0/8:cipso`	
	`192.168.0.0/32:cipso`	Adresse du réseau `192.168.0.0`. N'est pas une adresse générique.
	`192.168.118.0/32:cipso`	Adresse du réseau `192.168.118.0`. N'est pas une adresse générique.
	`192.0.0.0/32:cipso`	Adresse du réseau `192.0.0.0`. N'est pas une adresse générique.
	`0.0.0.0/32:cipso`	Adresse hôte `0.0.0.0`. N'est pas une adresse générique.
	`0.0.0.0:cipso`	Toutes les adresses de tous les réseaux
IPv6	`2001\:DB8\:22\:5000\:\:21f7:cipso`	`2001:DB8:22:5000::21f7`
	`2001\:DB8\:22\:5000\:\:0/52:cipso`	De `2001:DB8:22:5000::0` à `2001:DB8:22:5fff:ffff:ffff:ffff:ffff`
	`0\:\:0/0:cipso`	Toutes les adresses de tous les réseaux

Notez que l'adresse `0.0.0.0/32` correspond à l'adresse spécifique `0.0.0.0`. L'entrée `tnrhdb` `0.0.0.0/32:admin_low` sert sur un système où l'adresse littérale `0.0.0.0` est utilisée comme adresse IP source. Par exemple, les clients DHCP contactent le serveur DHCP en tant que `0.0.0.0` avant que le serveur ne fournisse une adresse IP aux clients.

Pour créer une entrée `tnrhdb` sur un serveur Sun Ray utilisé par les clients DHCP, reportez-vous à l'Exemple 13–13. `0.0.0.0:admin_low` étant l'entrée générique par défaut, reportez-vous à la section "Procédure de limitation des hôtes pouvant être contactés sur le réseau de confiance" à la page 196 pour connaître les aspects à prendre en compte avant de supprimer ou de modifier ce paramétrage par défaut.

Pour plus d'informations sur les longueurs de préfixe dans les adresses IPv4 et IPv6, reportez-vous à la section "Designing Your CIDR IPv4 Addressing Scheme" du *System Administration Guide: IP Services* et à la section "IPv6 Addressing Overview" du *System Administration Guide: IP Services*.

Présentation du routage dans Trusted Extensions

Dans Trusted Extensions, les routes reliant les hôtes de différents réseaux doivent permettre le maintien de la sécurité à chaque étape de la transmission. Trusted Extensions ajoute des attributs de sécurité étendus aux protocoles de routage dans le SE Oracle Solaris. À la différence du SE Oracle Solaris, cette version de Trusted Extensions ne prend pas en charge le routage dynamique. Pour plus d'informations sur la spécification d'un routage statique, reportez-vous à l'option `-p` de la page de manuel `route(1M)`.

Les passerelles et les routeurs acheminent des paquets. Dans cette section, les termes "passerelle" et "routeur" sont utilisés de façon interchangeable.

Pour les communications entre les hôtes d'un même sous-réseau, les contrôles d'accréditation sont effectuées au niveau des extrémités uniquement car aucun routeur n'est impliqué. Les vérifications de plage d'étiquettes s'effectuent au niveau de la source. Si l'hôte récepteur exécute Trusted Extensions, des vérifications de plage d'étiquettes sont également effectuées sur la destination.

Lorsque les hôtes source et de destination appartiennent à des sous-réseaux différents, le paquet est envoyé depuis l'hôte source vers une passerelle. La plage d'étiquettes de la destination et de la passerelle du premier saut sont vérifiées à la source lorsqu'une route est sélectionnée. La passerelle transmet le paquet vers le réseau auquel l'hôte de destination est connecté. Un paquet peut transiter par plusieurs passerelles avant d'atteindre la destination.

Informations générales sur le routage

Sur les passerelles Trusted Extensions, les vérifications de plage d'étiquettes sont effectuées à certaines occasions. Un système Trusted Extensions qui achemine un paquet entre deux hôtes sans étiquette compare l'étiquette par défaut de l'hôte source à l'étiquette par défaut de l'hôte de destination. Lorsque les hôtes sans étiquette ont la même étiquette par défaut, le paquet est acheminé.

Chaque passerelle gère une liste des routes conduisant à toutes les destinations. Le routage Oracle Solaris standard fait des choix afin d'optimiser l'itinéraire. Trusted Extensions fournit un logiciel supplémentaire qui contrôle les exigences de sécurité s'imposant aux itinéraires choisis. Les choix Oracle Solaris qui ne répondent pas aux exigences de sécurité sont ignorés.

Entrées de la table de routage dans Trusted Extensions

Dans Trusted Extensions, les entrées de la table de routage peuvent comprendre des attributs de sécurité. Les attributs de sécurité peuvent inclure un mot-clé `cipso`. Ils doivent également inclure une étiquette maximale, une étiquette minimale et un DOI.

Les attributs du modèle de sécurité de la passerelle sont utilisés pour les entrées n'incluant aucun attribut de sécurité.

Contrôles d'accréditation dans Trusted Extensions

Le logiciel Trusted Extensions détermine la conformité d'une route avec les exigences de sécurité. Le logiciel exécute une série de tests appelés *contrôles d'accréditation* sur l'hôte source, l'hôte de destination et les passerelles intermédiaires.

Remarque – Dans cette section, le contrôle d'accréditation effectué sur une plage d'étiquettes comprend également un contrôle sur un ensemble d'étiquettes de sécurité.

Le contrôle d'accréditation contrôle la plage d'étiquettes et les informations d'étiquette CIPSO. Les attributs de sécurité d'une route sont obtenus à partir de l'entrée de la table de routage ou du modèle de sécurité de la passerelle lorsque l'entrée ne comprend aucun attribut de sécurité.

Pour les communications entrantes, le logiciel Trusted Extensions obtient, dans la mesure du possible, directement les étiquettes à partir des paquets. L'obtention d'étiquettes à partir de paquets n'est possible que lorsque les messages sont envoyés à partir des systèmes prenant en charge l'étiquetage. Lorsque le paquet ne fournit pas d'étiquette, une étiquette par défaut est assignée au message à partir de fichiers de la base de données de gestion de réseaux de confiance. Ces étiquettes sont ensuite utilisées lors des contrôles d'accréditation. Trusted Extensions applique plusieurs contrôles aux messages sortants, aux messages transférés et aux messages entrants.

Contrôles d'accréditation des sources

Les contrôles d'accréditation suivants sont effectués sur le processus d'envoi ou la zone d'envoi :

- Pour toutes les destinations, l'étiquette des données doit être comprise dans la plage d'étiquettes du saut suivant de la route, c'est-à-dire du premier saut. En outre, l'étiquette doit être incluse dans les attributs de sécurité de la passerelle du premier saut.
- Pour toutes les destinations, le DOI d'un paquet sortant doit correspondre au DOI de l'hôte de destination. Le DOI doit également correspondre au DOI de tous les sauts de la route, y compris au DOI de la passerelle du premier saut.

- Lorsque l'hôte de destination est un hôte sans étiquette, l'une des conditions suivantes doit être satisfaite :
  - L'étiquette de l'hôte émetteur doit correspondre à l'étiquette par défaut de l'hôte de destination.
  - L'hôte émetteur est habilité à communiquer sous plusieurs étiquettes et l'étiquette de l'émetteur domine l'étiquette par défaut de la destination.
  - L'hôte émetteur est habilité à communiquer sous plusieurs étiquettes et l'étiquette de l'émetteur est `ADMIN_LOW`. En d'autres termes, l'expéditeur effectue ses envois à partir de la zone globale.

Remarque – Un contrôle du premier saut est effectué lorsqu'un message est envoyé depuis un hôte appartenant à un réseau vers un hôte appartenant à un autre réseau via une passerelle.

Contrôles d'accréditation sur les passerelles

Sur un système de passerelle Trusted Extensions, les contrôles d'accréditation suivants sont effectués sur la passerelle du prochain saut :

- Si le paquet entrant est sans étiquette, le paquet hérite de l'étiquette par défaut de l'hôte source issue de l'entrée `tnrhdb`. Dans le cas contraire, le paquet se voit affecter l'étiquette CIPSO spécifiée.
- Les contrôles de transfert des paquets sont semblables aux contrôles d'accréditation des sources :
  - Pour toutes les destinations, l'étiquette de données doit être comprise dans la plage d'étiquettes du prochain saut. En outre, l'étiquette doit être incluse dans les attributs de sécurité de l'hôte du prochain saut.
  - Pour toutes les destinations, le DOI d'un paquet sortant doit correspondre au DOI de l'hôte de destination. Le DOI doit également correspondre au DOI de l'hôte du prochain saut.
  - L'étiquette d'un paquet sans étiquette doit correspondre à l'étiquette par défaut de l'hôte de destination.
  - L'étiquette d'un paquet CIPSO doit être comprise dans la plage d'étiquettes de l'hôte de destination.

Contrôles d'accréditation des destinations

Lorsqu'un hôte Trusted Extensions reçoit des données, le logiciel effectue les contrôles suivants :

- Si le paquet entrant est sans étiquette, le paquet hérite de l'étiquette par défaut de l'hôte source issue de l'entrée `tnrhdb`. Sinon, l'étiquette CIPSO indiquée est affectée au paquet.
- L'étiquette et le DOI du paquet doivent correspondre à l'étiquette et au DOI de la zone de destination ou du processus de destination. Un processus écoutant sur un port multiniveau constitue toutefois l'exception. Le processus d'écoute peut recevoir un paquet s'il est habilité à communiquer sous plusieurs étiquettes et qu'il se trouve dans la zone globale ou qu'il possède une étiquette qui domine l'étiquette du paquet.

Administration du routage dans Trusted Extensions

Trusted Extensions prend en charge plusieurs méthodes de routage de communications entre des réseaux. Le rôle d'administrateur de sécurité permet de paramétrer des routes conformes au niveau de sécurité requis par la stratégie de sécurité de votre site.

Par exemple, les sites peuvent restreindre les communications avec l'extérieur du réseau local à une étiquette unique. Cette étiquette est appliquée aux informations mises à la disposition du public. Des étiquettes telles que `UNCLASSIFIED` ou `PUBLIC` peuvent correspondre à des informations mises à la disposition du public. Pour appliquer la restriction, ces sites assignent un modèle à étiquette unique connecté au réseau externe. Pour plus d'informations sur TCP/IP et sur le routage, reportez-vous aux sections suivantes :

- “Planning for Routers on Your Network” du *System Administration Guide: IP Services*
- “Configuring Systems on the Local Network” du *System Administration Guide: IP Services*
- “Major TCP/IP Administrative Tasks (Task Map)” du *System Administration Guide: IP Services*
- “Préparation du réseau pour le service DHCP (liste des tâches)” du *Guide d'administration système : services IP*

Choix de routeurs dans Trusted Extensions

En matière de routeurs, les hôtes Trusted Extensions offrent le niveau de sécurité le plus élevé. D'autres types de routeurs risquent de ne pas reconnaître les attributs de sécurité Trusted Extensions. Sans l'intervention des administrateurs, les paquets peuvent être acheminés via des routeurs qui n'assurent pas la protection MAC.

- Les routeurs CIPSO rejettent les paquets lorsqu'ils ne trouvent pas le bon type d'information dans la section des options IP du paquet. Par exemple, un routeur CIPSO rejette un paquet s'il ne parvient pas à trouver une option CIPSO dans les options IP lorsque l'option est requise, ou lorsque le DOI dans les options IP n'est pas compatible avec l'accréditation de la destination.
- D'autres types de routeurs qui n'exécutent pas Trusted Extensions peuvent être configurés pour transmettre les paquets ou pour rejeter les paquets incluant l'option CIPSO. Seules les passerelles qui reconnaissent CIPSO telles que celles fournies par Trusted Extensions sont en mesure d'exploiter les contenus de l'option IP CIPSO pour appliquer le MAC.

Pour prendre en charge le routage sécurisé, les tables de routage Solaris10 sont étendues et incluent les attributs de sécurité Trusted Extensions. Les attributs sont décrits dans la section "Entrées de la table de routage dans Trusted Extensions" à la page 179. Trusted Extensions prend en charge le routage statique, dans lequel l'administrateur crée manuellement les entrées de la table de routage. Pour plus d'informations, reportez-vous à l'option `-p` sur la page de manuel `route`(1M).

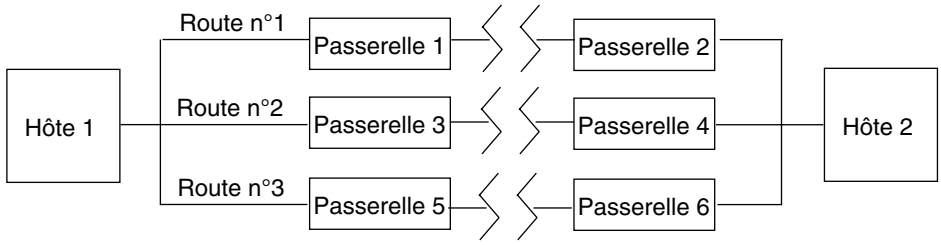
Le logiciel de routage tente de trouver un itinéraire vers l'hôte de destination dans les tables de routage. Lorsque l'hôte n'est pas explicitement nommé, le logiciel de routage recherche une entrée correspondant au sous-réseau où réside l'hôte. Lorsque ni l'hôte, ni le réseau où réside l'hôte n'est défini, l'hôte envoie le paquet vers une passerelle par défaut, lorsqu'une telle passerelle est définie. Plusieurs passerelles par défaut peuvent être définies et toutes sont traitées de façon égale.

Dans cette version de Trusted Extensions, l'administrateur de sécurité configure les routes manuellement, puis modifie manuellement la table de routage lorsque les circonstances changent. Par exemple, de nombreux sites possèdent une passerelle unique qui communique avec le monde extérieur. Cette passerelle unique peut être définie de façon statique comme passerelle *par défaut* sur chaque hôte du réseau. La prise en charge du routage dynamique sera peut-être intégrée dans les futures versions de Trusted Extensions.

Passerelles dans Trusted Extensions

Vous trouverez ci-dessous un exemple de routage dans Trusted Extensions. Le diagramme et le tableau présentent trois itinéraires possibles entre l'hôte 1 et l'hôte 2.

FIGURE 12–1 Routes et entrées de table de routage Trusted Extensions types



Route	Passerelle du premier saut	Étiquette minimale	Étiquette maximale	DOI
N°1	Passerelle 1	`CONFIDENTIAL`	`SECRET`	1
N°2	Passerelle 3	`ADMIN_LOW`	`ADMIN_HIGH`	1
N°3	Passerelle 5			

- La route n°1 permet de transmettre des paquets dans la plage d'étiquettes allant de `CONFIDENTIAL` à `SECRET`.
- La route n°2 permet de transmettre des paquets dont l'étiquette est comprise entre `ADMIN_LOW` et `ADMIN_HIGH`.
- La route n°3 ne spécifie aucune information de routage. Par conséquent, ses attributs de sécurité sont obtenus à partir du modèle provenant de la base de données `tnrhtp` pour la passerelle 5.

Commandes de routage dans Trusted Extensions

Pour afficher les étiquettes et les attributs de sécurité étendus des sockets, Trusted Extensions modifie les commandes réseau d'Oracle Solaris suivantes :

- La commande `netstat -rR` affiche les attributs de sécurité dans les entrées de la table de routage.
- La commande `netstat -aR` affiche les attributs de sécurité des sockets.
- La commande `route -p` associée à l'option `add` (ajouter) ou `delete` (supprimer) permet de modifier les entrées de la table de routage.

Pour plus d'informations, reportez-vous aux pages de manuel `netstat(1M)` et `route(1M)`.

Pour des exemples, reportez-vous à la section "Procédure de configuration de routes à l'aide d'attributs de sécurité" à la page 201.

◆ ◆ ◆ CHAPITRE 13

Gestion des réseaux dans Trusted Extensions (tâches)

Ce chapitre fournit des informations sur l'implémentation et les procédures permettant de sécuriser un réseau Trusted Extensions.

Gestion du réseau de confiance (liste des tâches)

Le tableau suivant contient des liens vers les listes des tâches répertoriant les procédures courantes de gestion de réseaux de confiance.

Tâche	Description	Voir
Configuration de bases de données réseau.	Crée des modèles d'hôte distant et assigne des hôtes aux modèles.	"Configuration des bases de données réseau de confiance (liste des tâches)" à la page 186
Configuration du routage et vérification des bases de données réseau et des informations réseau dans le noyau.	Configure des routes statiques permettant aux paquets étiquetés d'atteindre leur destination via des passerelles étiquetées et non étiquetées. Affiche également l'état de votre réseau.	"Configuration de routes et vérification des informations réseau dans Trusted Extensions (liste des tâches)" à la page 200
Dépannage des problèmes de réseau.	Étapes à suivre lors du diagnostic de problèmes de réseau liés à des paquets étiquetés.	"Dépannage du réseau de confiance (liste des tâches)" à la page 207

Configuration des bases de données réseau de confiance (liste des tâches)

Le logiciel Trusted Extensions comprend les bases de données `tnrhtp` et `tnrhdb`. Ces bases de données fournissent des étiquettes aux hôtes distants qui contactent le système. La Console de gestion Solaris fournit l'interface graphique que vous utilisez pour administrer ces bases de données.

La liste ci-dessous décrit les tâches à exécuter pour créer des modèles de sécurité et les appliquer aux hôtes.

Tâche	Description	Voir
Évaluation de la nécessité d'utiliser des modèles de sécurité personnalisés sur votre site.	Évalue les modèles existants en fonction des exigences de sécurité de votre site.	“Procédure d'évaluation de la nécessité d'utiliser des modèles de sécurité personnalisés sur votre site ” à la page 187
Accès à l'outil Modèles de sécurité dans la Console de gestion Solaris.	Accède à l'outil de modification des bases de données du réseau de confiance.	“Procédure d'ouverture des outils de gestion de réseaux de confiance” à la page 188
Modification de modèles de sécurité.	Modifie les définitions des attributs de sécurité de votre réseau de confiance en modifiant les bases de données du réseau de confiance.	“Procédure de construction d'un modèle d'hôte distant” à la page 189
	Change la valeur du DOI en une valeur autre que 1.	Exemple 13–1
	Crée un modèle de sécurité pour les hôtes étiquetés limitant la communication entre les autres hôtes à une seule étiquette.	Exemple 13–2
	Crée un modèle de sécurité pour les hôtes non étiquetés agissant en tant que passerelles à étiquette unique.	Exemple 13–3
	Crée un modèle de sécurité pour les hôtes dont la plage d'étiquettes est limitée.	Exemple 13–4
	Crée un modèle de sécurité pour un hôte spécifiant un ensemble d'étiquettes discrètes dans sa plage d'étiquettes.	Exemple 13–5
	Crée un modèle de sécurité pour des réseaux et systèmes non étiquetés.	Exemple 13–6
	Crée un modèle de sécurité pour deux systèmes de développeurs.	Exemple 13–7

Tâche	Description	Voir
Ajout d'hôtes au réseau connu.	Ajoute des systèmes et des réseaux au réseau de confiance.	"Procédure d'ajout d'hôtes au réseau connu du système " à la page 194
Fourniture d'accès à des hôtes distants à l'aide d'entrées génériques.	Permet à des hôtes faisant partie d'un intervalle d'adresses IP de communiquer avec un système en assignant indirectement chaque hôte au même modèle de sécurité.	Exemple 13–8 Exemple 13–9 Exemple 13–10
Modification de l'entrée générique `admin_low` dans le fichier `tnrhdb`.	Renforce la sécurité en remplaçant l'entrée générique par des adresses spécifiques que l'hôte doit contacter au moment de l'initialisation.	"Procédure de limitation des hôtes pouvant être contactés sur le réseau de confiance" à la page 196
	Renforce la sécurité en remplaçant l'entrée générique par un réseau d'hôtes étiquetés en tant que valeur par défaut.	Exemple 13–11
Création d'une entrée pour l'adresse d'hôte `0.0.0.0`.	Configure un serveur Sun Ray de manière à ce qu'il accepte le contact initial provenant d'un client distant.	Exemple 13–13
Assignation de modèles de sécurité.	Associe un modèle à une adresse IP ou à une liste d'adresses IP contiguës.	"Procédure d'assignation d'un modèle de sécurité à un hôte ou à un groupe d'hôtes" à la page 194

▼ Procédure d'évaluation de la nécessité d'utiliser des modèles de sécurité personnalisés sur votre site

Avant de commencer Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

1 Familiarisez-vous avec les modèles de Trusted Extensions.

Lisez le fichier `tnrhtp` sur un hôte local. Les commentaires qu'il contient sont utiles. Vous pouvez également afficher les valeurs des attributs de sécurité dans l'outil Security Templates (Modèles de sécurité) de la Console de gestion Solaris.

- Les modèles par défaut conviennent pour n'importe quel type d'installation. La plage d'étiquettes de chaque modèle s'étend de `ADMIN_LOW` à `ADMIN_HIGH`.
- Le modèle `cipso` définit un type d'hôte CIPSO dont la valeur du DOI est `1`. La plage d'étiquettes du modèle s'étend de `ADMIN_LOW` à `ADMIN_HIGH`.
- Le modèle `admin_low` définit un hôte non étiqueté dont la valeur du DOI est `1`. L'étiquette par défaut du modèle est `ADMIN_LOW`. La plage d'étiquettes du modèle s'étend de `ADMIN_LOW` à `ADMIN_HIGH`. Dans la configuration par défaut, l'adresse `0.0.0.0` est assignée à ce modèle. Par conséquent, tous les hôtes non CIPSO sont traités comme des hôtes fonctionnant sous l'étiquette de sécurité `ADMIN_LOW`.

2 **Conservez les modèles par défaut.**

Pour permettre une assistance en cas de besoin, vous ne devez pas supprimer ni modifier les modèles par défaut. Vous pouvez modifier l'hôte auquel ces modèles par défaut sont assignés. Pour consulter un exemple, reportez-vous à la section "Procédure de limitation des hôtes pouvant être contactés sur le réseau de confiance" à la page 196.

3 **Créez de nouveaux modèles si vous souhaitez effectuer l'une des opérations suivantes :**

- Limiter la plage d'étiquettes d'un hôte ou d'un groupe d'hôtes.
- Créer un hôte à étiquette unique.
- Créer un hôte capable de reconnaître certaines étiquettes discrètes.
- Utiliser un DOI autre que `1`.
- Utiliser une étiquette par défaut autre que `ADMIN_LOW` pour les hôtes non étiquetés.

Pour plus d'informations, reportez-vous à la section "Procédure de construction d'un modèle d'hôte distant" à la page 189.

▼ Procédure d'ouverture des outils de gestion de réseaux de confiance

Avant de commencer Vous devez accéder à la zone globale à l'aide d'un rôle capable de modifier la sécurité du réseau. Par exemple, les rôles auxquels les profils de droits Information Security (Sécurité des informations) et Network Security (Sécurité du réseau) sont assignés sont autorisés à modifier les paramètres de sécurité. Le rôle d'administrateur de sécurité inclut ces profils.

Pour utiliser la boîte à outils LDAP, vous devez avoir effectué toutes les tâches décrites dans la section "Configuration de la Console de gestion Solaris pour LDAP (liste des tâches)" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.

1 **Démarrez la Console de gestion Solaris.**

Pour plus d'informations, reportez-vous à la section "Initialisation du serveur Console de gestion Solaris dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.

2 **Utilisez l'outil approprié.**

- Pour modifier un modèle, utilisez l'outil Security Templates (Modèles de sécurité).

  Tous les modèles actuellement définis s'affichent dans le volet de droite. Lorsque vous sélectionnez ou créez un modèle, l'aide en ligne est disponible dans le volet de gauche.
- Pour assigner un hôte à un modèle, utilisez l'outil Security Templates.
- Pour créer un hôte pouvant être assigné à un modèle, utilisez l'outil Computers and Networks (Ordinateurs et réseaux).

- Pour assigner une étiquette à une zone, utilisez l'outil Trusted Network Zones (Zones de réseau de confiance). Pour plus d'informations sur les zones dans Trusted Extensions, reportez-vous à la section Chapitre 10, “Gestion des zones dans Trusted Extensions (tâches)”.

▼ Procédure de construction d'un modèle d'hôte distant

Avant de commencer Vous devez accéder à la zone globale à l'aide d'un rôle capable de modifier la sécurité du réseau. Par exemple, les rôles auxquels les profils de droits Information Security (Sécurité des informations) et Network Security (Sécurité du réseau) sont assignés sont autorisés à modifier les paramètres de sécurité. Le rôle d'administrateur de sécurité inclut ces profils.

1. **Dans la Console de gestion Solaris, accédez à l'outil Security Templates (Modèles de sécurité).**

   Reportez-vous à la section “Procédure d'ouverture des outils de gestion de réseaux de confiance” à la page 188 pour connaître les étapes à effectuer.

2. **Sous Computers and Networks (Ordinateurs et réseaux), double-cliquez sur Security Templates.**

   Les modèles existants apparaissent dans le volet d'affichage. Ces modèles décrivent les attributs de sécurité des hôtes que ce système peut contacter. Il s'agit notamment d'hôtes CIPSO qui exécutent Trusted Extensions et d'hôtes non étiquetés.

3. **Examinez le modèle `cipso`.**

   Voyez à quels hôtes et réseaux ce modèle est déjà assigné.

4. **Examinez le modèle `admin_low`.**

   Voyez à quels hôtes et réseaux ce modèle est déjà assigné.

5. **Créez un modèle.**

   Si les modèles fournis ne décrivent pas suffisamment les hôtes autorisés à communiquer avec ce système, choisissez Add Template (Ajouter un modèle) dans le menu Action.

   Utilisez l'aide en ligne si vous avez besoin d'aide. Avant d'affecter des hôtes aux modèles, créez tous les modèles requis par votre site.

6. **(Facultatif) Modifiez un modèle existant qui n'est pas un modèle par défaut.**

   Double-cliquez sur le modèle et utilisez l'aide en ligne pour obtenir de l'assistance. Vous pouvez modifier les hôtes ou les réseaux assignés.

Exemple 13–1 Création d'un modèle de sécurité avec une valeur de DOI différente

Dans cet exemple, le réseau de l'administrateur de sécurité possède un DOI dont la valeur est différente de 1. L'équipe ayant initialement configuré le système a effectué les tâches décrites dans la section "Configuration du domaine d'interprétation" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.

L'administrateur de sécurité confirme dans un premier temps la valeur du DOI dans le fichier /etc/system :

```
# grep doi /etc/system
set default_doi = 4
```

Ensuite, dans l'outil Security Templates (Modèles de sécurité), la valeur du doi de chaque modèle créé par l'administrateur est définie sur 4. Pour le système à étiquette unique décrit dans l'Exemple 13–2, l'administrateur de sécurité crée le modèle suivant :

```
template: CIPSO_PUBLIC
host_type: CIPSO
doi: 4
min_sl: PUBLIC
max_sl: PUBLIC
```

Exemple 13–2 Création d'un modèle de sécurité à étiquette unique

Dans cet exemple, l'administrateur de sécurité souhaite créer une passerelle qui permette uniquement la transmission de paquets d'une seule étiquette, l'étiquette PUBLIC. À l'aide de l'outil Security Templates de la Console de gestion Solaris, l'administrateur crée un modèle et assigne l'hôte de passerelle au modèle.

Il ajoute tout d'abord l'hôte de passerelle et l'adresse IP à l'outil Computers and Networks (Ordinateurs et réseaux).

```
gateway-1
192.168.131.75
```

Puis il crée le modèle dans l'outil Security Templates.Ci-dessous, les valeurs du modèle :

```
template: CIPSO_PUBLIC
host_type: CIPSO
doi: 1
min_sl: PUBLIC
max_sl: PUBLIC
```

L'outil fournit la valeur hexadécimale pour PUBLIC, 0X0002-08-08.

L'hôte gateway-1 (passerelle 1) est ensuite assigné au modèle par le biais de son nom et de son adresse IP.

```
gateway-1
192.168.131.75
```

Sur un hôte local, l'entrée `tnrhtp` se présente de la manière suivante :

```
cipso_public:host_type=cipso;doi=1;min_sl=0X0002-08-08;max_sl=0X0002-08-08;
```

Sur un hôte local, l'entrée `tnrhdb` se présente de la manière suivante :

```
# gateway-1
192.168.131.75:cipso_public
```

Exemple 13–3 Création d'un modèle de sécurité pour un routeur non étiqueté

Tous les routeurs IP sont capables de transférer des messages pourvus d'étiquettes CIPSO, et ce même si les étiquettes ne sont pas explicitement prises en charge par le routeur. Ces routeurs non étiquetés nécessitent une étiquette par défaut définissant le niveau de traitement des connexions au routeur (pour la gestion du routeur par exemple). Dans cet exemple, l'administrateur de sécurité crée un routeur capable de transférer le trafic de n'importe quelle étiquette, mais toutes les communications directes avec le routeur sont gérées sous l'étiquette par défaut `PUBLIC`.

Dans la Console de gestion Solaris, l'administrateur crée un modèle auquel il assigne l'hôte de passerelle.

Il ajoute tout d'abord le routeur et son adresse IP à l'outil Computers and Networks (Ordinateurs et réseaux).

```
router-1
192.168.131.82
```

Il crée ensuite le modèle dans l'outil Security Templates (Modèles de sécurité). Le modèle contient les valeurs suivantes :

```
Template Name: UNL_PUBLIC
Host Type: UNLABELED
DOI: 1
Default Label: PUBLIC
Minimum Label: ADMIN_LOW
Maximum Label: ADMIN_HIGH
```

L'outil fournit la valeur hexadécimale des étiquettes.

Enfin, il assigne le routeur `routeur-1` au modèle par le biais de son nom et de son adresse IP.

```
router-1
192.168.131.82
```

Exemple 13–4 Création d'un modèle de sécurité prenant en charge une plage d'étiquettes limitée

Dans cet exemple, l'administrateur de sécurité souhaite créer une passerelle limitant les paquets à une plage d'étiquettes restreinte. Dans la Console de gestion Solaris, l'administrateur crée un modèle auquel il assigne l'hôte de passerelle.

Il ajoute tout d'abord l'hôte et son adresse IP à l'outil Computers and Networks (Ordinateurs et réseaux).

```
gateway-ir
192.168.131.78
```

Il crée ensuite le modèle dans l'outil Security Templates. Le modèle contient les valeurs suivantes :

```
Template Name: CIPSO_IUO_RSTRCT
Host Type: CIPSO
DOI: 1
Minimum Label: CONFIDENTIAL : INTERNAL USE ONLY
Maximum Label: CONFIDENTIAL : RESTRICTED
```

L'outil fournit la valeur hexadécimale des étiquettes.

Enfin, il assigne la passerelle `gateway-ir` au modèle par le biais de son nom et de son adresse IP.

```
gateway-ir
192.168.131.78
```

Exemple 13–5 Création d'un modèle de sécurité prenant en charge un ensemble d'étiquettes de sécurité

Dans cet exemple, l'administrateur de sécurité souhaite créer un modèle de sécurité capable de reconnaître deux étiquettes seulement. Dans la Console de gestion Solaris, l'administrateur crée un modèle auquel il assigne l'hôte de passerelle.

Il ajoute tout d'abord tous les hôtes et toutes les adresses IP qui utiliseront ce modèle à l'outil Computers and Networks (Ordinateurs et réseaux).

```
host-slset1
192.168.132.21

host-slset2
192.168.132.22

host-slset3
192.168.132.23

host-slset4
192.168.132.24
```

Il crée ensuite le modèle dans l'outil Security Templates. Le modèle contient les valeurs suivantes :

```
Template Name: CIPSO_PUB_RSTRCT
Host Type: CIPSO
DOI: 1
Minimum Label: PUBLIC
Maximum Label: CONFIDENTIAL : RESTRICTED
SL Set: PUBLIC, CONFIDENTIAL : RESTRICTED
```

L'outil fournit la valeur hexadécimale des étiquettes.

Il assigne ensuite la plage d'adresses IP au modèle à l'aide du bouton générique et d'un préfixe.

```
192.168.132.0/17
```

Exemple 13–6 Création d'un modèle non étiqueté sous l'étiquette PUBLIC

Dans cet exemple, l'administrateur de sécurité permet à un sous-réseau de systèmes Oracle Solaris d'adopter l'étiquette PUBLIC dans le réseau de confiance. Le modèle contient les valeurs suivantes :

```
Template Name: public
Host Type: Unlabeled
Default Label: Public
Minimum Label: Public
Maximum Label: Public
DOI: 1

Wildcard Entry: 10.10.0.0
Prefix: 16
```

Tous les systèmes du sous-réseau `10.10.0.0` sont traités sous l'étiquette PUBLIC.

Exemple 13–7 Création d'un modèle étiqueté pour les développeurs

Dans cet exemple, l'administrateur de sécurité crée un modèle SANDBOX. Ce modèle est assigné aux systèmes utilisés par les développeurs de logiciels de confiance. Les deux systèmes auxquels ce modèle est assigné créent et testent des programmes étiquetés. Cependant, leurs tests n'affectent pas les autres systèmes étiquetés, car l'étiquette SANDBOX est disjointe des autres étiquettes du réseau.

```
Template Name: cipso_sandbox
Host Type: CIPSO
Minimum Label: SANDBOX
Maximum Label: SANDBOX
DOI: 1

Hostname: DevMachine1
IP Address: 196.168.129.129

Hostname: DevMachine2
IP Address: 196.168.129.102
```

Les développeurs qui utilisent ces systèmes peuvent communiquer les uns avec les autres à l'aide de l'étiquette SANDBOX.

▼ Procédure d'ajout d'hôtes au réseau connu du système

L'outil Computers (Ordinateurs) de la Console de gestion Solaris est identique à l'outil Computers d'SE Oracle Solaris. La procédure est décrite ici pour votre commodité. Une fois que vous connaissez les hôtes, vous les assignez à un modèle de sécurité.

Avant de commencer Vous devez assumer un rôle d'administrateur autorisé à gérer les réseaux. Par exemple, les rôles incluant les profils de droits Network Management (Gestion du réseau) ou System Administrator (Administrateur système) peuvent gérer des réseaux.

1. **Dans la Console de gestion Solaris, accédez à l'outil Computers.**

   Pour plus d'informations, reportez-vous à la section "Procédure d'ouverture des outils de gestion de réseaux de confiance" à la page 188.

2. **Dans l'outil Computers, confirmez que vous souhaitez afficher tous les ordinateurs du réseau.**

3. **Ajoutez un hôte que ce système peut contacter.**

   Vous devez ajouter tous les hôtes que ce système est susceptible de contacter, y compris les routeurs statiques et les serveurs d'audit.

   a. **Dans le menu Action, sélectionnez Add Computer (Ajouter un ordinateur).**

   b. **Identifiez l'hôte par son nom et son adresse IP.**

   c. **(Facultatif) Fournissez des informations supplémentaires sur l'hôte.**

   d. **Pour ajouter l'hôte, cliquez sur Appliquer.**

   e. **Lorsque les entrées sont terminées, cliquez sur OK.**

4. **Ajoutez un groupe d'hôtes que ce système peut contacter.**

   Utilisez l'aide en ligne pour ajouter des groupes d'hôtes à l'aide d'une adresse IP de réseau.

▼ Procédure d'assignation d'un modèle de sécurité à un hôte ou à un groupe d'hôtes

Avant de commencer Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

Tous les hôtes que vous souhaitez assigner à un modèle doivent exister dans l'outil Computers and Networks (Ordinateurs et réseaux). Pour plus d'informations, reportez-vous à la section "Procédure d'ajout d'hôtes au réseau connu du système " à la page 194.

1. **Dans la Console de gestion Solaris, accédez à l'outil Security Templates (Modèles de sécurité).**

   Pour plus d'informations, reportez-vous à la section "Procédure d'ouverture des outils de gestion de réseaux de confiance" à la page 188.

2. **Double-cliquez sur le nom du modèle approprié.**

3. **Cliquez sur l'onglet Hosts Assigned to Template (Hôtes assignés au modèle).**

4. **Pour assigner le modèle à un hôte unique, effectuez l'une des opérations suivantes :**

   a. **Dans le champ Nom d'hôte, saisissez le nom de l'hôte.**

   b. **Dans le champ Adresse IP, saisissez l'adresse de hôte.**

   c. **Cliquez sur le bouton Add (Ajouter).**

   d. **Cliquez sur OK pour enregistrer vos modifications.**

5. **Pour assigner un modèle à un groupe d'hôtes possédant des adresses contiguës, procédez comme suit :**

   a. **Cliquez sur Wildcard (Générique).**

   b. **Dans le champ IP Address (Adresse IP), saisissez l'adresse IP.**

   c. **Dans le champ Prefix (Préfixe), entrez le préfixe qui décrit le groupe d'adresses contiguës.**

   d. **Cliquez sur le bouton Add (Ajouter).**

   e. **Cliquez sur OK pour enregistrer vos modifications.**

Exemple 13–8 Ajout d'un réseau IPv4 en tant qu'entrée générique

Dans l'exemple suivant, un administrateur de sécurité assigne plusieurs sous-réseaux IPv4 à un même modèle de sécurité. Dans l'onglet Hosts Assigned to Template (Hôtes assignés au modèle), l'administrateur ajoute les entrées génériques suivantes :

```
IP Address: 192.168.113.0
IP address: 192.168.75.0
```

Exemple 13–9 Ajout d'une liste d'hôtes IPv4 en tant qu'entrée générique

Dans l'exemple ci-dessous, un administrateur de sécurité assigne au même modèle de sécurité à des adresses IPv4 contiguës non alignées sur des limites d'octets. Dans l'onglet Hosts Assigned to Template (Hôtes assignés au modèle), l'administrateur ajoute les entrées génériques suivantes :

```
IP Address: 192.168.113.100
Prefix Length: 25
```

Cette entrée générique couvre la plage d'adresses comprise entre `192.168.113.0` et `192.168.113.127`. L'adresse inclut `192.168.113.100`.

Exemple 13–10 Ajout d'une liste d'hôtes IPv6 en tant qu'entrée générique

Dans l'exemple suivant, un administrateur de sécurité assigne des adresses IPv6 contiguës au même modèle de sécurité. Dans l'onglet Hosts Assigned to Template (Hôtes assignés au modèle), l'administrateur ajoute les entrées génériques suivantes :

```
IP Address: 2001:a08:3903:200::0
Prefix Length: 56
```

Cette entrée générique couvre la plage d'adresses comprise entre `2001:a08:3903:200::0` et `2001:a08:3903:2ff:ffff:ffff:ffff:ffff`. L'adresse inclut `2001:a08:3903:201:20e:cff:fe08:58c`.

▼ Procédure de limitation des hôtes pouvant être contactés sur le réseau de confiance

Cette procédure empêche que les hôtes étiquetés ne soient contactés par des hôtes non étiquetés arbitraires. Lorsque Trusted Extensions est installé, ce modèle par défaut définit chaque hôte sur le réseau. Utilisez cette procédure pour énumérer des hôtes non étiquetés spécifiques.

Le fichier local `tnrhdb` présent sur chaque système est utilisé pour établir le contact avec le réseau lors de l'initialisation. Par défaut, tous les hôtes qui ne sont pas pourvus d'un modèle CIPSO sont définis par le modèle `admin_low`. Ce modèle définit tous les systèmes non définis par ailleurs (`0.0.0.0`) comme étant des systèmes sans étiquette et leur assigne l'étiquette par défaut `admin_low`.

Attention – Le modèle `admin_low` par défaut peut présenter un risque de sécurité sur le réseau Trusted Extensions. Si la sécurité du site nécessite une protection renforcée, l'administrateur de sécurité peut supprimer l'entrée générique `0.0.0.0` une fois le système installé. L'entrée doit être remplacée par une série d'entrées correspondant à chacun des hôtes que le système contacte lors de l'initialisation.

Doivent par exemple figurer dans le fichier local `tnrhdb` après la suppression de l'entrée générique `0.0.0.0` les serveurs DNS, les serveurs d'annuaire personnel, les serveurs d'audit, les adresses de diffusion et de multidiffusion et les routeurs.

Si une application reconnaît initialement les clients sur l'adresse d'hôte `0.0.0.0`, vous devez ajouter l'entrée d'hôte `0.0.0.0/32:admin_low` dans la base de données `tnrhdb`. Par exemple, pour recevoir les demandes de connexion initiale de clients Sun Ray potentiels, les serveurs Sun Ray doivent inclure cette entrée. Une fois que le serveur a reconnu les clients, une adresse IP est attribuée aux clients et ces derniers sont connectés en tant que clients CIPSO.

Avant de commencer

Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

Tous les hôtes qui doivent être contactés lors de l'initialisation doivent exister dans l'outil Computers and Networks (Ordinateurs et réseaux).

1. **Dans la Console de gestion Solaris, accédez à l'outil Security Templates (Modèles de sécurité) dans l'étendue Fichiers.**

   L'étendue fichiers protège le système lors de l'initialisation. Pour accéder à l'outil Security Templates, reportez-vous à la section "Procédure d'ouverture des outils de gestion de réseaux de confiance" à la page 188.

2. **Modifiez les hôtes assignés au modèle `admin_low`.**

   a. **Double-cliquez sur le modèle `admin_low`.**

      Tous les hôtes ajoutés peuvent être contactés pendant l'initialisation sous l'étiquette `ADMIN_LOW`.

   b. **Cliquez sur l'onglet Hosts Assigned to Template (Hôtes assignés au modèle).**

      Tous les hôtes ajoutés peuvent être contactés pendant l'initialisation sous l'étiquette `ADMIN_LOW`.

   c. **Ajoutez tous les hôtes non étiquetés qui doivent être contactés lors de l'initialisation.**

      Pour plus d'informations, reportez-vous à la section "Procédure d'assignation d'un modèle de sécurité à un hôte ou à un groupe d'hôtes" à la page 194.

      Incluez tous les routeurs infra-réseau n'exécutant pas Trusted Extensions via lesquels cet hôte doit communiquer

d. Ajoutez les plages d'hôtes qui doivent être contactés lors de l'initialisation.

e. Supprimez l'entrée `0.0.0.0`.

3 Modifiez les hôtes assignés au modèle `cipso`.

a. Double-cliquez sur le modèle `cipso`.

Tous les hôtes ajoutés peuvent être contactés durant l'initialisation.

b. Cliquez sur l'onglet Hosts Assigned to Template (Hôtes assignés au modèle).

Tous les hôtes ajoutés peuvent être contactés pendant l'initialisation sous l'étiquette `ADMIN_LOW`.

c. Ajoutez chaque hôte étiqueté qui doit être contacté lors de l'initialisation.

Pour plus d'informations, reportez-vous à la section "Procédure d'assignation d'un modèle de sécurité à un hôte ou à un groupe d'hôtes" à la page 194.

- Incluez le serveur LDAP.
- Incluez tous les routeurs infra-réseau exécutant Trusted Extensions via lesquels cet hôte doit communiquer
- Assurez-vous que toutes les interfaces réseau sont assignées au modèle.
- Incluez les adresses de diffusion.

d. Ajoutez les plages d'hôtes qui doivent être contactés lors de l'initialisation.

4 Assurez-vous que les assignations d'hôtes n'empêchent pas le système de s'initialiser.

Exemple 13–11 Modification de l'étiquette de l'entrée `tnrhdb 0.0.0.0`

Dans cet exemple, l'administrateur de sécurité crée un système de passerelles publiques. L'administrateur supprime l'entrée `0.0.0.0` du modèle `admin_low` et assigne l'entrée à un modèle sans étiquette nommé `public`. Le système reconnaît ensuite tout système non répertorié dans son fichier `tnrhdb` comme un système non étiqueté possédant les attributs de sécurité du modèle de sécurité `public`.

Le tableau suivant décrit un modèle sans étiquette conçu spécifiquement pour les passerelles publiques.

```
Template Name: public
Host Type: Unlabeled
Default Label: Public
Minimum Label: Public
Maximum Label: Public
DOI: 1
```

Exemple 13–12 Énumération des ordinateurs à contacter durant l'initialisation dans la base de données `tnrhdb`

L'exemple suivant présente la base de données `tnrhdb` locale comportant des entrées pour un client LDAP avec deux interfaces réseau. Le client communique avec un autre réseau et des routeurs.

```
127.0.0.1:cipso             Loopback address
192.168.112.111:cipso       Interface 1 of this host
192.168.113.111:cipso       Interface 2 of this host
10.6.6.2:cipso              LDAP server
192.168.113.6:cipso         Audit server
192.168.112.255:cipso       Subnet broadcast address
192.168.113.255:cipso       Subnet broadcast address
192.168.113.1:cipso         Router
192.168.117.0:cipso         Another Trusted Extensions network
192.168.112.12:public       Specific network router
192.168.113.12:public       Specific network router
224.0.0.2:public            Multicast address
255.255.255.255:admin_low       Broadcast address
```

Exemple 13–13 Transformation de l'adresse hôte `0.0.0.0` en une entrée `tnrhdb` valide

Dans cet exemple, l'administrateur de sécurité configure un serveur Sun Ray de manière à ce qu'il accepte les requêtes de connexion initiales de clients potentiels. Le serveur utilise une topologie privée et les valeurs par défaut :

```
# utadm -a bge0
```

L'administrateur détermine tout d'abord le nom de domaine de la Console de gestion Solaris :

```
SMCserver # /usr/sadm/bin/dtsetup scopes
Getting list of managable scopes...
Scope 1 file:/machine1.ExampleCo.COM/machine1.ExampleCo.COM
```

L'administrateur ajoute ensuite l'entrée pour la connexion initiale du client à la base de données `tnrhdb` du serveur Sun Ray. Étant donné que l'administrateur est en train d'effectuer un test, l'adresse générique par défaut est toujours utilisée pour toutes les adresses inconnues :

```
SunRayServer # /usr/sadm/bin/smtnrhdb \
add -D file:/machine1.ExampleCo.COM/machine1.ExampleCo.COM \
-- -w 0.0.0.0 -p 32 -n admin_low
Authenticating as user: root

Please enter a string value for: password ::
... from machine1.ExampleCo.COM was successful.
```

Après cette commande, la base de données `tnhrdb` se présente de la manière suivante. Le résultat de la commande `smtnrhdb` est mis en évidence :

```
## tnrhdb database
## Sun Ray server address
       192.168.128.1:cipso
## Sun Ray client addresses on 192.168.128 network
       192.168.128.0/24:admin_low
## Initial address for new clients
       0.0.0.0/32:admin_low
## Default wildcard address
0.0.0.0:admin_low
     Other addresses to be contacted at boot
```

```
# tnchkdb -h /etc/security/tsol/tnrhdb
```

Après la réussite de cette phase de test, l'administrateur renforce la sécurité de la configuration en supprimant l'adresse générique par défaut, il vérifie la syntaxe de la base de données `tnrhdb` puis il recommence le test. La base de données `tnhrdb` finale se présente de la manière suivante :

```
## tnrhdb database
## Sun Ray server address
       192.168.128.1:cipso
## Sun Ray client addresses on 192.168.128 network
       192.168.128.0/24:admin_low
## Initial address for new clients
       0.0.0.0/32:admin_low
## 0.0.0.0:admin_low - no other systems can enter network at admin_low
     Other addresses to be contacted at boot
```

Configuration de routes et vérification des informations réseau dans Trusted Extensions (liste des tâches)

La liste des tâches ci-dessous décrit les tâches permettant de configurer le réseau et de vérifier la configuration.

Tâche	Description	Voir
Configuration de routes statiques.	Décrit manuellement la route optimale d'un hôte à un autre hôte.	"Procédure de configuration de routes à l'aide d'attributs de sécurité" à la page 201
Vérification de l'exactitude des bases de données réseau locales.	Utilise la commande `tnchkdb` pour vérifier la validité syntaxique des bases de données réseau locales.	"Procédure de vérification de la syntaxe des bases de données d'un réseau de confiance" à la page 202
Comparaison des entrées de la base de données réseau et des entrées du cache du noyau.	Utilise la commande `tninfo` pour déterminer si le cache du noyau a été mis à jour avec les dernières informations de la base de données.	"Procédure de comparaison des informations des base de données du réseau de confiance et du cache du noyau" à la page 203

Tâche	Description	Voir
Synchronisation du cache du noyau avec les bases de données réseau.	Utilise la commande `tnctl` pour mettre à jour le cache du noyau avec les toutes dernières informations de la base de données réseau dans un système en cours d'exécution.	"Procédure de synchronisation du cache du noyau avec les bases de données d'un réseau de confiance" à la page 204

▼ Procédure de configuration de routes à l'aide d'attributs de sécurité

Avant de commencer Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

1 **Ajoutez chaque hôte et passerelle de destination que vous utilisez pour acheminer des paquets dans le réseau de confiance.**

Les adresses sont ajoutées au fichier `/etc/hosts` local ou à son équivalent sur le serveur LDAP. Utilisez l'outil Computers and Networks (Ordinateurs et réseaux) dans la Console de gestion Solaris. L'étendue fichiers modifie le fichier `/etc/hosts`. L'étendue LDAP modifie les entrées sur le serveur LDAP. Pour plus d'informations, reportez-vous à la section "Procédure d'ajout d'hôtes au réseau connu du système " à la page 194.

2 **Assignez chaque hôte, réseau et passerelle de destination à un modèle de sécurité.**

Les adresses sont ajoutées au fichier `/etc/security/tsol/tnrhdb` local ou à son équivalent sur le serveur LDAP. Utilisez l'outil Security Templates (Modèles de sécurité) dans la Console de gestion Solaris. Pour plus d'informations, reportez-vous à la section "Procédure d'assignation d'un modèle de sécurité à un hôte ou à un groupe d'hôtes" à la page 194.

3 **Configurez les routes.**

Dans une fenêtre de terminal, utilisez la commande `route add` pour spécifier des routes.

La première entrée configure une route par défaut. L'entrée spécifie une adresse de passerelle, `192.168.113.1`, à utiliser lorsqu'aucune route spécifique n'est définie pour la destination de l'hôte ou celle du paquet.

```
# route add default 192.168.113.1  -static
```

Pour plus d'informations, reportez-vous à la page de manuel `route`(1M).

4 **Configurez une ou plusieurs entrées de réseau.**

Utilisez l'indicateur `-secattr` pour spécifier les attributs de sécurité.

Dans la liste de commandes suivante, la deuxième ligne présente une entrée de réseau. La troisième ligne présente une entrée de réseau possédant une plage d'étiquettes allant de PUBLIC à CONFIDENTIAL : INTERNAL USE ONLY.

```
# route add default 192.168.113.36
# route add -net 192.168.102.0 gateway-101
# route add -net 192.168.101.0 gateway-102 \
-secattr min_sl="PUBLIC",max_sl="CONFIDENTIAL : INTERNAL USE ONLY",doi=1
```

5 **Configurez une ou entrée d'hôtes ou plus.**

La nouvelle ligne (la dernière) montre une entrée d'hôte pour l'hôte à étiquette unique gateway-pub. gateway-pub a une plage d'étiquettes comprise entre PUBLIC et PUBLIC.

```
# route add default 192.168.113.36
# route add -net 192.168.102.0 gateway-101
# route add -net 192.168.101.0 gateway-102 \
-secattr min_sl="PUBLIC",max_sl="CONFIDENTIAL : INTERNAL USE ONLY",doi=1
# route add -host 192.168.101.3 gateway-pub \
-secattr min_sl="PUBLIC",max_sl="PUBLIC",doi=1
```

Exemple 13–14 Ajout d'une route possédant une plage d'étiquettes allant de CONFIDENTIAL : INTERNAL USE ONLY à CONFIDENTIAL : RESTRICTED

La commande route suivante ajoute à la table de routage les hôtes à l'adresse 192.168.115.0 utilisant 192.168.118.39 comme passerelle. La plage d'étiquettes va de CONFIDENTIAL : INTERNAL USE ONLY à CONFIDENTIAL : RESTRICTED et la valeur du DOI est 1.

```
$ route add -net 192.168.115.0 192.168.118.39 \
-secattr min_sl="CONFIDENTIAL : INTERNAL USE ONLY",max_sl="CONFIDENTIAL : RESTRICTED",doi=1
```

La commande netstat -rR permet d'afficher le résultat des hôtes ajoutés. Dans l'extrait ci-dessous, les autres routes sont remplacées par des points de suspension (...).

```
$ netstat -rRn
...
192.168.115.0        192.168.118.39        UG       0      0
        min_sl=CNF : INTERNAL USE ONLY,max_sl=CNF : RESTRICTED,DOI=1,CIPSO
...
```

▼ Procédure de vérification de la syntaxe des bases de données d'un réseau de confiance

La commande tnchkdb vérifie que la syntaxe de chaque base de données réseau est exacte. La Console de gestion Solaris exécute automatiquement cette commande lorsque vous utilisez l'outil Security Templates (Modèles de sécurité) ou l'outil Trusted Network Zones (Zones du réseau de confiance). En règle générale, vous exécutez cette commande pour vérifier la syntaxe des fichiers de la base de données que vous êtes en train de configurer pour une utilisation ultérieure.

Avant de commencer Vous devez accéder à la zone globale à l'aide d'un rôle habilité à vérifier les paramètres du réseau. Les rôles d'administrateur de sécurité et d'administrateur système sont habilités à vérifier ces paramètres.

- **Dans une fenêtre de terminal, exécutez la commande `tnchkdb`.**

```
$ tnchkdb [-h tnrhdb-path] [-t tnrhtp-path] [-z tnzonecfg-path]
checking /etc/security/tsol/tnrhtp ...
checking /etc/security/tsol/tnrhdb ...
checking /etc/security/tsol/tnzonecfg ...
```

Exemple 13–15 Test de la syntaxe d'une base de données réseau

Dans cet exemple, l'administrateur de sécurité teste un fichier de base de données réseau en vue d'une éventuelle utilisation. Au départ, l'administrateur utilise la mauvaise option. Les résultats de la vérification sont imprimés sur la ligne pour le fichier `tnrhdb` :

```
$ tnchkdb -h /opt/secfiles/trial.tnrhtp
checking /etc/security/tsol/tnrhtp ...
checking /opt/secfiles/trial.tnrhtp ...
line 12: Illegal name: min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
line 14: Illegal name: min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
checking /etc/security/tsol/tnzonecfg ...
```

Lorsque l'administrateur de sécurité vérifie le fichier à l'aide de l'option `-t`, la commande confirme l'exactitude de la syntaxe de la base de données `tnrhtp` à l'essai :

```
$ tnchkdb -t /opt/secfiles/trial.tnrhtp
checking /opt/secfiles/trial.tnrhtp ...
checking /etc/security/tsol/tnrhdb ...
checking /etc/security/tsol/tnzonecfg ...
```

▼ Procédure de comparaison des informations des base de données du réseau de confiance et du cache du noyau

Les bases de données du réseau peuvent contenir des informations qui ne figurent pas dans le cache du noyau. Cette procédure vérifie que les informations sont identiques. Lorsque vous utilisez la Console de gestion Solaris pour mettre à jour le réseau, le cache du noyau est mis à jour avec les informations des bases de données réseau. La commande `tninfo` est utile durant le test et le débogage.

Avant de commencer Vous devez accéder à la zone globale à l'aide d'un rôle habilité à vérifier les paramètres du réseau. Les rôles d'administrateur de sécurité et d'administrateur système sont habilités à vérifier ces paramètres.

- **Dans une fenêtre de terminal, exécutez la commande `tninfo`.**

- `tninfo -h` *hostname* affiche l'adresse IP et le modèle pour l'hôte spécifié.
- `tninfo -t` *templatename* affiche les informations suivantes :

  ```
  template: template-name
  host_type: either CIPSO or UNLABELED
  doi: 1
  min_sl: minimum-label
  hex: minimum-hex-label
  max_sl: maximum-label
  hex:maximum-hex-label
  ```
- `tninfo -m` *zone-name* affiche la configuration de port multiniveau (MLP) d'une zone.

Exemple 13–16 Affichage de ports multiniveau sur un hôte

Dans cet exemple, un système est configuré avec plusieurs zones étiquetées. Toutes les zones partagent la même adresse IP. Certaines zones sont également configurées avec des adresses spécifiques à leur zone. Dans cette configuration, le port TCP permettant de naviguer sur le Web (port `8080`) est un MLP situé sur une interface partagée de la zone publique. L'administrateur a également configuré `telnet`, le port TCP `23`, comme MLP de la zone publique. Étant donné que ces deux MLP se trouvent sur une interface partagée, aucune autre zone, pas même la zone globale, ne peut recevoir de paquets sur les ports `8080` et `23` dans l'interface partagée.

En outre, le port TCP de `ssh`, le port `22`, est un MLP par zone de la zone publique. Le service `ssh` de la zone publique peut recevoir sur l'adresse spécifique à sa zone n'importe quel paquet correspondant à la page d'étiquettes de l'adresse.

La commande suivante indique les MLP pour la zone publique :

```
$ tninfo -m public
private: 22/tcp
shared:  23/tcp;8080/tcp
```

La commande suivante indique les MLP pour la zone globale. Notez que les ports `23` et `8080` ne peuvent pas être de type MLP dans la zone globale car celle-ci partage la même adresse que la zone publique :

```
$ tninfo -m global
private: 111/tcp;111/udp;514/tcp;515/tcp;631/tcp;2049/tcp;
         6000-6003/tcp;38672/tcp;60770/tcp;
shared:  6000-6003/tcp
```

▼ Procédure de synchronisation du cache du noyau avec les bases de données d'un réseau de confiance

Lorsque le noyau n'a pas été mis à jour avec les informations des bases de données du réseau de confiance, vous pouvez procéder de différentes manières pour mettre à jour le cache du noyau.

La Console de gestion Solaris exécute automatiquement cette commande lorsque vous utilisez les outils Security Templates (Modèles de sécurité) ou Trusted Network Zones (Zones de réseau de confiance).

Avant de commencer Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

- **Pour synchroniser le cache du noyau avec les bases de données réseau, exécutez l'une des commandes suivantes :**

  - **Redémarrage du service `tnctl`.**

    Attention – N'utilisez pas cette méthode sur des systèmes où les informations des bases de données du réseau de confiance sont obtenues à partir d'un serveur LDAP. Les informations de la base de données locale écraseraient les informations obtenues à partir du serveur LDAP.

    ```
    $ svcadm restart  svc:/network/tnctl
    ```

    Cette commande permet d'importer dans le noyau toutes les informations des bases de données locales du réseau de confiance.

  - **Mise à jour du cache du noyau avec vos entrées récemment ajoutées.**

    ```
    $ tnctl -h hostname
    ```

    Cette commande importe uniquement dans le noyau les informations de l'option sélectionnée. Pour plus d'informations sur les options, reportez-vous à l'Exemple 13–17 et à la page de manuel `tnctl`(1M).

  - **Modification du service `tnd`.**

    Remarque – Le service `tnd` ne peut être exécuté que si le service `ldap` est en cours d'exécution.

    - **Modification de l'intervalle d'interrogation `tnd`.**

      Cette commande ne met pas à jour le cache du noyau. Cependant, vous pouvez réduire l'intervalle d'interrogation pour augmenter la fréquence de mise à jour du cache du noyau. Pour plus d'informations, reportez-vous à la page de manuel `tnd`(1M).

    - **Actualisation de `tnd`.**

      Cette commande de l'utilitaire de gestion des services (SMF) déclenche une mise à jour immédiate du noyau avec les modifications récentes apportées aux bases de données du réseau de confiance.

      ```
      $ svcadm refresh svc:/network/tnd
      ```

- **Redémarrage de `tnd` à l'aide de SMF.**

  ```
  $ svcadm restart svc:/network/tnd
  ```

Attention – Évitez d'exécuter la commande `tnd` pour redémarrer `tnd`. Cette commande peut interrompre des communications en cours.

Exemple 13–17 Mise à jour du noyau avec vos entrées `tnrhdb` les plus récentes

Dans cet exemple, l'administrateur a ajouté trois adresses à la base de données locale `tnrhdb`. L'administrateur supprime tout d'abord l'entrée générique `0.0.0.0`.

```
$ tnctl -d -h 0.0.0.0:admin_low
```

Il visualise ensuite le format des trois dernières entrées dans la base de données `/etc/security/tsol/tnrhdb` :

```
$ tail /etc/security/tsol/tnrhdb
#\:\:0:admin_low
127.0.0.1:cipso
#\:\:1:cipso
192.168.103.5:admin_low
192.168.103.0:cipso
0.0.0.0/32:admin_low
```

Puis il met à jour le cache du noyau :

```
$ tnctl -h 192.168.103.5
tnctl -h 192.168.103.0
tnctl -h 0.0.0.0/32
```

Enfin, l'administrateur vérifie que le cache du noyau a bien été mis à jour. La sortie de la première entrée se présente de la manière suivante :

```
$ tninfo -h 192.168.103.5
IP Address: 192.168.103.5
Template: admin_low
```

Exemple 13–18 Mise à jour des informations réseau dans le noyau

Dans cet exemple, l'administrateur met à jour le réseau de confiance avec un serveur d'impression public et s'assure que les paramètres du noyau sont corrects.

```
$ tnctl -h public-print-server
$ tninfo -h public-print-server
IP Address: 192.168.103.55
Template: PublicOnly
$ tninfo -t PublicOnly
================================
Remote Host Template Table Entries
```

```
--------------------------------
template: PublicOnly
host_type: CIPSO
doi: 1
min_sl: PUBLIC
hex: 0x0002-08-08
max_sl: PUBLIC
hex: 0x0002-08-08
```

Dépannage du réseau de confiance (liste des tâches)

La liste ci-dessous décrit les tâches à effectuer pour déboguer votre réseau.

Tâche	Description	Voir
Recherche des raisons empêchant deux hôtes de communiquer.	Vérifie que les interfaces de chaque système sont actives.	"Procédure de vérification de l'état d'activité des interfaces d'un hôte" à la page 207
	Utilise des outils de débogage lorsque deux hôtes ne parviennent pas à communiquer.	"Débogage du réseau Trusted Extensions" à la page 208
Recherche des raisons empêchant un client LDAP de joindre le serveur LDAP.	Répare la perte de connexion entre un serveur LDAP et un client.	"Procédure de débogage d'une connexion client au serveur LDAP" à la page 211

▼ Procédure de vérification de l'état d'activité des interfaces d'un hôte

Utilisez cette procédure si votre système ne communique pas avec les hôtes comme prévu.

Avant de commencer Vous devez accéder à la zone globale à l'aide d'un rôle habilité à vérifier les paramètres du réseau. Les rôles d'administrateur de sécurité et d'administrateur système sont habilités à vérifier ces paramètres.

1 Assurez-vous que l'interface réseau est active.

La sortie suivante indique que le système comporte deux interfaces réseau, `hme0` et `hme0:3`. Aucune des interfaces n'est active.

```
# ifconfig -a
...
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
         inet 192.168.0.11 netmask ffffff00 broadcast 192.168.0.255
hme0:3 flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
         inet 192.168.0.12 netmask ffffff00 broadcast 192.168.0.255
```

2 **Si l'interface n'est pas active, activez-la puis vérifiez qu'elle est bien active.**

La sortie suivante indique que les deux interfaces sont actives.

```
# ifconfig hme0 up
# ifconfig -a
...
hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,...
hme0:3 flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,..
```

▼ Débogage du réseau Trusted Extensions

Pour déboguer deux hôtes qui sont censés communiquer mais qui ne le font pas, vous pouvez utiliser les outils de débogage Trusted Extensions et Solaris. Par exemple, vous pouvez utiliser des commandes de débogage du réseau d'Oracle Solaris telles que `snoop` et `netstat`. Pour plus d'informations, reportez-vous aux pages de manuel `snoop`(1M) et `netstat`(1M). Pour connaître les commandes spécifiques à Trusted Extensions, reportez-vous au Tableau 2–4.

- Pour les problèmes relatifs à l'établissement de contact avec des zones étiquetées, reportez-vous à la section "Gestion des zones (liste des tâches)" à la page 134.
- Pour le débogage des montages NFS, reportez-vous à la section "Dépannage des échecs de montage dans Trusted Extensions" à la page 165.
- Pour le débogage des communications LDAP, reportez-vous à la section "Procédure de débogage d'une connexion client au serveur LDAP" à la page 211.

Avant de commencer Vous devez accéder à la zone globale à l'aide d'un rôle habilité à vérifier les paramètres du réseau. Le rôle d'administrateur de sécurité ou le rôle d'administrateur système sont habilités à vérifier ces paramètres.

1 **Pour réparer le démon `tnd`, modifiez l'intervalle d'interrogation et recueillez des informations de débogage.**

Remarque – Le service `tnd` ne peut être exécuté que si le service `ldap` est en cours d'exécution.

Pour plus d'informations, reportez-vous à la page de manuel `tnd`(1M).

2 Vérifiez que les hôtes qui ne parviennent pas à communiquer utilisent le même service de nommage.

a. Pour chaque hôte, consultez le fichier `nsswitch.conf`.

i. Consultez les valeurs des bases de données Trusted Extensions dans le fichier `nsswitch.conf`.

Par exemple, sur un site utilisant le protocole LDAP pour administrer le réseau, les entrées sont similaires à l'exemple suivant :

```
# Trusted Extensions
tnrhtp: files ldap
tnrhdb: files ldap
```

ii. Si les valeurs sont différentes, corrigez le fichier `nsswitch.conf`.

Pour modifier ces entrées, l'administrateur système utilise l'action Name Service Switch (Commutateur du service de noms). Pour plus d'informations, reportez-vous à la section "Démarrage d'actions d'administration CDE dans Trusted Extensions " à la page 58. Cette action permet de préserver les autorisations des fichiers DAC et MAC requis.

b. Assurez-vous que le service de nommage LDAP est configuré.

```
$ ldaplist -l
```

c. Assurez-vous que les deux hôtes se trouvent dans le service de nommage LDAP.

```
$ ldaplist -l hosts | grep hostname
```

3 Assurez-vous que chaque hôte est correctement défini.

a. Utilisez la Console de gestion Solaris pour contrôler les définitions.

- Dans l'outil Security Templates (Modèles de sécurité), assurez-vous que chaque hôte est assigné à un modèle de sécurité compatible avec le modèle de sécurité de l'autre hôte.
- Pour un système non étiqueté, vérifiez que l'assignation d'étiquette par défaut est correcte.
- Dans l'outil Trusted Network Zones (Zones de réseau de confiance), vérifiez que les ports multiniveau (les MLP) sont correctement configurés.

b. Utilisez la ligne de commande pour vérifier que les informations réseau du noyau sont actuelles.

Vérifiez que l'assignation dans le cache du noyau de chaque hôte correspond à l'assignation sur le réseau et sur l'autre hôte.

Pour obtenir des informations de sécurité pour la source, la destination et les hôtes de passerelle dans la transmission, utilisez la commande `tninfo`.

- **Affiche l'adresse IP et le modèle de sécurité assigné pour un hôte donné.**

  ```
  $ tninfo -h hostname
  IP Address: IP-address
  Template: template-name
  ```

- **Affiche une définition de modèle.**

  ```
  $ tninfo -t template-name
  template: template-name
  host_type: one of CIPSO or UNLABELED
  doi: 1
  min_sl: minimum-label
  hex: minimum-hex-label
  max_sl: maximum-label
  hex: maximum-hex-label
  ```

- **Affiche les MLP pour une zone.**

  ```
  $ tninfo -m zone-name
  private: ports-that-are-specific-to-this-zone-only
  shared: ports-that-the-zone-shares-with-other-zones
  ```

4 Corrigez les informations erronées.

- Pour consulter ou modifier les informations de sécurité réseau, utilisez les outils Console de gestion Solaris. Pour plus d'informations, reportez-vous à la section "Procédure d'ouverture des outils de gestion de réseaux de confiance" à la page 188
- Pour mettre à jour le cache du noyau, redémarrez le service `tnctl` sur l'hôte dont les informations ne sont pas à jour. Ce processus peut prendre un certain temps. Actualisez ensuite le service `tnd`. Si l'actualisation échoue, essayez de redémarrer le service `tnd`. Pour plus d'informations, reportez-vous à la section "Procédure de synchronisation du cache du noyau avec les bases de données d'un réseau de confiance" à la page 204.

Remarque – Le service `tnd` ne peut être exécuté que si le service `ldap` est en cours d'exécution.

Le redémarrage permet de vider le cache du noyau. Pendant l'initialisation, des informations de base de données sont inscrites dans le cache. Le fichier `nsswitch.conf` détermine si les bases de données locales ou les bases de données LDAP remplissent le noyau.

5 Collectez des informations de transmission pour faciliter le débogage.

- **Contrôlez votre configuration de routage.**

  Utilisez la sous-commande `get` de la commande `route`.

  ```
  $ route get [ip] -secattr sl=label,doi=integer
  ```

Pour plus d'informations, consultez la page de manuel `route`(1M).

- **Visualisez les informations d'étiquette dans les paquets.**

  Utilisez la commande `snoop -v`.

  L'option `-v` affiche les détails des en-têtes de paquets, notamment les informations d'étiquette. Étant donné que cette commande fournit un grand nombre de détails, vous pouvez avoir intérêt à limiter le nombre de paquets examinés par la commande. Pour plus d'informations, reportez-vous à la page de manuel `snoop`(1M).

- **Visualisez les entrées de la table de routage et les attributs de sécurité sur des sockets.**

  Utilisez l'option `-R` à l'aide de la commande `netstat -a|-r`.

  L'option `-aR` affiche les attributs de sécurité étendus des sockets. L'option `-rR` affiche les entrées de la table de routage. Pour plus d'informations, reportez-vous à la page de manuel `netstat`(1M).

▼ Procédure de débogage d'une connexion client au serveur LDAP

Une configuration incorrecte de l'entrée du client sur le serveur LDAP peut empêcher le client de communiquer avec le serveur. De la même façon, une mauvaise configuration des fichiers sur le client peut empêcher la communication. Contrôlez les entrées et les fichiers suivants lors d'une tentative de débogage d'un problème de communication entre client et serveur.

Avant de commencer Vous·devez être dans le rôle d'administrateur de sécurité dans la zone globale.

1. **Assurez-vous que les modèles d'hôte distant pour le serveur LDAP et la passerelle vers le serveur LDAP sont corrects.**

   ```
   # tninfo -h LDAP-server
   # route get LDAP-server
   # tninfo -h gateway-to-LDAP-server
   ```

   Si une assignation de modèle d'hôte distant est incorrecte, assignez l'hôte au modèle correct à l'aide de l'outil Security Templates (Modèles de sécurité) dans la Console de gestion Solaris.

2. **Consultez et corrigez le fichier `/etc/hosts`.**

   Votre système, les interfaces des zones étiquetées de votre système, la passerelle au serveur LDAP et le serveur LDAP doivent être répertoriés dans le fichier. Il peut contenir plus d'entrées.

   Recherchez les entrées dupliquées. Supprimez toutes les entrées correspondant à des zones étiquetées sur d'autres systèmes. Par exemple, si `Lserver` est le nom de votre serveur LDAP et si `LServer-zones` est l'interface partagée pour les zones étiquetées, supprimez `LServer-zones` de `/etc/hosts`.

3 **Si vous utilisez DNS, vérifiez et corrigez les entrées dans le fichier `resolv.conf`.**

```
# more resolv.conf
search list of domains
domain domain-name
nameserver IP-address

...
nameserver IP-address
```

4 **Vérifiez que les entrées `tnrhdb` et `tnrhtp` du fichier `nsswitch.conf` sont exactes.**

5 **Vérifiez que le client est correctement configuré sur le serveur.**

```
# ldaplist -l tnrhdb client-IP-address
```

6 **Vérifiez que les interfaces de vos zones étiquetées sont correctement configurées sur le serveur LDAP.**

```
# ldaplist -l tnrhdb client-zone-IP-address
```

7 **Vérifiez que vous pouvez faire un `ping` sur le serveur LDAP à partir de toutes les zones en cours d'exécution.**

```
# ldapclient list
...
NS_LDAP_SERVERS= LDAP-server-address
# zlogin zone-name1 ping LDAP-server-address
LDAP-server-address is alive
# zlogin zone-name2 ping LDAP-server-address
LDAP-server-address is alive
...
```

8 **Configurez le serveur LDAP, puis redémarrez.**

a. **Pour connaître la procédure, reportez-vous à la section "Établissement de la zone globale en tant que client LDAP dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.**

b. **Dans chaque zone étiquetée, rétablissez la zone en tant que client du serveur LDAP.**

```
# zlogin zone-name1
# ldapclient init \
-a profileName=profileName \
-a domainName=domain \
-a proxyDN=proxyDN \
-a proxyPassword=password  LDAP-Server-IP-Address
# exit
# zlogin zone-name2 ...
```

c. Arrêtez toutes les zones, verrouillez les systèmes de fichiers, puis redémarrez.

Si vous utilisez Oracle Solaris ZFS, arrêtez les zones, verrouillez les systèmes de fichiers, puis redémarrez. Si vous n'utilisez pas ZFS, vous pouvez redémarrer sans arrêter les zones ni verrouiller les systèmes de fichiers.

```
# zoneadm list
# zoneadm -z zone-name halt
# lockfs -fa
# reboot
```

◆ ◆ ◆ CHAPITRE 14

Messagerie multiniveau dans Trusted Extensions (présentation)

Ce chapitre traite de la sécurité et des logiciels de messagerie multiniveau dans les systèmes configurés avec Trusted Extensions.

Service de messagerie multiniveau

Trusted Extensions offre une messagerie multiniveau pour tous les types d'applications de messagerie électronique. Lorsque les utilisateurs standard démarrent leur logiciel de messagerie, l'application s'ouvre dans l'étiquette en cours de l'utilisateur. Lorsque des utilisateurs travaillent dans un système multiniveau, ils peuvent, s'ils le souhaitent, lier ou copier les fichiers d'initialisation de leur logiciel de messagerie. Pour plus d'informations, reportez-vous à la section "Procédure de configuration des fichiers de démarrage pour les utilisateurs dans Trusted Extensions " à la page 92.

Fonctions de messagerie Trusted Extensions

Dans Trusted Extensions, le rôle d'administrateur système configure et administre des serveurs de messagerie en fonction des instructions du *Guide d'administration système : Administration avancée* et du *Guide d'administration système : services IP* Oracle Solaris. En outre, l'administrateur de sécurité détermine la configuration requise des fonctions de messagerie Trusted Extensions.

Les aspects de gestion des messages électroniques suivants sont spécifiques à Trusted Extensions :

- Le fichier `.mailrc` se trouve sous l'étiquette minimale d'un utilisateur.

  Par conséquent, les utilisateurs qui travaillent avec plusieurs étiquettes ne possèdent pas de fichier `.mailrc` aux étiquettes de niveau supérieur, à moins qu'ils ne copient ou ne lient le fichier `.mailrc` se trouvant dans le répertoire de leur étiquette minimale à chacun des répertoires de niveau supérieur.

  Le rôle d'administrateur de sécurité ou l'utilisateur concerné peut ajouter le fichier `.mailrc` dans `.copy_files` ou dans `.link_files` . Pour une description de ces fichiers, reportez-vous à la page de manuel `updatehome(1M)`. Pour consulter des suggestions de configuration, reportez-vous à la section "Fichiers `.copy_files` et `.link_files`" à la page 86.

- Votre lecteur de courrier électronique peut s'exécuter sous chaque étiquette d'un système. Certaines opérations de configuration sont nécessaires pour connecter un client de messagerie au serveur.

  Par exemple, pour utiliser la messagerie Mozilla comme messagerie multiniveau, vous devez configurer le client de messagerie Mozilla à chaque étiquette pour le spécifier en tant que serveur de messagerie. Le serveur de messagerie ne doit pas nécessairement être identique pour toutes les étiquettes mais le serveur doit être spécifié.

- L'outil Mailing Lists (Listes de diffusion) de la Console de gestion Solaris gère les alias de messagerie.

  En fonction de l'étendue de la boîte à outils Console de gestion Solaris sélectionnée, vous pouvez mettre à jour le fichier `/etc/aliases` local ou l'entrée LDAP sur l'Oracle Directory Server Enterprise Edition.

- Trusted Extensions contrôle les étiquettes de l'hôte et de l'utilisateur avant d'envoyer ou de transférer un message.
  - Le logiciel vérifie que le message s'inscrit dans la plage d'accréditations de l'hôte. Les vérifications sont décrites dans cette liste et au Chapitre 13, "Gestion des réseaux dans Trusted Extensions (tâches) ".
  - Le logiciel vérifie que l'e-mail est compris entre l'autorisation et l'étiquette minimale du compte.
  - Les utilisateurs peuvent lire les e-mails reçus correspondant à la plage d'accréditations. Au cours d'une session, les utilisateurs peuvent uniquement lire les messages correspondant à leur étiquette en cours.

    Pour contacter un utilisateur standard par e-mail, un rôle d'administration doit envoyer un e-mail à partir d'un espace de travail possédant une étiquette que l'utilisateur est autorisé à lire. L'étiquette par défaut de l'utilisateur est généralement un bon choix.

◆ ◆ ◆ CHAPITRE 15

Gestion de l'impression étiquetée (tâches)

Ce chapitre explique comment utiliser le logiciel Trusted Extensions pour configurer l'impression étiquetée. Il explique également comment configurer les travaux d'impression sans les options d'étiquetage.

Étiquettes, imprimantes et impression

Trusted Extensions utilise des étiquettes pour contrôler l'accès aux imprimantes. Les étiquettes permettent de contrôler l'accès aux imprimantes et aux informations relatives aux travaux d'impression de la file d'attente. Le logiciel permet également d'étiqueter les sorties d'impression. Des étiquettes sont appliquées aux pages de corps de texte ainsi qu'aux pages de garde et de fin. Les pages de garde et de fin peuvent également inclure des instructions de traitement.

L'administrateur système assure la gestion courante de l'imprimante. Le rôle de l'administrateur de sécurité gère la sécurité de l'imprimante, notamment les étiquettes et la manière dont les sorties étiquetées sont gérées. Les administrateurs suivent les procédures d'administration des imprimantes Oracle Solaris de base, puis ils assignent des étiquettes aux serveurs d'impression et aux imprimantes.

Trusted Extensions prend en charge l'impression à niveau unique et l'impression multiniveau. L'impression multiniveau est uniquement implémentée dans la zone globale. Pour utiliser le serveur d'impression de la zone globale, une zone étiquetée doit avoir un nom d'hôte différent de celui de la zone globale. Une manière d'obtenir un nom d'hôte distinct est d'assigner une adresse IP à la zone étiquetée. L'adresse serait différente de l'adresse IP de la zone globale.

Restriction de l'accès aux imprimantes et aux informations relatives aux travaux d'impression dans Trusted Extensions

Les utilisateurs et les rôles des systèmes configurés avec Trusted Extensions créent des travaux d'impression correspondant à l'étiquette de leur session. Les travaux d'impression peuvent uniquement être imprimés sur des imprimantes qui reconnaissent cette étiquette. L'étiquette doit se trouver dans la plage d'étiquettes du périphérique.

Les utilisateurs et les rôles peuvent afficher les travaux d'impression dont l'étiquette est identique à l'étiquette de la session. Dans la zone globale, un rôle peut visualiser les travaux dont l'étiquette est dominée par l'étiquette de la zone.

Les imprimantes configurées avec Trusted Extensions impriment des étiquettes sur les sorties d'imprimante. Les imprimantes gérées par des serveurs d'impression non étiquetés n'impriment pas les étiquettes sur les sorties d'imprimante. Ces imprimantes ont la même étiquette que leur serveur non étiqueté. Par exemple, une étiquette arbitraire peut être assignée à un serveur d'impression Oracle Solaris dans la base de données `tnrhdb` du service de nommage LDAP. Les utilisateurs peuvent ensuite imprimer des travaux sous cette étiquette arbitraire sur l'imprimante Oracle Solaris. À l'instar des imprimantes Trusted Extensions, ces imprimantes Oracle Solaris peuvent uniquement accepter les travaux d'impression provenant d'utilisateurs qui travaillent sous l'étiquette assignée au serveur d'impression.

Sorties d'imprimante étiquetées

Trusted Extensions imprime les informations de sécurité sur les pages de corps de texte, les pages de garde et les pages de fin. Ces informations proviennent du fichier `label_encodings` et du fichier `tsol_separator.ps`.

L'administrateur de sécurité peut effectuer les opérations suivantes pour modifier les valeurs par défaut de configuration des étiquettes et ajouter des instructions de traitement aux sorties d'imprimante :

- Localiser ou personnaliser le texte des pages de garde et de fin
- Spécifier d'autres étiquettes à imprimer sur les pages de corps de texte ou dans les différents champs des pages de garde et de fin
- Modifier ou omettre le texte ou les étiquettes

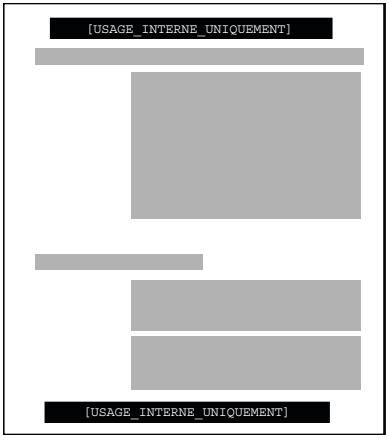
L'administrateur de sécurité peut également configurer des comptes utilisateurs pour qu'ils utilisent des imprimantes n'imprimant pas d'étiquettes sur la sortie. Les utilisateurs peuvent également être autorisés à ne pas imprimer certaines bannières ou étiquettes sur les sorties d'imprimante.

Pages de corps de texte étiquetées

Par défaut, la classification "Protéger en tant que" est imprimée dans la partie supérieure et inférieure de chaque page de corps de texte. La classification "Protéger en tant que" est la classification dominante lorsque la classification de l'étiquette du travail est comparée à la `minimum protect as classification` (classification de protection en tant que minimale). La `minimum protect as classification` est définie dans le fichier `label_encodings`.

Par exemple, si l'utilisateur est connecté à une session à usage interne uniquement (Internal Use Only), les travaux d'impression étiquetés de l'utilisateur correspondent à cette étiquette. Si la `minimum protect as classification` du fichier `label_encodings` est Public, l'étiquette Internal Use Only (Usage interne uniquement) est imprimée sur les pages de corps de texte.

FIGURE 15–1 Impression de l'étiquette d'un travail dans la partie supérieure et inférieure d'une page de corps de texte



Pages de garde et de fin étiquetées

Les figurent suivantes montrent une page de garde par défaut et indique en quoi elle diffère d'une page de fin par défaut. Les légendes identifient les différentes sections. Notez que la page de fin utilise une ligne de contour différente.

Le texte, les étiquettes et les avertissements qui s'affichent sur les travaux d'impression sont configurables. Le texte peut également être localisé et remplacé par un texte dans une autre langue.

FIGURE 15–2 Page de garde type d'un travail d'impression étiqueté

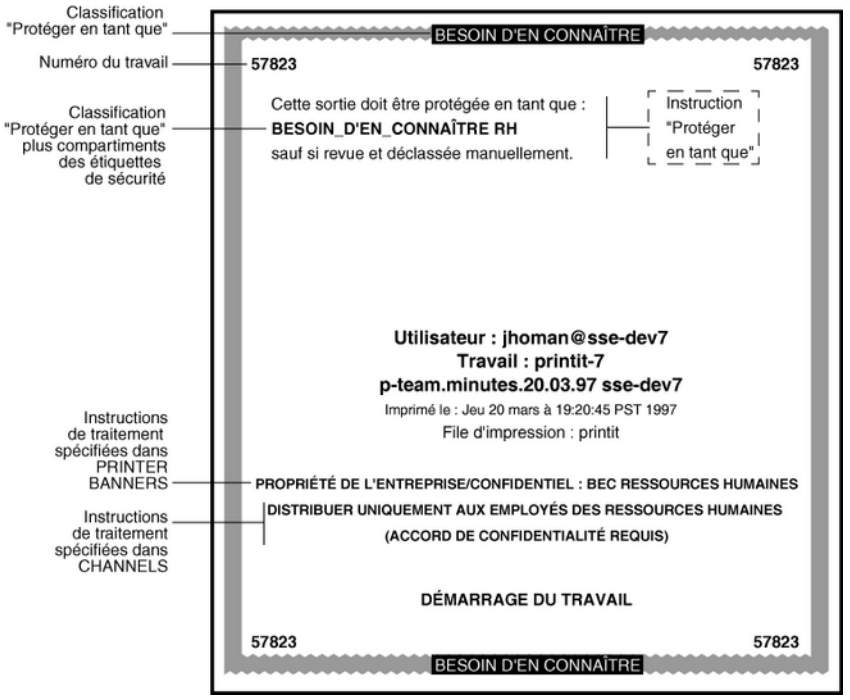
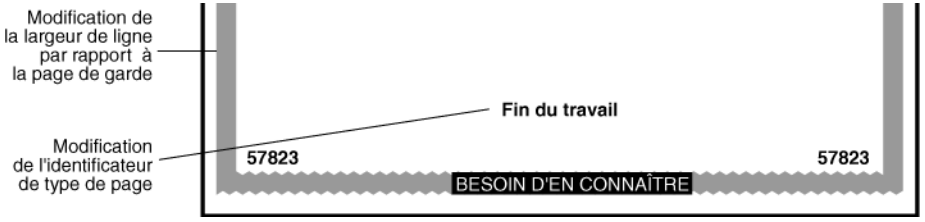


FIGURE 15–3 Page de fin : différences par rapport à la page de garde



Le tableau suivant présente des aspects de l'impression de confiance que l'administrateur de sécurité peut changer en modifiant le fichier `/usr/lib/lp/postscript/tsol_separator.ps`.

Remarque – Pour localiser ou internationaliser les sorties d'imprimante, consultez les commentaires dans le fichier `tsol_separator.ps`.

TABLEAU 15–1 Valeurs configurables dans le fichier `tsol_separator.ps`

Sortie	Valeur par défaut	Mode de définition	Modification
`PRINTER BANNERS`	`/Caveats Job_Caveats`	`/Caveats Job_Caveats`	Reportez-vous à la section "Specifying Printer Banners" du *Oracle Solaris Trusted Extensions Label Administration*.
`CHANNELS`	`/Channels Job_Channels`	`/Channels Job_Channels`	Reportez-vous à la section "Specifying Channels" du *Oracle Solaris Trusted Extensions Label Administration*.
Étiquette dans la partie supérieure des pages de garde et de fin	`/HeadLabel Job_Protect def`	Voir la description pour `/PageLabel`.	Même procédure que pour la modification de `/PageLabel`. Reportez-vous également à la section "Specifying the Protect As Classification" du *Oracle Solaris Trusted Extensions Label Administration*.
Étiquette dans la partie supérieure et inférieure des pages de corps de texte	`/PageLabel Job_Protect def`	Compare l'étiquette du travail à la `minimum protect as classification` dans le fichier `label_encodings`. Imprime la classification la plus dominante. Inclut des compartiments lorsque l'étiquette du travail d'impression en contient.	Modifiez la définition de `/PageLabel` pour spécifier une autre valeur. Ou saisissez une chaîne de caractères de votre choix. Ou n'imprimez rien du tout.

Texte et étiquette dans la mention de classification "Protéger en tant que"	`/Protect Job_Protect def`
	`/Protect_Text1 () def`
	`/Protect_Text2 () def`
		Voir la description pour `/PageLabel`.
		Texte affiché au-dessus de l'étiquette.
		Texte affiché au-dessous de l'étiquette.
			Même procédure que pour la modification de `/PageLabel`.
			Remplacez `()` dans `Protect_Text1` et `Protect_Text2` par une chaîne de texte.

Impression PostScript d'informations de sécurité

L'impression étiquetée dans Trusted Extensions s'appuie sur les fonctions d'impression de Solaris. Dans le SE Oracle Solaris, les scripts du modèle d'imprimante gèrent la création de la page de garde. Pour implémenter l'étiquetage, un script de modèle d'imprimante commence par convertir le travail d'impression en un fichier PostScript. Le fichier PostScript est ensuite manipulé pour insérer des étiquettes sur les pages de corps de texte et créer des pages de garde et de fin.

Les scripts de modèle d'imprimante &Solaris peuvent également traduire PostScript dans la langue d'origine d'une imprimante. Lorsqu'une imprimante accepte l'entrée PostScript, Oracle Solaris envoie le travail d'impression à l'imprimante. Lorsqu'une imprimante n'accepte pas l'entrée PostScript, le logiciel convertit le format PostScript en image raster. L'image raster est ensuite convertie au format d'imprimante approprié.

Étant donné que le logiciel PostScript est utilisé pour imprimer les informations d'étiquettes, par défaut, les utilisateurs ne peuvent pas imprimer de fichiers PostScript. Cette restriction empêche un programmeur PostScript expérimenté de créer un fichier PostScript modifiant les étiquettes sur les sorties d'imprimante.

Le rôle d'administrateur de sécurité peut passer outre à cette restriction en assignant l'autorisation `Print Postscript` à des comptes de rôles et à des utilisateurs dignes de confiance. L'autorisation n'est assignée que s'il est certain que le compte concerné n'usurpera pas les étiquettes sur les sorties d'imprimante. En outre, l'octroi à un utilisateur de l'autorisation d'imprimer des fichiers PostScript doit être compatible avec la stratégie de sécurité du site.

Scripts de modèle d'imprimante

Un script de modèle d'imprimante permet à un modèle d'imprimante particulier de fournir des pages de garde et de fin. Trusted Extensions fournit quatre scripts :

- `tsol_standard` : pour les imprimantes PostScript directement reliées, par exemple, via un port parallèle
- `tsol_netstandard` : pour les imprimantes PostScript accessibles via le réseau
- `tsol_standard_foomatic` : pour les imprimantes directement reliées qui n'impriment pas le format PostScript
- `tsol_netstandard_foomatic` : pour les imprimantes accessibles via le réseau qui n'impriment pas le format PostScript

Les scripts `foomatic` sont utilisés lorsqu'un nom de pilote d'imprimante commence par `Foomatic`. Les pilotes Foomatic sont des pilotes d'imprimante PostScript (PPD).

Remarque – Lorsque vous ajoutez une imprimante à une zone étiquetée, "Utiliser PPD" est spécifié par défaut dans le Gestionnaire d'impression. Un fichier PPD est ensuite utilisé pour traduire les pages de garde et de fin dans la langue de l'imprimante.

Filtres de conversion supplémentaires

Un filtre de conversion convertit des fichiers texte au format PostScript. Les programmes du filtre sont des programmes de confiance exécutés par le démon d'imprimante. Les fichiers convertis au format PostScript par n'importe quel programme de filtrage installé offrent la garantie de présenter des étiquettes et des textes de page de garde et de fin authentiques.

Oracle Solaris fournit la plupart des filtres requis par un site. Le rôle d'administrateur système d'un site peut installer des filtres supplémentaires. L'authenticité des étiquettes et des pages de garde et de fin de ces filtres est garantie. Pour ajouter des filtres de conversion, reportez-vous au Chapitre 7, "Customizing LP Printing Services and Printers (Tasks)" du *System Administration Guide: Printing*.

Interopérabilité de Trusted Extensions et de l'impression Trusted Solaris 8

Les systèmes Trusted Solaris 8 et Trusted Extensions contenant des fichiers `label_encodings` compatibles et s'identifiant mutuellement à l'aide d'un modèle CIPSO peuvent s'utiliser l'un l'autre pour l'impression à distance. Le tableau suivant décrit la configuration requise des systèmes pour permettre l'impression. Par défaut, les utilisateurs ne peuvent pas lister ou annuler les travaux d'impression d'un serveur d'impression distant exécutant l'autre système d'exploitation. Si vous le souhaitez, vous pouvez autoriser des utilisateurs à le faire.

Système d'origine	Système du serveur d'impression	Action	Résultats
Trusted Extensions	Trusted Solaris 8	Configurez l'impression : dans le fichier `tnrhdb` de Trusted Extensions, assignez un modèle comportant la plage d'étiquettes appropriée au serveur d'impression Trusted Solaris 8. L'étiquette peut être CIPSO ou sans étiquette.	Une imprimante Trusted Solaris 8 peut imprimer des travaux d'impression provenant d'un système Trusted Extensions dans les limites de la plage d'étiquettes de l'imprimante.
Trusted Extensions	Trusted Solaris 8	Autorisez des utilisateurs : dans le système Trusted Extensions créez un profil qui ajoute les autorisations nécessaires. Assignez le profil à des utilisateurs.	Les utilisateurs Trusted Extensions peuvent lister ou annuler les travaux d'impression qu'ils envoient vers une imprimante Trusted Solaris 8. Les utilisateurs ne peuvent ni visualiser, ni supprimer les travaux ayant une autre étiquette.

Système d'origine	Système du serveur d'impression	Action	Résultats
Trusted Solaris 8	Trusted Extensions	Configurez l'impression : dans le fichier `tnrhdb` Trusted Solaris 8, assignez un modèle comportant la plage d'étiquettes appropriée au serveur d'impression Trusted Extensions. L'étiquette peut être CIPSO ou sans étiquette.	Une imprimante Trusted Extensions peut imprimer des travaux provenant d'un système Trusted Solaris 8 dans les limites de la plage d'étiquettes de l'imprimante.
Trusted Solaris 8	Trusted Extensions	Autorisez des utilisateurs : dans le système Trusted Solaris 8 créez un profil qui ajoute les autorisations nécessaires. Assignez le profil à des utilisateurs.	Les utilisateurs Trusted Solaris 8 peuvent lister ou annuler les travaux d'impression qu'ils envoient vers une imprimante Trusted Extensions. Les utilisateurs ne peuvent ni visualiser, ni supprimer les travaux ayant une autre étiquette.

Interfaces d'impression Trusted Extensions (référence)

Les commandes utilisateur suivantes sont étendues pour être conformes à la stratégie de sécurité de Trusted Extensions :

- `annuler` : pour annuler un travail, l'appelant doit avoir une étiquette égale à celle du travail d'impression. Par défaut, les utilisateurs standard ne peuvent annuler que leurs propres travaux.
- `lp` : Trusted Extensions ajoute l'option `-o nolabels`. Les utilisateurs doivent être autorisés à imprimer sans étiquette. De même, les utilisateurs doivent être autorisés à utiliser l'option `-o nobanner`.
- `Ipstat` : pour obtenir l'état d'un travail, l'appelant doit avoir une étiquette égale à celle du travail d'impression. Par défaut, les utilisateurs standard ne peuvent consulter que leurs propres travaux d'impression.

Les commandes d'administration suivantes sont étendues pour être conformes à la stratégie de sécurité de Trusted Extensions. Comme dans le SE Oracle Solaris, ces commandes ne peuvent être exécutées que par un rôle comprenant le profil de droits Printer management (Gestion des imprimantes).

- `lpmove` : pour déplacer un travail, l'appelant doit avoir une étiquette égale à celle du travail d'impression. Par défaut, les utilisateurs standard ne peuvent déplacer que leurs propres travaux d'impression.
- `lpadmin` : dans la zone globale, cette commande fonctionne pour tous les travaux. Dans une zone étiquetée, l'appelant doit dominer l'étiquette du travail d'impression pour visualiser un travail, et posséder une étiquette égale à celle du travail d'impression pour modifier un travail.

  Trusted Extensions ajoute des scripts de modèles d'imprimante à l'option `-m`. Trusted Extensions ajoute l'option `-o nolabels`.
- `lpsched` : dans la zone globale, cette commande aboutit toujours. Comme dans le SE Oracle Solaris, utilisez la commande `svcadm` pour activer, désactiver, démarrer ou redémarrer le service d'impression. Dans une zone étiquetée, l'appelant doit avoir une étiquette égale à celle du service d'impression pour modifier le service d'impression. Pour plus d'informations sur l'utilitaire de gestion des services, reportez-vous aux pages de manuel `smf(5)`, `svcadm(1M)`, et `svcs(1)`.

Trusted Extensions ajoute l'autorisation `solaris.label.print` au profil de droits Printer Management (Gestion des imprimantes). L'autorisation `solaris.print.unlabeled` est requise pour imprimer des pages de corps de texte sans étiquette.

Gestion de l'impression dans Trusted Extensions (liste des tâches)

Les procédures Trusted Extensions de configuration de l'impression sont effectuées après la configuration de l'imprimante dans Oracle Solaris. La liste des tâches suivante contient des liens vers les principales tâches de gestion de l'impression étiquetée.

Tâche	Description	Voir
Configuration d'imprimantes pour l'impression étiquetée.	Permet aux utilisateurs d'imprimer sur une imprimante Trusted Extensions. Les travaux d'impression sont étiquetés.	"Configuration de l'impression étiquetée (liste des tâches)" à la page 226
Suppression des étiquettes visibles sur les sorties d'imprimante.	Permet aux utilisateurs d'imprimer sous une étiquette spécifique sur une imprimante Oracle Solaris. Les travaux d'impression ne sont pas étiquetés. Ou empêche l'impression d'étiquettes sur une imprimante Trusted Extensions.	"Réduction des restrictions d'impression dans Trusted Extensions (liste des tâches)" à la page 240

Configuration de l'impression étiquetée (liste des tâches)

La liste des tâches ci-dessous décrit des procédures de configuration courantes liées à l'impression étiquetée.

Remarque – Les clients d'impression peuvent uniquement imprimer des travaux d'impression dont l'étiquette est comprise dans la plage d'étiquettes du serveur d'impression Trusted Extensions.

Tâche	Description	Voir
Configuration de l'impression à partir de la zone globale.	Crée un serveur d'impression multiniveau dans la zone globale.	"Procédure de configuration d'un serveur d'impression multiniveau et des imprimantes correspondantes" à la page 226
Configuration de l'impression pour un réseau de systèmes.	Crée un serveur d'impression multiniveau dans la zone globale et permet aux zones étiquetées d'utiliser l'imprimante.	"Procédure de configuration d'une imprimante réseau pour les clients Sun Ray" à la page 228
Configuration de l'impression pour les systèmes sans étiquette appartenant au même sous-réseau que les systèmes étiquetés.	Permet à des systèmes sans étiquette d'utiliser l'imprimante réseau.	"Procédure de configuration de l'impression en cascade sur un système étiqueté" à la page 232
Configuration de l'impression à partir d'une zone étiquetée.	Crée un serveur d'impression à étiquette unique pour une zone étiquetée.	"Procédure de configuration d'une zone pour l'impression à étiquette unique" à la page 235
Configuration d'un client d'impression multiniveau.	Connecte un hôte Trusted Extensions à une imprimante.	"Procédure d'octroi de l'autorisation d'accéder à une imprimante à un client Trusted Extensions" à la page 236
Restriction de la plage d'étiquettes d'une imprimante.	Limite une imprimante Trusted Extensions à une plage d'étiquettes réduite.	"Procédure de configuration d'une plage d'étiquettes restreinte pour une imprimante" à la page 239

▼ Procédure de configuration d'un serveur d'impression multiniveau et des imprimantes correspondantes

Les imprimantes gérées par un serveur d'impression Trusted Extensions impriment des étiquettes sur les pages de corps de texte ainsi que sur les pages de garde et de fin. Elles peuvent imprimer des travaux d'impression dans la plage d'étiquettes du serveur d'impression. Tout hôte Trusted Extensions pouvant atteindre le serveur d'impression peut utiliser les imprimantes connectées à ce serveur.

Avant de commencer Choisissez un serveur d'impression pour votre réseau Trusted Extensions. Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale de ce serveur d'impression.

1 **Démarrez la Console de gestion Solaris.**

Pour plus d'informations, reportez-vous à la section "Administration du système local avec Console de gestion Solaris " à la page 57.

2 **Choisissez la boîte à outils Files (Fichiers).**

`Scope=Files, Policy=TSOL` figure dans le titre de la boîte à outils.

3 **Activez l'impression multiniveau en configurant la zone globale à l'aide du port du serveur d'impression, 515/tcp.**

Créez un port multiniveau (MLP) pour le serveur d'impression en ajoutant le port à la zone globale.

a. **Accédez à l'outil Trusted Network Zones (Zones de réseau de confiance).**

b. **Dans Multilevel Ports for Zone's IP Addresses (Ports multiniveau pour adresses IP de la zone) ajoutez 515/tcp.**

c. **Cliquez sur OK.**

4 **Définissez les caractéristiques de chaque imprimante connectée.**

Utilisez la ligne de commande. L'interface graphique du gestionnaire d'impression ne fonctionne pas dans la zone globale.

```
# lpadmin -p printer-name -v /dev/null \
-o protocol=tcp -o dest=printer-IP-address:9100 -T PS -I postscript
# accept printer-name
# enable printer-name
```

5 **Assignez un script de modèle d'imprimante à chaque imprimante connectée au serveur d'impression.**

Le script du modèle active les pages de garde et de fin pour l'imprimante spécifiée.

Pour obtenir une description des scripts, reportez-vous à la section "Scripts de modèle d'imprimante" à la page 222. Si le nom du pilote de l'imprimante commence par `Foomatic`, spécifiez l'un des scripts de modèle foomatic. Sur une seule ligne, utilisez la commande suivante :

```
$ lpadmin -p printer \
 -m { tsol_standard | tsol_netstandard |
      tsol_standard_foomatic | tsol_netstandard_foomatic }
```

Si la plage d'étiquettes d'imprimante par défaut comprise entre `ADMIN_LOW` et `ADMIN_HIGH` convient à toutes les imprimantes, votre configuration d'étiquettes est terminée.

6 **Configurez l'imprimante dans chaque zone étiquetée où l'impression est autorisée.**

Utilisez l'adresse IP `all-zones` de la zone globale en tant que serveur d'impression.

a. **Connectez-vous en tant qu'utilisateur root à la console de zone de la zone étiquetée.**

```
# zlogin -C labeled-zone
```

b. **Ajoutez l'imprimante à la zone.**

```
# lpadmin -p printer-name -s all-zones-IP-address
```

c. **(Facultatif) Définissez l'imprimante comme imprimante par défaut.**

```
# lpadmin -d printer-name
```

7 **Testez l'imprimante dans chaque zone.**

Remarque – À compter de la version Solaris 10 7/10, les fichiers possédant une étiquette d'administration, à savoir `ADMIN_HIGH` ou `ADMIN_LOW`, impriment `ADMIN_HIGH` dans le corps de texte de l'impression. Les pages de garde et de fin sont étiquetées à l'aide des étiquettes et des compartiments les plus élevés dans le fichier `label_encodings`.

En tant qu'utilisateur `root` et en tant qu'utilisateur standard, effectuez les étapes suivantes :

a. **Imprimez des fichiers ordinaires à partir de la ligne de commande.**

b. **Imprimez des fichiers à partir de vos applications (StarOffice par exemple), de votre navigateur et de votre éditeur.**

c. **Assurez-vous que les pages de garde et de fin et que les bannières de sécurité s'impriment correctement.**

Voir aussi

- **Limiter la plage d'étiquettes de l'imprimante** : “Procédure de configuration d'une plage d'étiquettes restreinte pour une imprimante” à la page 239
- **Empêcher la sortie étiquetée** : “Réduction des restrictions d'impression dans Trusted Extensions (liste des tâches)” à la page 240
- **Utiliser cette zone en tant que serveur d'impression** : “Procédure d'octroi de l'autorisation d'accéder à une imprimante à un client Trusted Extensions” à la page 236

▼ Procédure de configuration d'une imprimante réseau pour les clients Sun Ray

Cette procédure permet de configurer une imprimante PostScript sur un serveur Sun Ray possédant une interface `all-zones` unique. L'imprimante est mise à la disposition de tous les

utilisateurs de clients Sun Ray de ce serveur. La configuration initiale est effectuée dans la zone globale. Une fois la zone globale configurée, chaque zone étiquetée est configurée pour utiliser l'imprimante.

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

1. **Dans la zone globale, assignez une adresse IP à l'imprimante réseau.**

   Pour de plus amples instructions, reportez-vous au Chapitre 5, "Setting Up Printers by Using LP Print Commands (Tasks)" du *System Administration Guide: Printing*.

2. **Démarrez la Console de gestion Solaris.**

   - Pour de plus amples instructions, reportez-vous à la section "Initialisation du serveur Console de gestion Solaris dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.
   - Sélectionnez la boîte à outils `Scope=Files, Policy=TSOL` et connectez-vous.

3. **Affectez l'imprimante au modèle `admin_low`.**

   a. **Dans l'outil Computers and Networks (Ordinateurs et réseaux), double-cliquez sur les modèles de sécurité.**

   b. **Double-cliquez sur `admin_low`.**

   c. **Dans l'onglet Hosts Assigned to Template (Hôtes assignés au modèle), ajoutez l'adresse IP de l'imprimante.**

      Pour plus d'informations, consultez l'aide en ligne dans le volet de gauche.

4. **Ajoutez le port d'imprimante à l'interface partagée de la zone globale.**

   a. **Dans l'outil Computers and Networks (Ordinateurs et réseaux), double-cliquez sur Trusted Network Zones (Zones de réseau de confiance).**

   b. **Double-cliquez sur `global`.**

   c. **Ajoutez le port `515` et le protocole `tcp` à la liste Multilevel Ports for Shared IP Addresses (Ports multiniveau pour adresses IP partagées).**

5 Vérifiez que les assignations de la Console de gestion Solaris se trouvent dans le noyau.

```
# tninfo -h printer-IP-address
   IP address= printer-IP-address
   Template = admin_low

# tninfo -m global
   private: 111/tcp;111/udp;513/tcp;515/tcp;631/tcp;2049/tcp;6000-6050/tcp;
7007/tcp;7010/tcp;7014/tcp;7015/tcp;32771/tcp;32776/ip
   shared: 515/tcp;6000-6050/tcp;7007/tcp;7010/tcp;7014/tcp;7015/tcp
```

Remarque – Les autres ports multiniveau privés et partagés (les MLP) tels que `6055` et `7007` prennent en charge la configuration Sun Ray requise.

---

6 Assurez-vous que les services d'impression sont activés dans la zone globale.

```
# svcadm enable print/server
# svcadm enable rfc1179
```

7 Si votre système a été installé à l'aide de `netservices limited`, autorisez l'imprimante à atteindre le réseau.

Le service `rfc1179` doit écouter sur des adresses autres que `localhost`. Le service LP n'écoute que sur les canaux nommés.

```
# inetadm -m svc:/application/print/rfc1179:default bind_addr=''
# svcadm refresh rfc1179
```

Remarque – Si vous exécutez `netservices open`, la commande précédente génère l'erreur suivante : `Error: "inetd" property group missing`.

---

8 Permettez à tous les utilisateurs d'imprimer en PostScript.

Dans l'éditeur de confiance, créez le fichier `/etc/default/print` et ajoutez la ligne suivante :

```
PRINT_POSTSCRIPT=1
```

Des applications telles que StarOffice et `gedit` génèrent des sorties PostScript.

9 Ajoutez tous les filtres LP au service d'impression.

Dans la zone globale, exécutez le script C-Shell :

```
csh
    cd /etc/lp/fd/
    foreach a (*.fd)
        lpfilter -f $a:r -F $a
    end
```

10 Ajoutez une imprimante dans la zone globale.

Utilisez la ligne de commande. L'interface graphique du gestionnaire d'impression ne fonctionne pas dans la zone globale.

```
# lpadmin -p printer-name -v /dev/null -m tsol_netstandard \
-o protocol=tcp -o dest=printer-IP-address:9100 -T PS -I postscript
```

```
# accept printer-name
# enable printer-name
```

11 (Facultatif) Définissez l'imprimante comme imprimante par défaut.

```
# lpadmin -d printer-name
```

12 Dans chaque zone étiquetée, configurez l'imprimante.

Utilisez l'adresse IP `all-zones` en tant que serveur d'impression pour la zone globale. Si votre carte réseau (NIC) `all-zones` est une interface réseau virtuelle (VNI), utilisez l'adresse IP pour le VNI en tant qu'argument de l'option `-s`.

a. Connectez-vous en tant qu'utilisateur root à la console de zone de la zone étiquetée.

```
# zlogin -C labeled-zonename
```

b. Ajoutez l'imprimante à la zone.

```
# lpadmin -p printer-name -s global-zone-shared-IP-address
```

c. (Facultatif) Définissez l'imprimante comme imprimante par défaut.

```
# lpadmin -d printer-name
```

13 Testez l'imprimante dans chaque zone.

Remarque – À compter de la version Solaris 10 7/10, les fichiers possédant une étiquette d'administration, à savoir `ADMIN_HIGH` ou `ADMIN_LOW`, impriment `ADMIN_HIGH` dans le corps de texte de l'impression. Les pages de garde et de fin sont étiquetées à l'aide des étiquettes et des compartiments les plus élevés dans le fichier `label_encodings`.

En tant qu'utilisateur `root` et en tant qu'utilisateur standard, effectuez les étapes suivantes :

a. Imprimez des fichiers ordinaires à partir de la ligne de commande.

b. Imprimez des fichiers à partir de vos applications (StarOffice par exemple), de votre navigateur et de votre éditeur.

c. Assurez-vous que les pages de garde et de fin et que les bannières de sécurité s'impriment correctement.

Exemple 15–1 Détermination de l'état de l'imprimante pour une imprimante réseau

Dans cet exemple, l'administrateur vérifie l'état de l'imprimante réseau à partir de la zone globale et à partir d'une zone étiquetée.

```
global # lpstat -t
    scheduler is running
    system default destination: math-printer
```

```
     system for _default: trusted1 (as printer math-printer)
     device for math-printer: /dev/null
     character set
     default accepting requests since Feb 28 00:00 2008
     lex accepting requests since Feb 28 00:00 2008
     printer math-printer is idle. enabled since Feb 28 00:00 2008. available.

Solaris1# lpstat -t
   scheduler is not running
   system default destination: math-printer
   system for _default: 192.168.4.17 (as printer math-printer)
   system for math-printer: 192.168.4.17
   default accepting requests since Feb 28 00:00 2008
   math-printer accepting requests since Feb 28 00:00 2008
   printer _default is idle. enabled since Feb 28 00:00 2008. available.
   printer math-printer is idle. enabled since Feb 28 00:00 2008. available.
```

▼ Procédure de configuration de l'impression en cascade sur un système étiqueté

L'impression en cascade est un processus permettant d'imprimer à partir d'une session de bureau Windows vers une interface de zone étiquetée Trusted Extensions où l'adresse IP de zone de l'interface physique agit en tant que spooler d'impression. Le processus d'écoute du port multiniveau (MLP) qui se trouve sur l'adresse IP de zone de l'interface physique communique avec le sous-système d'impression Trusted Extensions et imprime le fichier avec les pages de garde et de fin portant l'étiquette appropriée.

Cette procédure permet aux systèmes non étiquetés appartenant au même sous-réseau que des systèmes étiquetés d'utiliser l'imprimante réseau étiquetée. Le service `rfc1179` gère l'impression en cascade. Vous devez effectuer cette procédure dans chacune des zones étiquetées à partir desquelles vous autorisez l'impression en cascade.

Avant de commencer Vous avez effectué les étapes de la section "Procédure de configuration d'une imprimante réseau pour les clients Sun Ray" à la page 228.

1 Connectez-vous en tant qu'utilisateur root à la console de zone de la zone étiquetée.

```
# zlogin -C labeled-zonename
```

2 Supprimez la dépendance du service `rfc1179` vis-à-vis du service d'impression/du serveur.

```
labeled-zone # cat <<EOF | svccfg
      select application/print/rfc1179
      delpg lpsched
      end
   EOF

labeled-zone # svcadm refresh application/print/rfc1179
```

3 Assurez-vous que le service `rfc1179` est activé.

labeled-zone `# svcadm enable rfc1179`

4 Si la zone étiquetée a été installée à l'aide de `netservices limited`, autorisez l'imprimante à atteindre le réseau.

Le service `rfc1179` doit écouter sur des adresses autres que `localhost`. Le service LP n'écoute que sur les canaux nommés.

```
# inetadm -m svc:/application/print/rfc1179:default bind_addr=''
# svcadm refresh rfc1179
```

Remarque – Si vous exécutez `netservices open`, la commande précédente génère le message suivant : `Error: "inetd" property group missing`.

---

5 Configurez l'impression en cascade à partir de la zone étiquetée.

labeled-zone `# lpset -n system -a spooling-type=cascade` *printer-name*

Cette commande met à jour le fichier `/etc/printers.conf` de la zone.

6 Testez un système Oracle Solaris appartenant au même sous-réseau que la zone étiquetée.

Par exemple, testez le système `Solaris1`. Ce système appartient au même sous-réseau que la zone `internal`. Les paramètres de configuration sont les suivants :

- L'adresse IP de `math-printer` est 192.168.4.6
- L'adresse IP de `Solaris1` est 192.168.4.12
- L'adresse IP de la zone `internal` est 192.168.4.17

```
Solaris1# uname -a
SunOS Solaris1 Generic_120011-11 sun4u sparc SUNW,Sun-Blade-1000
Solaris1# lpadmin -p math-printer -s 192.168.4.17
Solaris1# lpadmin -d math-printer

Solaris1# lpstat -t
   scheduler is not running
   system default destination: math-printer
   system for _default: 192.168.4.17 (as printer math-printer)
   system for math-printer: 192.168.4.17
   default accepting requests since Feb 28 00:00 2008
   math-printer accepting requests since Feb 28 00:00 2008
   printer _default is idle. enabled since Feb 28 00:00 2008. available.
   printer math-printer is idle. enabled since Feb 28 00:00 2008. available.
```

- **Testez la commande `lp`.**

```
Solaris1# lp /etc/hosts
   request id is math-printer-1 (1 file)
```

- **Testez l'impression à partir d'applications telles que StarOffice et à partir du navigateur.**

7 Testez un serveur Windows 2003 appartenant au même sous-réseau que cette zone étiquetée.

a. Configurez l'imprimante sur le serveur Windows.

Utilisez l'interface graphique du menu Démarrer->Paramètres->Imprimantes et télécopieurs.

Effectuez la configuration d'imprimante suivante :

- Ajouter une imprimante
- Imprimante locale connectée à cet ordinateur
- Créer un nouveau port : port TCP/IP standard
- Nom d'imprimante ou adresse IP : 192.168.4.17, c'est-à-dire l'adresse IP de la zone étiquetée
- Nom du port : Accepter la valeur par défaut
- Informations supplémentaires requises concernant le ports : Accepter la valeur par défaut
  - Type de périphérique = Personnalisé
  - Paramètres – protocole = LPR
  - Paramètres LPR – Nom de file d'attente = math-printer, c'est-à-dire, le nom de la file d'attente UNIX
  - Comptage des octets LPR activé

Terminez la configuration de l'imprimante en spécifiant le fabricant, le modèle, le pilote et les autres paramètres de l'imprimante.

8 Testez l'imprimante en sélectionnant l'imprimante à partir d'une application.

Par exemple, testez le système `winserver` appartenant au même sous-réseau que la zone `internal`. Les paramètres de configuration sont les suivants :

- L'adresse IP de `math-printer` est 192.168.4.6
- L'adresse IP de `winserver` est 192.168.4.200
- L'adresse IP de `internal` est 192.168.4.17

```
winserver C:/> ipconfig
Windows IP Configuration
   Ethernet adapter TP-NIC:
      Connection-specific DNS Suffix  . :
      IP Address. . . . . . . . . . . . : 192.168.4.200
      Subnet Mask . . . . . . . . . . . : 255.255.255.0
      Default Gateway . . . . . . . . . : 192.168.4.17
```

▼ Procédure de configuration d'une zone pour l'impression à étiquette unique

Avant de commencer La zone ne doit pas partager d'adresse IP avec la zone globale. Vous devez être dans le rôle d'administrateur système dans la zone globale.

1. **Ajoutez un espace de travail.**

   Pour plus d'informations, reportez-vous à la section "Procédure d'ajout d'un espace de travail possédant une étiquette particulière" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

2. **Modifiez l'étiquette du nouvel espace de travail et remplacez-la par celle de la zone qui servira de serveur d'impression pour cette étiquette.**

   Pour plus d'informations, reportez-vous à la section "Procédure de modification de l'étiquette d'un espace de travail" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

3. **Définissez les caractéristiques des imprimantes connectées.**

   a. **Sous l'étiquette de la zone, démarrez le gestionnaire d'impression.**

      Par défaut, la case "Use PPD" (Utiliser PPD) est cochée. Le système recherche le pilote approprié pour l'imprimante.

   b. **(Facultatif) Pour spécifier un autre pilote d'imprimante, effectuez les opérations suivantes :**

      i. **Désactivez la case à cocher "Use PPD".**

      ii. **Définissez la marque et le modèle de l'imprimante qui utilise un pilote différent.**

      Dans le gestionnaire d'impression, vous devez fournir les valeurs pour les deux premiers champs, le gestionnaire d'impression fournit ensuite le nom du pilote.

      ```
      Printer Make      manufacturer
      Printer Model     manufacturer-part-number
      Printer Driver    automatically filled in
      ```

4. **Assignez un script de modèle d'imprimante à chacune des imprimantes connectées à la zone.**

   Le script de modèle active les pages de garde et de fin pour l'imprimante spécifiée.

   Pour le choix de vos scripts, reportez-vous à la section "Scripts de modèle d'imprimante" à la page 222. Si le nom du pilote de l'imprimante commence par `Foomatic`, spécifiez l'un des scripts de modèle foomatic. Utilisez la commande suivante :

   ```
   $ lpadmin -p printer -m model
   ```

   Les imprimantes connectées peuvent uniquement imprimer des travaux ayant l'étiquette de la zone.

5 **Testez l'imprimante.**

Remarque – À compter de la version Solaris 10 7/10, les fichiers possédant une étiquette d'administration, à savoir `ADMIN_HIGH` ou `ADMIN_LOW`, impriment `ADMIN_HIGH` dans le corps de texte de l'impression. Les pages de garde et de fin sont étiquetées à l'aide des étiquettes et des compartiments les plus élevés dans le fichier `label_encodings`.

En tant qu'utilisateur `root` et en tant qu'utilisateur standard, effectuez les étapes suivantes :

a. **Imprimez des fichiers ordinaires à partir de la ligne de commande.**

b. **Imprimez des fichiers à partir de vos applications (StarOffice par exemple), de votre navigateur et de votre éditeur.**

c. **Assurez-vous que les pages de garde et de fin et que les bannières de sécurité s'impriment correctement.**

Voir aussi **Empêcher la sortie étiquetée** : “Réduction des restrictions d'impression dans Trusted Extensions (liste des tâches)” à la page 240

▼ Procédure d'octroi de l'autorisation d'accéder à une imprimante à un client Trusted Extensions

Au départ, seule la zone dans laquelle un serveur d'impression a été configuré peut imprimer sur les imprimantes de ce serveur d'impression. L'administrateur système doit explicitement ajouter l'accès à ces imprimantes pour d'autres zones et d'autres systèmes. Les possibilités sont les suivantes :

- Pour une zone globale, ajoutez l'accès aux imprimantes connectées à une zone globale sur un système différent.
- Pour une zone étiquetée, ajoutez l'accès aux imprimantes connectées à la zone globale de son système.
- Pour une zone étiquetée, ajoutez l'accès à une imprimante pour laquelle une zone distante d'étiquette identique est configurée.
- Pour une zone étiquetée, ajoutez l'accès à des imprimantes connectées à une zone globale sur un système différent.

Avant de commencer

Un serveur d'impression a été configuré avec une plage d'étiquettes ou une étiquette unique et les imprimantes qui y sont connectées ont été configurées. Pour plus d'informations, reportez-vous aux sections suivantes :

- "Procédure de configuration d'un serveur d'impression multiniveau et des imprimantes correspondantes" à la page 226
- "Procédure de configuration d'une zone pour l'impression à étiquette unique" à la page 235
- "Procédure d'assignation d'une étiquette à un serveur d'impression non étiqueté" à la page 241

Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale ou vous devez être habilité à assumer un rôle.

1 Effectuez les procédures permettant à vos systèmes d'accéder à une imprimante.

- **Configurez la zone globale sur un système qui n'est pas un serveur d'impression de manière à ce qu'elle utilise la zone globale d'un autre système pour accéder à des imprimantes.**

  a. Sur le système qui ne dispose d'aucun accès à des imprimantes, prenez le rôle d'administrateur de sécurité.

  b. Ajoutez l'accès à l'imprimante connectée au serveur d'impression Trusted Extensions.

  ```
  $ lpadmin -s printer
  ```

- **Configurez une zone étiquetée de manière à ce qu'elle utilise sa zone globale pour accéder à une imprimante.**

  a. Modifiez l'étiquette de l'espace de travail du rôle et remplacez-la par celle de la zone étiquetée.

  Pour plus d'informations, reportez-vous à la section "Procédure de modification de l'étiquette d'un espace de travail" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

  b. Ajoutez l'accès à l'imprimante.

  ```
  $ lpadmin -s printer
  ```

- **Configurez une zone étiquetée de manière à ce qu'elle utilise la zone étiquetée d'un autre système pour accéder à des imprimantes.**

  Les étiquettes des zones doivent être identiques.

  a. Sur le système qui ne dispose d'aucun accès à des imprimantes, prenez le rôle d'administrateur de sécurité.

b. Modifiez l'étiquette de l'espace de travail du rôle et remplacez-la par celle de la zone étiquetée.

Pour plus d'informations, reportez-vous à la section "Procédure de modification de l'étiquette d'un espace de travail" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

c. Ajoutez l'accès à l'imprimante connectée au serveur d'impression de la zone étiquetée distante.

```
$ lpadmin -s printer
```

- **Configurez une zone étiquetée de manière à ce qu'elle utilise un serveur d'impression non étiqueté pour accéder à des imprimantes.**

  L'étiquette de la zone doit être identique à celle du serveur d'impression.

  a. Sur le système qui ne dispose d'aucun accès à des imprimantes, prenez le rôle d'administrateur de sécurité.

  b. Modifiez l'étiquette de l'espace de travail du rôle et remplacez-la par celle de la zone étiquetée.

  Pour plus d'informations, reportez-vous à la section "Procédure de modification de l'étiquette d'un espace de travail" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

  c. Ajoutez l'accès à l'imprimante connectée au serveur d'impression d'étiquette quelconque.

  ```
  $ lpadmin -s printer
  ```

2 Testez les imprimantes.

À compter de la version Solaris 10 7/10, les fichiers possédant une étiquette d'administration : à savoir `ADMIN_HIGH` ou `ADMIN_LOW`, impriment `ADMIN_HIGH` dans le corps de texte de l'impression. Les pages de garde et de fin sont étiquetées à l'aide des étiquettes et des compartiments les plus élevés dans le fichier `label_encodings`.

Sur chaque client, assurez-vous que l'impression fonctionne pour l'utilisateur `root` et les rôles dans la zone globale ainsi que pour l'utilisateur `root`, les rôles et les utilisateurs standard dans les zones étiquetées.

a. Imprimez des fichiers ordinaires à partir de la ligne de commande.

b. Imprimez des fichiers à partir de vos applications (StarOffice par exemple), de votre navigateur et de votre éditeur.

c. Assurez-vous que les pages de garde et de fin et que les bannières de sécurité s'impriment correctement.

▼ Procédure de configuration d'une plage d'étiquettes restreinte pour une imprimante

La plage d'étiquettes d'imprimante par défaut va de `ADMIN_LOW` à `ADMIN_HIGH`. Cette procédure permet de réduire la plage d'étiquettes pour une imprimante contrôlée par un serveur d'impression Trusted Extensions.

Avant de commencer Vous devez être dans le rôle d'administrateur système dans la zone globale.

1. **Démarrez le gestionnaire d'allocation de périphériques (Device Allocation Manager).**
   - **Sélectionnez l'option Allocate Device (Allouer un périphérique) dans le menu Trusted Path (Chemin de confiance).**
   - **Dans Trusted CDE, lancez le gestionnaire d'allocation de périphériques à partir du tableau secondaire Tools (Outils) du tableau de bord.**
2. **Cliquez sur le bouton Device Administration (Administration des périphériques) pour afficher la boîte de dialogue Device Allocation: Administration (Allocation de périphériques : Administration).**
3. **Saisissez un nom pour la nouvelle imprimante.**

   Si l'imprimante est connectée à votre système, recherchez son nom.
4. **Cliquez sur le bouton Configure (Configurer) pour afficher la boîte de dialogue Device Allocation: Configuration (Allocation de périphériques : Configuration).**
5. **Modifiez la plage d'étiquettes de l'imprimante.**
   a. **Cliquez sur le bouton Min Label (Étiquette min) pour modifier l'étiquette minimale.**

      Sélectionnez une étiquette dans le générateur d'étiquettes. Pour plus d'informations sur le générateur d'étiquettes, reportez-vous à la section "Générateur d'étiquettes dans Trusted Extensions" à la page 45.
   b. **Cliquez sur le bouton Max Label (Étiquette max) pour modifier l'étiquette maximale.**
6. **Enregistrez les modifications.**
   a. **Cliquez sur OK dans la boîte de dialogue de configuration.**
   b. **Cliquez sur OK dans la boîte de dialogue d'administration.**
7. **Fermez le gestionnaire d'allocation de périphériques.**

Réduction des restrictions d'impression dans Trusted Extensions (liste des tâches)

Les tâches suivantes sont facultatives. Elles réduisent la sécurité d'impression que Trusted Extensions fournit par défaut lors de l'installation du logiciel.

Tâche	Description	Voir
Configuration d'une imprimante de manière à ce qu'elle n'étiquette pas les sorties.	Empêche l'impression des informations de sécurité sur les pages de corps de texte et supprime les pages de garde et de fin.	"Procédure de suppression des étiquettes sur les sorties d'imprimante" à la page 241
Configuration d'imprimantes à étiquette unique n'étiquetant pas les sorties.	Permet aux utilisateurs d'imprimer sous une étiquette spécifique sur une imprimante Oracle Solaris. Les travaux d'impression ne sont pas étiquetés.	"Procédure d'assignation d'une étiquette à un serveur d'impression non étiqueté" à la page 241
Suppression de l'étiquetage visible des pages de corps de texte.	Modifie le fichier `tsol_separator.ps` de manière à empêcher l'impression d'étiquettes sur les pages de corps de texte de tous les travaux d'impression envoyés à partir d'un hôte Trusted Extensions.	"Procédure de suppression des étiquettes de pages de tous les travaux d'impression" à la page 242
Suppression des pages de garde et de fin.	Autorise des utilisateurs spécifiques à imprimer des travaux sans page de garde ni de page de fin.	"Procédure d'octroi à des utilisateurs spécifiques de l'autorisation de supprimer les pages de garde et de fin" à la page 243
Octroi à des utilisateurs de confiance de l'autorisation d'imprimer des travaux sans les étiquettes.	Autorise des utilisateurs spécifiques ou l'ensemble des utilisateurs d'un système donné à imprimer des travaux d'impression sans étiquettes.	"Procédure d'octroi à des utilisateurs spécifiques de l'autorisation de supprimer les étiquettes de pages" à la page 243
Octroi de l'autorisation d'imprimer des fichiers PostScript.	Autorise des utilisateurs spécifiques ou l'ensemble des utilisateurs d'un système donné à imprimer des fichiers PostScript.	"Procédure d'octroi à des utilisateurs de l'autorisation d'imprimer des fichiers PostScript dans Trusted Extensions" à la page 244
Assignation d'autorisations d'impression.	Autorise des utilisateurs à s'affranchir de certaines restrictions d'impression par défaut.	"Procédure de création d'un profil de droits pour des autorisations commodes" à la page 99 "Procédure de modification des valeurs par défaut de `policy.conf`" à la page 91

▼ Procédure de suppression des étiquettes sur les sorties d'imprimante

Les imprimantes ne disposant pas d'un script de modèle d'imprimante Trusted Extensions n'impriment pas de pages de garde ou de fin étiquetées. Les pages de corps de texte n'incluent pas non plus d'étiquettes.

Avant de commencer Vous devez être dans le rôle de l'administrateur de sécurité dans la zone globale.

- **Effectuez l'une des opérations suivantes pour l'étiquette appropriée :**

  - **À partir du serveur d'impression, annulez complètement l'impression des bannières.**

    ```
    $ lpadmin -p printer -o nobanner=never
    ```

    Les pages de corps de texte sont toujours étiquetées.

  - **Définissez le script de modèle d'imprimante sur un script Oracle Solaris.**

    ```
    $ lpadmin -p printer  \
    -m { standard | netstandard | standard_foomatic | netstandard_foomatic }
    ```

    Aucune étiquette n'apparaît sur les sorties d'imprimante.

▼ Procédure d'assignation d'une étiquette à un serveur d'impression non étiqueté

Un serveur d'impression Oracle Solaris est un serveur d'impression non étiqueté auquel il est possible d'assigner une étiquette permettant à Trusted Extensions d'accéder à l'imprimante correspondant à cette étiquette. Les imprimantes connectées à un serveur d'impression non étiqueté peuvent uniquement imprimer des travaux correspondant à l'étiquette assignée au serveur d'impression. Les travaux sont imprimés sans étiquette ni de page de fin, et peuvent aussi être imprimés sans page de garde. Si un travail est imprimé avec une page de garde, la page ne contient aucune information de sécurité.

Il est possible de configurer un système Trusted Extensions de manière à ce qu'il soumette des travaux à une imprimante gérée par un serveur d'impression non étiqueté. Les utilisateurs peuvent imprimer sur l'imprimante sans étiquetage des travaux correspondant à l'étiquette que l'administrateur de sécurité assigne au serveur d'impression.

Avant de commencer Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

1. **Ouvrez la Console de gestion Solaris dans l'étendue appropriée.**

   Pour plus d'informations, reportez-vous à la section "Initialisation du serveur Console de gestion Solaris dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.

2. **Sous System Configuration (Configuration système), accédez à l'outil Computers and Networks (Ordinateurs et réseaux).**

   Saisissez un mot de passe lorsque vous y êtes invité.

3. **Assignez un modèle non étiqueté au serveur d'impression.**

   Pour plus d'informations, reportez-vous à la section "Procédure d'assignation d'un modèle de sécurité à un hôte ou à un groupe d'hôtes" à la page 194.

   Choisissez une étiquette. Les utilisateurs qui travaillent sous cette étiquette peuvent envoyer des travaux d'impression à l'imprimante Oracle Solaris correspondant à l'étiquette du serveur d'impression. Les pages s'impriment sans étiquette, et aucune page de garde ou de fin n'est imprimée pour ces travaux.

Exemple 15–2 Envoi de travaux d'impression publics vers une imprimante sans étiquetage

Les fichiers disponibles pour le grand public sont adaptés à l'impression sur une imprimante non étiquetée. Dans cet exemple, les rédacteurs marketing doivent produire des documents destinés à être imprimés sans étiquette au haut et au bas des pages.

L'administrateur de sécurité assigne un type d'hôte non étiqueté au serveur d'impression Oracle Solaris. Le modèle est décrit dans la section Exemple 13–6. L'étiquette arbitraire du modèle est `PUBLIC`. L'imprimante `pr-nolabel1` est connectée à ce serveur d'impression. Les travaux d'impression d'utilisateurs se trouvant dans une zone `PUBLIC` sont imprimés sans étiquette sur l'imprimante `pr-nolabel1`. En fonction des paramètres de l'imprimante, les travaux peuvent ou non inclure des pages de garde. Les pages de garde ne contiennent pas d'informations de sécurité.

▼ Procédure de suppression des étiquettes de pages de tous les travaux d'impression

Cette procédure permet d'empêcher l'impression d'étiquettes visibles sur les pages de corps de texte de tous les travaux d'impression effectués par une imprimante Trusted Extensions.

Avant de commencer Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

1. **Modifiez le fichier `/usr/lib/lp/postscript/tsol_separator.ps`.**

   Servez-vous de l'éditeur de confiance. Pour plus d'informations, reportez-vous à la section "Modification des fichiers d'administration dans Trusted Extensions" à la page 59.

2 **Recherchez la définition de `/PageLabel`.**

Trouvez les lignes suivantes :

```
%% To eliminate page labels completely, change this line to
%% set the page label to an empty string: /PageLabel () def
/PageLabel Job_PageLabel def
```

Remarque – La valeur `Job_PageLabel` peut être différente sur votre site.

3 **Remplacez la valeur de `/PageLabel` par un ensemble de parenthèses vides.**

```
/PageLabel () def
```

▼ Procédure d'octroi·à·des·utilisateurs·spécifiques de l'autorisation de supprimer les étiquettes de pages

Cette procédure permet d'autoriser un utilisateur ou un rôle à imprimer des travaux d'impression ne comportant pas d'étiquette dans la partie supérieure et inférieure de chaque page de corps de texte sur une imprimante Trusted Extensions. La suppression s'applique à toutes les étiquettes sous lesquelles l'utilisateur peut travailler.

Avant de commencer Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

1 **Déterminez les utilisateurs autorisés à imprimer des travaux sans étiquettes de pages.**

2 **Autorisez ces utilisateurs et rôles à imprimer les travaux d'impression sans étiquettes de pages.**

Assignez un profil de droits incluant l'autorisation Print without Label (Impression sans étiquette) à ces utilisateurs et rôles. Pour plus d'informations, reportez-vous à la section "Procédure de création d'un profil de droits pour des autorisations commodes" à la page 99.

3 **Indiquez aux utilisateurs ou aux rôles concernés d'utiliser la commande `lp` pour soumettre des travaux d'impression :**

```
% lp -o nolabels staff.mtg.notes
```

▼ Procédure d'octroi à des utilisateurs spécifiques de l'autorisation de supprimer les pages de garde et de fin

Avant de commencer Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

1. **Créez un profil de droits incluant l'autorisation Print without Banner (Imprimer sans page de garde).**

   Assignez le profil à chaque utilisateur ou rôle autorisé à imprimer sans page de garde ni de fin.

   Pour plus d'informations, reportez-vous à la section "Procédure de création d'un profil de droits pour des autorisations commodes" à la page 99.

2. **Indiquez aux utilisateur ou aux rôles concernés d'utiliser la commande `lp` pour soumettre des travaux d'impression :**

   ```
   % lp -o nobanner staff.mtg.notes
   ```

▼ Procédure d'octroi à des utilisateurs de l'autorisation d'imprimer des fichiers PostScript dans Trusted Extensions

Avant de commencer Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

- **Utilisez l'une des trois méthodes suivantes pour autoriser des utilisateurs à imprimer des fichiers PostScript :**

  - **Pour autoriser l'impression PostScript sur un système, modifiez le fichier `/etc/default/print`.**

    a. **Créez ou modifiez le fichier `/etc/default/imprimer`.**

       Servez-vous de l'éditeur de confiance. Pour plus d'informations, reportez-vous à la section "Modification des fichiers d'administration dans Trusted Extensions" à la page 59.

    b. **Saisissez l'entrée suivante :**

       ```
       PRINT_POSTSCRIPT=1
       ```

    c. **Enregistrez le fichier et fermez l'éditeur.**

  - **Pour autoriser tous les utilisateurs à imprimer des fichiers PostScript à partir d'un système, modifiez le fichier `/etc/security/policy.conf`.**

    a. **Modifiez le fichier `policy.conf`.**

       Servez-vous de l'éditeur de confiance. Pour plus d'informations, reportez-vous à la section "Modification des fichiers d'administration dans Trusted Extensions" à la page 59.

b. Ajoutez l'autorisation `solaris.print.ps`.

`AUTHS_GRANTED=`*other-authorizations*`,solaris.print.ps`

c. Enregistrez le fichier et fermez l'éditeur.

- **Pour permettre à des utilisateurs ou rôles d'imprimer des fichiers PostScript à partir de n'importe quel système, attribuez l'autorisation correspondante à ces utilisateurs et rôles seulement.**

  Assignez un profil incluant l'autorisation `Print Postscript` (Imprimer Postscript) à ces utilisateurs et rôles. Pour plus d'informations, reportez-vous à la section "Procédure de création d'un profil de droits pour des autorisations commodes" à la page 99.

Exemple 15–3 Activation de l'impression PostScript à partir d'un système public

Dans l'exemple suivant, l'administrateur de sécurité a contraint un kiosque public à fonctionner sous l'étiquette `PUBLIC`. Le système contient également quelques icônes permettant d'accéder à des sujets intéressants. Ces sujets peuvent être imprimés.

L'administrateur de sécurité crée un fichier `/etc/default/print` sur le système. Le fichier contient une entrée activant l'impression des fichiers PostScript. Aucun utilisateur n'a besoin de l'autorisation `Print Postscript`.

```
# vi /etc/default/print

# PRINT_POSTSCRIPT=0
PRINT_POSTSCRIPT=1
```

◆ ◆ ◆ CHAPITRE 16

Périphériques dans Trusted Extensions (présentation)

Ce chapitre décrit les extensions fournies par Trusted Extensions pour la protection des périphériques Oracle Solaris.

Protection des périphériques avec le logiciel Trusted Extensions

Sur un système Oracle Solaris les périphériques peuvent être protégés par allocation et par autorisation. Par défaut, les périphériques sont disponibles sans autorisation pour les utilisateurs standard. Un système configuré avec le logiciel Trusted Extensions utilise les mécanismes de protection des périphériques du SE Oracle Solaris.

Toutefois, Trusted Extensions requiert par défaut qu'un périphérique soit alloué pour être utilisé et que son utilisateur soit autorisé à l'utiliser. En outre, les périphériques sont protégés par des étiquettes. Trusted Extensions fournit aux administrateurs une interface graphique leur permettant de gérer les périphériques. La même interface est utilisée par les utilisateurs pour l'allocation des périphériques.

Remarque – Dans Trusted Extensions, les utilisateurs ne peuvent pas utiliser les commandes `allocate` et `deallocate`. Ils doivent utiliser le gestionnaire d'allocation de périphériques (Device Allocation Manager). Dans Solaris Trusted Extensions (JDS), le titre de l'interface graphique est Device Manager (Gestionnaire de périphériques).

Pour plus d'informations sur la protection des périphériques dans le SE Oracle Solaris, reportez-vous au Chapitre 4, “Controlling Access to Devices (Tasks)” du *System Administration Guide: Security Services*.

Sur un système configuré avec Trusted Extensions, deux rôles protègent les périphériques.

- Le rôle d'administrateur système contrôle l'accès aux périphériques.

  L'administrateur système rend allouable un périphérique. Les périphériques qu'il rend non allouables ne peuvent être utilisés par personne. Seuls des utilisateurs autorisés peuvent allouer des périphériques allouables.
- Le rôle d'administrateur de sécurité restreint les étiquettes permettant d'accéder à un périphérique et définit la stratégie de périphérique. C'est l'administrateur de la sécurité qui décide qui est autorisé à allouer un périphérique.

Vous trouverez ci-dessous les principales fonctions de contrôle de périphériques avec le logiciel Trusted Extensions :

- Par défaut, un utilisateur non autorisé sur un système Trusted Extensions ne peut pas allouer de périphériques tels que les lecteurs de bande, les unités de CD-ROM ou les unités de disquette.

  Un utilisateur standard doté de l'autorisation Allocate Device (Allouer un périphérique) peut importer ou exporter des informations sous l'étiquette de laquelle l'utilisateur alloue le périphérique.
- Les utilisateurs appellent le gestionnaire d'allocation de périphériques (Device Allocation Manager) lorsqu'ils sont directement connectés. Pour allouer un périphérique à distance, les utilisateurs doivent avoir accès à la zone globale. En règle générale, seuls les rôles ont accès à cette zone.
- La plage d'étiquettes de chaque périphérique peut être restreinte par l'administrateur de sécurité. Les utilisateurs standard ont un accès limité aux seuls périphériques dont la plage d'étiquettes inclut les étiquettes avec lesquelles ils sont autorisés à travailler. La plage d'étiquettes par défaut d'un périphérique est comprise entre `ADMIN_LOW` et `ADMIN_HIGH`.
- Les plages d'étiquettes peuvent être restreintes pour les périphériques allouables et non allouables. Les périphériques non allouables sont des périphériques tels que les mémoires graphiques et les imprimantes.

Plages d'étiquettes des périphériques

Pour éviter toute copie d'informations sensibles, chaque périphérique allouable dispose d'une plage d'étiquettes. Pour utiliser un périphérique allouable, l'utilisateur doit être en train de travailler avec une étiquette comprise dans la plage. Dans le cas contraire, l'allocation lui est refusée. L'étiquette en cours de l'utilisateur est appliquée aux données importées ou exportées

lorsque le périphérique est alloué à l'utilisateur. L'étiquette des données exportées s'affiche lorsque le périphérique est libéré. L'utilisateur doit étiqueter physiquement le support contenant les données exportées.

Effets de la plage d'étiquettes sur un périphérique

Pour restreindre l'accès par connexion directe via la console, l'administrateur de sécurité peut définir une plage d'étiquettes restreinte sur la mémoire graphique.

Par exemple, une plage d'étiquettes restreinte peut être spécifiée pour limiter l'accès à un système public. La plage d'étiquettes permet alors aux utilisateurs d'accéder au seul système dont l'étiquette est comprise dans la plage de la mémoire graphique.

Lorsqu'un hôte dispose d'une imprimante locale, une plage d'étiquettes restreinte sur l'imprimante limite le nombre de travaux pouvant être imprimés.

Stratégies d'accès aux périphériques

Trusted Extensions observe les mêmes stratégies de périphérique que le SE Oracle Solaris. L'administrateur de sécurité peut modifier les stratégies par défaut et en définir de nouvelles. La commande `getdevpolicy` récupère les informations sur la stratégie de périphérique et la commande `update_drv` permet de modifier la stratégie. Pour plus d'informations, reportez-vous à la section "Configuring Device Policy (Task Map)" du *System Administration Guide: Security Services*. Reportez-vous également aux pages de manuel `getdevpolicy(1M)` et `update_drv(1M)`.

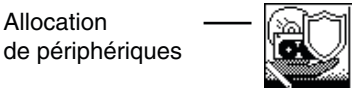
Scripts de nettoyage de périphériques

Un script de nettoyage de périphériques s'exécute à chaque fois qu'un périphérique est alloué ou libéré. Le SE Oracle Solaris propose des scripts pour des lecteurs de bande ainsi que les unités de CD-ROM et de disquette. Si votre site ajoute des types de périphérique allouable au système, les périphériques ajoutés peuvent avoir besoin de scripts. Pour connaître les scripts existants, accédez au répertoire `/etc/security/lib`. Pour plus d'informations, reportez-vous à la section "Device-Clean Scripts" du *System Administration Guide: Security Services*.

Pour le logiciel Trusted Extensions, les scripts de nettoyage de périphériques doivent satisfaire à certaines exigences. Les conditions requises sont décrites dans la page de manuel `device_clean(5)`.

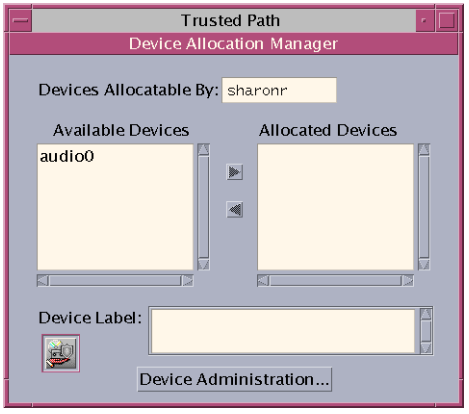
Interface graphique du gestionnaire d'allocation de périphériques

Le gestionnaire d'allocation de périphériques (Device Allocation Manager) est utilisé par les administrateurs pour administrer les périphériques allouables et non allouables. Le gestionnaire d'allocation de périphériques est également utilisé par les utilisateurs standard pour allouer et libérer des périphériques. Les utilisateurs doivent disposer de l'autorisation Allocate Device (Allouer un périphérique). Dans un espace de travail Solaris Trusted Extensions (CDE), le gestionnaire d'allocation de périphériques est ouvert à partir du tableau de bord. L'icône se présente de la manière suivante :



Dans un espace de travail Solaris Trusted Extensions (JDS), l'interface graphique est nommée Device Manager (Gestionnaire de périphériques). Cette interface graphique est démarrée à partir du menu Trusted Path (Chemin de confiance) en sélectionnant Allocate Device (Allouer un périphérique). DansTrusted CDE, elle peut également être démarrée à partir du menu Trusted Path (Chemin de confiance). La figure ci-dessous illustre un gestionnaire d'allocation de périphériques ouvert par un utilisateur autorisé à allouer le périphérique `audio`.

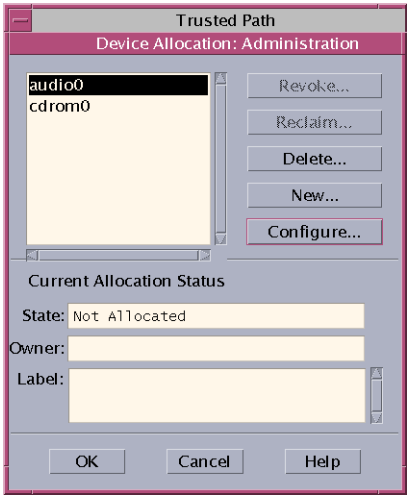
FIGURE 16–1 Gestionnaire d'allocation de périphériques ouvert par un utilisateur



Une liste vide apparaît lorsque les utilisateurs ne sont pas autorisés à allouer des périphériques. Cela peut également indiquer que les périphériques allouables sont actuellement alloués par un

autre utilisateur ou qu'ils sont en erreur. Si un utilisateur ne parvient pas à trouver un périphérique dans la liste Available Devices (Périphériques disponibles), il doit contacter l'administrateur responsable.

La fonction Device Administration (Administration de périphériques) est disponible pour les rôles dotés de l'une des deux autorisations requises au moins pour administrer les périphériques. Les autorisations d'administration sont Configure Device Attributes (Configurer les attributs des périphériques) et Revoke or Reclaim Device (Révoquer ou récupérer un périphérique). La figure suivante montre une boîte de dialogue Device Allocation Administration (Administration de l'allocation de périphériques).



Dans Solaris Trusted Extensions (JDS), le bouton Device Administration (Administration de périphériques) s'appelle Administration.

Application de la sécurité des périphériques dans Trusted Extensions

L'administrateur de sécurité désigne les utilisateurs autorisés à allouer des périphériques et veille à ce que chacun d'entre eux soit formé. L'utilisateur est autorisé à effectuer les opérations suivantes :

- Étiqueter et manipuler correctement tout support contenant des informations sensibles exportées afin qu'elles ne tombent pas entre les mains de personnes non autorisées.

  Par exemple, si des informations d'étiquette `NEED TO KNOW ENGINEERING` sont stockées sur une disquette, l'utilisateur qui exporte les informations doit physiquement apposer l'étiquette `NEED TO KNOW ENGINEERING` sur le disque. La disquette doit être stockée dans un emplacement accessible aux seuls membres du groupe ingénierie concernés.
- Assurez-vous que les étiquettes des informations importées (lues) depuis les supports de ces périphériques soient correctement tenues à jour.

  Un utilisateur autorisé doit allouer le périphérique sous l'étiquette correspondant à celle des informations à importer. Par exemple, si un utilisateur alloue une unité de disquette sous l'étiquette `PUBLIC`, il ne doit importer que des informations étiquetées `PUBLIC`.

L'administrateur de sécurité est également chargé de veiller au respect de ces exigences de sécurité.

Périphériques dans Trusted Extensions (référence)

La protection des périphériques Trusted Extensions utilise des interfaces Oracle Solaris et Trusted Extensions.

Pour connaître les interfaces de ligne de commande Oracle Solaris, reportez-vous à la section "Device Protection (Reference)" du *System Administration Guide: Security Services*.

Les administrateurs qui n'ont pas accès au gestionnaire d'allocation de périphériques peuvent administrer les périphériques allouables via la ligne de commande. Les commandes `allocate` et `deallocate` comportent des options d'administration. Pour consulter des exemples, reportez-vous aux sections "Forcibly Allocating a Device" du *System Administration Guide: Security Services* et "Forcibly Deallocating a Device" du *System Administration Guide: Security Services*.

Pour consulter les interfaces de ligne de commande Trusted Extensions, reportez-vous aux pages de manuel `add_allocatable(1M)` et `remove_allocatable(1M)`.

◆ ◆ ◆ CHAPITRE 17

Gestion des périphériques pour Trusted Extensions (tâches)

Ce chapitre décrit l'administration et l'utilisation des périphériques sur un système configuré avec Trusted Extensions.

Manipulation des périphériques dans Trusted Extensions (liste des tâches)

La liste des tâches suivante contient des liens vers des listes des tâches destinées aux administrateurs et aux utilisateurs et concernant la gestion des périphériques.

Tâche	Description	Voir
Utilisation des périphériques.	Permet d'utiliser un périphérique en tant que rôle ou en tant qu'utilisateur standard.	"Utilisation de périphériques dans Trusted Extensions (liste des tâches)" à la page 254
Gestion des périphériques.	Permet de configurer des périphériques pour les utilisateurs ordinaires.	"Gestion des périphériques dans Trusted Extensions (liste des tâches)" à la page 254
Personnalisation des autorisations de périphériques.	Le rôle d'administrateur de sécurité crée des autorisations, les ajoute au périphérique, les place dans un profil de droits et affecte ce profil à l'utilisateur.	"Personnalisation des autorisations de périphériques dans Trusted Extensions (liste des tâches)" à la page 264

Utilisation de périphériques dans Trusted Extensions (liste des tâches)

Dans Trusted Extensions, tous les rôles sont autorisés à allouer un périphérique. Les rôles comme les utilisateurs doivent utiliser à cet effet le gestionnaire d'allocation de périphériques (Device Allocation Manager). La commande `allocate` (allouer) d'Oracle Solaris ne fonctionne pas dans Trusted Extensions. La liste des tâches suivante contient des liens vers des procédures utilisateur qui incluent l'utilisation de périphériques pour effectuer des tâches d'administration.

Tâche	Voir
Allocation et libération d'un périphérique.	"Procédure d'allocation d'un périphérique dans Trusted Extensions" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions* "Zone de commutation de l'espace de travail" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*
Utilisation d'un support portable pour le transfert de fichiers.	"Copie de fichiers dans Trusted Extensions à partir d'un support amovible" du *Guide de configuration d'Oracle Solaris Trusted Extensions* "Copie de fichiers sur un support amovible dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions*

Gestion des périphériques dans Trusted Extensions (liste des tâches)

La liste des tâches ci-dessous décrit des procédures permettant d'assurer la protection des périphériques sur votre site.

Tâche	Description	Voir
Définition ou modification de la stratégie des périphériques.	Permet de modifier les privilèges qui sont nécessaires pour accéder à un périphérique.	"Configuring Device Policy (Task Map)" du *System Administration Guide: Security Services*
Octroi de l'autorisation d'allouer un périphérique à des utilisateurs.	Le rôle d'administrateur de sécurité assigne à l'utilisateur un profil comportant l'autorisation Allocate Device (Allouer un périphérique).	"How to Authorize Users to Allocate a Device" du *System Administration Guide: Security Services*
	Le rôle d'administrateur de sécurité affecte à l'utilisateur un profil doté des autorisations spécifiques au site.	"Personnalisation des autorisations de périphériques dans Trusted Extensions (liste des tâches)" à la page 264
Configuration d'un périphérique.	Permet de choisir des fonctions de sécurité pour protéger le périphérique.	"Procédure de configuration d'un périphérique dans Trusted Extensions" à la page 255

Tâche	Description	Voir
Révocation ou récupération d'un périphérique.	Permet d'utiliser le gestionnaire d'allocation de périphériques pour mettre à disposition un périphérique.	"Procédure de révocation ou de récupération d'un périphérique dans Trusted Extensions" à la page 259
	Permet d'utiliser les commandes d'Oracle Solaris pour mettre à disposition ou rendre indisponible un périphérique.	"Forcibly Allocating a Device" du *System Administration Guide: Security Services* "Forcibly Deallocating a Device" du *System Administration Guide: Security Services*
Interdiction de l'accès à un périphérique allouable.	Offre un contrôle d'accès détaillé à un périphérique.	Exemple 17–4
	Permet d'interdire l'accès à un périphérique allouable à tous les utilisateurs.	Exemple 17–1
Protection des imprimantes et mémoires graphiques.	Garantit que les périphériques non allouables ne sont pas allouables.	"Procédure de protection des périphériques non allouables dans Trusted Extensions" à la page 260
Configuration de périphériques de connexion série.	Permet de se connecter par port série.	"Procédure de configuration d'une ligne série pour les connexions" à la page 261
Activation d'un programme de lecteur de CD à utiliser.	Permet l'ouverture automatique d'un programme de lecture audio lorsqu'un CD audio est inséré.	"Procédure de configuration d'un programme de lecture audio pour permettre son utilisation dans Trusted CDE" à la page 262
Désactivation de l'affichage du gestionnaire de fichiers.	Permet d'empêcher l'affichage du gestionnaire de fichiers (File Manager) après l'allocation d'un périphérique.	"Procédure de désactivation de l'affichage du gestionnaire de fichiers après l'allocation d'un périphérique" à la page 263
Utilisation d'un nouveau script de nettoyage de périphérique.	Permet de placer un nouveau script aux endroits appropriés.	"Procédure d'ajout d'un script Device_Clean dans Trusted Extensions" à la page 263

▼ Procédure de configuration d'un périphérique dans Trusted Extensions

Par défaut, un périphérique allouable dispose d'une plage d'étiquettes allant de `ADMIN_LOW` à `ADMIN_HIGH` et doit être alloué pour pouvoir être utilisé. Des utilisateurs doivent également être autorisés à allouer le périphérique. Ces valeurs par défaut peuvent être modifiées.

Les périphériques suivants peuvent être alloués pour permettre leur utilisation :

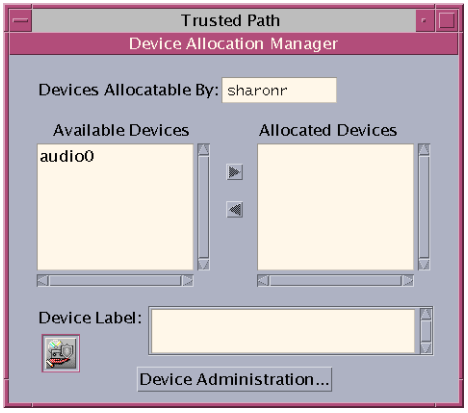
- `audio`*n* : représente un microphone et un haut-parleur ;
- `cdrom`*n* : représente une unité de CD-ROM ;
- `floppy`*n* : représente une unité de disquette ;

- `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 support USB enfichable à chaud.

Avant de commencer Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

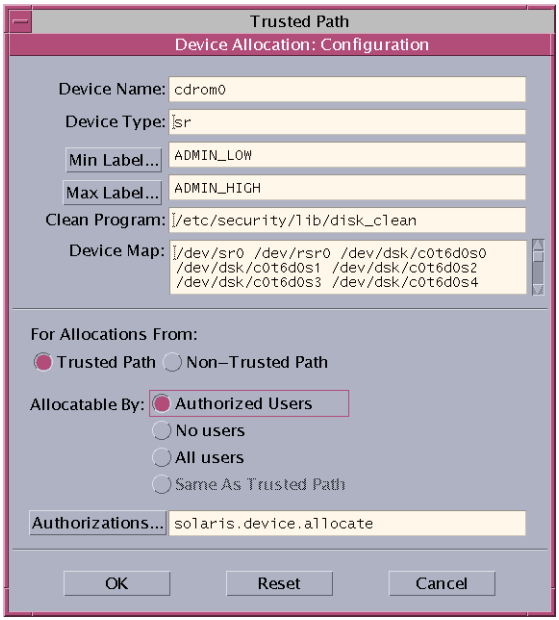
1 Dans le menu Trusted Path (Chemin de confiance), sélectionnez Allocate Device (Allouer un périphérique).

Le gestionnaire d'allocation de périphériques (Device Allocation Manager) s'affiche.



2 Affichez les paramètres de sécurité par défaut.

Cliquez sur Device Administration (Gestion des périphériques), puis mettez en surbrillance le périphérique. La figure ci-dessous montre une unité de CD-ROM avec les paramètres de sécurité par défaut.



3 (Facultatif) Limitez la plage d'étiquettes sur le périphérique.

a. Définissez l'étiquette minimale.

Cliquez sur le bouton Min Label... (Étiquette min). Choisissez une étiquette minimale dans le générateur d'étiquettes. Pour plus d'informations sur le générateur d'étiquettes, reportez-vous à la section “Générateur d'étiquettes dans Trusted Extensions” à la page 45.

b. Définissez l'étiquette maximale.

Cliquez sur le bouton Max Label... (Étiquette max). Choisissez une étiquette maximale dans le générateur d'étiquettes.

4 Indiquez si le périphérique peut être alloué localement.

Dans la boîte de dialogue de configuration de l'allocation des périphériques, sous Allocations From Trusted Path (Allocations du chemin de confiance), sélectionnez une option dans la liste

Allocatable By (Allouable par). Par défaut, l'option Authorized Users (Utilisateurs autorisés) est cochée. Par conséquent, le périphérique est allouable et les utilisateurs doivent être autorisés.

- **Pour rendre le périphérique non allouable, cliquez sur No Users (Aucun utilisateur).**

  Lors de la configuration d'une imprimante, d'une mémoire graphique ou d'un autre périphérique qui ne doit pas être allouable, sélectionnez No Users.

- **Pour rendre le périphérique allouable sans exiger d'autorisation, cliquez sur All Users (Tous les utilisateurs).**

5 **Indiquez si le périphérique peut être alloué à distance.**

Dans la section For Allocations From Non-Trusted Path (Pour des allocations à partir d'un chemin qui n'est pas de confiance), sélectionnez une option dans la liste Allocatable by. Par défaut, l'option Same As Trusted Path (Identique au chemin de confiance) est cochée.

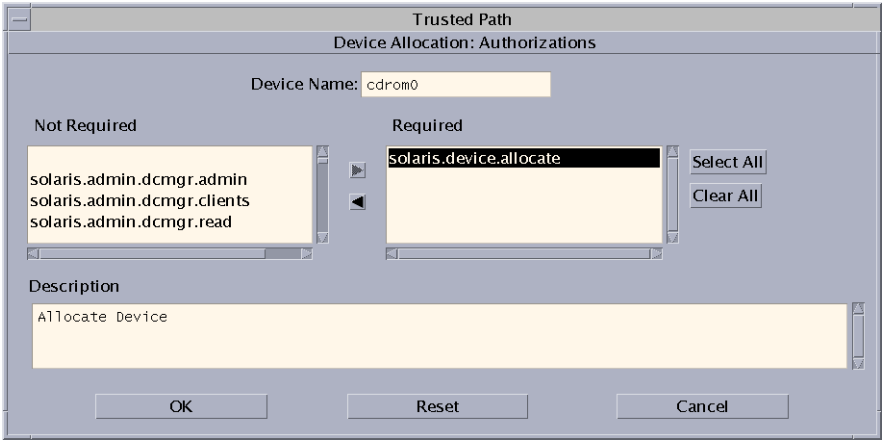
- **Pour exiger que les utilisateurs soient autorisés, sélectionnez l'option Allocatable by Authorized Users (Attribuable par des utilisateurs autorisés).**

- **Pour rendre le périphérique non allouable par des utilisateurs distants, sélectionnez No Users.**

- **Pour rendre le périphérique allouable par n'importe quel utilisateur, sélectionnez Tous les utilisateurs.**

6 **Si le périphérique est allouable *et* que votre site a créé de nouvelles autorisations de périphériques, sélectionnez l'autorisation appropriée.**

La boîte de dialogue ci-dessous montre que l'autorisation `solaris.device.allocate` est requise pour allouer le périphérique `cdrom0`.



Pour créer et utiliser des autorisations de périphériques spécifiques au site, reportez-vous à la section "Personnalisation des autorisations de périphériques dans Trusted Extensions (liste des tâches)" à la page 264.

7 **Cliquez sur OK pour enregistrer vos modifications.**

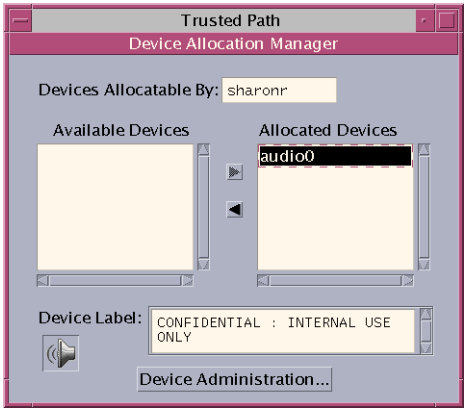
▼ Procédure de révocation ou de récupération d'un périphérique dans Trusted Extensions

Si un périphérique n'est pas répertorié dans le gestionnaire d'allocation de périphériques, il est peut-être déjà alloué ou dans un état d'erreur d'allocation. L'administrateur système peut récupérer le périphérique pour l'utiliser.

Avant de commencer Vous devez être dans le rôle d'administrateur système dans la zone globale. Ce rôle inclut l'autorisation `solaris.device.revoke`.

1 **Dans le menu Trusted Path (Chemin de confiance), sélectionnez Allocate Device (Allouer un périphérique).**

Dans la figure ci-dessous, le périphérique audio est déjà alloué à un utilisateur.



2 **Cliquez sur le bouton Device Administration (Gestion des périphériques).**

3 **Vérifiez l'état d'un périphérique.**

Sélectionnez le nom du périphérique et vérifiez le champ State (État).

- **Si le champ State affiche Allocate Error State (État d'erreur d'allocation), cliquez sur le bouton Reclaim (Récupérer).**

- **Si le champ State affiche Allocated (Alloué), effectuez l'une des opérations suivantes :**
  - **Demandez à l'utilisateur dans le champ Owner (Propriétaire) de libérer le périphérique.**
  - **Forcez la libération du périphérique en cliquant sur le bouton Revoke (Révoquer).**

4. **Fermez le gestionnaire d'allocation de périphériques.**

▼ Procédure de protection des périphériques non allouables dans Trusted Extensions

L'option No Users (Aucun utilisateur) dans la section Allocatable By (Attribuable par) de la boîte de dialogue Device Configuration (Configuration des périphériques) est utilisée le plus souvent pour la mémoire graphique et l'imprimante, qui ne doivent pas nécessairement être allouées pour pouvoir être utilisées.

Avant de commencer Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

1. **Dans le menu Trusted Path (Chemin de confiance), sélectionnez Allocate Device (Allouer un périphérique).**
2. **Dans le gestionnaire d'allocation de périphériques, cliquez sur le bouton Device Administration (Gestion des périphériques).**
3. **Sélectionnez la nouvelle imprimante ou la nouvelle mémoire graphique.**
   a. **Pour rendre le périphérique non allouable, cliquez sur No Users.**
   b. **(Facultatif) Limitez la plage d'étiquettes sur le périphérique.**
      i. **Définissez l'étiquette minimale.**

         Cliquez sur le bouton Min Label... (Étiquette min). Choisissez une étiquette minimale dans le générateur d'étiquettes. Pour plus d'informations sur le générateur d'étiquettes, reportez-vous à la section "Générateur d'étiquettes dans Trusted Extensions" à la page 45.

      ii. **Définissez l'étiquette maximale.**

         Cliquez sur le bouton Max Label... (Étiquette max). Choisissez une étiquette maximale dans le générateur d'étiquettes.

Exemple 17–1 Interdiction de l'allocation distante d'un périphérique audio

L'option No Users (Aucun utilisateur) de la section Allocatable By (Allouable par) empêche les utilisateurs distants d'entendre les conversations autour d'un système distant.

L'administrateur de sécurité configure le périphérique audio dans le gestionnaire d'allocation de périphériques comme suit :

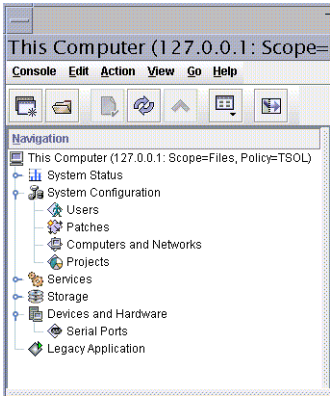
```
Device Name: audio
For Allocations From: Trusted Path
Allocatable By: Authorized Users
Authorizations: solaris.device.allocate

Device Name: audio
For Allocations From: Non-Trusted Pathh
Allocatable By: No Users
```

▼ Procédure de configuration d'une ligne série pour les connexions

Avant de commencer Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

1 **Ouvrez la Console de gestion Solaris dans l'étendue Fichiers.**

FIGURE 17–1 Outil Serial Ports dans la Console de gestion Solaris



2 **Sous Devices and Hardware, accédez à Serial Ports (Ports série).**

Saisissez un mot de passe lorsque vous y êtes invité. Suivez les procédures indiquées dans l'aide en ligne pour configurer le port série.

3 **Pour modifier la plage d'étiquettes par défaut, ouvrez le gestionnaire d'allocation de périphériques.**

La plage d'étiquettes par défaut va de `ADMIN_LOW` à `ADMIN_HIGH`.

Exemple 17–2 Restriction de la plage d'étiquettes d'un port série

Après la création d'un périphérique de connexion série, l'administrateur de sécurité limite la plage d'étiquettes du port série à une seule étiquette, `Public`. L'administrateur définit les valeurs suivantes dans les boîtes de dialogue Device Administration (Gestion des périphériques).

```
Device Name: /dev/term/[a|b]
Device Type: tty
Clean Program: /bin/true
Device Map: /dev/term/[a|b]
Minimum Label: Public
Maximum Label: Public
Allocatable By: No Users
```

▼ Procédure de configuration d'un programme de lecture audio pour permettre son utilisation dans Trusted CDE

La procédure suivante permet à un lecteur audio de s'ouvrir automatiquement dans l'espace de travail d'un Trusted CDE lorsqu'un utilisateur insère un CD de musique. Pour la procédure de l'utilisateur, reportez-vous à l'exemple de la section "Procédure d'allocation d'un périphérique dans Trusted Extensions" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

Remarque – Dans un espace de travail Trusted JDS, les utilisateurs spécifient le comportement des supports amovibles de la même manière qu'ils le spécifieraient dans un espace de travail non de confiance.

Avant de commencer Vous devez être dans le rôle d'administrateur système dans la zone globale.

1 **Modifiez le fichier `/etc/rmmount.conf`.**

Utilisez l'éditeur de confiance. Pour plus d'informations, reportez-vous à la section "Modification des fichiers d'administration dans Trusted Extensions" à la page 59.

2 **Ajoutez le programme de lecture de CD de votre site à l'action `cdrom` dans le fichier.**

`action` *media* `action_`*program*`.so` *path-to-program*

Exemple 17–3 Configuration de l'utilisation d'un programme de lecture audio

Dans l'exemple suivant, l'administrateur système rend le programme `workman` disponible pour tous les utilisateurs d'un système. Le programme `workman` est un programme de lecture audio.

```
# /etc/rmmount.conf file
action cdrom action_workman.so /usr/local/bin/workman
```

▼ Procédure de désactivation de l'affichage du gestionnaire de fichiers après l'allocation d'un périphérique

Par défaut, le gestionnaire de fichiers s'affiche lorsqu'un périphérique est monté. Si vous ne montez pas de périphériques comportant des systèmes de fichiers, vous souhaitez peut-être ne pas voir s'afficher le gestionnaire de fichiers.

Avant de commencer Vous devez être dans le rôle d'administrateur système dans la zone globale.

1. **Modifiez le fichier `/etc/rmmount.conf`.**

   Utilisez l'éditeur de confiance. Pour plus d'informations, reportez-vous à la section "Modification des fichiers d'administration dans Trusted Extensions" à la page 59.

2. **Recherchez les actions `filemgr` suivantes :**

   ```
   action cdrom action_filemgr.so
   action floppy action_filemgr.so
   ```

3. **Mettez en commentaire l'action appropriée.**

   L'exemple suivant présente les actions `action_filemgr.so` mises en commentaire pour les périphériques `cdrom` et `diskette`.

   ```
   # action cdrom action_filemgr.so
   # action floppy action_filemgr.so
   ```

   Lorsqu'une unité de CD-ROM ou de disquette est allouée, le gestionnaire de fichiers ne s'affiche pas.

▼ Procédure d'ajout d'un script Device_Clean dans Trusted Extensions

Si aucun script `device_clean` n'est spécifié lors de la création d'un périphérique, le script par défaut `/bin/true` est utilisé.

Avant de commencer

Ayez à votre disposition un script qui purge toutes les données utilisables à partir du périphérique physique et qui renvoie `0` pour indiquer la réussite. Sur les périphériques avec des supports amovibles, le script tente d'éjecter le support si l'utilisateur ne le fait pas. Le script place le périphérique dans l'état d'erreur d'allocation si le support n'est pas éjecté. Pour plus d'informations sur les conditions requises, reportez-vous à la page de manuel `device_clean(5)`.

Vous devez être dans le rôle d'administrateur système dans la zone globale.

1. **Copiez le script dans le répertoire `/etc/security/lib`.**
2. **Dans la boîte de dialogue de gestion des périphériques, spécifiez le chemin d'accès complet du script.**
   a. **Ouvrez le gestionnaire d'allocation de périphériques.**
   b. **Cliquez sur le bouton Device Administration (Gestion des périphériques).**
   c. **Sélectionnez le nom du périphérique, puis cliquez sur le bouton Configure (Configurer).**
   d. **Dans le champ Clean Program (Programme de nettoyage), saisissez le chemin d'accès complet du script.**
3. **Enregistrez vos modifications.**

Personnalisation des autorisations de périphériques dans Trusted Extensions (liste des tâches)

La liste des tâches ci-dessous décrit des procédures permettant de modifier les autorisations de périphériques sur votre site.

Tâche	Description	Voir
Création d'autorisations de périphériques.	Permet de créer des autorisations spécifiques au site.	"Procédure de création d'autorisations de périphériques" à la page 265
Ajout d'autorisations à un périphérique.	Permet d'ajouter des autorisations spécifiques au site à des périphériques sélectionnés.	"Procédure d'ajout d'autorisations spécifiques à un site à un périphérique dans Trusted Extensions" à la page 268
Octroi d'autorisations de périphériques aux utilisateurs et aux rôles.	Permet aux utilisateurs et aux rôles d'utiliser les nouvelles autorisations.	"Procédure d'assignation d'autorisations de périphériques" à la page 268

▼ Procédure de création d'autorisations de périphériques

Si aucune autorisation n'est spécifiée lors de la création d'un périphérique, tous les utilisateurs peuvent, par défaut, utiliser le périphérique. Si une autorisation est spécifiée, seuls les utilisateurs autorisés peuvent, par défaut, utiliser le périphérique.

Pour empêcher tout accès à un périphérique allouable sans l'utilisation d'autorisations, reportez-vous à l'Exemple 17–1.

Avant de commencer Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

1 **Modifiez le fichier `auth_attr`.**

Utilisez l'éditeur de confiance. Pour plus d'informations, reportez-vous à la section "Modification des fichiers d'administration dans Trusted Extensions" à la page 59.

2 **Créez un en-tête pour les nouvelles autorisations.**

Utilisez le nom de domaine Internet de votre organisation en ordre inverse suivi de composants quelconques facultatifs, tels que le nom de votre société. Séparez les composants par des points. Ajoutez un point après les noms d'en-tête.

domain-suffix`.`*domain-prefix*`.`*optional*`.:::`*Company* `Header::help=`*Company*`.html`

3 **Ajoutez les entrées des nouvelles autorisations.**

Ajoutez les autorisations (une autorisation par ligne). Les lignes sont fractionnées pour permettre leur affichage. Les autorisations comprennent des autorisations `grant` qui permettent aux administrateurs d'affecter les nouvelles autorisations.

```
domain-suffix.domain-prefix.grant:::Grant All Company Authorizations::
help=CompanyGrant.html
domain-suffix.domain-prefix.grant.device:::Grant Company Device Authorizations::
help=CompanyGrantDevice.html
domain-suffix.domain-prefix.device.allocate.tape:::Allocate Tape Device::
help=CompanyTapeAllocate.html
domain-suffix.domain-prefix.device.allocate.floppy:::Allocate Floppy Device::
help=CompanyFloppyAllocate.html
```

4 **Enregistrez le fichier et fermez l'éditeur.**

5 **Si vous utilisez le protocole LDAP comme service de nommage, mettez à jour les entrées `auth_attr` sur l'Oracle Directory Server Enterprise Edition (serveur LDAP).**

Pour plus d'informations, reportez-vous à la page de manuel `ldapaddent(1M)`.

6 **Ajoutez les nouvelles autorisations aux profils de droits appropriés. Affectez ensuite les profils aux utilisateurs et aux rôles.**

Utilisez la Console de gestion Solaris. Assumez le rôle d'administrateur de sécurité, puis suivez la procédure d'Oracle Solaris "How to Create or Change a Rights Profile" du *System Administration Guide: Security Services*.

7 **Utilisez l'autorisation pour limiter l'accès aux lecteurs de bande et aux unités de disquette.**

Ajoutez les nouvelles autorisations à la liste des autorisations nécessaires dans le gestionnaire d'allocation de périphériques. Pour plus d'informations sur cette procédure, reportez-vous à la section "Procédure d'ajout d'autorisations spécifiques à un site à un périphérique dans Trusted Extensions" à la page 268.

Exemple 17–4 Création d'autorisations de périphériques détaillées

Un administrateur de sécurité de NewCo a besoin de construire des autorisations de périphériques détaillées pour la société.

Tout d'abord, l'administrateur crée les fichiers d'aide suivants et les place dans le répertoire `/usr/lib/help/auths/locale/C` :

```
Newco.html
NewcoGrant.html
NewcoGrantDevice.html
NewcoTapeAllocate.html
NewcoFloppyAllocate.html
```

L'administrateur ajoute ensuite un en-tête pour toutes les autorisations de `newco.com` dans le fichier `auth_attr`.

```
# auth_attr file
com.newco.:::NewCo Header::help=Newco.html
```

Puis l'administrateur ajoute les entrées des autorisations au fichier :

```
com.newco.grant:::Grant All NewCo Authorizations::
help=NewcoGrant.html
com.newco.grant.device:::Grant NewCo Device Authorizations::
help=NewcoGrantDevice.html
com.newco.device.allocate.tape:::Allocate Tape Device::
help=NewcoTapeAllocate.html
com.newco.device.allocate.floppy:::Allocate Floppy Device::
help=NewcoFloppyAllocate.html
```

Les lignes sont fractionnées pour permettre leur affichage.

Les entrées dans `auth_attr` créent les autorisations suivantes :

- une autorisation d'accorder toutes les autorisations de NewCo ;
- une autorisation d'accorder les autorisations de périphériques de NewCo ;

- une autorisation d'allouer un lecteur de bande ;
- une autorisation d'allouer une unité de disquette.

Exemple 17–5 Création d'autorisations de chemin de confiance et de chemin non de confiance

Par défaut, l'autorisation Allocate Devices (Allouer des périphériques) permet l'allocation de tous les périphériques depuis le chemin de confiance et depuis d'autres emplacements que le chemin de confiance.

Dans l'exemple suivant, la stratégie de sécurité du site exige la limitation de l'allocation de CD-ROM distant. L'administrateur de sécurité crée l'autorisation `com.someco.device.cdrom.local`. Cette autorisation concerne les unités de CD-ROM qui sont allouées via le chemin de confiance. L'autorisation `com.someco.device.cdrom.remote` est destinée aux rares utilisateurs autorisés à allouer des unités de CD-ROM depuis un emplacement autre que le chemin de confiance.

L'administrateur de sécurité crée les fichiers d'aide, ajoute les autorisations à la base de données `auth_attr`, ajoute les autorisations aux périphériques, puis place les autorisations dans des profils de droits. Les profils sont affectés aux utilisateurs autorisés à allouer des périphériques.

- Entrées de la base de données `auth_attr` :

```
com.someco.:::SomeCo Header::help=Someco.html
com.someco.grant:::Grant All SomeCo Authorizations::
help=SomecoGrant.html
com.someco.grant.device:::Grant SomeCo Device Authorizations::
help=SomecoGrantDevice.html
com.someco.device.cdrom.local:::Allocate Local CD-ROM Device::
help=SomecoCDAllocateLocal.html
com.someco.device.cdrom.remote:::Allocate Remote CD-ROM Device::
help=SomecoCDAllocateRemote.html
```

- L'assignation du gestionnaire d'allocation de périphériques est présentée ci-dessous :

  Le chemin de confiance permet aux utilisateurs autorisés d'utiliser le gestionnaire d'allocation de périphériques pour allouer l'unité de CD-ROM locale.

```
Device Name: cdrom_0
For Allocations From: Trusted Path
Allocatable By: Authorized Users
Authorizations: com.someco.device.cdrom.local
```

  Le chemin non de confiance permet aux utilisateurs d'allouer un périphérique à distance à l'aide de la commande `allocate`.

```
Device Name: cdrom_0
For Allocations From: Non-Trusted Path
Allocatable By: Authorized Users
Authorizations: com.someco.device.cdrom.remote
```

- Entrées du profil de droits :

```
# Local Allocator profile
com.someco.device.cdrom.local
```

```
# Remote Allocator profile
com.someco.device.cdrom.remote
```

- Profils de droits des utilisateurs autorisés :

```
# List of profiles for regular authorized user
Local Allocator Profile
...

# List of profiles for role or authorized user
Remote Allocator Profile
...
```

▼ Procédure d'ajout d'autorisations spécifiques à un site à un périphérique dans Trusted Extensions

Avant de commencer Vous devez être dans le rôle d'administrateur de sécurité ou dans un rôle qui inclut l'autorisation Configure Device Attributes (Configurer les attributs des périphériques). Vous devez avoir créé des autorisations spécifiques à un site, comme décrit à la section "Procédure de création d'autorisations de périphériques" à la page 265.

1. **Suivez la procédure "Procédure de configuration d'un périphérique dans Trusted Extensions" à la page 255.**

   a. **Sélectionnez le périphérique que vous souhaitez protéger au moyen des nouvelles autorisations.**

   b. **Ouvrez la boîte de dialogue de gestion des périphériques.**

   c. **Dans la boîte de dialogue de configuration des périphériques, cliquez sur le bouton Authorizations (Autorisations).**

      Les nouvelles autorisations s'affichent dans la liste Not Required (Non requis).

   d. **Ajoutez les nouvelles autorisations à la liste des autorisations requises.**

2. **Cliquez sur OK pour enregistrer vos modifications.**

▼ Procédure d'assignation d'autorisations de périphériques

L'autorisation Allocate Device (Allouer un périphérique) permet aux utilisateurs d'allouer un périphérique. Les autorisations Allocate Device et Revoke or Reclaim Device (Révoquer ou récupérer un périphérique) sont appropriées pour les rôles d'administration.

Avant de commencer

Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

Si les profils existants ne sont pas appropriés, l'administrateur de sécurité peut créer un nouveau profil. Pour obtenir un exemple, reportez-vous à la section "Procédure de création d'un profil de droits pour des autorisations commodes" à la page 99.

- **Assignez à l'utilisateur un profil de droits qui contient l'autorisation Allocate Device.**

  Pour obtenir de l'aide, reportez-vous à l'aide en ligne. Pour la procédure étape par étape, reportez-vous à la section "How to Change the RBAC Properties of a User" du *System Administration Guide: Security Services*.

  Les profils de droits suivants permettent à un rôle d'allouer des périphériques :

  - All Authorizations (Toutes les autorisations) ;
  - Device Management (Gestion des périphériques) ;
  - Media Backup (Sauvegarde des supports) ;
  - Media Restore (Restauration des supports) ;
  - Object Label Management (Gestion de l'étiquette des objets) ;
  - Software Installation (Installation de logiciels).

  Les profils de droits suivants permettent à un rôle de révoquer ou récupérer des périphériques :

  - All Authorizations (Toutes les autorisations) ;
  - Device Management (Gestion des périphériques) ;

  Les profils de droits suivants permettent à un rôle de créer ou de configurer des périphériques :

  - All Authorizations (Toutes les autorisations) ;
  - Device Security (Sécurité des périphériques).

Exemple 17–6 Affectation de nouvelles autorisations de périphériques

Dans cet exemple, l'administrateur de sécurité configure les nouvelles autorisations de périphériques pour le système et affecte le profil de droits incluant les nouvelles autorisations à des utilisateurs dignes de confiance. L'administrateur de sécurité effectue les opérations suivantes :

1. Il crée de nouvelles autorisations de périphériques, comme décrit à la section "Procédure de création d'autorisations de périphériques" à la page 265.
2. Dans le gestionnaire d'allocation de périphériques, il ajoute les nouvelles autorisations de périphériques aux lecteurs de bande et aux unités de disquette.
3. Il place les nouvelles autorisations dans le profil de droits NewCo Allocation.
4. Il ajoute le profil de droits NewCo Allocation aux profils des utilisateurs et des rôles qui sont autorisés à allouer des lecteurs de bande et des unités de disquette.

Les utilisateurs et les rôles autorisés peuvent maintenant utiliser les lecteurs de bande et les unités de disquette sur ce système.

◆ ◆ ◆ CHAPITRE 18

Audit de Trusted Extensions (présentation)

Ce chapitre décrit les ajouts à l'audit fournis par Trusted Extensions.

Trusted Extensions et audit

Sur un système configuré avec le logiciel Trusted Extensions, la configuration et la gestion de l'audit sont semblables à celles effectuées sur un système Oracle Solaris. Voici cependant quelques différences.

- Le logiciel Trusted Extensions ajoute des classes d'audit, des événements d'audit, des jetons d'audit et des options de stratégie d'audit au système.
- Par défaut, l'audit est activé dans le logiciel Trusted Extensions.
- L'audit par zone d'Oracle Solaris n'est pas pris en charge. Dans Trusted Extensions, toutes les zones font l'objet d'un audit identique.
- Trusted Extensions fournit des outils d'administration permettant de gérer les caractéristiques d'audit des utilisateurs et de modifier les fichiers d'audit.
- Deux rôles, celui de l'administrateur système et celui de l'administrateur de sécurité, sont utilisés pour configurer et gérer l'audit dans Trusted Extensions.

  L'administrateur de sécurité prévoit ce qui doit être audité et tous les mappages d'événement à classe spécifiques à un site. Comme dans le SE Oracle Solaris, l'administrateur système prévoit l'espace disque requis pour les fichiers d'audit, crée un serveur d'administration de l'audit et installe les fichiers de configuration de l'audit.

Gestion de l'audit par rôle dans Trusted Extensions

L'audit dans Trusted Extensions nécessite la même planification que dans le SE Oracle Solaris. Pour plus d'informations sur la planification, reportez-vous au Chapitre 29, "Planning for Oracle Solaris Auditing" du *System Administration Guide: Security Services*.

Configuration des rôles pour l'administration de l'audit

Dans Trusted Extensions, l'audit relève de la responsabilité de deux rôles. Le rôle d'administrateur système définit les disques et le réseau de stockage de l'audit. Le rôle d'administrateur de sécurité détermine ce qui doit être audité et spécifie les informations dans les fichiers de configuration de l'audit. Comme dans le SE Oracle Solaris, vous pouvez créer les rôles dans le logiciel. Les profils de droits pour ces deux rôles sont fournis. L'équipe de configuration initiale a créé le rôle d'administrateur de sécurité lors de la configuration initiale. Pour plus d'informations, reportez-vous à la section "Création du rôle d'administrateur de sécurité dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.

Remarque – Un système enregistre uniquement les événements concernant la sécurité spécifiés par les fichiers de configuration de l'audit ; ces événements sont donc présélectionnés. Par conséquent, une vérification ultérieure de l'audit ne peut prendre en compte que les événements qui ont été enregistrés. En cas d'erreur de configuration, des tentatives de violation de la sécurité du système risquent de ne pas être détectées ou l'administrateur risque de ne pas être en mesure d'identifier l'utilisateur responsable d'une tentative de violation de la sécurité. Les administrateurs doivent régulièrement analyser les pistes d'audit pour rechercher les failles de sécurité.

Tâches d'audit dans Trusted Extensions

Les procédures de configuration et de gestion de l'audit dans Trusted Extensions diffèrent légèrement des procédures dans Oracle Solaris.

- La configuration de l'audit est effectuée dans la zone globale par l'un des deux rôles d'administration. Ensuite, l'administrateur système copie des fichiers d'audit personnalisés spécifiques à partir de la zone globale vers chaque zone étiquetée. Avec cette procédure, les actions de l'utilisateur sont auditées de la même manière dans la zone globale et dans les zones étiquetées.

  Pour plus d'informations, reportez-vous aux sections "Tâches d'audit de l'administrateur de sécurité" à la page 273 et "Tâches d'audit de l'administrateur système" à la page 273

- Les administrateurs Trusted Extensions utilisent un éditeur de confiance pour modifier les fichiers de configuration de l'audit. Dans Trusted CDE, les administrateurs Trusted Extensions utilisent des actions CDE pour appeler l'éditeur de confiance. Pour obtenir la liste des actions, reportez-vous à la section "Actions Trusted CDE" à la page 37.
- Les administrateurs Trusted Extensions utilisent la Console de gestion Solaris pour configurer des utilisateurs spécifiques. Des caractéristiques d'audit spécifiques aux utilisateurs peuvent être spécifiées dans cet outil. La spécification de caractéristiques propres à un utilisateur n'est nécessaire que lorsque les caractéristiques d'audit de l'utilisateur diffèrent des caractéristiques d'audit des systèmes sur lesquels il travaille. Pour une introduction à l'outil, reportez-vous à la section "Outils de la Console de gestion Solaris" à la page 40.

Tâches d'audit de l'administrateur de sécurité

Les tâches suivantes sont liées à la sécurité et relèvent donc de la responsabilité de l'administrateur de sécurité. Suivez les instructions d'Oracle Solaris, mais utilisez les outils d'administration de Trusted Extensions.

Tâche	Pour obtenir les instructions Oracle Solaris	Instructions Trusted Extensions
Configuration des fichiers d'audit.	Reportez-vous à la section "Configuring Audit Files (Task Map)" du *System Administration Guide: Security Services*	Utilisez l'éditeur de confiance. Pour plus d'informations, reportez-vous à la section "Modification des fichiers d'administration dans Trusted Extensions" à la page 59.
(Facultatif) Modification de la stratégie d'audit par défaut.	Reportez-vous à la section "How to Configure Audit Policy" du *System Administration Guide: Security Services*	Utilisez l'éditeur de confiance.
Désactivation et réactivation de l'audit.	Reportez-vous à la section "How to Disable the Audit Service" du *System Administration Guide: Security Services*	L'audit est activé par défaut.
Gestion de l'audit.	Reportez-vous à la section "Oracle Solaris Auditing (Task Map)" du *System Administration Guide: Security Services*	Utilisez l'éditeur de confiance. Ignorez les tâches d'audit par zone.

Tâches d'audit de l'administrateur système

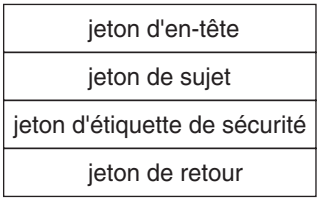
Les tâches suivantes relèvent de la responsabilité de l'administrateur système. Suivez les instructions d'Oracle Solaris, mais utilisez les outils d'administration de Trusted Extensions.

Tâche	Pour obtenir les instructions Oracle Solaris	Instructions de Trusted Extensions
Création d'un système de fichiers ZFS dédié aux fichiers d'audit. Création d'un alias `audit_warn`.	Reportez-vous à la section "Managing Audit Records" du *System Administration Guide: Security Services* Reportez-vous à la section "How to Configure the audit_warn Email Alias" du *System Administration Guide: Security Services*	Effectuez toutes les tâches d'administration dans la zone globale. Utilisez l'éditeur de confiance.
Copie ou montage en loopback des fichiers d'audit personnalisés dans les zones étiquetées.	Reportez-vous à la section "Configuring the Audit Service in Zones (Tasks)" du *System Administration Guide: Security Services*	Montez en loopback ou copiez les fichiers dans chaque zone étiquetée après la création des zones. Copiez les fichiers dans la première zone étiquetée, puis copiez la zone.
(Facultatif) Distribution des fichiers de configuration de l'audit.	Aucune d'instruction	Reportez-vous à la section "Copie de fichiers dans Trusted Extensions à partir d'un support amovible" du *Guide de configuration d'Oracle Solaris Trusted Extensions*
Gestion de l'audit.	Reportez-vous à la section "Oracle Solaris Auditing (Task Map)" du *System Administration Guide: Security Services*	Ignorez les tâches d'audit par zone.
Sélection d'enregistrements d'audit par étiquette.	Reportez-vous à la section "How to Select Audit Events From the Audit Trail" du *System Administration Guide: Security Services*	Pour sélectionner des enregistrements par étiquette, utilisez la commande `auditreduce` avec l'option `-l`.

Référence de l'audit Trusted Extensions

Le logiciel Trusted Extensions ajoute des classes d'audit, des événements d'audit, des jetons d'audit et des options de stratégie d'audit au SE Oracle Solaris. Plusieurs commandes d'audit sont étendues pour permettre la prise en charge des étiquettes. Les enregistrements d'audit de Trusted Extensions incluent une étiquette, comme indiqué à la figure suivante.

FIGURE 18–1 Enregistrement d'audit standard sur un système étiqueté



Classes d'audit de Trusted Extensions

Les classes d'audit que le logiciel Trusted Extensions ajoute au SE Oracle Solaris sont répertoriées par ordre alphabétique dans le tableau ci-dessous. Les classes sont répertoriées dans le fichier `/etc/security/audit_class`. Pour plus d'informations sur ces classes d'audit, reportez-vous à la page de manuel `audit_class(4)`.

TABLEAU 18–1 Classes d'audit du serveur X

Nom court	Nom long	Masque d'audit
xc	X - Création/destruction d'objet	0x00800000
xp	X - Opérations privilégiées/administratives	0x00400000
xs	X - Opérations qui échouent toujours en mode silencieux si elles sont incorrectes	0x01000000
xx	X - Tous les événements X dans les classes xc, xp et xs (métaclasse)	0x01c00000

Les événements d'audit du serveur X sont mappés à ces classes selon les critères suivants :

- **xc :** cette classe effectue un contrôle portant sur la création et la destruction d'objets du serveur. Par exemple, cette classe effectue un contrôle de la fonction `CreateWindow()`.
- **xp :** cette classe effectue un contrôle sur l'utilisation des privilèges. L'utilisation des privilèges peut avoir réussi ou échoué. Par exemple, `ChangeWindowAttributes()` fait l'objet d'un audit lorsqu'un client tente de modifier les attributs d'une fenêtre d'un autre client. Cette classe comprend également des routines d'administration telles que la fonction `SetAccessControl()`.
- **xs :** cette classe effectue un contrôle sur les routines qui ne renvoient pas de messages d'erreur X aux clients à la suite d'un échec lorsque cet échec est dû à des attributs de sécurité. Par exemple, la fonction `GetImage()` ne renvoie pas d'erreur `BadWindow` si elle n'est pas en mesure de lire à partir d'une fenêtre en raison de l'absence de privilèges.

Ces événements doivent être sélectionnés pour le contrôle uniquement en cas de réussite. Lorsque des événements xs sont sélectionnés pour le contrôle alors qu'ils échouent, la piste d'audit se remplit d'enregistrements non pertinents.

- **xx :** cette classe comprend toutes les classes d'audit X.

Événements d'audit de Trusted Extensions

Le logiciel Trusted Extensions ajoute des événements d'audit au système. Les nouveaux événements d'audit et les nouvelles classes d'audit auxquelles les événements appartiennent sont répertoriés dans le fichier `/etc/security/audit_event`. Les numéros des événements d'audit de Trusted Extensions sont compris entre 9000 et 10000. Pour plus d'informations sur les événements d'audit, reportez-vous à la page de manuel `audit_event(4)`.

Jetons d'audit de Trusted Extensions

Les jetons d'audit que le logiciel Trusted Extensions ajoute au SE Oracle Solaris sont répertoriés par ordre alphabétique dans le tableau ci-dessous. Les jetons sont également répertoriés sur la page de manuel `audit.log(4)`.

TABLEAU 18–2 Jetons d'audit de Trusted Extensions

Nom du jeton	Description
"Jeton `label`" à la page 277	Étiquette de sensibilité
"Jeton `xatom`" à la page 277	Identification de l'atome de la fenêtre X
"Jeton `xclient`" à la page 278	Identification du client X
"Jeton `xcolormap`" à la page 278	Informations sur la couleur de la fenêtre X
"Jeton `xcursor`" à la page 278	Informations sur le curseur de la fenêtre X
"Jeton `xfont`" à la page 279	Informations sur les polices de la fenêtre X
"Jeton `xgc`" à la page 279	Informations sur le contexte graphique de la fenêtre X
"Jeton `xpixmap`" à la page 279	Informations de mappage de pixels de la fenêtre X
"Jeton `xproperty`" à la page 280	Informations sur la propriété de la fenêtre X
"Jeton `xselect`" à la page 280	Informations sur les données de la fenêtre X
"Jeton `xwindow`" à la page 281	Informations sur la fenêtre de la fenêtre X

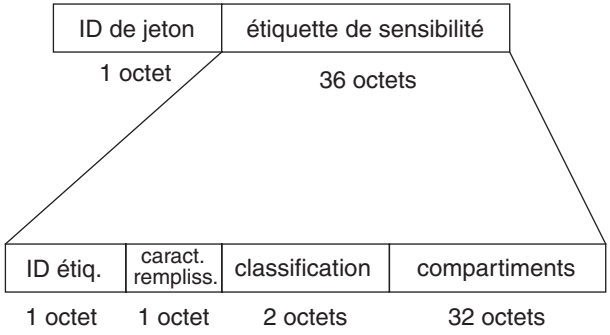
Jeton `label`

Le jeton `label` contient une étiquette de sensibilité. Ce jeton contient les champs suivants :

- un ID de jeton ;
- une étiquette de sensibilité.

La figure suivante montre le format du jeton.

FIGURE 18–2 Format du jeton `label`



La commande `praudit` affiche un jeton `label` comme suit :

```
sensitivity label,ADMIN_LOW
```

Jeton `xatom`

Le jeton `xatom` contient des informations concernant un atome X. Ce jeton contient les champs suivants :

- un ID de jeton ;
- la longueur de la chaîne ;
- Une chaîne de texte qui identifie l'atome.

La commande `praudit` affiche un jeton `xatom` comme suit :

```
X atom,_DT_SAVE_MODE
```

Jeton `xclient`

Le jeton `xclient` contient des informations concernant le client X. Ce jeton contient les champs suivants :

- un ID de jeton ;
- l'ID de client.

La commande `praudit` affiche un jeton `xclient` comme suit :

```
X client,15
```

Jeton `xcolormap`

Le jeton `xcolormap` contient des informations sur les palettes de couleurs. Ce jeton contient les champs suivants :

- un ID de jeton ;
- l'identificateur du serveur X ;
- l'ID utilisateur du créateur.

La figure suivante montre le format du jeton.

FIGURE 18–3 Format des jetons `xcolormap`, `xcursor` , `xfont`, `xgc`, `xpixmap` et `xwindow`

ID de jeton	XID	UID créateur
1 octet	4 octets	4 octets

La commande `praudit` affiche un jeton `xcolormap` comme suit :

```
X color map,0x08c00005,srv
```

Jeton `xcursor`

Le jeton `xcursor` contient des informations sur les curseurs. Ce jeton contient les champs suivants :

- un ID de jeton ;
- l'identificateur du serveur X ;
- l'ID utilisateur du créateur.

La Figure 18–3 montre le format du jeton.

La commande `praudit` affiche un jeton `xcursor` comme suit :

```
X cursor,0x0f400006,srv
```

Jeton `xfont`

Le jeton `xfont` contient des informations sur les polices. Ce jeton contient les champs suivants :

- un ID de jeton ;
- l'identificateur du serveur X ;
- l'ID utilisateur du créateur.

La Figure 18–3 montre le format du jeton.

La commande `praudit` affiche un jeton `xfont` comme suit :

```
X font,0x08c00001,srv
```

Jeton `xgc`

Le jeton `xgc` contient des informations concernant le xgc. Ce jeton contient les champs suivants :

- un ID de jeton ;
- l'identificateur du serveur X ;
- l'ID utilisateur du créateur.

La Figure 18–3 montre le format du jeton.

La commande `praudit` affiche un jeton `xgc` comme suit :

```
Xgraphic context,0x002f2ca0,srv
```

Jeton `xpixmap`

Le jeton `xpixmap` contient des informations sur les mappages de pixels. Ce jeton contient les champs suivants :

- un ID de jeton ;
- l'identificateur du serveur X ;
- l'ID utilisateur du créateur.

La Figure 18–3 montre le format du jeton.

La commande `praudit` affiche un jeton `xpixmap` comme suit :

```
X pixmap,0x08c00005,srv
```

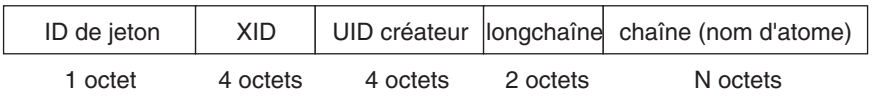
Jeton `xproperty`

Le jeton `xproperty` contient des informations relatives aux diverses propriétés d'une fenêtre. Ce jeton contient les champs suivants :

- un ID de jeton ;
- l'identificateur du serveur X ;
- l'ID utilisateur du créateur ;
- une longueur de chaîne ;
- une chaîne de texte qui identifie l'atome.

La figure suivante montre un format de jeton `xproperty`.

FIGURE 18–4 Format de jeton `xproperty`



La commande `praudit` affiche un jeton `xproperty` comme suit :

```
X property,0x000075d5,root,_MOTIF_DEFAULT_BINDINGS
```

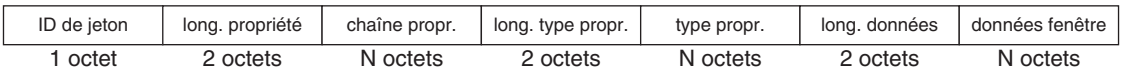
Jeton `xselect`

Le jeton `xselect` contient les données qui sont déplacées entre les fenêtres. Ces données sont un flux d'octets sans structure interne supposée et une chaîne de propriété. Ce jeton contient les champs suivants :

- un ID de jeton ;
- la longueur de la chaîne de propriété ;
- la chaîne de propriété ;
- la longueur du type de propriété ;
- la chaîne du type de propriété ;
- un champ de longueur qui donne le nombre d'octets des données ;
- une chaîne d'octets qui contient les données.

La figure suivante montre le format du jeton.

FIGURE 18–5 Format du jeton `xselect`



La commande `praudit` affiche un jeton `xselect` comme suit :

```
X selection,entryfield,halogen
```

Jeton `xwindow`

Le jeton `xwindow` contient des informations sur une fenêtre. Ce jeton contient les champs suivants :

- un ID de jeton ;
- l'identificateur du serveur X ;
- l'ID utilisateur du créateur.

La Figure 18–3 montre le format du jeton.

La commande `praudit` affiche un jeton `xwindow` comme suit :

```
X window,0x07400001,srv
```

Options de stratégie d'audit de Trusted Extensions

Trusted Extensions ajoute deux options aux options de stratégie d'audit d'Oracle Solaris existantes. Affichez la liste des stratégies pour visualiser les ajouts :

```
$ auditconfig -lspolicy
...
windata_down Include downgraded window information in audit records
windata_up   Include upgraded window information in audit records
...
```

Extensions des commandes d'audit dans Trusted Extensions

Les commandes `auditconfig`, `auditreduce` et `bsmrecord` sont étendues pour gérer les informations de Trusted Extensions :

- La commande `auditconfig` inclut les stratégies d'audit de Trusted Extensions. Pour plus d'informations, reportez-vous à la page de manuel `auditconfig(1M)`.
- La commande `auditreduce` ajoute l'option `-l` pour filtrer des enregistrements en fonction de l'étiquette. Pour plus d'informations, reportez-vous à la page de manuel `auditreduce(1M)`.
- La commande `bsmrecord` inclut les événements d'audit de Trusted Extensions. Pour plus d'informations, reportez-vous à la page de manuel `bsmrecord(1M)`.

◆ ◆ ◆ CHAPITRE 19

Gestion des logiciels dans Trusted Extensions (tâches)

Ce chapitre contient des informations permettant de s'assurer que les logiciels tiers s'exécutent de manière fiable sur un système configuré avec Trusted Extensions.

Ajout de logiciels à Trusted Extensions

Tout logiciel pouvant être ajouté à un système Oracle Solaris peut être ajouté à un système configuré avec Trusted Extensions. En outre, il est possible d'ajouter les programmes utilisant des API Trusted Extensions. L'ajout de logiciels à un système Trusted Extensions est similaire à l'ajout de logiciels à un système Oracle Solaris qui exécute des zones non globales.

Par exemple, des problèmes relatifs à l'empaquetage affectent les systèmes ayant installé des zones non globales. Les paramètres de package définissent les éléments suivants :

- **L'étendue de la zone du package :** détermine le type de zone dans laquelle un package spécifique peut être installé.
- **La visibilité du package :** détermine si un package doit être installé et être identique dans toutes les zones.
- **La limitation du package :** détermine si un package doit uniquement être installé dans la zone actuelle.

Dans Trusted Extensions, les programmes sont généralement installés dans la zone globale pour être utilisés par les utilisateurs standard dans des zones étiquetées. Pour plus d'informations sur les packages des zones, reportez-vous au Chapitre 25, "About Packages and Patches on a Solaris System With Zones Installed (Overview)" du *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*. Reportez-vous également à la page de manuel `pkgadd(1M)`.

Sur un site Trusted Extensions, l'administrateur système et l'administrateur de sécurité travaillent ensemble à l'installation des logiciels. L'administrateur de sécurité vérifie que les logiciels ajoutés respectent la stratégie de sécurité. Lorsqu'un logiciel requiert des privilèges ou des autorisations pour fonctionner, il affecte un profil de droits approprié aux utilisateurs du logiciel.

L'importation d'un logiciel à partir d'un support amovible nécessite une autorisation. Un compte avec l'autorisation Allouer un périphérique peut importer ou exporter des données à partir d'un support amovible. Les données peuvent inclure du code exécutable. Un utilisateur standard ne peut importer que des données sous une étiquette comprise dans son autorisation.

L'administrateur système est chargé d'ajouter les programmes approuvés par l'administrateur de sécurité.

Mécanismes de sécurité d'Oracle Solaris pour les logiciels

Trusted Extensions utilise les mêmes mécanismes de sécurité que le SE Oracle Solaris. Il s'agit notamment des mécanismes suivants :

- **Autorisations :** une autorisation peut être nécessaire pour permettre l'utilisation d'un programme. Pour plus d'informations sur les autorisations, reportez-vous à la section "Oracle Solaris RBAC Elements and Basic Concepts" du *System Administration Guide: Security Services*. Voir aussi les pages de manuel `auth_attr`(4) et `getauthattr`(3SECDB).
- **Privilèges :** des privilèges peuvent être assignés à des programmes et des processus. Pour plus d'informations sur les privilèges, reportez-vous au Chapitre 8, "Using Roles and Privileges (Overview)" du *System Administration Guide: Security Services*. Reportez-vous également à la page de manuel `privileges`(5).

  La commande `ppriv` fournit un utilitaire de débogage. Pour plus d'informations, reportez-vous à la page de manuel `ppriv`(1). Pour obtenir des instructions sur l'utilisation de cet utilitaire avec des programmes qui fonctionnent dans des zones non globales, reportez-vous à la section "Using the ppriv Utility" du *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*
- **Profils de droits :** les profils de droits rassemblent les attributs de sécurité à affecter à des utilisateurs ou à des rôles en un point unique. Pour plus d'informations sur les profils de droits, reportez-vous à la section "RBAC Rights Profiles" du *System Administration Guide: Security Services*. Trusted Extensions ajoute des actions CDE aux fichiers exécutables auxquels des attributs de sécurité peuvent être assignés.
- **Bibliothèques de confiance :** les bibliothèques partagées dynamiquement et utilisées par `setuid`, `setgid` et les programmes privilégiés peuvent uniquement être chargés à partir de répertoires de confiance. Comme dans le SE Oracle Solaris, la commande `crle` est utilisée

pour ajouter les répertoires de bibliothèque partagés d'un programme exécuté avec des privilèges à la liste de répertoires de confiance. Pour plus d'informations, reportez-vous à la page de manuel `crle(1)`.

Évaluation de la sécurité d'un logiciel

Lorsque des privilèges ont été assignés à un logiciel ou lorsque ce dernier s'exécute à l'aide d'un autre ID d'utilisateur ou ID de groupe, le logiciel devient *de confiance*. Ce type de logiciel peut contourner certains aspects de la stratégie de sécurité de Trusted Extensions. Gardez à l'esprit qu'un logiciel peut être de confiance bien qu'il puisse ne pas être digne de confiance. Pour accorder des privilèges à un logiciel, l'administrateur de sécurité doit attendre qu'un examen minutieux ait révélé que le logiciel utilise les privilèges de manière fiable.

Les programmes d'un système de confiance se répartissent en trois catégories :

- **Les programmes qui n'exigent aucun attribut de sécurité :** certains programmes s'exécutent à un seul niveau et ne nécessitent aucun privilège. Ces programmes peuvent être installés dans un répertoire public tel que `/usr/local`. Pour y accéder, assignez les programmes sous forme de commandes dans les profils de droits des utilisateurs et des rôles.
- **Les programmes qui s'exécutent en tant que root :** certains programmes s'exécutent avec `setuid 0`. Un ID d'utilisateur effectif de `0` peut être affecté à de tels programmes dans un profil de droits. L'administrateur de sécurité affecte ensuite le profil à un rôle d'administration.

  Astuce – Si l'application est capable d'utiliser les privilèges de manière fiable, affectez les privilèges nécessaires à l'application et n'exécutez pas le programme en tant que `root`.

- **Les programmes qui requièrent des privilèges :** certains programmes peuvent nécessiter des privilèges pour des motifs qui ne sont pas évidents. Même si un programme ne semble pas exécuter de fonction contrevenant à la stratégie de sécurité du système, il peut être en train d'effectuer en interne une opération qui ne respecte pas la sécurité. Par exemple, le programme peut utiliser un fichier journal partagé, ou peut lire dans `/dev/kmem`. Pour les questions de sécurité, reportez-vous à la page de manuel `mem(7D)`.

  Parfois, ignorer une stratégie interne n'a pas d'incidence particulière sur le fonctionnement de l'application. Au contraire, il peut en résulter un bénéfice pour les utilisateurs.

  Si votre organisation a accès au code source, vérifiez si vous pouvez supprimer les opérations pouvant outrepasser les stratégies de sécurité sans affecter les performances de l'application.

Responsabilités du développeur lors de la création des programmes de confiance

Bien que le développeur d'un programme puisse manipuler des jeux de privilèges dans le code source, si l'administrateur de sécurité n'attribue pas les privilèges requis au programme, le programme échoue. Le développeur et l'administrateur de sécurité doivent coopérer lors de la création des programmes de confiance.

Un développeur qui écrit un programme de confiance doit effectuer les opérations suivantes :

1. Comprendre où le programme requiert des privilèges pour pouvoir mener à bien sa mission.
2. Connaître et mettre en œuvre des techniques telles que la séparation des privilèges pour pouvoir utiliser les privilèges en toute sécurité dans les programmes.
3. Être conscient des implications en matière de sécurité lorsqu'il affecte des privilèges à un programme. Le programme doit respecter la stratégie de sécurité.
4. Compiler le programme en utilisant des bibliothèques partagées liées au programme à partir d'un répertoire de confiance.

   Pour plus d'informations, reportez-vous au *Developer's Guide to Oracle Solaris Security*. Pour voir des exemples de code pour Trusted Extensions, reportez-vous au *Oracle Solaris Trusted Extensions Developer's Guide* .

Responsabilités de l'administrateur de sécurité pour les programmes de confiance

L'administrateur de sécurité est responsable du test et de l'évaluation des nouveaux logiciels. Une fois le logiciel considéré comme digne de confiance, l'administrateur de sécurité configure des profils de droits et tout autre attribut relatif à la sécurité pour le programme.

Les responsabilités suivantes lui incombent alors :

1. S'assurer que le programmeur et le processus de distribution de programmes sont de confiance.
2. Déterminer les privilèges requis par le programme de l'une des manières suivantes :
   - En demandant au programmeur.
   - En recherchant les privilèges que le programme s'attend à utiliser dans le code source.
   - En recherchant dans le code source les autorisations que le programme exige de ses utilisateurs.
   - En utilisant les options de débogage de la commande `ppriv` afin de détecter l'utilisation de privilèges. Pour voir des exemples, reportez-vous à la page de manuel `ppriv(1)`.
3. Examiner le code source pour s'assurer que son comportement est fiable par rapport aux privilèges dont le programme a besoin pour fonctionner.

Si ce n'est pas le cas et vous avez la possibilité de modifier le code source du programme, modifiez ce code. Un consultant en sécurité ou un développeur possédant des connaissances dans ce domaine peuvent s'en charger. Les modifications peuvent inclure la séparation des privilèges ou la recherche d'autorisations.

L'assignation de privilèges doit être effectuée manuellement. Un programme qui échoue en raison d'un manque de privilèges peut s'en voir assigner de nouveaux. L'administrateur de sécurité peut également décider d'assigner un ID d'utilisateur ou un ID de groupe pour rendre le privilège non nécessaire.

Processus autorisés dans le système de multifenêtrage

Dans Solaris Trusted Extensions (CDE), les processus du système de multifenêtrage suivants sont autorisés :

- Tableau de bord
- Panneaux secondaires du tableau de bord
- Menu de l'espace de travail
- Gestionnaire de fichiers
- Gestionnaire d'applications

Les processus autorisés du système de multifenêtrage sont accessibles à tous, mais l'accès aux actions d'administration est limité aux rôles dans la zone globale.

Dans le gestionnaire de fichiers ne figure pas dans l'un des profils de compte, l'icône de l'action n'est pas visible. Dans le menu de l'espace de travail, si une action ne figure pas dans l'un des profils de compte, celle-ci est visible, mais une erreur s'affiche si elle est appelée.

Dans Trusted CDE, le gestionnaire de fenêtres `dtwm` appelle le script `Xtsolusersession`. D'une part, le script fonctionne avec ce gestionnaire pour appeler des actions qui sont démarrées à partir du système de multifenêtrage. D'autre part, il vérifie les profils de droits d'accès du compte lorsque ce dernier tente de lancer une action. Dans l'un ou l'autre cas, si l'action fait partie d'un profil de droits assigné, elle est exécutée avec les attributs de sécurité spécifiés dans le profil.

Ajout d'actions Trusted CDE

Le processus de création et d'utilisation d'actions CDE dans Trusted Extensions est semblable au processus dans le SE Oracle Solaris. L'ajout d'actions est décrit au Chapitre 4, “Adding and Administering Applications” du *Solaris Common Desktop Environment: Advanced User's and System Administrator's Guide*.

Comme dans le SE Oracle Solaris, l'utilisation d'actions peut être contrôlée par le mécanisme de profil de droits. Dans Trusted Extensions, des attributs de sécurité ont été assignés à plusieurs

actions dans les profils de droits de rôles d'administration. L'administrateur de sécurité peut également utiliser l'outil Rights (Droits) pour assigner des attributs de sécurité à de nouvelles actions.

Le tableau suivant récapitule les principales différences entre un système Oracle Solaris et un système Trusted Extensions lorsque vous créez et utilisez des actions.

TABLEAU 19–1 Contraintes imposées aux actions CDE dans Trusted Extensions

Actions CDE d'Oracle Solaris	Actions Trusted CDE
De nouvelles actions peuvent être créées par n'importe quel utilisateur dans le répertoire personnel du créateur.	Une action peut uniquement être utilisée si elle se trouve dans un profil de droits assigné à l'utilisateur. Le chemin de recherche pour les actions diffère. Les actions du répertoire personnel d'un utilisateur sont traitées en dernier au lieu de l'être en premier. Par conséquent, personne ne peut personnaliser les actions existantes.
Une nouvelle action peut automatiquement être utilisée par son créateur.	Les utilisateurs peuvent créer une nouvelle action dans leur répertoire personnel, mais elle peut ne pas être utilisable. Les utilisateurs auxquels le profil All (Tout) est assigné peuvent utiliser les actions qu'ils créent. Sinon, l'administrateur de sécurité doit ajouter le nom de la nouvelle action à l'un des profils de droits du compte. Pour démarrer l'action, l'utilisateur se sert du gestionnaire de fichiers. L'administrateur système peut placer des actions dans les répertoires publics.
Les actions peuvent être glissées et déposées dans le tableau de bord.	Le tableau de bord fait partie du chemin de confiance. Le gestionnaire de fenêtres ne reconnaît que les actions ajoutées administrativement se trouvant dans les sous-répertoires `/usr/dt` et `/etc/dt`. Même si le profil All (Tout) lui est assigné, un utilisateur ne peut pas faire glisser une nouvelle action vers le tableau de bord. Les actions à partir du répertoire personnel d'un utilisateur ne sont pas reconnues par le gestionnaire de fenêtres. Le gestionnaire vérifie uniquement les répertoires publics.
Les actions peuvent effectuer des opérations privilégiées si elles sont exécutées par `root`.	Les actions peuvent effectuer des opérations privilégiées si des privilèges leur ont été affectés dans un profil de droits assigné à un utilisateur.
Les actions ne sont pas gérées par la Console de gestion Solaris.	Les actions sont affectées à des profils de droits dans l'outil Rights (Droits) de Console de gestion Solaris. Si de nouvelles actions sont ajoutées, l'administrateur de sécurité peut les rendre disponibles.

Gestion des logiciels dans Trusted Extensions (tâches)

La gestion des logiciels dans Trusted Extensions est semblable à la gestion des logiciels sur un système Oracle Solaris qui a installé des zones non globales. Pour plus d'informations sur les zones, reportez-vous à la Partie II, “Zones” du *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*.

▼ Ajout d'un package logiciel dans Trusted Extensions

Avant de commencer Vous devez être dans un rôle qui peut allouer un périphérique.

1. **Démarrez à partir de l'espace de travail approprié.**
   - **Pour installer un package logiciel dans la zone globale, restez dans cette dernière.**
   - **Pour installer un package logiciel dans une zone étiquetée, créez un espace de travail sous cette étiquette.**

     Pour plus d'informations, reportez-vous à la section "Procédure de modification de l'étiquette d'un espace de travail" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.
2. **Allouez l'unité de CD-ROM.**

   Pour plus d'informations, reportez-vous à la section "Procédure d'allocation d'un périphérique dans Trusted Extensions" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.
3. **Installez le logiciel.**

   Pour plus d'informations, reportez-vous à la section "Where to Find Software Management Tasks" du *System Administration Guide: Basic Administration*.
4. **Libérez le périphérique lorsque vous avez terminé.**

   Pour plus d'informations, reportez-vous à la section "Procédure d'allocation d'un périphérique dans Trusted Extensions" du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

▼ Installation d'un fichier d'archive Java dans Trusted Extensions

Cette procédure permet de télécharger un fichier d'archive Java (JAR) vers la zone globale. L'administrateur peut mettre ce fichier à disposition des utilisateurs standard à partir de la zone globale.

Avant de commencer L'administrateur de sécurité a vérifié que la source du programme Java est de confiance, que la méthode de livraison est sécurisée et que le programme peut fonctionner de manière fiable.

Le rôle d'administrateur système de la zone globale vous est affecté. Dans Trusted CDE, le profil Droits d'installation de logiciels inclut l'action Open (Ouvrir) pour le code Java.

1. **Téléchargez le fichier JAR dans le répertoire `/tmp`.**

   Par exemple, si vous sélectionnez un logiciel à l'adresse `http://www.sunfreeware.com`, utilisez les instructions "outil `pkg-get` Solaris" du site.

2. **Ouvrez le gestionnaire de fichiers et accédez au répertoire `/tmp`.**
3. **Cliquez deux fois sur le fichier téléchargé.**
4. **Pour installer le logiciel, répondez aux questions dans les boîtes de dialogue.**
5. **Lisez le journal d'installation.**

Exemple 19–1 Téléchargement d'un fichier JAR vers une étiquette utilisateur

Pour limiter les risques en matière de sécurité, l'administrateur système télécharge le logiciel vers une étiquette unique comprise dans la plage d'accréditations d'un utilisateur standard. L'administrateur de sécurité teste ensuite le fichier JAR ainsi étiqueté. Si le logiciel réussit le test, il rétrograde l'étiquette sur : `ADMIN_LOW`. L'administrateur système installe le logiciel sur un serveur NFS pour qu'il soit disponible pour tous les utilisateurs.

1. L'administrateur système crée d'abord un espace de travail sous l'étiquette d'un utilisateur.
2. Dans cet espace, il télécharge le fichier JAR.
3. L'administrateur de sécurité teste le fichier sous cette étiquette.
4. Il fait ensuite passer l'étiquette du fichier à `ADMIN_LOW`.
5. Enfin, l'administrateur système copie le fichier sur un serveur NFS dont l'étiquette est `ADMIN_LOW`.

◆ ◆ ◆ ANNEXE A

Guide de référence rapide pour l'administration de Trusted Extensions

Les interfaces Trusted Extensions étendent le SE Oracle Solaris. Cette annexe fournit un guide de référence rapide des différences. Pour une liste détaillée des interfaces, y compris des routines de bibliothèque et des appels système, reportez-vous à l'Annexe B, “Liste des pages de manuel Trusted Extensions”.

Interfaces d'administration dans Trusted Extensions

Trusted Extensions fournit des interfaces pour son logiciel. Les interfaces suivantes sont uniquement disponibles lorsque le logiciel Trusted Extensions est en cours d'exécution :

`txzonemgr` Script
: Fournit un assistant basé sur des menus pour la création, l'installation, l'initialisation et le démarrage des zones étiquetées. Le titre du menu est Labeled Zone Manager (Gestionnaire de zones étiquetées). Le script fournit également des options de menu donnant accès à des options de réseau et de services de noms, et permettant de rendre la zone globale cliente d'un serveur LDAP existant.

Actions Trusted CDE
: Dans Trusted CDE, menu Workspace (Espace de travail) –> Application Manager (Gestionnaire d'applications) –> Trusted_Extensions contient des actions CDE permettant de configurer les fichiers, les zones d'installation et de démarrage et de simplifier d'autres tâches Trusted Extensions. Pour les tâches effectuées par ces actions, reportez-vous à la section “Actions Trusted CDE” à la page 37. Ces actions sont également décrites dans l'aide en ligne de Trusted CDE.

Admin Editor
: Cet éditeur de confiance permet de modifier les fichiers système. Dans Trusted CDE, menu Workspace (Espace de travail) –> Application Manager (Gestionnaire d'applications) –> Trusted_Extensions –> Admin Editor appelle l'éditeur de confiance Admin Editor. Dans Trusted JDS, l'éditeur est appelé à partir de la ligne de commande. Vous devez fournir le fichier à modifier en tant qu'argument, comme dans :

`/usr/dt/bin/trusted_edit` *filename*

Gestionnaire d'allocation de périphériques (Device Allocation Manager)
: Dans Trusted Extensions, cette interface graphique permet d'administrer les périphériques. La boîte de dialogue d'administration des périphériques (Device Administration) permet aux administrateurs de configurer les périphériques.

  Le gestionnaire d'allocation de périphériques permet aux rôles et aux utilisateurs standard d'allouer des périphériques. L'interface graphique est disponible à partir du menu Trusted Path (Chemin de confiance).

Générateur d'étiquettes (Label Builder)
: Cette application est appelée lorsque l'utilisateur a la possibilité de choisir une étiquette ou une autorisation. Cette application s'affiche également lorsqu'un rôle assigne des étiquettes ou des plages d'étiquettes à des périphériques, des zones, des utilisateurs ou des rôles.

Gestionnaire de sélection (Selection Manager)
: Cette application est appelée lorsqu'un utilisateur ou un rôle autorisé tente de mettre à niveau ou de rétrograder des informations.

Menu Trusted Path (Chemin de confiance)
: Ce menu gère les interactions avec la base informatique de confiance (TCB, Trusted Computing Base). Il contient notamment une option de menu Change Password (Modifier le mot de passe). Dans Trusted CDE, vous pouvez accéder au menu Trusted Path à partir de la zone de commutation de l'espace de travail. Dans Trusted JDS, vous accédez au menu Trusted Path en cliquant sur le symbole de confiance situé à gauche de la bande de confiance.

Commandes d'administration
: Trusted Extensions fournit des commandes permettant d'obtenir des étiquettes et d'effectuer d'autres tâches. Pour obtenir une liste des commandes, reportez-vous à la section "Outils de ligne de commande dans Trusted Extensions" à la page 46.

Interfaces Oracle Solaris étendues par Trusted Extensions

Trusted Extensions ajoute des commandes et des interfaces graphiques aux fichiers de configuration Oracle Solaris existants.

Commandes d'administration	Trusted Extensions ajoute des options aux commandes Oracle Solaris sélectionnées. Pour obtenir une liste, consultez le Tableau 2–5
Fichiers de configuration	Trusted Extensions ajoute deux privilèges : `net_mac_aware` et `net_mlp`. Pour l'utilisation de `net_mac_aware`, reportez-vous à la section "Accès aux répertoires montés via NFS dans Trusted Extensions" à la page 152.

	Trusted Extensions ajoute des autorisations à la base de données `auth_attr`. Pour obtenir une liste, reportez-vous à la section "Additional Rights and Authorizations in Trusted Extensions" du *Solaris Trusted Extensions Transition Guide*.
	Trusted Extensions ajoute des exécutables, notamment des actions CDE, à la base de données `exec_attr`.
	Trusted Extensions modifie les profils de droits existants dans la base de données `prof_attr`. Il ajoute également des profils à la base de données.
	Trusted Extensions ajoute des actions CDE aux exécutables qui peuvent être privilégiés dans la base de données `exec_attr`.
	Trusted Extensions ajoute des champs à la base de données `policy.conf`. Pour les champs, reportez-vous à la section "Valeurs par défaut du fichier `policy.conf` dans Trusted Extensions" à la page 83.
	Trusted Extensions ajoute des jetons d'audit, des événements d'audit, des classes d'audit et des options de stratégie d'audit. Pour obtenir une liste, reportez-vous à la section "Référence de l'audit Trusted Extensions" à la page 274.
Console de gestion Solaris	Trusted Extensions ajoute un outil Security Templates (Modèles de sécurité) à l'ensemble d'outils Computers and Networks (Ordinateurs et réseaux).
	Trusted Extensions ajoute un outil Trusted Network Zones (Zones de réseau de confiance) à l'ensemble d'outils Computers and Networks.
	Trusted Extensions ajoute un onglet Trusted Extensions Attributes (Attributs Trusted Extensions) aux outils Users (Utilisateurs) et Administrative Roles (Rôles d'administration).
Répertoires partagés à partir de zones	Trusted Extensions vous permet de partager des répertoires à partir de zones étiquetées. Les répertoires sont partagés sous l'étiquette de la zone

par le biais de la création d'un fichier `/etc/dfs/dfstab` à partir de la zone globale.

Renforcement des paramètres de sécurité par défaut dans Trusted Extensions

Trusted Extensions met en place des paramètres de sécurité par défaut plus stricts que le SE Oracle Solaris :

Audit	Par défaut, l'audit est activé. Un administrateur peut désactiver l'audit. Toutefois, l'audit est généralement requis sur les sites où Trusted Extensions est installé.
Périphériques	Par défaut, l'allocation de périphériques est activée. Par défaut, l'allocation de périphériques nécessite une autorisation. Par défaut, les utilisateurs standard ne peuvent donc pas utiliser de supports amovibles. Un administrateur peut lever l'obligation d'autorisation. Cependant, l'allocation de périphériques est généralement nécessaire sur les sites où Trusted Extensions est installé.
Impression	Les utilisateurs standard peuvent uniquement imprimer sur des imprimantes qui incluent leur propre étiquette dans la plage. Par défaut, les impressions comportent des pages de garde et de fin. L'étiquette du travail d'impression figure sur ces pages, ainsi que sur les pages de corps de texte. Par défaut, les utilisateurs ne peuvent pas imprimer les fichiers PostScript.
Rôles	Les rôles sont disponibles dans le SE Oracle Solaris, mais leur utilisation est facultative. Dans Trusted Extensions, les rôles sont nécessaires pour assurer une administration correcte. Dans le SE Oracle Solaris, l'utilisateur `root` peut devenir un rôle. Dans Trusted Extensions, l'utilisateur `root` est ainsi transformé en rôle afin de permettre de mieux auditer les utilisateurs agissant en tant que superutilisateurs.

Options limitées dans Trusted Extensions

Trusted Extensions restreint l'éventail des options de configuration d'Oracle Solaris :

Bureau	Trusted Extensions propose deux bureaux, Solaris Trusted Extensions (CDE) et Solaris Trusted Extensions (JDS). Trusted Extensions propose le bureau Solaris Trusted Extensions (GNOME).
Service de nommage	Le service de nommage LDAP est pris en charge. Toutes les zones doivent être administrées à partir d'un même service de nommage.
Zones	La zone globale est une zone d'administration. Seul l'utilisateur `root` ou un rôle sont autorisés à pénétrer dans la zone globale. Par conséquent, les interfaces d'administration disponibles pour les utilisateurs standard Oracle Solaris ne le sont pas pour les utilisateurs standard Trusted Extensions. Par exemple, dans Trusted Extensions, les utilisateurs ne sont pas autorisés à afficher la Console de gestion Solaris. Les zones non globales sont des zones étiquetées. Les utilisateurs travaillent dans des zones étiquetées.

◆ ◆ ◆ ANNEXE B

Liste des pages de manuel Trusted Extensions

Trusted Extensions est une configuration du SE Oracle Solaris. Cette annexe fournit une brève description des pages de manuel Oracle Solaris qui contiennent des informations relatives à Trusted Extensions.

Pages de manuel Trusted Extensions par ordre alphabétique

Les pages de manuel suivantes décrivent le logiciel Trusted Extensions sur un système Oracle Solaris. Ces pages de manuel s'appliquent uniquement aux systèmes configurés avec Trusted Extensions.

Page de manuel Oracle Solaris	Synopsis
`add_allocatable`(1M)	Ajoute des entrées aux bases de données d'allocation
`atohexlabel`(1M)	Convertit une étiquette lisible par l'utilisateur en son équivalent textuel interne
`blcompare`(3TSOL)	Compare des étiquettes binaires
`blminmax`(3TSOL)	Détermine le lien entre deux étiquettes
`chk_encodings`(1M)	Vérifie la syntaxe du fichier label_encodings
`dtappsession`(1)	Démarre une nouvelle session du gestionnaire d'applications
`fgetlabel`(2)	Identifie l'étiquette du fichier
`getlabel`(1)	Affiche l'étiquette de fichiers
`getlabel`(2)	Identifie l'étiquette d'un fichier
`getpathbylabel`(3TSOL)	Identifie le nom du chemin d'accès à la zone
`getplabel`(3TSOL)	Identifie l'étiquette d'un processus

getuserrange(3TSOL)	Identifie la plage d'étiquettes d'un utilisateur
getzoneidbylabel(3TSOL)	Identifie l'ID d'une zone à partir de l'étiquette de la zone
getzonelabelbyid(3TSOL)	Identifie l'étiquette d'une zone à partir de l'ID de la zone
getzonelabelbyname(3TSOL)	Identifie l'étiquette d'une zone à partir du nom de la zone
getzonepath(1)	Affiche le chemin racine de la zone correspondant à l'étiquette spécifiée
getzonerootbyid(3TSOL)	Identifie le nom du chemin racine d'une zone à partir de l'ID racine de la zone
getzonerootbylabel(3TSOL)	Identifie le nom du chemin racine d'une zone à partir de l'étiquette de la zone
getzonerootbyname(3TSOL)	Détermine le nom du chemin racine d'une zone à partir du nom de la zone
hextoalabel(1M)	Convertit une étiquette textuelle interne en son équivalent lisible par l'utilisateur
labelbuilder(3TSOL)	Crée une interface utilisateur basée sur Motif permettant de générer de façon interactive une autorisation ou une étiquette valide
labelclipping(3TSOL)	Convertit une étiquette binaire et la détoure à la largeur spécifiée
label_encodings(4)	Décrit le fichier label_encodings
label_to_str(3TSOL)	Convertit les étiquettes en chaînes lisibles par l'utilisateur
labels(5)	Décrit les attributs d'étiquette Trusted Extensions
libtsnet(3LIB)	Est la bibliothèque réseau Trusted Extensions
libtsol(3LIB)	Est la bibliothèque Trusted Extensions
m_label(3TSOL)	Alloue et libère des ressources pour une nouvelle étiquette
pam_tsol_account(5)	Contrôle les limitations de comptes dues à des étiquettes
plabel(1)	Identifie l'étiquette d'un processus

remove_allocatable(1M)	Supprime des entrées dans des bases de données d'allocation
sel_config(4)	Correspond aux règles de sélection pour les opérations copier, couper, coller et glisser-déposer
setflabel(3TSOL)	Déplace un fichier vers une zone possédant l'étiquette de sensibilité correspondante
smtnrhdb(1M)	Gère des entrées dans la base de données de gestion de réseau Trusted Extensions
smtnrhtp(1M)	Gère des entrées dans la base de données modèle pour la gestion de réseau Trusted Extensions
smtnzonecfg(1M)	Gère des entrées dans la base de données de configuration pour la gestion de réseau Trusted Extensions dans des zones non globales
str_to_label(3TSOL)	Redistribue des chaînes lisibles par l'utilisateur à une étiquette
tnctl(1M)	Configure les paramètres réseau de Trusted Extensions
tnd(1M)	Est le démon du réseau de confiance
tninfo(1M)	Affiche les informations réseau et les statistiques Trusted Extensions au niveau du noyau
trusted_extensions(5)	Présente Trusted Extensions
TrustedExtensionsPolicy(4)	Est le fichier de configuration de l'extension de Trusted Extensions pour serveur X
tsol_getrhtype(3TSOL)	Identifie le type d'hôte à partir des informations réseau Trusted Extensions
updatehome(1M)	Met à jour les fichiers de copie et de liaison du répertoire personnel pour l'étiquette en cours
XTSOLgetClientAttributes(3XTSOL)	Identifie les attributs d'étiquette d'un client X
XTSOLgetPropAttributes(3XTSOL)	Identifie les attributs d'étiquette d'une fenêtre
XTSOLgetPropLabel(3XTSOL)	Identifie l'étiquette d'une propriété de fenêtre
XTSOLgetPropUID(3XTSOL)	Identifie l'UID d'une propriété de fenêtre
XTSOLgetResAttributes(3XTSOL)	Identifie tous les attributs d'étiquette d'une fenêtre ou d'un pixmap

XTSOLgetResLabel(3XTSOL)	Identifie l'étiquette d'une fenêtre, d'un pixmap ou d'une palette de couleurs
XTSOLgetResUID(3XTSOL)	Identifie l'UID d'une fenêtre ou d'un pixmap
XTSOLgetSSHeight(3XTSOL)	Identifie la hauteur de la bande d'écran
XTSOLgetWorkstationOwner(3XTSOL)	Identifie la propriété de la station de travail
XTSOLIsWindowTrusted(3XTSOL)	Détermine si une fenêtre est créée par un client de confiance
XTSOLMakeTPWindow(3XTSOL)	Fait de cette fenêtre une fenêtre de chemin de confiance
XTSOLsetPolyInstInfo(3XTSOL)	Définit les informations d'instanciation multiple
XTSOLsetPropLabel(3XTSOL)	Définit l'étiquette d'une propriété de fenêtre
XTSOLsetPropUID(3XTSOL)	Définit l'UID d'une propriété de fenêtre
XTSOLsetResLabel(3XTSOL)	Définit l'étiquette d'une fenêtre ou d'un pixmap
XTSOLsetResUID(3XTSOL)	Définit l'UID d'une fenêtre, d'un pixmap ou d'une palette de couleurs
XTSOLsetSessionHI(3XTSOL)	Définit l'étiquette haute sensibilité de la session sur le serveur de la fenêtre
XTSOLsetSessionLO(3XTSOL)	Définit l'étiquette basse sensibilité de la session sur le serveur de la fenêtre
XTSOLsetSSHeight(3XTSOL)	Définit la hauteur de la bande d'écran
XTSOLsetWorkstationOwner(3XTSOL)	Définit le propriétaire de la station de travail

Pages de manuel Oracle Solaris modifiées par Trusted Extensions

Trusted Extensions ajoute des informations aux pages de manuel Oracle Solaris suivantes.

Page de manuel Oracle Solaris	Modification apportée à Trusted Extensions
allocate(1)	Ajoute des options permettant de prendre en charge l'allocation d'un périphérique dans une zone et son nettoyage dans un environnement avec fenêtres
auditconfig(1M)	Ajoute la stratégie de fenêtre pour les informations étiquetées

audit_class(4)	Ajoute des classes d'audit du serveur X
audit_event(4)	Ajoute des événements d'audit
auditreduce(1M)	Ajoute un sélecteur d'étiquettes
auth_attr(4)	Ajoute des autorisations d'étiquettes
automount(1M)	Ajoute la capacité à monter et par conséquent à afficher des répertoires personnels de niveau inférieur
cancel(1)	Ajoute des restrictions d'étiquette à la capacité d'un utilisateur à annuler un travail d'impression
deallocate(1)	Ajoute des options permettant la prise en charge de la libération d'un périphérique dans une zone, le nettoyage du périphérique dans un environnement avec fenêtres et la spécification du type de périphérique à libérer
device_clean(5)	Est appelé par défaut dans Trusted Extensions
exec_attr(4)	Ajoute des actions CDE en tant que type d'objet de profil
getpflags(2)	Reconnaît les indicateurs de traitement `net_mac_aware` et `NET_MAC_AWARE_INHERIT`
getsockopt(3SOCKET)	Identifie l'état du contrôle d'accès obligatoire `SO_MAC_EXEMPT` du socket
getsockopt(3XNET)	Identifie l'état du contrôle d'accès obligatoire `SO_MAC_EXEMPT` du socket
ifconfig(1M)	Ajoute l'interface `all-zones`
is_system_labeled(3C)	Détermine si le système est configuré avec Trusted Extensions
ldaplist(1)	Ajoute des bases de données réseau Trusted Extensions
list_devices(1)	Ajoute des attributs, tels que des étiquettes, associés à un périphérique
lp(1)	Ajoute l'option `-nolabels`
lpadmin(1M)	Ajoute des restrictions d'étiquette à la capacité d'un administrateur à gérer l'impression
lpmove(1M)	Ajoute des restrictions d'étiquette à la capacité d'un administrateur à déplacer un travail d'impression
lpq(1B)	Ajoute des restrictions d'étiquette à l'affichage des informations de file d'impression

lprm(1B)	Ajoute des restrictions d'étiquette à la capacité de l'appelant à supprimer des requêtes d'impression
lpsched(1M)	Ajoute des restrictions d'étiquette à la capacité de l'administrateur à arrêter et à redémarrer le service d'impression
lpstat(1)	Ajoute des restrictions d'étiquette à l'affichage de l'état du service d'impression
netstat(1M)	Ajoute l'option `-R` pour afficher les attributs de sécurité étendus
privileges(5)	Ajoute des privilèges Trusted Extensions tels que `PRIV_FILE_DOWNGRADE_SL`
prof_attr(4)	Ajoute des profils de droits, tels que Object Label Management (Gestion de l'étiquette des objets)
route(1M)	Ajoute l'option `-secattr` pour ajouter des attributs de sécurité étendus à une route
setpflags(2)	Définit l'indicateur par processus `net_mac_aware`
setsockopt(3SOCKET)	Définit l'option `SO_MAC_EXEMPT`
setsockopt(3XNET)	Définit le contrôle d'accès obligatoire, `SO_MAC_EXEMPT`, sur le socket
smexec(1M)	Ajoute des options permettant la prise en charge du type d'action CDE
smrole(1M)	Ajoute des options permettant la prise en charge de l'étiquette d'un rôle
smuser(1M)	Ajoute des options permettant la prise en charge de l'étiquette et d'autres attributs de sécurité d'un utilisateur, tels que le temps d'inactivité autorisé
socket.h(3HEAD)	Prend en charge l'option `SO_MAC_EXEMPT` pour les homologues sans étiquette
tar(1)	Ajoute l'intégration des étiquettes dans les fichiers tar et l'extraction des fichiers en fonction de l'étiquette
tar.h(3HEAD)	Ajoute des types d'attributs utilisés dans des fichiers tar étiquetés
ucred_getlabel(3C)	Ajoute la possibilité d'obtenir la valeur de l'étiquette à partir des informations d'identification d'un utilisateur

user_attr(4)	Ajoute des attributs de sécurité de l'utilisateur spécifiques à Trusted Extensions

Index

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

X

Z