Configuration et administration d'Oracle® Solaris Trusted Extensions

Référence : E25900
Novembre 2011

ORACLE®

120424@25097

Table des matières

Liste des figures

Liste des tableaux

Préface

Configuration et administration d'Oracle Solaris Trusted Extensions décrit les procédures d'activation et de configuration initiale de la fonction Trusted Extensions sur le système d'exploitation Oracle Solaris (SE Oracle Solaris). Ce guide fournit également des procédures de gestion des utilisateurs, des zones, des périphériques et des hôtes sur un système 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*. Ce document présente les différences d'implémentation en fonction des divers types de plates-formes.

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 d'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

Trusted Extensions et le système d'exploitation Oracle Solaris

Trusted Extensions s'exécute sur le SE Oracle Solaris. Étant donné que le logiciel Trusted Extensions peut modifier le SE Oracle Solaris, Trusted Extensions peut nécessiter un paramétrage particulier des options d'installation d'Oracle Solaris. La partie I de ce guide décrit comment préparer le SE Oracle Solaris pour Trusted Extensions, comment activer Trusted Extensions, et comment effectuer la configuration initiale du logiciel. La partie II de ce guide explique comment administrer les fonctions du système réservées exclusivement à Trusted Extensions.

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

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
Initialisation et arrêt d'Oracle Solaris sur les plates-formes SPARC	Initialisation et arrêt d'un système, gestion des services d'initialisation, modification du comportement d'initialisation, initialisation à partir de ZFS, gestion de l'archive d'initialisation et dépannage de l'initialisation sur les plates-formes SPARC
Initialisation et arrêt d'Oracle Solaris sur les plates-formes x86	Initialisation et arrêt d'un système, gestion des services d'initialisation, modification du comportement d'initialisation, initialisation à partir de ZFS, gestion de l'archive d'initialisation et dépannage de l'initialisation sur les plates-formes x86
Administration d'Oracle Solaris : Tâches courantes	Utilisation des commandes Oracle Solaris, initialisation et arrêt d'un système, gestion des comptes utilisateurs et des groupes d'utilisateurs, gestion des services, des pannes matérielles, des informations système, des ressources système et des performances système, gestion du logiciel, de l'impression, de la console et des terminaux et dépannage des problèmes logiciels et du système
Administration d'Oracle Solaris : Périphériques et systèmes de fichiers	Médias amovibles, disques et périphériques, systèmes de fichiers, et sauvegarde et restauration des données
Administration d'Oracle Solaris : Services IP	Administration de réseau TCP/IP, administration d'adresses IPv4 et IPv6, DHCP, IPsec, IKE, filtre IP et IPQoS
Oracle Solaris Administration: Naming and Directory Services	Services d'annuaire et de nommage DNS, NIS et LDAP, y compris transition de NIS vers LDAP
Administration d'Oracle Solaris : interfaces réseau et virtualisation réseau	Interface IP manuelle et automatique, y compris configuration sans fil Wi-Fi, administration des ponts, des réseaux locaux virtuels, des agrégations, LLDP et IPMP ; cartes d'interface réseau virtuelles et gestion des ressources.
Administration d'Oracle Solaris : Services réseau	Serveurs cache Web, services à facteur temps, systèmes de fichiers de réseau (NFS et Autofs), messagerie, SLP et PPP
Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources	Fonctions de gestion des ressources, qui vous permettent de contrôler la façon dont les applications utilisent les ressources système disponibles ; technologie de partitionnement logiciel Oracle Solaris Zones, qui virtualise les services de système d'exploitation pour créer un environnement isolé pour les applications en cours d'exécution; et Oracle Solaris Zones 10, qui héberge les environnements Oracle Solaris 10 exécutés sur le noyau Oracle Solaris 11
Administration d'Oracle Solaris : services de sécurité	Audit, gestion de périphériques, sécurité des fichiers, BART, services Kerberos, PAM, structure cryptographique, gestion des clés, privilèges, RBAC, SASL Secure Shell et analyse des virus

Titre du manuel	Sujets
Oracle Solaris Administration: SMB and Windows Interoperability	Service SMB, qui vous permet de configurer un système Oracle Solaris pour mettre les partages SMB à disposition des clients SMB ; client SMB, qui vous permet d'accéder aux partages SMB ; services de mappage d'identités natif, qui vous permettent de mapper les identités de groupe et d'utilisateur entre les systèmes Oracle Solaris et les systèmes Windows.
Administration d'Oracle Solaris : Systèmes de fichiers 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 des fichiers ZFS, utilisation de ZFS sur un système Oracle Solaris avec des zones installées, volumes émulés et dépannage et récupération de données
Configuration et administration d'Oracle Solaris Trusted Extensions	Installation, configuration et administration système spécifique à Trusted Extensions
Directives de sécurité d'Oracle Solaris 11	Sécurisation d'un système Oracle Solaris, et scénarios d'utilisation de ses fonctions de sécurité, telles que les zones, ZFS et Trusted Extensions
Transition d'Oracle Solaris 10 vers Oracle Solaris 11	Fournit les informations d'administration système et d'autres exemples de transition à partir d'Oracle Solaris 10 vers Oracle Solaris 11 dans les domaines suivants : gestion de l'installation, des périphériques, des disques et des systèmes de fichiers, gestion des logiciels, mise en réseau, gestion des systèmes, sécurité, virtualisation, fonctions du bureau, gestion des comptes utilisateur et des volumes émulés des environnements utilisateur et dépannage et récupération de données

Références connexes

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

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

Références à des sites Web tiers connexes

Des URL tierces offrant l'accès à des informations complémentaires sont citées dans ce document.

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

Accès au support technique Oracle

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

Conventions typographiques

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

TABLEAU P–1 Conventions typographiques

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

TABLEAU P–1 Conventions typographiques *(Suite)*

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

Invites de shell dans les exemples de commandes

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

TABLEAU P–2 Invites de shell

Shell	Invite
Bash shell, korn shell et bourne shell	`$`
Bash shell, korn shell et bourne shell pour superutilisateur	`#`
C shell	`nom_machine%`
C shell pour superutilisateur	`nom_machine#`

PARTIE I

Configuration initiale de Trusted Extensions

Les chapitres de cette partie décrivent comment préparer les systèmes Oracle Solaris pour exécuter Trusted Extensions. Les chapitres traitent de l'activation de Trusted Extensions et des tâches de configuration initiales.

Le Chapitre 1, “Planification de la sécurité pour Trusted Extensions” décrit les problèmes de sécurité à prendre en compte lors de la configuration du logiciel Trusted Extensions sur un ou plusieurs systèmes Oracle Solaris.

Le Chapitre 2, “Déroulement de la configuration de Trusted Extensions” contient des listes de tâches concernant la configuration du logiciel Trusted Extensions sur des systèmes Oracle Solaris.

Le Chapitre 3, “Ajout de la fonction Trusted Extensions à Oracle Solaris (tâches) ” fournit des instructions sur la préparation d'un système Oracle Solaris pour le logiciel Trusted Extensions. Il décrit comment activer Trusted Extensions et se connecter.

Le Chapitre 4, “Configuration de Trusted Extensions (tâches)” fournit des instructions sur la configuration du logiciel Trusted Extensions sur un système avec un moniteur.

Le Chapitre 5, “Configuration de LDAP pour Trusted Extensions (tâches)” fournit des instructions sur la configuration du service de nommage LDAP sur les systèmes Trusted Extensions.

◆ ◆ ◆ CHAPITRE 1

Planification de la sécurité pour Trusted Extensions

La fonction Trusted Extensions d'Oracle Solaris implémente une partie de votre stratégie de sécurité du site dans le logiciel. Ce chapitre fournit une présentation générale de la sécurité et présente les aspects administratifs de la configuration du logiciel.

Planification de la sécurité dans Trusted Extensions

Cette section décrit la planification nécessaire avant d'activer et de configurer le logiciel Trusted Extensions.

Pour une liste de contrôle des tâches de configuration de Trusted Extensions, reportez-vous à l'Annexe B, "Liste de contrôle de configuration pour Trusted Extensions". Si vous êtes intéressé par la localisation de votre site, reportez-vous à la section "Pour les clients internationaux de

Trusted Extensions" à la page 30. Si vous voulez exécuter une configuration évaluée, reportez-vous à la section "Prise de connaissance de votre stratégie de sécurité du site" à la page 28.

Prise de connaissance de Trusted Extensions

L'activation et la configuration de Trusted Extensions impliquent plus que le simple chargement de fichiers exécutables, la saisie des informations relatives à votre site et la définition des variables de configuration. Des connaissances générales approfondies sont également requises. Le logiciel Trusted Extensions fournit un environnement étiqueté qui repose sur deux fonctions d'Oracle Solaris :

- Les fonctions qui, dans la plupart des environnements UNIX sont assignées au superutilisateur sont traitées par les rôles d'administration séparés.
- La possibilité de passer outre à la stratégie de sécurité peut être affectée à des utilisateurs et applications spécifiques.

Dans Trusted Extensions, l'accès aux données est contrôlé par des balises de sécurité spéciales. Ces balises sont appelées des étiquettes. Les étiquettes sont affectées à des utilisateurs, des processus et des objets, tels que des fichiers de données et des répertoires. Ces étiquettes fournissent un contrôle d'accès obligatoire (MAC), en plus des autorisations UNIX ou contrôle d'accès discrétionnaire (DAC).

Prise de connaissance de votre stratégie de sécurité du site

Trusted Extensions vous permet d'intégrer efficacement votre stratégie de sécurité du site avec le SE Oracle Solaris. Par conséquent, il est nécessaire de bien comprendre l'étendue de votre stratégie et la manière dont le logiciel Trusted Extensions peut la mettre en œuvre. Une configuration bien planifiée doit fournir un équilibre entre la cohérence avec votre stratégie de sécurité du site et la commodité pour les utilisateurs qui travaillent sur le système.

Trusted Extensions est configuré par défaut pour être conforme aux Critères communs pour la sécurité des systèmes d'information (ISO/CEI 15408) au niveau d'assurance de l'évaluation EAL4 par rapport aux profils de protection suivants :

- Profil de protection Étiquettes de sécurité
- Profil de protection Accès contrôlé
- Profil de protection Contrôle d'accès basé sur le rôle

Pour satisfaire à ces niveaux évalués, vous devez configurer LDAP en tant que service de nommage. Notez que votre configuration risque de ne plus être conforme à l'évaluation si vous effectuez l'une des opérations suivantes :

- Modification des paramètres de commutation du noyau dans le fichier `/etc/system`.
- Désactivation du contrôle ou de l'allocation de périphériques.
- Modification des entrées par défaut dans les fichiers publics du répertoire `/usr`.

Pour plus d'informations, reportez-vous au site Web sur les Critères communs (`http://www.commoncriteriaportal.org/`) (en anglais).

Conception d'une stratégie d'administration de Trusted Extensions

Le rôle `root` ou le rôle d'administrateur système est responsable de l'activation de Trusted Extensions. Vous pouvez créer des rôles pour séparer les responsabilités administratives entre plusieurs domaines fonctionnels :

- L'administrateur de sécurité est responsable des tâches liées à la sécurité, telles que la mise en place et l'attribution des étiquettes de sécurité, la configuration du contrôle et la définition d'une stratégie de mots de passe.
- L'administrateur système est responsable des tâches non liées à la sécurité que sont la configuration, la maintenance et l'administration générale.
- Des rôles plus limités peuvent également être configurés. Par exemple, un opérateur peut être responsable de la sauvegarde des fichiers.

Dans le cadre de votre stratégie d'administration, vous devez prendre des décisions sur les points suivants :

- Les responsabilités d'administration incombant à chaque utilisateur
- L'identité des utilisateurs non administratifs autorisés à exécuter des applications sécurisées, et donc à passer outre à la stratégie de sécurité en cas de besoin
- Les données accessibles aux différents utilisateurs

Élaboration d'une stratégie d'étiquetage

La planification d'étiquettes nécessite la configuration d'une hiérarchie de niveaux de sensibilité et la hiérarchisation des informations sur votre système. Le fichier `label_encodings` contient ce type d'information pour votre site. Vous pouvez utiliser l'un des fichiers `label_encodings` fournis avec le logiciel Trusted Extensions. Vous pouvez également modifier l'un des fichiers fournis ou créer un nouveau fichier `label_encodings` spécifique à votre site. Le fichier doit contenir les extensions locales spécifiques à Oracle, au moins pour la section `COLOR NAMES`.

Attention – Si vous fournissez un fichier `label_encodings`, la meilleure pratique consiste à installer la version définitive du fichier avant que le système ne vérifie les étiquettes. Les étiquettes sont vérifiées au cours de la première initialisation après l'activation du service Trusted Extensions. Une fois que vous avez créé votre première zone ou votre modèle de réseau, les modifications apportées au fichier `label_encodings` doivent contenir les zones existantes et les modèles.

La planification des étiquettes implique également la planification de la configuration des étiquettes. Après l'activation du service Trusted Extensions, vous devez décider si le système doit autoriser les utilisateurs à se connecter à plusieurs étiquettes ou si le système peut être configuré avec une étiquette utilisateur uniquement. Par exemple, un serveur LDAP est un bon candidat pour avoir une zone étiquetée. Pour l'administration locale du serveur, vous pouvez créer une zone à l'étiquette minimale. Pour administrer le système, l'administrateur se connecte et assume le rôle approprié dans l'espace de travail de l'utilisateur.

Pour plus d'informations, reportez-vous à la section *Trusted Extensions Label Administration*. Vous pouvez également vous reporter à la section *Compartmented Mode Workstation Labeling: Encodings Format*.

Pour les clients internationaux de Trusted Extensions

Pour localiser un fichier `label_encodings`, les clients internationaux doivent *uniquement* localiser les noms des étiquettes. Les noms des étiquettes d'administration, `ADMIN_HIGH` et `ADMIN_LOW`, ne doivent pas être localisés. Tous les hôtes étiquetés que vous contactez, à partir de n'importe quel fournisseur, doivent disposer de noms d'étiquettes correspondant aux noms d'étiquettes dans le fichier `label_encodings`.

Planification du matériel et de la capacité du système pour Trusted Extensions

Le matériel du système comprend le système lui-même et les périphériques qui y sont connectés. Ceux-ci incluent les lecteurs de bandes, les microphones, les lecteurs de CD-ROM et les chargeurs de disques. La capacité du matériel englobe la mémoire système, les interfaces réseau et de l'espace disque.

- Suivez les recommandations relatives à l'installation d'une version d'Oracle Solaris comme décrit dans la section *Installation des systèmes Oracle Solaris 11* et la section d'installation *Release Notes* pour cette version.
- Pour les fonctions de Trusted Extensions, on peut ajouter à ces recommandations :
  - Une mémoire au-delà du minimum suggéré est requise sur les systèmes suivants :
    - Systèmes s'exécutant sur plusieurs étiquettes de sensibilité

- Systèmes utilisés par des utilisateurs pouvant occuper un rôle administratif
- Davantage d'espace disque est requis sur les systèmes suivants :
  - Systèmes qui stockent les fichiers sur plusieurs étiquettes
  - Systèmes dont les utilisateurs peuvent occuper un rôle administratif

Planification de votre réseau de confiance

Pour obtenir de l'aide dans la planification de votre matériel réseau, reportez-vous au Chapitre 1, “Planification du développement du réseau” du manuel *Administration d'Oracle Solaris : Services IP*.

Le logiciel Trusted Extensions reconnaît deux types d'hôtes, cipso et sans étiquette. Chaque type d'hôte dispose d'un modèle de sécurité par défaut, comme illustré dans le Tableau 1–1.

TABLEAU 1–1 Modèles d'hôtes par défaut dans Trusted Extensions

Type d'hôte	Nom du modèle	Objectif
`unlabeled`	`admin_low`	Est utilisé pour identifier les hôtes non approuvés qui peuvent communiquer avec la zone globale. De tels hôtes envoient des paquets qui n'incluent pas les étiquettes. Pour plus d'informations, reportez-vous à la section système sans étiquette.
`cipso`	`cipso`	Identifie les hôtes ou les réseaux qui envoient des paquets CIPSO. Les paquets CIPSO sont étiquetés.

Si votre réseau est accessible par d'autres réseaux, vous devez spécifier des domaines et hôtes accessibles. Vous devez également identifier les hôtes Trusted Extensions qui joueront le rôle de passerelles. Vous devez identifier la plage d'accréditations de l'étiquette pour ces passerelles, et l'étiquette de sensibilité sur laquelle les données d'autres hôtes peuvent être visualisées.

L'étiquetage d'hôtes, de passerelles et de réseaux est décrit au Chapitre 16, “Gestion des réseaux dans Trusted Extensions (tâches) ”. L'assignation d'étiquettes à des systèmes distants s'effectue après la configuration initiale.

Planification de zones dans Trusted Extensions

Le logiciel Trusted Extensions est ajouté à Oracle Solaris dans la zone globale. Vous pouvez ensuite configurer des zones non globales étiquetées. Vous pouvez créer une zone étiquetée pour chaque étiquette unique, même si vous n'avez pas besoin de créer une zone pour chaque étiquette dans votre fichier `label_encodings`. Un script fourni vous permet de créer facilement deux zones étiquetées pour l'étiquette utilisateur par défaut et l'autorisation utilisateur par défaut de votre fichier `label_encodings`.

Une fois les zones étiquetées créées, les utilisateurs standard peuvent utiliser le système configuré, mais ils ne sont pas connectés à d'autres systèmes.

- Dans Trusted Extensions, le transport local permettant la connexion au serveur X s'effectue via des sockets de domaine UNIX. Par défaut, le serveur X n'écoute pas pour les connexions TCP.
- Par défaut, les zones non globales ne peuvent pas communiquer avec des hôtes non approuvés. Vous devez spécifier les adresses IP d'hôte distant explicites ou les masques réseau qui peuvent être atteints par chaque zone.

Zones Trusted Extensions et Oracle Solaris

Les zones Trusted Extensions, c'est-à-dire les zones étiquetées sont des *marques* des zones Oracle Solaris. Les zones étiquetées sont principalement utilisées pour séparer les données. Dans Trusted Extensions, les utilisateurs standard ne peuvent pas se connecter à distance à une zone étiquetée, à moins que ce ne soit à partir d'une zone étiquetée à l'identique sur un autre système de confiance. Les administrateurs autorisés peuvent accéder à une zone étiquetée à partir de la zone globale. Pour plus d'informations sur les marques de zone, reportez-vous à la page de manuel `brands(5)`.

Création d'une zone dans Trusted Extensions

La création de zones dans Trusted Extensions se fait de façon similaire à la création de zones dans Oracle Solaris. Trusted Extensions fournit le script `txzonemgr` pour vous guider tout au long du processus. En effet, le script comporte plusieurs options de ligne de commande permettant d'automatiser la création de zones étiquetées.

Accès aux zones étiquetées

Sur un système correctement configuré, chaque zone doit être en mesure d'utiliser une adresse de réseau pour communiquer avec d'autres zones qui partagent la même étiquette. Les configurations suivantes fournissent une zone étiquetée permettant d'accéder à d'autres zones étiquetées :

- **Interface all-zones** : une adresse `all-zones` est attribuée. Dans cette configuration par défaut, une seule adresse IP est requise. Chaque zone, globale et étiquetée, peut communiquer avec des zones étiquetées identiques sur des systèmes distants via cette adresse partagée.

  Une amélioration de cette configuration consiste à créer une deuxième instance IP pour la zone globale à utiliser exclusivement. Cette deuxième instance ne doit pas être une adresse `all-zones`. L'instance IP pourrait être utilisée pour héberger un service multiniveau ou pour fournir une route vers un sous-réseau privé.
- **Instances IP** : comme dans le SE Oracle Solaris, une adresse IP est assignée à chaque zone, y compris à la zone globale. Les zones partagent la pile IP. Dans le cas le plus simple, toutes les zones partagent la même interface physique.

Une amélioration de cette configuration consiste à affecter une carte réseau (NIC) séparée à chaque zone. Ce type de configuration permet de séparer physiquement les réseaux à étiquette unique associés à chaque NIC.

Une amélioration supplémentaire consiste à utiliser une ou plusieurs interfaces `all-zones` en plus de l'instance IP par zone. Cette configuration offre la possibilité d'utiliser les interfaces internes, telles que `vni0`, pour atteindre la zone globale, protégeant ainsi cette dernière contre les attaques à distance. Par exemple, un service privilégié qui lie un port multiniveau sur une instance de `vni0` dans la zone globale peut uniquement être atteint en interne par les zones qui utilisent la pile partagée.

- **Pile IP exclusive** : comme dans Oracle Solaris, une adresse IP est assignée à chaque zone, y compris à la zone globale. Une carte d'interface réseau virtuelle (VNIC) est créée pour chaque zone étiquetée.

  Une amélioration de cette configuration consiste à créer chaque VNIC sur une interface réseau distincte. Ce type de configuration permet de séparer physiquement les réseaux à étiquette unique associés à chaque NIC. Les zones qui sont configurées à l'aide d'une pile IP exclusive ne peuvent pas utiliser l'interface `all-zones`.

Planification pour services multiniveau

Par défaut, Trusted Extensions ne fournit pas de services multiniveau. La plupart des services sont faciles à configurer en tant que services zone à zone, c'est-à-dire, en tant que services à étiquette unique. Par exemple, chaque zone étiquetée peut se connecter au serveur NFS exécuté au niveau de l'étiquette de la zone étiquetée.

Si votre site requiert des services multiniveau, ces services sont mieux configurés sur un système disposant d'au moins deux adresses IP. Les ports multiniveau requis par un service multiniveau peuvent être affectés à l'adresse IP associée à la zone globale. Une adresse `all-zones` peut être utilisée par les zones étiquetées pour atteindre les services.

Astuce – Si les utilisateurs des zones étiquetées ne sont pas autorisés à accéder aux services multiniveau, vous pouvez assigner une adresse IP au système. Cette configuration Trusted Extensions est généralement utilisée sur des ordinateurs portables.

Planification pour le service de nommage LDAP dans Trusted Extensions

Si vous ne prévoyez pas d'installer de réseau de systèmes étiquetés, vous pouvez ignorer cette section. Si vous avez l'intention d'utiliser LDAP, vos systèmes doivent être configurés en tant que clients LDAP avant l'ajout de la première zone étiquetée.

Si vous prévoyez d'exécuter Trusted Extensions sur un réseau de systèmes, utilisez LDAP en tant que service de nommage. Pour Trusted Extensions, un serveur Oracle Directory Server Enterprise Edition (serveur LDAP) rempli est requis lorsque vous configurez un réseau de systèmes. Si votre site dispose déjà d'un serveur LDAP, vous pouvez remplir le serveur avec les bases de données Trusted Extensions. Pour accéder au serveur, vous pouvez configurer un serveur proxy LDAP sur un système Trusted Extensions.

Si votre site ne dispose pas de serveur LDAP, vous devez alors planifier la création d'un serveur LDAP sur un système exécutant le logiciel Trusted Extensions. Les procédures sont décrites au Chapitre 5, “Configuration de LDAP pour Trusted Extensions (tâches)”.

Planification du contrôle dans Trusted Extensions

Par défaut, l'audit est activé lors de la première initialisation de Trusted Extensions. Par défaut, tous les événements de la classe `login/logout` font par conséquent l'objet d'un audit. Pour auditer les utilisateurs qui configurent le système, vous pouvez créer des rôles très tôt au cours du processus de configuration. Lorsque ces rôles configurent le système, les enregistrements d'audit incluent l'utilisateur connecté qui assume le rôle. Reportez-vous à la section “Création de rôles et d'utilisateurs dans Trusted Extensions” à la page 69.

La planification de l'audit dans Trusted Extensions est identique à la planification dans le SE Oracle Solaris. Pour plus de détails, reportez-vous à la section Partie VII, “Audit dans Oracle Solaris” du manuel *Administration d'Oracle Solaris : services de sécurité*. Bien que Trusted Extensions ajoute des classes, des événements et des jetons d'audit, le logiciel ne modifie pas le mode d'administration de l'audit. Pour en savoir plus sur les ajouts effectués à l'audit par Trusted Extensions, reportez-vous au Chapitre 22, “Audit de Trusted Extensions (présentation) ”.

Planification de la sécurité de l'utilisateur dans Trusted Extensions

Le logiciel Trusted Extensions fournit des paramètres de sécurité par défaut raisonnables pour les utilisateurs. Ces paramètres de sécurité par défaut sont répertoriés dans le Tableau 1–2. Lorsque deux valeurs sont répertoriées, la première valeur est la valeur par défaut. L'administrateur de sécurité peut modifier ces valeurs par défaut afin de refléter la stratégie de sécurité du site. Une fois que l'administrateur de sécurité a défini les valeurs par défaut, l'administrateur système peut créer tous les utilisateurs, qui héritent des valeurs par défaut définies. Pour obtenir des descriptions des mots-clés et valeurs de ces paramètres par défaut, reportez-vous aux pages de manuel `label_encodings(4)` et `policy.conf(4)`.

TABLEAU 1–2 Paramètres de sécurité par défaut Trusted Extensions pour les comptes utilisateur

Nom de fichier	Mot-clé	Valeur
`/etc/security/policy.conf`	`IDLECMD`	`lock` | `logout`
	`IDLETIME`	`30`
	`CRYPT_ALGORITHMS_ALLOW`	`1,2a,md5,5,6`
	`CRYPT_DEFAULT`	`sha256`
	`LOCK_AFTER_RETRIES`	`no` | `yes`
	`PRIV_DEFAULT`	`basic`
	`PRIV_LIMIT`	`all`
	`AUTHS_GRANTED`	`solaris.device.cdrw`
	`CONSOLE_USER`	`Console User`
	`PROFS_GRANTED`	`Basic Solaris User`
Section LOCAL DEFINITIONS de `/etc/security/tsol/label_encodings`	Default User Clearance	`CNF INTERNAL USE ONLY`
	Default User Sensitivity Label	`PUBLIC`

Remarque – Les variables `IDLECMD` et `IDLETIME` s'appliquent à la session de l'utilisateur de connexion. Si l'utilisateur de connexion assume un rôle, les valeurs `IDLECMD` et `IDLETIME` de l'utilisateur sont en vigueur pour ce rôle.

L'administrateur système peut configurer un modèle d'utilisateur standard qui définit les valeurs par défaut du système pour chaque utilisateur. Par exemple, le shell initial de tous les utilisateurs est par défaut un shell de type bash. L'administrateur système peut configurer un modèle qui donne à chaque utilisateur un shell pfbash.

Élaboration d'une stratégie de configuration pour Trusted Extensions

La section suivante décrit des stratégies de configuration, de la plus sûre à la moins sûre :

- Une équipe de deux personnes configure le logiciel. Le processus de configuration fait l'objet d'un contrôle.

  Deux personnes se trouvent sur l'ordinateur lorsque le logiciel est activé. Très tôt dans le processus de configuration, cette équipe crée des rôles discrets et décide des utilisateurs locaux qui peuvent les assumer. L'équipe configure également un audit en vue d'auditer les

événements exécutés par les rôles. Une fois les rôles affectés à des utilisateurs, et une fois l'ordinateur réinitialisé, les utilisateurs se connectent et assument un rôle limité. Le logiciel applique la division des tâches par rôle. La piste d'audit fournit un enregistrement de la procédure de configuration. Pour une illustration du processus de configuration sécurisé, reportez-vous à la Figure 1–1.

- Une seule personne active et configure le logiciel en assumant le rôle approprié. Le processus de configuration fait l'objet d'un contrôle.

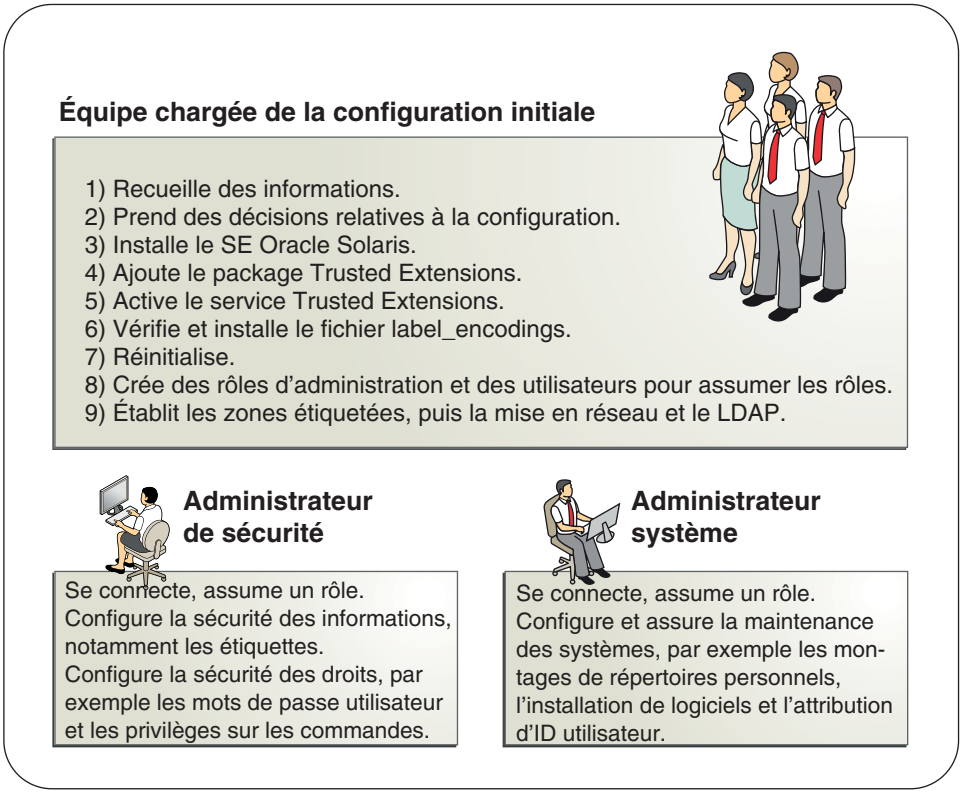
  Plus tôt dans le processus de configuration, le rôle `root` crée des rôles supplémentaires. Le rôle `root` configure également l'audit en vue de vérifier les événements exécutés par les rôles. Une fois que ces rôles supplémentaires ont été affectés à l'utilisateur initial et que l'ordinateur a été réinitialisé, l'utilisateur se connecte et assume le rôle approprié à la tâche en cours. La piste d'audit fournit un enregistrement de la procédure de configuration.
- Une seule personne active et configure le logiciel en assumant le rôle `root`. Le processus de configuration ne fait pas l'objet d'un contrôle.

  En utilisant cette stratégie, aucun enregistrement relatif au processus de configuration n'est conservé.
- L'équipe chargée de la configuration initiale remplace le rôle `root` par un utilisateur.

  Aucun enregistrement n'est conservé dans le logiciel du nom de l'utilisateur agissant en tant que `root`. Cette configuration peut être requise pour l'administration à distance d'un écouteur.

La figure suivante illustre la séparation des tâches en fonction des rôles. L'administrateur de sécurité configure notamment le contrôle, protège les systèmes de fichiers, définit la stratégie en matière de périphériques, détermine les programmes nécessitant des privilèges pour leur bonne exécution et protège les utilisateurs. L'administrateur système partage et monte les systèmes de fichiers, installe les packages de logiciels et crée des utilisateurs, entre autres tâches.

FIGURE 1–1 Administration d'un système Trusted Extensions : séparation des tâches en fonction du rôle de l'utilisateur



Résolution d'autres problèmes avant d'activer Trusted Extensions

Avant de configurer Trusted Extensions, vous devez protéger physiquement vos systèmes, déterminer les étiquettes à affecter aux zones et résoudre d'autres problèmes de sécurité. Pour plus d'informations sur les procédures, reportez-vous à la section "Résolution des problèmes de sécurité avant l'activation de Trusted Extensions" à la page 46.

Sauvegarde du système avant l'activation de Trusted Extensions

Si votre système contient des fichiers devant être enregistrés, effectuez une sauvegarde avant d'activer le service Trusted Extensions. La manière la plus sûre de sauvegarder des fichiers est

d'effectuer un vidage de niveau 0. Si aucune procédure de sauvegarde n'est en place, reportez-vous au guide de l'administrateur de votre système d'exploitation pour plus d'instructions.

Résultats de l'activation de Trusted Extensions du point de vue de l'administrateur

Une fois le logiciel Trusted Extensions activé et le système réinitialisé, les fonctions de sécurité suivantes sont en place. De nombreuses fonctions peuvent être configurées par l'administrateur de sécurité.

- Un fichier label_encodings Oracle est installé et configuré.
- Un ordinateur de confiance Solaris Trusted Extensions (GNOME) crée un environnement multifenêtre étiqueté qui fournit les espaces de travail d'administration de la zone globale. Ces espaces de travail sont protégés par le chemin de confiance, visible dans la bande de confiance.
- Comme dans le SE Oracle Solaris, des profils de droits pour les rôles sont définis. Comme dans le SE Oracle Solaris, `root` est le seul rôle défini.

  Pour utiliser des rôles supplémentaires dans l'administration de Trusted Extensions, vous devez créer ces rôles. Lors de la configuration, vous devez créer le rôle d'administrateur de sécurité.
- Trois bases de données réseau Trusted Extensions, `tnrhdb`, `tnrhtp` et `tnzonecfg` sont ajoutées. La commande `tncfg` permet aux administrateurs de visualiser et de modifier ces bases de données de confiance.
- Trusted Extensions fournit des interfaces graphiques pour administrer le système. Pour consulter la liste complète, reportez-vous au Chapitre 7, “Outils d'administration de Trusted Extensions”.
  - Le script `txzonemgr` permet aux administrateurs de configurer les zones et le réseau Trusted Extensions. Pour plus d'informations, reportez-vous à la page de manuel `txzonemgr(1M)`.
  - Le Device Manager (Gestionnaire de périphériques) gère l'allocation et l'étiquetage des périphériques connectés.

◆ ◆ ◆ CHAPITRE 2

Déroulement de la configuration de Trusted Extensions

Ce chapitre décrit les tâches d'activation et de configuration du logiciel Trusted Extensions d'Oracle Solaris.

Attention – Pour une activation et une configuration à distance de Trusted Extensions, lisez attentivement le Chapitre 12, "Administration à distance dans Trusted Extensions (tâches)" avant de procéder à l'initialisation dans l'environnement Trusted Extensions.

Liste des tâches : préparation et activation de Trusted Extensions

Pour préparer votre système et activer Trusted Extensions, effectuez les tâches suivantes.

Tâche	Voir
■ Préparation d'une installation Oracle Solaris existante pour Trusted Extensions ■ Installez le SE Oracle Solaris en gardant Trusted Extensions à l'esprit.	■ "Préparation d'un système Oracle Solaris installé pour Trusted Extensions" à la page 45 ■ "Installation d'Oracle Solaris en toute sécurité" à la page 44
Collecte d'informations et prise de décisions concernant votre système et votre réseau Trusted Extensions.	"Résolution des problèmes de sécurité avant l'activation de Trusted Extensions" à la page 46
Activation de Trusted Extensions.	"Activation de Trusted Extensions et réinitialisation" à la page 49

Liste des tâches : choix d'une configuration Trusted Extensions

Configuration de Trusted Extensions sur votre système à l'aide de l'une des méthodes de la liste des tâches suivante.

Tâche	Voir
Création d'un système Trusted Extensions de démonstration	"Liste des tâches : configuration de Trusted Extensions avec les valeurs par défaut fournies" à la page 40
Création d'un système Trusted Extensions d'entreprise	"Liste des tâches : configuration de Trusted Extensions pour répondre aux besoins de votre site" à la page 41
Configuration de Trusted Extensions sur un système distant.	Activez Trusted Extensions sans réinitialiser le système. Suivez les instructions décrites au Chapitre 12, "Administration à distance dans Trusted Extensions (tâches)". Continuez ensuite à l'aide des instructions relatives aux systèmes avec moniteur.

Liste des tâches : configuration de Trusted Extensions avec les valeurs par défaut fournies

Pour une configuration par défaut, effectuez les tâches suivantes dans l'ordre indiqué.

Tâche	Voir
Chargement des packages Trusted Extensions	"Ajout de packages Trusted Extensions à un système Oracle Solaris" à la page 45
Activation de Trusted Extensions et réinitialisation	"Activation de Trusted Extensions et réinitialisation" à la page 49
Ouverture d'une session.	"Connexion à Trusted Extensions" à la page 50
Création de deux zones étiquetées	"Procédure de création d'un système Trusted Extensions par défaut" à la page 58 Ou, "Procédure interactive de création de zones étiquetées" à la page 59
Création d'espaces de travail étiquetés pour les zones	"Procédure d'affectation d'étiquettes à deux espaces de travail comportant des zones" à la page 61

Liste des tâches : configuration de Trusted Extensions pour répondre aux besoins de votre site

Astuce – Pour un processus de configuration sécurisé, créez des rôles au tout début du processus.

L'ordre des tâches est affiché dans la liste des tâches ci-dessous.

- Les tâches de la section "Création de zones étiquetées" à la page 58 sont obligatoires.
- En fonction des besoins de votre site, effectuez des tâches de configuration supplémentaires.

Tâche	Voir
Configuration de la zone globale	"Configuration de la zone globale dans Trusted Extensions" à la page 53
Configuration des zones étiquetées	"Création de zones étiquetées" à la page 58
Configuration de la mise en réseau en vue de la communication avec d'autres systèmes	"Configuration des interfaces réseau dans Trusted Extensions" à la page 63
Configuration du service de nommage LDAP **Remarque –** Ignorez cette tâche si vous n'utilisez pas LDAP.	Chapitre 5, "Configuration de LDAP pour Trusted Extensions (tâches)"
Configuration complète du système	Partie II

◆ ◆ ◆ CHAPITRE 3

Ajout de la fonction Trusted Extensions à Oracle Solaris (tâches)

Ce chapitre explique comment préparer et activer le service Trusted Extensions sur un système Oracle Solaris. Ce chapitre comprend les sections suivantes :

Responsabilités de l'équipe chargée de la configuration initiale

Le logiciel Trusted Extensions est conçu pour être configuré par deux personnes possédant des responsabilités distinctes. Cette division des tâches peut être effectuée par les rôles. Les rôles discrets et les utilisateurs supplémentaires ne sont créés qu'après l'installation, c'est pourquoi il est recommandé de confier l'activation et la configuration du logiciel Trusted Extensions à une équipe chargée de la configuration initiale composée d'au moins deux personnes.

Préparation d'un système Oracle Solaris et ajout de Trusted Extensions

Le choix des options d'installation d'Oracle Solaris peut avoir une incidence sur l'utilisation et la sécurité de Trusted Extensions :

- Pour une bonne prise en charge de Trusted Extensions, vous devez installer le SE Oracle Solaris sous-jacent de façon sécurisée. Pour connaître les choix d'installation d'Oracle Solaris qui affectent Trusted Extensions, reportez-vous à la section "Installation d'Oracle Solaris en toute sécurité" à la page 44.
- Si vous utilisiez le SE Oracle Solaris, vérifiez votre configuration actuelle par rapport à la configuration requise de Trusted Extensions. Pour connaître les facteurs qui affectent Trusted Extensions, reportez-vous à la section "Préparation d'un système Oracle Solaris installé pour Trusted Extensions" à la page 45.

▼ Installation d'Oracle Solaris en toute sécurité

Cette tâche s'applique aux nouvelles installations d'Oracle Solaris. Si vous procédez à une mise à niveau, reportez-vous à la section "Préparation d'un système Oracle Solaris installé pour Trusted Extensions" à la page 45.

1 Lors de l'installation du SE Oracle Solaris, créez un compte utilisateur et le compte du rôle `root`.

Dans Trusted Extensions, vous utilisez le rôle `root` ainsi que les rôles que vous créez, afin de configurer le système.

2 Lorsque vous vous connectez pour la première fois à Oracle Solaris, attribuez un mot de passe au compte du rôle `root`.

a. Ouvrez une fenêtre de terminal.

b. Assumez le rôle root.

A l'invite, entrez un mot de passe différent de celui de votre compte utilisateur.

```
% su -
Your password has expired. Create a new password.
Enter new password:      Type a password for root
Retype the password:      Retype the root password
#
```

Affectez un mot de passe d'au moins six caractères alphanumériques. Le mot de passe doit être difficile à deviner, afin de réduire les risques d'accès non autorisé par un tiers qui tenterait de deviner les mots de passe.

Étapes suivantes Poursuivez à la section "Ajout de packages Trusted Extensions à un système Oracle Solaris" à la page 45.

▼ Préparation d'un système Oracle Solaris installé pour Trusted Extensions

Cette tâche s'applique aux systèmes Oracle Solaris existants et sur lesquels vous prévoyez d'exécuter Trusted Extensions.

Avant de commencer Vous devez être dans le rôle `root` dans la zone globale.

1 **Si des zones non globales sont installées sur votre système, supprimez-les.**

La marque étiquetée Trusted Extensions est une marque de zones exclusive. Reportez-vous à la page de manuel `brands(5)` et `trusted_extensions(5)`.

2 **Si votre système n'a pas de mot de passe root, créez-en un.**

Remarque – Les utilisateurs ne doivent en aucun cas divulguer leurs mots de passe à des tiers, car ceux-ci pourraient alors avoir accès aux données de l'utilisateur et ne seront alors pas identifiés de manière unique ou fiable. Cette divulgation peut être directe, si l'utilisateur donne délibérément son mot de passe à une autre personne, ou indirecte, par exemple si l'utilisateur l'écrit ou choisit un mot de passe non sécurisé. Oracle Solaris fournit une protection contre les mots de passe non sécurisés, mais ne peut pas empêcher un utilisateur de divulguer son mot de passe ni de l'écrire.

Étapes suivantes Poursuivez à la section "Ajout de packages Trusted Extensions à un système Oracle Solaris" à la page 45.

▼ Ajout de packages Trusted Extensions à un système Oracle Solaris

Avant de commencer Vous avez terminé les tâches de la section "Préparation d'un système Oracle Solaris installé pour Trusted Extensions" à la page 45 ou de la section "Installation d'Oracle Solaris en toute sécurité" à la page 44.

Le profil de droits Software Installation (Installation de logiciels) doit vous avoir été attribué.

1. **Une fois que vous êtes connecté en tant qu'utilisateur initial, assumez le rôle `root` dans une fenêtre de terminal.**

   ```
   % su -
   Enter Password:      Type root password
   #
   ```

2. **Téléchargez et installez le package Trusted Extensions.**

   Utilisez la ligne de commande ou l'interface graphique du gestionnaire de packages (Package Manager).

   - **Dans la fenêtre de terminal, utilisez la commande `pkg install`.**

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

     Pour installer des environnements linguistiques de confiance, spécifiez le nom abrégé de l'environnement linguistique. Par exemple, la commande suivante installe l'environnement linguistique en japonais :

     ```
     $ pkg install system/trusted/locale/ja &
     ```

   - **Dans la fenêtre de terminal, démarrez l'interface graphique du gestionnaire de packages.**

     ```
     $ packagemanager &
     ```

     a. **Sélectionnez les packages Trusted Extensions.**

        i. **Affichez les catégories dans la catégorie (GNOME) du bureau.**

        ii. **Sélectionnez la catégorie Trusted Extensions.**

        iii. **Dans la liste des packages, cliquez sur la case à cocher pour trusted-extensions.**

        iv. **(Facultatif) Dans la liste des packages, cliquez sur la case à cocher pour chacun des environnements linguistiques que vous souhaitez installer.**

     b. **Pour ajouter des packages, cliquez sur l'icône Installation/Mise à jour.**

Résolution des problèmes de sécurité avant l'activation de Trusted Extensions

Pour chaque système sur lequel Trusted Extensions sera configuré, vous devez effectuer certaines décisions en matière de configuration. Par exemple, vous devez décider si vous souhaitez installer la configuration Trusted Extensions par défaut ou personnaliser votre configuration.

▼ Sécurisation du matériel du système et prises de décision relatives à la sécurité avant l'activation de Trusted Extensions

Pour chaque système sur lequel Trusted Extensions va être configuré, prenez ces décisions en matière de configuration avant d'activer le logiciel.

1 **Décidez du niveau de sécurité de la protection du matériel du système.**

Au niveau d'un site sécurisé, cette étape est effectuée sur chaque système Oracle Solaris.

- Pour les systèmes SPARC, choisissez un niveau de sécurité PROM et fournissez un mot de passe.
- Pour les systèmes x86, protégez le BIOS.
- Sur tous les systèmes, protégez `root` à l'aide d'un mot de passe.

2 **Préparez votre fichier `label_encodings`.**

Si vous disposez d'un fichier `label_encodings` spécifique au site, vous devez le contrôler et l'installer avant de commencer toute autre tâche de configuration. Si votre site n'a pas de fichier `label_encodings`, vous pouvez utiliser le fichier par défaut fourni par Oracle. Oracle fournit également d'autres fichiers `label_encodings`, que vous pouvez trouver dans le répertoire `/etc/security/tsol`. Les fichiers Oracle sont des fichiers de démonstration. Ils risquent de ne pas être adaptés aux systèmes de production.

Pour personnaliser un fichier pour votre site, reportez-vous à la section *Trusted Extensions Label Administration*.

3 **À partir de la liste d'étiquettes dans votre fichier `label_encodings`, créez une liste des zones étiquetées que vous devez créer.**

Pour le fichier `label_encodings` par défaut, les étiquettes sont les suivantes et les noms de zones peuvent être similaires à ce qui suit :

Nom complet de l'étiquette	Nom de la zone proposée
`PUBLIC`	`public`
`CONFIDENTIAL: INTERNAL USE ONLY`	`internal`
`CONFIDENTIAL : NEED TO KNOW`	`needtoknow`
`CONFIDENTIAL : RESTRICTED`	`restricted`

Remarque – La méthode de configuration automatique crée les zones `public` et `internal`.

4 **Décidez quand créer les rôles.**

La stratégie de sécurité de votre site peut nécessiter que vous administriez Trusted Extensions en assumant un rôle. Si c'est le cas ou si vous êtes en train de configurer le système afin de satisfaire aux critères d'une configuration évaluée, vous devez créer des rôles très tôt au cours du processus de configuration.

Si vous n'êtes pas obligé de configurer le système en utilisant des rôles discrets, vous pouvez choisir de configurer le système dans le rôle `root`. Cette méthode de configuration est moins sûre. Le rôle `root` peut effectuer toutes les tâches sur le système, tandis que d'autres rôles exécutent généralement un ensemble plus limité de tâches. Par conséquent, la configuration est davantage contrôlée lorsqu'elle est effectuée par les rôles que vous créez.

5 **Décidez d'autres questions de sécurité pour chaque système et pour le réseau.**

Par exemple, vous pouvez être amené à prendre en compte les problèmes de sécurité suivants :

- Déterminez les périphériques qui peuvent être connectés au système et alloués pour utilisation.
- Identifiez les imprimantes dont les étiquettes sont accessibles à partir du système.
- Identifiez les systèmes qui ont une plage d'étiquettes limitée, tel qu'un système de passerelle ou un kiosque public.
- Identifiez les systèmes étiquetés pouvant communiquer avec des systèmes non étiquetés particuliers.

Activation du service Trusted Extensions et connexion

Dans le SE Oracle Solaris, Trusted Extensions est un service géré par l'utilitaire de gestion des services (SMF). Le nom du service est `svc:/system/labeld:default` . Par défaut, le service `labeld` est désactivé.

Remarque – Le système Trusted Extensions ne nécessite pas l'exécution par un réseau d'un bureau avec un affichage directement connecté, tel qu'un ordinateur portable ou une station de travail. La configuration du réseau est nécessaire pour communiquer avec d'autres systèmes.

▼ Activation de Trusted Extensions et réinitialisation

Le service `labeld` attache des étiquettes aux points d'extrémité de communications. Par exemple, les éléments suivants sont étiquetés :

- Toutes les zones et tous les répertoires et fichiers au sein de chaque zone
- Tous les processus, y compris les processus de fenêtrage
- Toutes les communications réseau

Avant de commencer

Vous avez terminé les tâches des sections "Préparation d'un système Oracle Solaris et ajout de Trusted Extensions " à la page 44 et "Résolution des problèmes de sécurité avant l'activation de Trusted Extensions" à la page 46.

Vous devez être dans le rôle `root` dans la zone globale.

1 Déplacez le panneau du haut de l'écran vers le bas de l'écran.

Attention – Si vous ne parvenez pas à déplacer le panneau, vous ne pourrez peut-être pas atteindre le menu principal ou les panneaux du bureau lorsque vous vous connecterez à Trusted Extensions.

a. Dans le panneau supérieur, cliquez avec le bouton droit de la souris et sélectionnez Properties (Propriétés).

b. Modifiez l'orientation du panneau supérieur vers le bas.

2 Ouvrez une fenêtre de terminal et activez le service `labeled`.

```
# svcadm enable -s labeld
```

Le service `labeled` ajoute des étiquettes au système et démarre les services d'allocation de périphériques.

Attention – N'effectuez pas d'autres tâches sur le système jusqu'à ce que le curseur revienne à l'invite.

3 Vérifiez que le service est activé.

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

Attention – Pour une activation et une configuration à distance de Trusted Extensions, lisez attentivement le Chapitre 12, "Administration à distance dans Trusted Extensions (tâches)". Ne réinitialisez pas le système avant de l'avoir configuré pour autoriser l'administration à distance. Si vous ne configurez pas le système Trusted Extensions pour l'administration à distance, il vous sera impossible d'atteindre un système distant.

4 **Réinitialisez le système.**

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

Étapes suivantes Poursuivez à la section "Connexion à Trusted Extensions" à la page 50.

▼ Connexion à Trusted Extensions

Une fois connecté, vous accédez à la zone globale, qui est un environnement qui reconnaît et applique le contrôle d'accès obligatoire.

Sur la plupart des sites, deux administrateurs ou plus constituent l'équipe chargée de la configuration initiale et sont présents lors de la configuration du système.

Avant de commencer Vous avez terminé les tâches de la section "Activation de Trusted Extensions et réinitialisation" à la page 49.

1 **Connectez-vous à l'aide du compte utilisateur que vous avez créé au cours de l'installation.**

Dans la boîte de dialogue de connexion, tapez *username*, puis saisissez le mot de passe.

Les utilisateurs ne doivent en aucun cas divulguer leurs mots de passe à des tiers, car ceux-ci pourraient alors avoir accès aux données de l'utilisateur et ne seront alors pas identifiés de manière unique ou fiable. La divulgation peut être directe, si l'utilisateur donne délibérément son mot de passe à une autre personne, ou indirecte, par exemple si l'utilisateur l'écrit ou choisit un mot de passe non sécurisé. Trusted Extensions fournit une protection contre les mots de passe non sécurisés, mais ne peut pas empêcher un utilisateur de divulguer son mot de passe ni de l'écrire.

2 **Utilisez la souris pour fermer la fenêtre d'état et la fenêtre d'autorisation.**

3 **Fermez la boîte de dialogue indiquant que l'étiquette `PUBLIC` ne correspond à aucune zone.**

Vous allez créer la zone après avoir assumé le rôle `root`.

4 **Assumez le rôle `root`.**

a. **Cliquez sur votre nom dans la bande de confiance.**

Le rôle `root` s'affiche dans un menu déroulant.

b. Sélectionnez le rôle `root`.

Si vous y êtes invité, créez un mot de passe pour le rôle.

Remarque – Vous devez vous déconnecter ou verrouiller l'écran avant de laisser un système sans surveillance. Sinon, n'importe qui peut accéder au système sans aucune identification ni authentification, et cette personne ne pourrait pas être identifiée de manière unique ou fiable.

Étapes suivantes Continuez à l'une des étapes suivantes :

- Pour configurer un système par défaut, reportez-vous à la section "Création de zones étiquetées" à la page 58
- Pour personnaliser votre système avant de créer des zones étiquetées, reportez-vous à la section "Configuration de la zone globale dans Trusted Extensions" à la page 53.
- Si votre système ne dispose pas d'affichage graphique, passez au Chapitre 12, "Administration à distance dans Trusted Extensions (tâches)".

◆ ◆ ◆ CHAPITRE 4

Configuration de Trusted Extensions (tâches)

Ce chapitre présente la configuration de Trusted Extensions sur un système avec un moniteur. Pour fonctionner correctement, le logiciel Trusted Extensions requiert la configuration d'étiquettes et de zones. Vous pouvez aussi configurer des communications réseau, des rôles et des utilisateurs pouvant assumer des rôles.

Pour d'autres tâches de configuration, reportez-vous à la Partie II.

Configuration de la zone globale dans Trusted Extensions

Pour personnaliser la configuration de Trusted Extensions, effectuez les procédures décrites dans la liste des tâches ci-dessous. Pour installer la configuration par défaut, reportez-vous à la section "Création de zones étiquetées" à la page 58.

Tâche	Description	Voir
Protection du matériel	Protège le matériel en exigeant un mot de passe pour toute modification de paramètres matériels.	"Contrôle de l'accès au matériel du système (tâches)" du manuel *Administration d'Oracle Solaris : services de sécurité*
Configuration des étiquettes	Des étiquettes *doivent* être configurées pour votre site. Si vous envisagez d'utiliser le fichier `label_encodings` par défaut, vous pouvez ignorer cette étape.	"Procédure de vérification et d'installation du fichier Label Encodings" à la page 54
Activation d'un réseau IPv6	Permet à IP de reconnaître les paquets étiquetés sur un réseau IPv6.	"Procédure d'activation du réseau IPv6 dans Trusted Extensions" à la page 56

Tâche	Description	Voir
Modification du DOI	Spécifie un domaine d'interprétation (DOI) qui n'est pas 1.	"Procédure de configuration du domaine d'interpretation" à la page 57
Configuration du serveur LDAP	Configure un serveur d'annuaire LDAP Trusted Extensions.	Chapitre 5, "Configuration de LDAP pour Trusted Extensions (tâches)"
Configuration de clients LDAP	Fait de ce système un client du serveur d'annuaire LDAP de Trusted Extensions.	"Établissement de la zone globale en tant que client LDAP dans Trusted Extensions" à la page 96

▼ Procédure de vérification et d'installation du fichier Label Encodings

Votre fichier de codage doit être compatible avec l'hôte Trusted Extensions avec lequel vous communiquez.

Remarque – Trusted Extensions installe un fichier `label_encodings` par défaut. Ce fichier par défaut est utile pour les démonstrations. Toutefois, ce fichier peut ne pas être le bon choix pour votre utilisation particulière. Si vous prévoyez d'utiliser le fichier par défaut, vous pouvez ignorer cette procédure.

- Si vous êtes déjà familiarisé avec les fichiers de codage, vous pouvez utiliser la procédure suivante.
- Si vous n'êtes pas familiarisé avec les fichiers de codage, consultez la section *Trusted Extensions Label Administration* pour connaître la configuration requise, les procédures et des exemples.

Attention – Vous *devez* installer les étiquettes avant de poursuivre ou la configuration échouera.

Avant de commencer Vous êtes l'administrateur de sécurité. L'administrateur de sécurité est responsable de la modification, la vérification et la maintenance du fichier `label_encodings`. Si vous prévoyez de modifier le fichier `label_encodings`, assurez-vous que le fichier lui-même est accessible en écriture. Pour plus d'informations, reportez-vous à la page de manuel `label_encodings(4)`.

Pour modifier le fichier `label_encodings`, vous devez être dans le rôle `root`.

1 Copiez le fichier `label_encodings` sur le disque.

Pour copier à partir d'un média amovible, reportez-vous à la section "Copie de fichiers dans Trusted Extensions à partir d'un média amovible" à la page 82.

2. **Dans une fenêtre de terminal, vérifiez la syntaxe du fichier.**

   a. **Exécutez la commande `chk_encodings`.**

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

   b. **Lisez la sortie et effectuez l'une des opérations suivantes :**

      - **Résolvez les erreurs.**

        Si la commande signale la présence d'erreurs, celles-ci *doivent* être résolues avant de continuer. Pour obtenir de l'aide, reportez-vous au Chapitre 3, “Creating a Label Encodings File (Tasks)” du manuel *Trusted Extensions Label Administration*

      - **Faites du fichier le fichier `label_encodings` actif.**

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

Attention – Votre fichier `label_encodings` *doit* réussir le test de vérification du fichier de codage (Check Encodings) avant de pouvoir continuer.

Exemple 4–1 Vérification de la syntaxe label_encodings sur la ligne de commande

Dans cet exemple, l'administrateur teste plusieurs fichiers `label_encodings` à l'aide de la ligne de commande.

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

Lorsque la direction décide d'utiliser le fichier `label_encodings2`, l'administrateur exécute une analyse sémantique du fichier.

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

---> VERSION = MYCOMPANY LABEL ENCODINGS  2.0 10/10/2010

---> CLASSIFICATIONS <---

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

---> COMPARTMENTS AND MARKINGS USAGE ANALYSIS <---
...
```

```
---> SENSITIVITY LABEL to COLOR MAPPING <---
...
```

L'administrateur imprime une copie de l'analyse sémantique pour ses archives, puis déplace le fichier dans le répertoire `/etc/security/tsol`.

```
# cp /var/encodings/label_encodings2 /etc/security/tsol/label.encodings.10.10.10
# cd /etc/security/tsol
# cp label_encodings label_encodings.tx.orig
# cp label.encodings.10.10.10 label_encodings
```

Enfin, l'administrateur vérifie que le fichier `label_encodings` est le fichier de l'entreprise.

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

---> VERSION = MYCOMPANY LABEL ENCODINGS  2.0 10/10/2010
```

Étapes suivantes Vous devez réinitialiser le système avant de créer des zones étiquetées.

▼ Procédure d'activation du réseau IPv6 dans Trusted Extensions

Attention – Le script `txzonemgr` ne prend pas en charge la syntaxe d'adresse IPv6. Par conséquent, vous pouvez utiliser la commande `tncfg` pour ajouter des hôtes IPv6 à votre réseau Trusted Extensions. Pour obtenir des exemples, reportez-vous à la section "Mécanisme de secours du réseau de confiance" à la page 209 et à l'Exemple 16–11.

Les options CIPSO n'ont pas de numéro IANA (Internet Assigned Numbers Authority) à utiliser dans le champ de type d'option IPv6 d'un paquet. L'entrée que vous avez définie au cours de cette procédure fournit un numéro à utiliser sur le réseau local jusqu'à ce que l'IANA affecte un numéro pour cette option. Trusted Extensions désactive le réseau IPv6 si ce numéro n'est pas défini.

Pour activer un réseau IPv6 dans Trusted Extensions, vous devez ajouter une entrée dans le fichier `/etc/system`.

Avant de commencer Vous êtes dans le rôle `root` dans la zone globale.

- **Saisissez l'entrée suivante dans le fichier `/etc/system` :**

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

Erreurs fréquentes

- Si des messages d'erreur au cours de l'initialisation indiquent que votre configuration IPv6 est incorrecte, corrigez l'entrée :

- Vérifiez que l'entrée est correctement orthographiée.
- Vérifiez que le système a été réinitialisé après l'ajout de l'entrée correcte au fichier `/etc/system`.

- Si vous installez Trusted Extensions sur un système Oracle Solaris sur lequel IPv6 est actuellement activé, mais vous échouez à ajouter l'entrée IP dans le fichier `/etc/system`, le message d'erreur suivant s'affiche : `t_optmgmt: System error: Cannot assign requested address` *time-stamp*

Étapes suivantes Vous devez réinitialiser le système avant de créer des zones étiquetées.

▼ Procédure de configuration du domaine d'interpretation

Toutes les communications vers et à partir d'un système configuré avec Trusted Extensions doivent respecter les règles d'étiquetage d'un seul domaine d'interprétation (DOI) CIPSO. Le DOI utilisé dans chaque message est identifié par un nombre entier dans l'en-tête d'option IP CIPSO. Par défaut, le DOI dans Trusted Extensions est `1`.

Si votre site n'utilise pas un DOI égal à `1`, vous devez modifier la valeur du `doi` dans chaque modèle de sécurité.

Avant de commencer Vous êtes dans le rôle `root` dans la zone globale.

- **Indiquez votre valeur de DOI dans les modèles de sécurité par défaut.**

```
# tncfg -t cipso set doi=n
# tncfg -t admin_low set doi=n
```

Remarque – Chaque modèle de sécurité doit indiquer votre valeur de DOI.

Voir aussi
- “Attributs de sécurité réseau dans Trusted Extensions” à la page 206
- “Procédure de création de modèles de sécurité” à la page 227

Étapes suivantes Si vous avez l'intention d'utiliser LDAP, reportez-vous au Chapitre 5, “Configuration de LDAP pour Trusted Extensions (tâches)”. Vous devez configurer LDAP avant de créer des zones étiquetées.

Sinon, poursuivez avec “Création de zones étiquetées” à la page 58.

Création de zones étiquetées

Les instructions de cette section configurent des zones étiquetées. Vous avez la possibilité de créer deux zones étiquetées de manière automatique ou de créer des zones manuellement.

Remarque – Si vous avez l'intention d'utiliser LDAP, reportez-vous au Chapitre 5, "Configuration de LDAP pour Trusted Extensions (tâches)". Vous devez configurer LDAP avant de créer des zones étiquetées.

Tâche	Description	Voir
1a. Création d'un système Trusted Extensions par défaut	La commande `txzonemgr -c` crée deux zones étiquetées à partir du fichier `label_encodings`.	"Procédure de création d'un système Trusted Extensions par défaut" à la page 58
1b. Création d'une configuration Trusted Extensions par défaut à l'aide d'une interface utilisateur graphique	Le script `txzonemgr` crée une interface utilisateur graphique qui présente les tâches appropriées lors de la configuration du système.	"Procédure interactive de création de zones étiquetées" à la page 59
1c. Réalisation manuelle des étapes de la création de zones	Le script `txzonemgr` crée une interface utilisateur graphique qui présente les tâches appropriées lors de la configuration du système.	"Procédure interactive de création de zones étiquetées" à la page 59
2. Création d'un environnement étiqueté opérationnel	Dans la configuration par défaut, appliquez les étiquettes `PUBLIC` et `INTERNAL USE ONLY` à deux espaces de travail.	"Procédure d'affectation d'étiquettes à deux espaces de travail comportant des zones" à la page 61
3. (Facultatif) Lien vers d'autres systèmes sur votre réseau	Configurez des interfaces réseau de zone étiquetée et connectez la zone globale et les zones étiquetées à d'autres systèmes.	"Configuration des interfaces réseau dans Trusted Extensions" à la page 63

▼ Procédure de création d'un système Trusted Extensions par défaut

Cette procédure crée un système Trusted Extensions opérationnel comportant deux zones étiquetées. Aucun hôte distant n'a été affecté aux modèles de sécurité du système, si bien que ce système ne peut pas communiquer avec des hôtes distants.

Avant de commencer Vous avez effectué l'étape "Connexion à Trusted Extensions" à la page 50. Vous avez assumé le rôle `root`.

1 Ouvrez une fenêtre de terminal dans le quatrième espace de travail.

2 **(Facultatif) Consultez la page de manuel `txzonemgr`.**

```
# man txzonemgr
```

3 **Créez une configuration par défaut.**

```
# /usr/sbin/txzonemgr -c
```

Cette commande copie le SE Oracle Solaris et le logiciel Trusted Extensions dans une zone, crée un instantané de la zone, applique une étiquette à la zone originale, puis utilise l'instantané pour créer une seconde zone étiquetée. Les zones sont initialisées.

- La première zone étiquetée est basée sur la valeur `Default User Sensitivity Label` du fichier `label_encodings`.
- La deuxième zone étiquetée est basée sur la valeur `Default User Clearance` du fichier `label_encodings`.

Cette étape peut prendre environ 20 minutes. Pour installer les zones, le script utilise pour les zones étiquetées le mot de passe root de la zone globale.

Étapes suivantes Pour utiliser votre configuration Trusted Extensions, passez à l'étape "Procédure d'affectation d'étiquettes à deux espaces de travail comportant des zones" à la page 61.

▼ Procédure interactive de création de zones étiquetées

Vous n'êtes pas obligé de créer une zone pour chaque étiquette de votre fichier `label_encodings`, mais vous pouvez le faire. Les interfaces utilisateur graphiques d'administration énumèrent les étiquettes pour lesquelles des zones peuvent être créées sur ce système. Au cours de cette procédure, vous créez deux zones étiquetées. Si vous utilisez le fichier `label_encodings` de Trusted Extensions, vous créez la configuration Trusted Extensions par défaut.

Avant de commencer Vous avez effectué l'étape "Connexion à Trusted Extensions" à la page 50. Vous avez assumé le rôle `root`.

Vous n'avez pas encore créé de zone.

1 **Exécutez la commande `txzonemgr` sans aucune option.**

```
# txzonemgr &
```

Le script ouvre la boîte de dialogue `Labeled Zone Manager` (Gestionnaire de zones étiquetées). Cette boîte de dialogue `zenity` vous invite à effectuer les tâches appropriées, selon l'état actuel de votre configuration.

Pour exécuter une tâche, sélectionnez l'option de menu, puis appuyez sur la touche Entrée ou cliquez sur OK. Lorsque vous êtes invité à saisir du texte, saisissez-le, puis appuyez sur la touche Entrée ou cliquez sur OK.

Astuce – Pour afficher l'état actuel d'achèvement de la zone, cliquez sur Return to Main Menu (Retourner au menu principal) dans le gestionnaire de zones étiquetées. Vous pouvez également cliquer sur le bouton Cancel (Annuler).

2 Installez les zones en choisissant l'une des méthodes suivantes :

- **Pour créer deux zones étiquetées, sélectionnez `public and internal zones` (zones publiques et internes) dans la boîte de dialogue.**
  - La première zone étiquetée est basée sur la valeur `Default User Sensitivity Label` du fichier `label_encodings`.
  - La deuxième zone étiquetée est basée sur la valeur `Default User Clearance` du fichier `label_encodings`.

  a. Répondez à l'invite pour identifier le système.

  Si la zone `public` utilise une pile IP exclusive ou si elle a une adresse IP définie dans le DNS, utilisez le nom d'hôte tel que défini dans le DNS. Dans le cas contraire, utilisez le nom du système.

  b. Ne répondez pas à l'invite de saisie de mot de passe root.

  Le mot de passe root a été défini à l'installation du système. Toute réponse à cette invite échouera.

  c. À l'invite de connexion à la zone, entrez votre nom de connexion et votre mot de passe utilisateur.

  Vérifiez ensuite que tous les services sont configurés en exécutant la commande `svcs -x`. Si aucun message ne s'affiche, tous les services sont configurés.

  d. Déconnectez-vous de la zone et fermez la fenêtre.

  Entrez exit à l'invite, puis choisissez Close window (Fermer la fenêtre) dans la console de la zone.

  Dans une autre fenêtre, l'installation de la deuxième zone se termine. Cette zone est construite à partir d'un instantané, si bien qu'elle se construit rapidement.

  e. Connectez-vous à la console de la seconde zone et vérifiez que tous les services sont en cours d'exécution.

  ```
  # svcs -x
  #
  ```

  Si aucun message ne s'affiche, tous les services sont configurés. Le gestionnaire de zones étiquetées s'affiche.

f. Double-cliquez sur la zone interne dans le gestionnaire de zones étiquetées.

Sélectionnez Reboot (Réinitialiser), puis cliquez sur le bouton Cancel (Annuler) pour revenir à l'écran principal. Toutes les zones sont en cours d'exécution. L'instantané non étiqueté n'est pas en cours d'exécution.

- **Pour créer des zones manuellement, sélectionnez Main Menu (Menu principal), puis Create a zone (Créer une zone).**

  Suivez les invites à l'écran. L'interface utilisateur graphique vous guide étape par étape au cours de la création d'une zone.

  Une fois la zone créée et initialisée, vous pouvez revenir à la zone globale pour créer d'autres zones. Ces zones sont créées à partir d'un instantané.

Exemple 4–2 Création d'une autre zone étiquetée

Dans cet exemple, l'administrateur crée une zone restreinte à partir du fichier `label_encodings` par défaut.

Pour commencer, l'administrateur ouvre le script `txzonemgr` en mode interactif.

```
# txzonemgr &
```

Il accède ensuite à la zone globale et crée une zone portant le nom `restricted` (restreinte).

```
Create a new zone:restricted
```

Puis il applique l'étiquette appropriée.

```
Select label:CNF : RESTRICTED
```

L'administrateur sélectionne l'option Clone dans la liste, puis il sélectionne `snapshot` (instantané) en tant que modèle pour la nouvelle zone.

Une fois que la zone `restricted` est disponible, l'administrateur clique sur Boot (Init) pour initialiser la seconde zone.

Pour activer l'accès à la zone `restricted`, l'administrateur modifie la valeur `Default User Clearance` dans le fichier `label_encodings` et la définit sur `CNF RESTRICTED`.

▼ Procédure d'affectation d'étiquettes à deux espaces de travail comportant des zones

Cette procédure crée deux espaces de travail étiquetés et ouvre une fenêtre étiquetée dans chaque espace de travail étiqueté. Lorsque cette tâche est terminée, vous disposez d'un système Trusted Extensions opérationnel mais non connecté à un réseau.

Avant de commencer

Vous avez effectué l'étape "Procédure de création d'un système Trusted Extensions par défaut" à la page 58 ou l'étape "Procédure interactive de création de zones étiquetées" à la page 59.

Vous êtes l'utilisateur initial.

1. **Créez un espace de travail `PUBLIC`.**

   L'étiquette de l'espace de travail `PUBLIC` à `Default User Sensitivity Label`.

   a. **Passez au deuxième espace de travail.**

   b. **Cliquez avec le bouton droit de la souris et sélectionnez Change Workspace Label (Modifier l'étiquette de l'espace de travail).**

   c. **Sélectionnez PUBLIC et cliquez sur OK.**

2. **Saisissez votre mot de passe lorsque vous y êtes invité.**

   Vous vous trouvez dans un espace de travail `PUBLIC`.

3. **Ouvrez une fenêtre de terminal.**

   La fenêtre est étiquetée `PUBLIC`.

4. **Créez un espace de travail INTERNAL USE ONLY.**

   Si vous utilisez un fichier `label_encodings`, vous créez un espace de travail à partir de la valeur `Default User Clearance`.

   a. **Passez au troisième espace de travail.**

   b. **Cliquez avec le bouton droit de la souris et sélectionnez Change Workspace Label (Modifier l'étiquette de l'espace de travail).**

   c. **Sélectionnez INTERNAL USE ONLY et cliquez sur OK.**

5. **Saisissez votre mot de passe lorsque vous y êtes invité.**

   Vous vous trouvez dans un espace de travail `INTERNAL`.

6. **Ouvrez une fenêtre de terminal.**

   La fenêtre est étiquetée `CONFIDENTIAL : INTERNAL USE ONLY`.

   Votre système est prêt à être utilisé. Vous avez deux espaces de travail d'utilisateur et un espace de travail de rôle. Dans cette configuration, les zones étiquetées utilisent la même adresse IP que la zone globale pour communiquer avec d'autres systèmes. Elles peuvent le faire car, par défaut, elles partagent la même adresse IP en tant qu'interface `all-zones`.

Étapes suivantes Si vous prévoyez de faire communiquer votre système Trusted Extensions avec d'autres systèmes, accédez à "Configuration des interfaces réseau dans Trusted Extensions" à la page 63.

Configuration des interfaces réseau dans Trusted Extensions

Le système Trusted Extensions ne nécessite pas l'exécution par un réseau d'un bureau avec un affichage directement connecté, tel qu'un ordinateur portable ou une station de travail. Toutefois, il est nécessaire de configurer le réseau pour permettre la communication avec d'autres systèmes. L'interface utilisateur graphique `txzonemgr` permet de configurer facilement les zones étiquetées et la zone globale afin de permettre la connexion à d'autres systèmes. Pour une description des options de configuration des zones étiquetées, reportez-vous à la section "Accès aux zones étiquetées" à la page 32. La liste des tâches ci-dessous décrit les tâches de configuration réseau et fournit des liens vers ces tâches.

Tâche	Description	Voir
Configuration d'un système par défaut pour les utilisateurs standard	Le système dispose d'une adresse IP et utilise une interface `all-zones` pour communiquer entre les zones étiquetées et la zone globale. La même adresse IP est utilisée pour communiquer avec des systèmes distants.	"Procédure de partage d'une seule adresse IP entre toutes les zones" à la page 64
Ajout d'une adresse IP à la zone globale	Le système dispose de plusieurs adresses IP et utilise l'adresse IP exclusive de la zone globale pour atteindre un sous-réseau privé. Les zones étiquetées ne peuvent pas atteindre ce sous-réseau.	"Procédure de partage d'une seule adresse IP entre toutes les zones" à la page 64
Attribution d'une adresse IP à chaque zone, où les zones partagent la pile IP	Le système dispose de plusieurs adresses IP. Dans le cas le plus simple, les zones partagent une interface physique.	"Procédure d'ajout d'une instance d'IP à une zone étiquetée" à la page 65
Ajout d'une interface `all-zones` à l'instance IP par zone	Le système peut offrir à ses zones étiquetées des services privilégiés qui sont protégés contre les attaques distantes.	"Procédure d'ajout d'une instance d'IP à une zone étiquetée" à la page 65
Attribution d'une adresse IP à chaque zone, où la pile IP est exclusive.	Une adresse IP est attribuée à chaque zone, y compris à la zone globale. Une carte d'interface réseau virtuelle est créée pour chaque zone étiquetée.	"Procédure d'ajout d'une interface réseau virtuelle à une zone étiquetée" à la page 66
Connexion des zones à des zones distantes	Cette tâche permet de configurer les interfaces réseau des zones étiquetées et la zone globale afin qu'elles atteignent les systèmes distants sous la même étiquette.	"Procédure de connexion d'un système Trusted Extensions à d'autres systèmes Trusted Extensions " à la page 67
Exécution d'un démon `nscd` distinct par zone	Dans un environnement où chaque sous-réseau possède son propre serveur de noms, cette tâche configure un démon `nscd` par zone.	"Procédure de configuration d'un service de noms distinct pour chaque zone étiquetée" à la page 68

▼ Procédure de partage d'une seule adresse IP entre toutes les zones

Cette procédure permet à chaque zone du système d'utiliser une seule adresse IP, à savoir l'adresse IP de la zone globale, pour atteindre d'autres zones ou hôtes possédant la même étiquette. Cette configuration correspond à la configuration par défaut. Vous devez effectuer cette procédure si vous avez configuré différemment les interfaces réseau et que vous voulez rétablir la configuration réseau par défaut du système.

Avant de commencer Vous devez être dans le rôle `root` dans la zone globale.

1. **Exécutez la commande `txzonemgr` sans aucune option.**

   ```
   # txzonemgr &
   ```

   La liste des zones s'affiche dans le gestionnaire de zones étiquetées. Pour plus d'informations sur cette interface utilisateur graphique, reportez-vous à la section "Procédure interactive de création de zones étiquetées" à la page 59.

2. **Double-cliquez sur la zone globale.**

3. **Double-cliquez sur Configure Network Interfaces (Configurer les interfaces réseau).**

   Une liste d'interfaces s'affiche. Recherchez une interface répertoriée présentant les caractéristiques suivantes :

   - Type de `phys`
   - Adresse IP de votre nom d'hôte
   - État de `up`

4. **Sélectionnez l'interface correspondant à votre nom d'hôte.**

5. **Dans la liste des commandes, sélectionnez Share with Shared-IP Zones (Partager avec les zones en mode IP partagé).**

   Toutes les zones peuvent utiliser cette adresse IP partagée pour communiquer avec des systèmes distants possédant la même étiquette qu'elles-mêmes.

6. **Cliquez sur Cancel (Annuler) pour revenir à la liste de commandes des zones.**

Étapes suivantes Pour configurer le réseau externe du système, reportez-vous à la section "Procédure de connexion d'un système Trusted Extensions à d'autres systèmes Trusted Extensions " à la page 67.

▼ Procédure d'ajout d'une instance d'IP à une zone étiquetée

Cette procédure est nécessaire si vous utilisez une pile IP partagée et des adresses par zone, et que vous envisagez de connecter les zones étiquetées à des zones étiquetées sur d'autres systèmes du réseau.

Dans cette procédure, vous créez une instance d'IP, c'est-à-dire une adresse spécifique à la zone, pour une ou plusieurs zones étiquetées. Les zones étiquetées utilisent leur zone par zone pour communiquer avec des zones étiquetées possédant la même étiquette sur le réseau.

Avant de commencer

Vous devez être dans le rôle `root` dans la zone globale.

La liste des zones s'affiche dans le gestionnaire de zones étiquetées. Pour ouvrir cette interface utilisateur graphique, reportez-vous à la section "Procédure interactive de création de zones étiquetées" à la page 59. La zone étiquetée que vous configurez doit être arrêtée.

1. **Dans le gestionnaire de zones étiquetées, double-cliquez sur une zone étiquetée à laquelle vous souhaitez ajouter une instance d'IP.**
2. **Double-cliquez sur Configure Network Interfaces (Configurer les interfaces réseau).**
   Une liste d'options de configuration s'affiche.
3. **Sélectionnez Add an IP instance (Ajouter une instance d'IP).**
4. **Si votre système possède plus d'une adresse IP, choisissez l'entrée correspondant à l'interface souhaitée.**
5. **Fournissez une adresse IP et un nombre de préfixes pour cette zone étiquetée.**
   Par exemple, tapez `192.168.1.2/24`. Si vous n'ajoutez pas le nombre de préfixes, vous êtes invité à spécifier un masque de réseau. Le masque de réseau équivalent pour cet exemple est `255.255.255.0`.
6. **Cliquez sur OK.**
7. **Pour ajouter un routeur par défaut, double-cliquez sur l'entrée que vous venez d'ajouter.**
   À l'invite, entrez l'adresse IP du routeur et cliquez sur OK.

   Remarque – Pour supprimer ou modifier le routeur par défaut, supprimez l'entrée, puis recréez l'instance d'IP.
8. **Cliquez sur Cancel (Annuler) pour revenir à la liste de commandes des zones.**

Étapes suivantes Pour configurer le réseau externe du système, reportez-vous à la section "Procédure de connexion d'un système Trusted Extensions à d'autres systèmes Trusted Extensions " à la page 67.

▼ Procédure d'ajout d'une interface réseau virtuelle à une zone étiquetée

Cette procédure est nécessaire si vous utilisez une pile IP exclusive et des adresses par zone, et que vous souhaitez connecter les zones étiquetées à des zones étiquetées sur d'autres systèmes du réseau.

Dans cette procédure, vous créez une VNIC et vous l'affectez à une zone étiquetée.

Avant de commencer Vous devez être dans le rôle `root` dans la zone globale.

La liste des zones s'affiche dans le gestionnaire de zones étiquetées. Pour ouvrir cette interface utilisateur graphique, reportez-vous à la section "Procédure interactive de création de zones étiquetées" à la page 59. La zone étiquetée que vous configurez doit être arrêtée.

1. **Dans le gestionnaire de zones étiquetées, double-cliquez sur la zone étiquetée à laquelle vous souhaitez ajouter une interface virtuelle.**

2. **Double-cliquez sur Configure Network Interfaces (Configurer les interfaces réseau).**

   Une liste d'options de configuration s'affiche.

3. **Double-cliquez sur Add a virtual interface (VNIC) (Ajouter une interface virtuelle (VNIC)).**

   Si votre système comporte plusieurs cartes VNIC, plusieurs choix s'affichent. Choisissez l'entrée correspondant à l'interface souhaitée.

4. **Affectez un nom d'hôte, ou attribuez une adresse IP et un nombre de préfixes.**

   Par exemple, tapez `192.168.1.2/24`. Si vous n'ajoutez pas le nombre de préfixes, vous êtes invité à spécifier un masque de réseau. Le masque de réseau équivalent pour cet exemple est `255.255.255.0`.

5. **Pour ajouter un routeur par défaut, double-cliquez sur l'entrée que vous venez d'ajouter.**

   À l'invite, entrez l'adresse IP du routeur et cliquez sur OK.

   Remarque – Pour supprimer ou modifier le routeur par défaut, supprimez l'entrée, puis recréez la VNIC.

6. **Cliquez sur Cancel (Annuler) pour revenir à la liste de commandes des zones.**

   L'entrée VNIC s'affiche. Le système attribue le nom *zonename* _*n*, par exemple `internal_0`.

Étapes suivantes Pour configurer le réseau externe du système, reportez-vous à la section "Procédure de connexion d'un système Trusted Extensions à d'autres systèmes Trusted Extensions " à la page 67.

▼ Procédure de connexion d'un système Trusted Extensions à d'autres systèmes Trusted Extensions

Dans cette procédure, vous définissez votre réseau Trusted Extensions en ajoutant des hôtes distants auxquels votre système Trusted Extensions peut se connecter.

Avant de commencer Le gestionnaire de zones étiquetées est affiché. Pour ouvrir cette interface utilisateur graphique, reportez-vous à la section "Procédure interactive de création de zones étiquetées" à la page 59. Vous êtes dans le rôle `root` dans la zone globale.

1. **Dans le gestionnaire de zones étiquetées, double-cliquez sur la zone globale.**
2. **Sélectionnez Add Multilevel Access to Remote Host (Ajouter l'accès multiniveau à un hôte distant).**
   a. **Saisissez l'adresse IP d'un autre système Trusted Extensions.**
   b. **Exécutez les commandes correspondantes sur l'autre système Trusted Extensions.**
3. **Cliquez sur Cancel (Annuler) pour revenir à la liste de commandes des zones.**
4. **Dans le gestionnaire de zones étiquetées, double-cliquez sur une zone étiquetée.**
5. **Sélectionnez Add Access to Remote Host (Ajouter l'accès à un hôte distant).**
   a. **Entrez l'adresse IP de la zone étiquetée de même étiquette sur un autre système Trusted Extensions.**
   b. **Exécutez les commandes correspondantes dans la zone de l'autre système Trusted Extensions.**

Voir aussi
- Chapitre 15, "Gestion de réseaux de confiance (présentation)"
- "Étiquetage d'hôtes et de réseaux (liste des tâches)" à la page 224

▼ Procédure de configuration d'un service de noms distinct pour chaque zone étiquetée

Cette procédure permet de configurer séparément un démon du service de noms (`nscd`) dans chaque zone étiquetée. Cette configuration ne satisfait pas les critères pour une configuration évaluée. Dans une configuration évaluée, le démon `nscd` s'exécute uniquement dans la zone globale. Les portes dans chaque zone étiquetée connectent la zone au démon `nscd` global.

Cette configuration prend en charge les environnements dans lesquels chaque zone est connectée à un sous-réseau s'exécutant à l'étiquette de la zone, et le sous-réseau possède son propre serveur de noms pour cette étiquette.

Remarque – Pour procéder à cette configuration, vous devez posséder des compétences avancées en matière de gestion de réseaux.

Avant de commencer Le gestionnaire de zones étiquetées est affiché. Pour ouvrir cette interface utilisateur graphique, reportez-vous à la section "Procédure interactive de création de zones étiquetées" à la page 59. Vous êtes dans le rôle `root` dans la zone globale.

1. **Dans le gestionnaire de zones étiquetées, sélectionnez Configure per-zone name service (Configurer un service de noms par zone) et cliquez sur OK.**

   Remarque – Cette option est destinée à être utilisée une fois, pendant la configuration initiale du système.

   ---

2. **Configurez le service `nscd` de chaque zone.**

   Pour obtenir de l'aide, reportez-vous à la page de manuel `nscd(1M)`.

3. **Réinitialisez le système.**

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

4. **Pour chaque zone, vérifiez la route et le démon du service de noms.**

   a. **Dans la console de la zone, répertoriez les services `nscd`.**

      ```
      zone-name # svcs -x name-service/cache
      svc:/system/name-service/cache:default (name service cache)
       State: online since September 10, 2011  10:10:11 AM PDT
         See: nscd(1M)
         See: /var/svc/log/system-name-service-cache:default.log
      Impact: None.
      ```

   b. **Vérifiez la route vers le sous-réseau.**

      ```
      zone-name # netstat -rn
      ```

Exemple 4–3 Suppression d'un cache de service de noms de chaque zone étiquetée

Après avoir testé un démon de service de noms par zone, l'administrateur système décide de supprimer les démons de services de noms des zones étiquetées et d'exécuter uniquement le démon dans la zone globale. Pour rétablir la configuration de service de noms par défaut du système, l'administrateur ouvre l'interface utilisateur graphique `txzonemgr`, sélectionne la zone globale, puis sélectionne `Unconfigure per-zone name service` (Annuler la configuration service de noms par zone) et `OK`. Cette sélection supprime le démon `nscd` de toutes les zones étiquetées. Ensuite, l'administrateur réinitialise le système.

Étapes suivantes Lors de la configuration des comptes utilisateur et des rôles de chaque zone, vous disposez de trois options.

- Vous pouvez créer les comptes LDAP dans un serveur d'annuaire LDAP multiniveau.
- Vous pouvez créer les comptes LDAP dans des serveurs d'annuaire LDAP distincts, à savoir un serveur par étiquette.
- Vous pouvez créer des comptes locaux.

La configuration d'un démon de service de noms par zone a des conséquences relatives au mot de passe pour tous les utilisateurs. Les utilisateurs doivent s'authentifier pour pouvoir accéder à n'importe laquelle de leurs zones étiquetées, y compris à la zone correspondant à leur étiquette par défaut. En outre, l'administrateur doit créer les comptes localement dans chaque zone, ou les comptes doivent exister dans un annuaire LDAP où la zone est client LDAP.

Dans le cas particulier où un compte de la zone globale exécute le gestionnaire de zones étiquetées, `txzonemgr`, les informations du compte sont copiées dans les zones étiquetées de manière à ce que ce compte au moins soit capable de se connecter à chaque zone. Par défaut, ce compte est le compte utilisateur initial.

Création de rôles et d'utilisateurs dans Trusted Extensions

La procédure de création de rôles dans Trusted Extensions est identique à la procédure de création de rôles dans le Oracle Solaris. Toutefois, pour une configuration évaluée, un rôle d'administrateur de sécurité est obligatoire.

Tâche	Description	Voir
Création d'un rôle d'administrateur de sécurité	Crée un rôle chargé de gérer les tâches ayant trait à la sécurité.	"Procédure de création du rôle d'administrateur sécurité dans Trusted Extensions" à la page 70
Création d'un rôle d'administrateur système	Crée un rôle chargé de gérer les tâches d'administration système qui ne sont pas liées à la sécurité.	"Procédure de création d'un rôle d'administrateur de sécurité" à la page 72

Tâche	Description	Voir
Création d'utilisateurs qui assumeront les rôles d'administration	Permet de créer un ou plusieurs utilisateurs qui peuvent assumer des rôles.	"Procédure de création d'utilisateurs pouvant assumer des rôles dans Trusted Extensions" à la page 72
Vérification de la capacité des rôles à exécuter leurs tâches	Teste les rôles.	"Procédure de vérification du fonctionnement des rôles Trusted Extensions" à la page 75
Autorisation des utilisateurs à se connecter à une zone étiquetée	Permet de démarrer le service `zones` afin que les utilisateurs standard puissent se connecter.	"Procédure d'autorisation des utilisateurs à se connecter à une zone étiquetée" à la page 75

▼ Procédure de création du rôle d'administrateur sécurité dans Trusted Extensions

Avant de commencer Vous êtes dans le rôle `root` dans la zone globale.

1 Pour créer le rôle, utilisez la commande `roleadd`.

Pour plus d'informations sur la commande, reportez-vous à la page de manuel `roleadd(1M)`.

Inspirez-vous des informations suivantes, données à titre d'exemple :

- Nom du rôle : `secadmin`
- `-c` Responsable local de la sécurité

  Ne pas fournir d'informations propriétaires.
- `-m` *répertoire-personnel*
- `-u` *UID-rôle*
- `-S` *référentiel*
- `-K` *clé=valeur*

  Affectez les profils de droits Information Security (Sécurité de l'information) et User Security (Sécurité des utilisateurs).

Remarque – Pour tous les rôles d'administration, utilisez les étiquettes d'administration en tant que plage d'étiquettes, effectuez un audit des utilisations de la commande `pfexec`, définissez `lock_after_retries=no` et ne définissez pas de date d'expiration des mots de passe.

```
# roleadd -c "Local Security Officer" -m \
-u 110 -K profiles="Information Security,User Security" -S files \
-K lock_after_retries=no \
-K min_label=ADMIN_LOW -K clearance=ADMIN_HIGH secadmin
```

2 Entrez un mot de passe initial pour le rôle.

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

Affectez un mot de passe d'au moins six caractères alphanumériques. Le mot de passe pour le rôle d'administrateur de sécurité, de même que tous les autres mots de passe, doit être difficile à deviner, afin de réduire les risques d'accès non autorisé par un tiers qui tenterait de deviner les mots de passe.

3 Inspirez-vous du rôle d'administrateur de sécurité lorsque vous créez d'autres rôles.

Les rôles suivants sont possibles :

- Rôle admin – profil de droits `System Administrator`
- Rôle oper – Profil de droits `Operator`

Exemple 4–4 Création du rôle d'administrateur de sécurité dans LDAP

Après avoir configuré le premier système avec un rôle d'administrateur de sécurité local, l'administrateur crée le rôle d'administrateur de sécurité dans le référentiel LDAP. Dans ce scénario, les clients LDAP peuvent être administrés par le rôle d'administrateur de sécurité défini dans LDAP.

```
# roleadd -c "Site Security Officer" -d server1:/rpool/pool1/BayArea/secadmin
-u 111 -K profiles="Information Security,User Security" -S ldap \
-K lock_after_retries=no -K audit_flags=lo,ex:no \
-K min_label=ADMIN_LOW -K clearance=ADMIN_HIGH secadmin
```

L'administrateur fournit un mot de passe initial pour le rôle.

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

Étapes suivantes Pour affecter le rôle local à un utilisateur local, reportez-vous à la section "Procédure de création d'utilisateurs pouvant assumer des rôles dans Trusted Extensions" à la page 72.

▼ Procédure de création d'un rôle d'administrateur de sécurité

Avant de commencer Vous êtes dans le rôle `root` dans la zone globale.

1 Affectez le profil de droits System Administrator (Administrateur système) au rôle.

```
# roleadd -c "Local System Administrator" -m -u 111  -K audit_flags=lo,ex:no\
-K profiles="System Administrator" -K lock_after_retries=no \
-K min_label=ADMIN_LOW -K clearance=ADMIN_HIGH sysadmin
```

2 Entrez un mot de passe initial pour le rôle.

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

▼ Procédure de création d'utilisateurs pouvant assumer des rôles dans Trusted Extensions

Si la stratégie de sécurité du site le permet, vous pouvez choisir de créer un utilisateur pouvant assumer plusieurs rôles d'administration.

Pour sécuriser la création des utilisateurs, le rôle d'administrateur système crée les utilisateurs et assigne le mot de passe initial et le rôle d'administrateur de sécurité affecte les attributs liés à la sécurité tels que les rôles.

Avant de commencer Vous devez être dans le rôle `root` dans la zone globale. Ou, si la séparation des tâches est appliquée, les utilisateurs qui peuvent prendre en charge les rôles distincts d'administrateur de sécurité et d'administrateur système doivent être présents pour assumer leurs rôles et effectuer les opérations appropriées dans cette procédure.

1 Créez un utilisateur.

Cette opération est effectuée par le rôle `root` ou le rôle d'administrateur système.

Ne placez pas d'informations propriétaires dans le commentaire.

```
# useradd -c "Second User" -u 1201 -d /home/jdoe jdoe
```

2 Après avoir créé l'utilisateur, modifiez les attributs de sécurité de l'utilisateur.

Cette opération est effectuée par le rôle `root` ou le rôle d'administrateur de sécurité.

Remarque – Pour les utilisateurs qui peuvent assumer des rôles, désactivez le verrouillage des comptes et ne définissez pas de date d'expiration du mot de passe. En outre, effectuez un audit des utilisations de la commande `pfexec`.

```
# usermod -K lock_after_retries=no -K idletime=5 -K idlecmd=lock \
-K audit_flags=lo,ex:no jdoe
```

Remarque – Les valeurs de `idletime` et `idlecmd` continuent à s'appliquer lorsque l'utilisateur assume un rôle. Pour plus d'informations, reportez-vous à la section "Valeurs par défaut du fichier `policy.conf` dans Trusted Extensions" à la page 142.

3 Affectez un mot de passe d'au moins six caractères alphanumériques.

```
# passwd jdoe
New Password:       Type password
Re-enter new Password:      Retype password
```

Remarque – Lorsque l'équipe de configuration initiale choisit un mot de passe, elle doit faire en sorte qu'il soit difficile à deviner, afin de réduire les risques d'accès non autorisé par un tiers qui tenterait de deviner les mots de passe.

4 Attribuez un rôle à l'utilisateur.

Cette opération est effectuée par le rôle `root` ou le rôle d'administrateur de sécurité.

```
# usermod -R oper jdoe
```

5 Personnalisez l'environnement de l'utilisateur.

a. Attribuez les autorisations appropriées.

Après avoir contrôlé la stratégie de sécurité de votre site, vous pouvez décider d'accorder à vos premiers utilisateurs le profil de droits Convenient Authorization (Autorisations appropriées). Avec ce profil, les utilisateurs peuvent allouer des périphériques, imprimer des fichiers PostScript, imprimer sans étiquette, se connecter à distance et arrêter le système. Pour créer le profil, reportez-vous à la section "Procédure de création d'un profil de droits pour des autorisations commodes" à la page 155.

b. Personnalisez les fichiers d'initialisation utilisateur.

Reportez-vous à la section "Personnalisation de l'environnement de l'utilisateur pour en assurer la sécurité (liste des tâches) " à la page 147.

c. Créez des fichiers de copie et de lien multiniveau.

Sur un système multiniveau, les utilisateurs et les rôles peuvent être configurés avec des fichiers qui répertorient les fichiers d'initialisation utilisateur à copier ou lier à d'autres étiquettes. Pour plus d'informations, reportez-vous à la section "Fichiers `.copy_files` et `.link_files`" à la page 145.

Exemple 4–5 Utilisation de la commande useradd pour créer un utilisateur local

Dans cet exemple, le rôle `root` crée un utilisateur local pouvant assumer le rôle d'administrateur de sécurité. Pour en savoir plus, reportez-vous aux pages de manuel `useradd(1M)` et `atohexlabel(1M)`.

Cet utilisateur aura une plage d'étiquettes plus étendue que la plage d'étiquettes par défaut. Ainsi, l'utilisateur `root` détermine le format hexadécimal de l'étiquette minimale et de l'étiquette d'autorisation de l'utilisateur.

```
# atohexlabel public
0x0002-08-08
# atohexlabel -c "confidential restricted"
0x0004-08-78
```

Ensuite, le rôle `root` doit consulter le Tableau 1–2, puis créer l'utilisateur. L'administrateur place le répertoire personnel de l'utilisateur sous `/export/home1` plutôt qu'à l'emplacement par défaut `/export/home` .

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

Le rôle `root` fournit alors un mot de passe initial.

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

Enfin, le rôle `root` ajoute le rôle d'administrateur de sécurité à la définition de l'utilisateur. Le rôle a été créé à la section "Procédure de création du rôle d'administrateur sécurité dans Trusted Extensions" à la page 70.

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

▼ Procédure de vérification du fonctionnement des rôles Trusted Extensions

Pour vérifier chaque rôle, assumez le rôle correspondant. Effectuez ensuite des tâches qui ne peuvent être effectuées que par ce rôle et tentez d'effectuer des tâches que ce rôle n'est pas autorisé à effectuer.

Avant de commencer Si vous avez configuré DNS ou le routage, vous devez réinitialiser l'ordinateur après avoir créé les rôles et avant de pouvoir vérifier leur fonctionnement.

1. **Pour chaque rôle, connectez-vous en tant qu'utilisateur qui peut assumer le rôle.**

2. **Assumez le rôle.**

   Dans la bande de confiance ci-après, le nom d'utilisateur est `tester`.

   a. **Cliquez sur votre nom d'utilisateur dans la bande de confiance.**

   b. **À partir de la liste des rôles qui vous sont affectés, sélectionnez un rôle.**

3. **Testez le rôle.**

   Pour plus d'informations sur les autorisations requises pour modifier les propriétés d'un utilisateur, reportez-vous à la page de manuel `passwd(1)`.

   - L'administrateur système doit être en mesure de créer un utilisateur et de modifier les propriétés d'un utilisateur qui nécessitent l'autorisation `solaris.user.manage`, tels que le shell de connexion de l'utilisateur. L'administrateur système ne doit pas être en mesure de modifier les propriétés d'un utilisateur qui nécessitent l'autorisation `solaris.account.setpolicy`.
   - Le rôle d'administrateur de la sécurité doit être en mesure de modifier les propriétés d'un utilisateur qui nécessitent l'autorisation `solaris.account.setpolicy`. L'administrateur de sécurité ne doit pas être en mesure de créer un utilisateur ou de modifier le shell de connexion d'un utilisateur.

▼ Procédure d'autorisation des utilisateurs à se connecter à une zone étiquetée

Lorsque le système est réinitialisé, l'association entre les périphériques et le stockage sous-jacent doit être rétablie.

Avant de commencer Vous avez créé au moins une zone étiquetée. Après avoir configuré le système, vous avez réinitalisé. Vous pouvez assumer le rôle `root`.

1. **Connectez-vous et assumez le rôle `root`.**
2. **Vérifiez l'état du service de zones.**

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

3. **Redémarrez le service.**

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

4. **Déconnectez-vous.**

   Les utilisateurs standard peuvent désormais se connecter. Leur session se trouve dans une zone étiquetée.

Création de répertoires personnels centralisés dans Trusted Extensions

Dans Trusted Extensions, les utilisateurs ont besoin d'accéder à leurs répertoires personnels sur chaque étiquette sur laquelle ils travaillent. Par défaut, les répertoires personnels sont créés automatiquement par l'agent de montage automatique qui s'exécute dans chaque zone. Toutefois, si vous utilisez un serveur NFS pour centraliser les répertoires personnels, vous devez activer l'accès au répertoire personnel sous chaque étiquette pour vos utilisateurs.

▼ Procédure de création du serveur d'annuaires personnel dans Trusted Extensions

Avant de commencer Vous êtes dans le rôle `root` dans la zone globale.

1. **Ajoutez le logiciel Trusted Extensions au serveur d'annuaires personnel et configurez ses zones étiquetées.**

   - Étant donné que les utilisateurs requièrent un répertoire personnel sous chaque étiquette à laquelle ils peuvent se connecter, créez un serveur d'annuaires personnel sous chaque étiquette des utilisateurs. Par exemple, si vous créez une configuration par défaut, créez un serveur d'annuaires personnel pour l'étiquette `PUBLIC` et un serveur pour l'étiquette `INTERNAL`.

2. **Pour chaque zone étiquetée, suivez la procédure de montage automatique décrite à la section "Procédure de montage NFS de fichiers dans une zone étiquetée" à la page 197. Revenez ensuite à cette procédure.**

3. **Vérifiez que les répertoires personnels ont été créés.**

   a. **Déconnectez-vous du serveur d'annuaires personnel.**

   b. **En tant qu'utilisateur standard, connectez-vous au serveur d'annuaires personnel.**

   c. **Dans la zone de connexion, ouvrez un terminal.**

   d. **Dans la fenêtre de terminal, vérifiez que le répertoire personnel de l'utilisateur existe.**

   e. **Créez des espaces de travail pour chaque zone dans laquelle l'utilisateur peut travailler.**

   f. **Dans chaque zone, ouvrez une fenêtre de terminal afin de vérifier que le répertoire personnel de l'utilisateur existe.**

4. **Déconnectez-vous du serveur d'annuaires personnel.**

▼ Procédure permettant aux utilisateurs d'accéder à leurs répertoires personnels distants sous chaque étiquette en se connectant à chaque serveur NFS

Cette procédure permet d'autoriser les utilisateurs à créer un répertoire personnel sous chaque étiquette en les autorisant à se connecter directement à chaque serveur d'annuaires personnel. Après avoir créé chaque répertoire personnel sur le serveur central, les utilisateurs peuvent accéder à leurs répertoires personnels à partir de n'importe quel système.

En tant qu'administrateur, vous pouvez également créer un point de montage sur chaque serveur d'annuaires personnel en exécutant un script et en modifiant ensuite l'agent de montage automatique. Pour cette méthode, reportez-vous à la section "Procédure permettant aux utilisateurs d'accéder à leurs répertoires personnels distants en configurant l'agent de montage automatique sur chaque serveur" à la page 78.

Avant de commencer Les serveurs d'annuaires personnels de votre domaine Trusted Extensions sont configurés.

- **Autorisez la connexion directe des utilisateurs à chaque serveur d'annuaires personnel.**

  En règle générale, vous avez créé un serveur NFS par étiquette.

  a. **Demandez à chaque utilisateur de se connecter à chaque serveur NFS sous l'étiquette du serveur.**

  b. **Lorsque la connexion est établie, indiquez à l'utilisateur de se déconnecter du serveur.**

     Un répertoire personnel pour l'utilisateur est disponible sous l'étiquette du serveur lorsque la connexion est établie.

  c. **Demandez aux utilisateurs de se connecter à partir de leur poste de travail normal.**

     Le répertoire personnel correspondant à leur étiquette par défaut est disponible à partir du serveur d'annuaires personnel. Lorsqu'un utilisateur modifie l'étiquette d'une session ou ajoute un espace de travail sur une autre étiquette, le répertoire personnel de l'utilisateur pour cette étiquette est monté.

Étapes suivantes Les utilisateurs peuvent se connecter sous une autre étiquette à partir de leur étiquette par défaut en choisissant une autre étiquette dans le générateur d'étiquettes (Label Builder) au cours de la connexion.

▼ Procédure permettant aux utilisateurs d'accéder à leurs répertoires personnels distants en configurant l'agent de montage automatique sur chaque serveur

Au cours de cette procédure, vous exécutez un script qui crée un point de montage pour les répertoires personnels sur chaque serveur NFS. Vous modifiez ensuite l'entrée `auto_home` sous l'étiquette du serveur pour ajouter le point de montage. Les utilisateurs peuvent alors s'y connecter.

Avant de commencer Les serveurs d'annuaires personnels de votre domaine Trusted Extensions sont configurés en tant que clients LDAP. Les comptes utilisateur ont été créés sur le serveur LDAP à l'aide de la commande `useradd` avec l'option `-S ldap`. Vous devez être dans le rôle `root`.

1 **Écrivez un script qui crée un point de montage de répertoire personnel pour chaque utilisateur.**

L'exemple de script suppose que :

- Le serveur LDAP est un serveur différent du serveur d'annuaires personnel NFS.
- Les systèmes client sont également des systèmes différents.
- L'entrée `hostname` spécifie l'adresse IP externe de la zone, c'est-à-dire le serveur d'annuaires personnel NFS pour l'étiquette de celle-ci.

- Le script sera exécuté sur le serveur NFS dans la zone qui sert les clients sous cette étiquette.

```
#!/bin/sh
hostname=$(hostname)
scope=ldap

for j in $(getent passwd|tr ' ' _); do
    uid=$(echo $j|cut -d: -f3)
    if [ $uid -ge 100 ]; then
        home=$(echo $j|cut -d: -f6)
        if [[ $home == /home/* ]]; then
            user=$(echo $j|cut -d: -f1)
            echo Updating home directory for $user
            homedir=/export/home/$user
            usermod -md ${hostname}:$homedir -S $scope $user
            mp=$(mount -p|grep  " $homedir zfs" )
            dataset=$(echo $mp|cut -d" " -f1)
            if [[ -n $dataset ]]; then
                zfs set sharenfs=on $dataset
            fi
        fi
    fi
done
```

2 **Sur chaque serveur NFS, exécutez le script précédent dans la zone étiquetée qui sert les clients sous cette étiquette.**

Dépannage de votre configuration Trusted Extensions

Une mauvaise configuration du bureau peut empêcher l'utilisation du système.

▼ Procédure de déplacement des panneaux du bureau vers le bas de l'écran

Remarque – Par défaut, les panneaux du bureau sont placés dans la partie supérieure de l'écran. Toutefois, dans Trusted Extensions; la bande de confiance couvre la partie supérieure de l'écran. Par conséquent, les panneaux doivent être placés sur le côté de l'écran ou en bas de l'espace de travail. Un espace de travail par défaut comporte deux panneaux du bureau.

Avant de commencer Vous devez être dans le rôle `root` pour modifier la position des panneaux du bureau pour le système.

1 **Si un seul panneau du bureau est visible au bas de l'écran, effectuez l'une des actions suivantes :**

- **Utilisez le bouton droit de la souris pour ajouter des applets au panneau visible.**

- **Déplacez le second panneau de bureau masqué vers le bas de l'écran en effectuant l'étape suivante.**

2 **Sinon, créez un panneau de bureau pour le bas de l'écran pour votre connexion uniquement ou pour tous les utilisateurs du système.**

- **Pour déplacer les panneaux pour votre connexion uniquement, modifiez le fichier `top_panel_screen` *n* dans votre répertoire personnel.**

  a. **Accédez au répertoire contenant le fichier définissant les emplacements des panneaux.**

  ```
  % cd $HOME/.gconf/apps/panel/toplevels
  % ls
  %gconf.xml    bottom_panel_screen0/   top_panel_screen0/
  % cd top_panel_screen0
  % ls
  %gconf.xml             top_panel_screen0/
  ```

  b. **Modifiez le fichier `%gconf.xml`, qui définit l'emplacement des panneaux supérieurs.**

  ```
  % vi %gconf.xml
  ```

  c. **Recherchez toutes les lignes d'orientation et remplacez la chaîne `top` par la chaîne `bottom`.**

  Par exemple, modifiez la ligne d'orientation de manière à ce qu'elle ressemble à la ligne suivante :

  ```
  /toplevels/orientation" type="string">
                  <stringvalue>bottom</stringvalue>
  ```

- **Pour déplacer les panneaux pour tous les utilisateurs du système, modifiez la configuration du bureau.**

  Dans une fenêtre de terminal dans le rôle `root`, exécutez les commandes suivantes :

  ```
  # export SETUPPANEL="/etc/gconf/schemas/panel-default-setup.entries"
  # export TMPPANEL="/tmp/panel-default-setup.entries"
  # sed 's/<string>top<\/string>/<string>bottom<\/string>/' $SETUPPANEL > $TMPPANEL
  # cp $TMPPANEL $SETUPPANEL
  # svcadm restart gconf-cache
  ```

3 **Déconnectez-vous du système, puis reconnectez-vous.**

Si vous avez plus d'un panneau de bureau, les panneaux s'empilent au bas de l'écran.

Tâches de configuration supplémentaires de Trusted Extensions

Les deux tâches suivantes permettent de transférer une copie exacte des fichiers de configuration sur chaque système Trusted Extensions de votre site. La dernière tâche permet de supprimer les personnalisations de Trusted Extensions d'un système Oracle Solaris.

▼ Copie de fichiers sur un média amovible dans Trusted Extensions

Lors de la copie sur un média amovible, étiquetez le média avec l'étiquette de sensibilité des informations.

Remarque – Pendant la configuration de Trusted Extensions, le rôle `root` peut utiliser des médias amovibles pour transférer les fichiers `label_encodings` à tous les systèmes. Étiquetez le média avec `Trusted Path`.

Avant de commencer Pour copier les fichiers d'administration, vous devez être dans le rôle `root` dans la zone globale.

1. **Allouez le périphérique approprié.**

   Utilisez le gestionnaire de périphériques (Device Manager) et insérez un média vierge. Pour plus d'informations, reportez-vous à la section "Procédure d'allocation d'un périphérique dans Trusted Extensions" du manuel *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

   Le navigateur de fichiers affiche le contenu du média vierge.

2. **Ouvrez un deuxième navigateur de fichiers.**

3. **Accédez au dossier contenant les fichiers à copier.**

4. **Pour chaque fichier, effectuez les opérations suivantes :**

   a. **Mettez l'icône du fichier en surbrillance.**

   b. **Faites glisser le fichier vers le navigateur de fichiers du média amovible.**

5. **Libérez le périphérique.**

   Pour plus d'informations, reportez-vous à la section "Procédure de libération d'un périphérique dans Trusted Extensions" du manuel *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

6 **Dans le navigateur de fichiers du média amovible, sélectionnez Eject (Ejecter) dans le menu File (Fichier).**

Remarque – N'oubliez pas de placer physiquement sur le média une étiquette indiquant le niveau de sensibilité des fichiers copiés.

Exemple 4–6 Conservation de fichiers de configuration identiques sur tous les systèmes

L'administrateur système souhaite s'assurer que tous les systèmes sont configurés avec les mêmes paramètres. Par conséquent, il crée sur le premier système configuré un répertoire qui ne peut pas être supprimé entre les réinitialisations. Dans ce répertoire, l'administrateur place les fichiers qui doivent être identiques ou très similaires sur tous les systèmes.

Par exemple, l'administrateur modifie le fichier `policy.conf` ainsi que les fichiers `login` et `passwd` pour ce site. L'administrateur copie donc les fichiers suivants dans le répertoire permanent.

```
# mkdir /export/commonfiles
# cp  /etc/security/policy.conf \
# cp  /etc/default/login \
# cp  /etc/default/passwd \
# cp  /etc/security/tsol/label_encodings \
/export/commonfiles
```

L'administrateur utilise le gestionnaire de périphériques (Device Manager) pour allouer un CD-ROM dans la zone globale, transfère les fichiers vers le CD, et appose une étiquette `Trusted Path`.

▼ Copie de fichiers dans Trusted Extensions à partir d'un média amovible

Il est recommandé de renommer le fichier Trusted Extensions original avant de le remplacer. Lors de la configuration d'un système, le rôle `root` renomme et copie les fichiers d'administration.

Avant de commencer Pour copier les fichiers d'administration, vous devez être dans le rôle `root` dans la zone globale.

1 **Allouez le périphérique approprié.**

Pour plus d'informations, reportez-vous à la section "Procédure d'allocation d'un périphérique dans Trusted Extensions" du manuel *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

Le navigateur de fichiers affiche le contenu.

2 **Insérez le média contenant les fichiers d'administration.**

3. **Si le système contient un fichier du même nom, copiez le fichier d'origine sous un nouveau nom.**

   Par exemple, ajoutez `.orig` à la fin du fichier d'origine :

   ```
   # cp /etc/security/tsol/label_encodings /etc/security/tsol/label_encodings.orig
   ```

4. **Ouvrez un navigateur de fichiers.**

5. **Accédez au répertoire de destination souhaité, par exemple `/etc/security/tsol`.**

6. **Pour chaque fichier que vous souhaitez copier, effectuez les opérations suivantes :**

   a. **Dans le navigateur de fichiers du média monté, mettez l'icône du fichier en surbrillance.**

   b. **Faites ensuite glisser le fichier vers le répertoire de destination dans le deuxième navigateur de fichiers.**

7. **Libérez le périphérique.**

   Pour plus d'informations, reportez-vous à la section "Procédure de libération d'un périphérique dans Trusted Extensions" du manuel *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

8. **Lorsque vous y êtes invité, éjectez et retirez le média.**

▼ Suppression de Trusted Extensions du système

Vous devez effectuer des étapes spécifiques pour supprimer la fonction Trusted Extensions d'un système Oracle Solaris.

Avant de commencer Vous êtes dans le rôle `root` dans la zone globale.

1. **Archivez toutes les données dans des zones étiquetées que vous souhaitez conserver.**

   Si vous utilisez des médias amovibles, fixez une étiquette physique indiquant l'étiquette de sensibilité de la zone sur chaque zone archivée.

2. **Supprimez les zones étiquetées du système.**

   Pour plus d'informations, reportez-vous à la section "Suppression d'une zone non globale" du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*.

3. **Désactivez le service Trusted Extensions.**

   ```
   # svcadm disable labeld
   ```

4. **Désactivez l'allocation de périphériques.**

   ```
   # svcadm disable allocate
   ```

5 **(Facultatif) Réinitialisez le système.**

6 **Configurez le système.**

La configuration de différents services peut être nécessaire pour votre système Oracle Solaris. Peuvent être concernés par exemple la configuration réseau de base, les services de nommage et le montage de systèmes de fichiers.

◆ ◆ ◆ CHAPITRE 5

Configuration de LDAP pour Trusted Extensions (tâches)

Ce chapitre présente la configuration du serveur Oracle Directory Server Enterprise Edition (serveur d'annuaire) à utiliser avec Trusted Extensions. Le serveur d'annuaire fournit les services LDAP. LDAP est le service de nommage pris en charge pour Trusted Extensions. La dernière section, “Création d'un client LDAP Trusted Extensions ” à la page 96, présente la configuration d'un client LDAP.

Vous avez le choix entre deux options lors de la configuration du serveur d'annuaire. Vous pouvez configurer un serveur LDAP sur un système Trusted Extensions, ou utiliser un serveur existant et vous y connecter à l'aide d'un serveur proxy Trusted Extensions.

Pour configurer le serveur LDAP, suivez les instructions de l'*une* des listes de tâches ci-dessous :

- “Configuration de LDAP sur un réseau Trusted Extensions (liste des tâches)” à la page 85
- “Configuration d'un serveur proxy LDAP sur un système Trusted Extensions (liste des tâches)” à la page 86

Configuration de LDAP sur un réseau Trusted Extensions (liste des tâches)

Tâche	Description	Voir
Définition d'un serveur LDAP Trusted Extensions	Si vous n'avez pas encore de serveur Oracle Directory Server Enterprise Edition, faites de votre premier système Trusted Extensions le serveur d'annuaire. Ce système n'a aucune zone étiquetée. Les autres systèmes Trusted Extensions sont des clients de ce serveur.	“Collecte d'informations pour le serveur d'annuaire pour LDAP” à la page 87 “Installation du serveur Oracle Directory Server Enterprise Edition” à la page 88 “Configuration des journaux pour le serveur Oracle Directory Server Enterprise Edition” à la page 91

Tâche	Description	Voir
Ajout de bases de données Trusted Extensions au serveur	Remplissez le serveur LDAP avec les données des fichiers du système Trusted Extensions.	"Remplissage du serveur Oracle Directory Server Enterprise Edition" à la page 93
Configuration de tous les autres systèmes Trusted Extensions en tant que clients de ce serveur	Lorsque vous configurez un autre système avec Trusted Extensions, faites du système un client de ce serveur LDAP.	"Établissement de la zone globale en tant que client LDAP dans Trusted Extensions" à la page 96

Configuration d'un serveur proxy LDAP sur un système Trusted Extensions (liste des tâches)

Utilisez cette liste des tâches si vous avez déjà un serveur Oracle Directory Server Enterprise Edition en cours d'exécution sur un système Oracle Solaris.

Tâche	Description	Voir
Ajout de bases de données Trusted Extensions au serveur	Les bases de données du réseau Trusted Extensions, `tnrhdb` et `tnrhtp`, doivent être ajoutées au serveur LDAP.	"Remplissage du serveur Oracle Directory Server Enterprise Edition" à la page 93
Configuration d'un serveur proxy LDAP	Faites du système Trusted Extensions le serveur proxy pour tous les autres systèmes Trusted Extensions. Les autres systèmes utilisent ce serveur proxy pour accéder au serveur LDAP.	"Création d'un serveur proxy LDAP" à la page 95
Configuration du serveur proxy afin que le LDAP dispose d'un port multiniveau	Activez le serveur proxy Trusted Extensions pour communiquer avec le serveur LDAP sur des étiquettes spécifiques.	"Configuration d'un port multiniveau pour le serveur Oracle Directory Server Enterprise Edition" à la page 92
Configuration de tous les autres systèmes Trusted Extensions en tant que clients du serveur proxy LDAP	Lorsque vous configurez un autre système avec Trusted Extensions, faites du système un client du serveur proxy LDAP.	"Établissement de la zone globale en tant que client LDAP dans Trusted Extensions" à la page 96

Configuration du serveur Oracle Directory Server Enterprise Edition sur un système Trusted Extensions

Le service de nommage LDAP est le service de nommage pris en charge pour Trusted Extensions. Si votre site n'exécute pas encore le service de nommage LDAP, configurez un serveur Oracle Directory Server Enterprise Edition (serveur d'annuaire) sur un système configuré avec Trusted Extensions.

Si votre site exécute déjà un serveur d'annuaire, vous devez ajouter les bases de données Trusted Extensions au serveur. Pour accéder au serveur d'annuaire, vous devez ensuite configurer un serveur proxy LDAP sur un système Trusted Extensions.

Remarque – Si vous n'utilisez pas ce serveur LDAP en tant que serveur NFS, vous n'avez pas besoin d'installer de zones étiquetées sur ce serveur.

▼ Collecte d'informations pour le serveur d'annuaire pour LDAP

- **Déterminez les valeurs des éléments suivants.**

  Les éléments sont répertoriés dans l'ordre où ils apparaissent dans l'Assistant d'installation de Sun Java Enterprise System.

Invite de l'Assistant d'installation	Action ou informations
Oracle Directory Server Enterprise Edition *version*	
ID utilisateur de l'administrateur	La valeur par défaut est `admin`.
Mot de passe de l'administrateur	Créez un mot de passe, tel que `admin123`.
DN du gestionnaire d'annuaire	La valeur par défaut est `cn=Directory Manager`.
Mot de passe du gestionnaire d'annuaire	Créez un mot de passe, tel que `dirmgr89`.
Root du serveur d'annuaire	La valeur par défaut est `/var/Sun/mps`. Ce chemin est également utilisé par la suite si le logiciel proxy est installé.
Identificateur du serveur	La valeur par défaut est le système local.
Port du serveur	Si vous avez l'intention d'utiliser le serveur d'annuaire pour fournir des services de nommage LDAP standard aux systèmes clients, utilisez la valeur par défaut, `389`.
	Si vous envisagez d'utiliser le serveur d'annuaire pour prendre en charge l'installation ultérieure d'un serveur proxy, saisissez un port non standard, tel que `10389`.
Suffixe	Incluez votre composant de domaine, comme dans `dc=example-domain,dc=com`.
Domaine d'administration	Construisez-le afin qu'il corresponde au suffixe, comme dans `example-domain.com`.
Utilisateur du système	La valeur par défaut est `root`.

Invite de l'Assistant d'installation	Action ou informations
Groupe du système	La valeur par défaut est `root`.
Emplacement de stockage des données	La valeur par défaut est `Store configuration data on this server`.
Emplacement de stockage des données	La valeur par défaut est `Store user data and group data on this server`.
Port d'administration	La valeur par défaut est le port du serveur. Une convention suggérée pour changer la valeur par défaut est *version du logiciel* multiplié par `1000`. Pour la version `5.2` du logiciel, cette convention donnerait le port `5200`.

▼ Installation du serveur Oracle Directory Server Enterprise Edition

Les packages du serveur d'annuaire sont disponibles à partir du site Web Oracle pour les produits logiciels Sun (`http://www.oracle.com/us/sun/sun-products-map-075562.html`).

Avant de commencer

Vous vous trouvez sur un système Trusted Extensions comportant une zone globale. Le système n'a aucune zone étiquetée. Vous devez être superutilisateur dans la zone globale.

Les serveurs LDAP Trusted Extensions sont configurés pour les clients qui utilisent `pam_unix` pour l'authentification auprès du référentiel LDAP. Avec `pam_unix`, le fonctionnement du mot de passe, et par conséquent sa stratégie, sont déterminés par le client. Plus précisément, la stratégie définie par le serveur LDAP n'est pas utilisée. Pour connaître les paramètres de mot de passe pouvant être définis sur le client, reportez-vous à la section "Gestion des informations de mot de passe" du manuel *Administration d'Oracle Solaris : services de sécurité*. Pour en savoir plus sur `pam_unix`, reportez-vous à la page de manuel `pam.conf(4)`.

Remarque – L'utilisation de `pam_ldap` sur un client LDAP ne constitue pas une configuration évaluée pour Trusted Extensions.

---

1 Avant d'installer les packages du serveur d'annuaire, ajoutez le FQDN pour l'entrée de nom d'hôte de votre système.

FQDN (Fully Qualified Domain Name) signifie nom de domaine complet. Ce nom se compose du nom d'hôte et du domaine d'administration, par exemple :

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

2 **Téléchargez les packages Oracle Directory Server Enterprise Edition à partir du site Web Oracle pour les produits logiciels Sun (`http://www.oracle.com/us/sun/sun-products-map-075562.html`).**

Sélectionnez la versions la plus récente du logiciel approprié pour votre plate-forme.

3 **Installez les packages du serveur d'annuaire.**

Répondez aux questions posées à l'aide des informations recueillies à l'étape "Collecte d'informations pour le serveur d'annuaire pour LDAP" à la page 87. Pour obtenir une liste complète des questions, des valeurs par défaut et des réponses suggérées, reportez-vous au Chapitre 11, "Setting Up Oracle Directory Server Enterprise Edition With LDAP Clients (Tasks)" du manuel *Oracle Solaris Administration: Naming and Directory Services* et au Chapitre 12, "Setting Up LDAP Clients (Tasks)" du manuel *Oracle Solaris Administration: Naming and Directory Services*.

4 **(Facultatif) Ajoutez les variables d'environnement pour le serveur d'annuaire à votre chemin.**

```
# $PATH
/usr/sbin:.../opt/SUNWdsee/dsee6/bin:/opt/SUNWdsee/dscc6/bin:/opt/SUNWdsee/ds6/bin:
/opt/SUNWdsee/dps6/bin
```

5 **(Facultatif) Ajoutez les pages de manuel du serveur d'annuaire à votre `MANPATH`.**

```
/opt/SUNWdsee/dsee6/man
```

6 **Activez le programme `cacaoadm` et vérifiez qu'il est activé.**

```
# /usr/sbin/cacaoadm enable
# /usr/sbin/cacaoadm start
start: server (pid n) already running
```

7 **Assurez-vous que le serveur d'annuaire se lance à chaque démarrage.**

Les packages Oracle Directory Server Enterprise Edition contiennent des modèles de services SMF pour le serveur d'annuaire.

- **Pour un serveur d'annuaire Trusted Extensions, activez le service.**

```
# dsadm stop /export/home/ds/instances/your-instance
# dsadm enable-service -T SMF /export/home/ds/instances/your-instance
# dsadm start /export/home/ds/instances/your-instance
```

Pour plus d'informations sur la commande `dsadm`, reportez-vous à la page de manuel `dsadm`(1M).

- **Pour un serveur d'annuaire proxy, activez le service.**

```
# dpadm stop /export/home/ds/instances/your-instance
# dpadm enable-service -T SMF /export/home/ds/instances/your-instance
# dpadm start /export/home/ds/instances/your-instance
```

Pour plus d'informations sur la commande `dpadm`, reportez-vous à la page de manuel `dpadm`(1M).

8 Vérifiez votre installation.

```
# dsadm info /export/home/ds/instances/your-instance
Instance Path:         /export/home/ds/instances/your-instance
Owner:                 root(root)
Non-secure port:       389
Secure port:           636
Bit format:            32-bit
State:                 Running
Server PID:            298
DSCC url:              -
SMF application name:  ds--export-home-ds-instances-your-instance
Instance version:      D-A00
```

Erreurs fréquentes Pour connaître les stratégies de résolution des problèmes de configuration LDAP, reportez-vous au Chapitre 13, “LDAP Troubleshooting (Reference)” du manuel *Oracle Solaris Administration: Naming and Directory Services*.

▼ Création d'un client LDAP pour le serveur d'annuaire

Vous utilisez ce client pour remplir votre serveur d'annuaire pour LDAP. Vous devez exécuter cette tâche avant de remplir le serveur d'annuaire.

Vous pouvez créer le client temporairement sur le serveur d'annuaire Trusted Extensions, puis supprimer le client du serveur, ou vous pouvez créer un client indépendant.

Avant de commencer Vous êtes dans le rôle `root` dans la zone globale.

1 Ajoutez un logiciel Trusted Extensions logiciel à un système.

Vous pouvez utiliser le serveur d'annuaire Trusted Extensions ou ajouter Trusted Extensions sur un système séparé.

2 Sur le client, configurez le serveur LDAP dans le service `name-service/switch` service.

a. Affichez la configuration actuelle.

```
# svccfg -s name-service/switch listprop config
config                      application
config/value_authorization  astring       solaris.smf.value.name-service.switch
config/default              astring       "files ldap"
config/host                 astring       "files dns"
config/netgroup             astring       ldap
config/printer              astring       "user files ldap"
```

b. Remplacez la valeur par défaut de la propriété par la valeur suivante :

```
# svccfg -s name-service/switch setprop config/host = astring: "files ldap dns"
```

3. **Dans la zone globale, exécutez la commande `ldapclient init`.**

   Dans cet exemple, le client LDAP se trouve dans le domaine `example-domain.com`. L'adresse IP du serveur est `192.168.5.5`.

```
# ldapclient init -a domainName=example-domain.com -a profileName=default \
> -a proxyDN=cn=proxyagent,ou=profile,dc=example-domain,dc=com \
> -a proxyDN=cn=proxyPassword={NS1}ecc423aad0 192.168.5.5
System successfully configured
```

4. **Définissez le paramètre `enableShadowUpdate` du serveur sur `TRUE`.**

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

   Pour plus d'informations sur le paramètre `enableShadowUpdate`, reportez-vous à la section "enableShadowUpdate Switch" du manuel *Oracle Solaris Administration: Naming and Directory Services* et à la page de manuel `ldapclient`(1M).

▼ Configuration des journaux pour le serveur Oracle Directory Server Enterprise Edition

Cette procédure configure trois types de journaux : les journaux d'accès, les journaux d'audit et les journaux des erreurs. Les paramètres par défaut suivants n'ont pas été modifiés :

- Tous les journaux sont activés et mis en tampon.
- Les journaux sont placés dans le répertoire `/export/home/ds/instances/`*your-instance*`/logs/`*LOG_TYPE* approprié.
- Les événements sont enregistrés au niveau de journal 256.
- Les journaux sont protégés par des autorisations de fichier `600`.
- Les journaux d'accès sont permutés quotidiennement.
- Les journaux des erreurs sont permutés hebdomadairement.

Les paramètres dans cette procédure satisfont aux exigences suivantes :

- Les journaux d'audit sont permutés quotidiennement.
- Les fichiers journaux plus anciens que 3 mois expirent.
- Tous les fichiers journaux utilisent un maximum de 20 000 Mo d'espace disque.
- 100 fichiers journaux maximum sont conservés, et chaque fichier pèse au maximum 500 Mo.
- Les journaux les plus anciens sont supprimés si l'espace disque disponible est inférieur à 500 Mo.
- Des informations supplémentaires sont collectées dans les journaux des erreurs.

Avant de commencer Vous devez être superutilisateur dans la zone globale.

1 Configurez les journaux d'accès.

Le *LOG_TYPE* pour l'accès est `ACCESS`. La syntaxe de configuration des journaux est la suivante :

`dsconf set-log-prop` *LOG_TYPE property*:*value*

```
# dsconf set-log-prop ACCESS max-age:3M
# dsconf set-log-prop ACCESS max-disk-space-size:20000M
# dsconf set-log-prop ACCESS max-file-count:100
# dsconf set-log-prop ACCESS max-size:500M
# dsconf set-log-prop ACCESS min-free-disk-space:500M
```

2 Configurez les journaux d'audit.

```
# dsconf set-log-prop AUDIT max-age:3M
# dsconf set-log-prop AUDIT max-disk-space-size:20000M
# dsconf set-log-prop AUDIT max-file-count:100
# dsconf set-log-prop AUDIT max-size:500M
# dsconf set-log-prop AUDIT min-free-disk-space:500M
# dsconf set-log-prop AUDIT rotation-interval:1d
```

Par défaut, l'intervalle de permutation des journaux d'audit est une semaine.

3 Configurez les journaux des erreurs.

Dans cette configuration, vous pouvez spécifier d'autres données à collecter dans le journal des erreurs.

```
# dsconf set-log-prop ERROR max-age:3M
# dsconf set-log-prop ERROR max-disk-space-size:20000M
# dsconf set-log-prop ERROR max-file-count:30
# dsconf set-log-prop ERROR max-size:500M
# dsconf set-log-prop ERROR min-free-disk-space:500M
# dsconf set-log-prop ERROR verbose-enabled:on
```

4 (Facultatif) Effectuez une configuration avancée des journaux.

Vous pouvez également configurer les paramètres suivants pour chaque journal :

```
# dsconf set-log-prop LOG_TYPE rotation-min-file-size:undefined
# dsconf set-log-prop LOG_TYPE rotation-time:undefined
```

Pour plus d'informations sur la commande `dsconf`, reportez-vous à la page de manuel `dsconf`(1M).

▼ Configuration d'un port multiniveau pour le serveur Oracle Directory Server Enterprise Edition

Pour fonctionner dans Trusted Extensions, le port du serveur d'annuaire doit être configuré en tant que port multiniveau (MLP) dans la zone globale.

Avant de commencer Vous devez être superutilisateur dans la zone globale.

1. **Démarrez `txzonemgr`.**

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

2. **Ajoutez un port multiniveau pour le protocole TCP à la zone globale.**

   Le numéro de port est 389.

3. **Ajoutez un port multiniveau pour le protocole UDP à la zone globale.**

   Le numéro de port est 389.

▼ Remplissage du serveur Oracle Directory Server Enterprise Edition

Plusieurs bases de données LDAP ont été créées ou modifiées afin de contenir les données Trusted Extensions relatives à la configuration de l'étiquette, aux utilisateurs et aux systèmes distants. Dans cette procédure, vous remplissez les bases de données du serveur d'annuaire avec des informations Trusted Extensions.

Avant de commencer Vous devez être superutilisateur dans la zone globale. Vous êtes sur un client LDAP où la mise à jour en double est activée. Pour connaître les conditions requises, reportez-vous à la section "Création d'un client LDAP pour le serveur d'annuaire" à la page 90.

1. **Créez une zone de préparation pour les fichiers que vous prévoyez d'utiliser pour remplir les bases de données du service de nommage.**

   ```
   # mkdir -p /setup/files
   ```

2. **Copiez l'échantillon de fichiers `/etc` dans la zone de préparation.**

   ```
   # cd /etc
   # cp aliases group networks netmasks protocols /setup/files
   # cp rpc services auto_master /setup/files

   # cd /etc/security/tsol
   # cp tnrhdb tnrhtp /setup/files
   ```

Attention – Ne copiez pas les fichiers `*attr`. Associez plutôt l'option `-S ldap` aux commandes permettant d'ajouter des utilisateurs, des rôles et des profils de droits au référentiel LDAP. Ces commandes ajoutent des entrées pour les bases de données `user_attr`, `auth_attr`, `exec_attr`, et `prof_attr`. Pour plus d'informations, reportez-vous aux pages de manuel `user_attr(4)` et `useradd(1M)`.

3. **Supprimez l'entrée `+auto_master` du fichier `/setup/files/auto_master`.**

4 Créez les mappages automatiques de zone dans la zone de préparation.

```
# cp /zone/public/root/etc/auto_home_public /setup/files
# cp /zone/internal/root/etc/auto_home_internal /setup/files
# cp /zone/needtoknow/root/etc/auto_home_needtoknow /setup/files
# cp /zone/restricted/root/etc/auto_home_restricted /setup/files
```

Dans la liste de mappages automatiques suivante, la première ligne de chaque paire indique le nom du fichier. La deuxième ligne de chaque paire montre le contenu du fichier. Les noms de zones identifient les étiquettes sur la base du fichier `label_encodings` par défaut fourni avec le logiciel Trusted Extensions.

- Remplacez vos noms de zones par ceux qui apparaissent dans ces lignes.
- *myNFSserver* identifie le serveur NFS pour les répertoires personnels.

```
/setup/files/auto_home_public
 * myNFSserver_FQDN:/zone/public/root/export/home/&

/setup/files/auto_home_internal
 * myNFSserver_FQDN:/zone/internal/root/export/home/&

/setup/files/auto_home_needtoknow
 * myNFSserver_FQDN:/zone/needtoknow/root/export/home/&

/setup/files/auto_home_restricted
 * myNFSserver_FQDN:/zone/restricted/root/export/home/&
```

5 Utilisez la commande `ldapaddent` pour remplir le serveur d'annuaire avec chaque fichier de la zone de préparation.

Par exemple, la commande suivante permet de remplir le serveur à partir du fichier `hosts` de la zone de préparation.

```
# /usr/sbin/ldapaddent -D "cn=directory manager" \
-w dirmgr123 -a simple -f /setup/files/hosts hosts
```

6 Si vous avez exécuté la commande `ldapclient` sur le serveur d'annuaire Trusted Extensions, désactivez le client sur ce système.

Dans la zone globale, exécutez la commande `ldapclient l`. Utilisez la sortie détaillée pour vérifier que le système n'est plus un client LDAP.

```
# ldapclient -v uninit
```

Pour plus d'informations, reportez-vous à la page de manuel `ldapclient(1M)`.

7 Pour remplir la base de données du réseau Trusted Extensions dans LDAP, utilisez la commande `tncfg` avec l'option `-S ldap`.

Pour plus d'instructions, reportez-vous à la section "Étiquetage d'hôtes et de réseaux (liste des tâches)" à la page 224.

Création d'un proxy Trusted Extensions pour un serveur Oracle Directory Server Enterprise Edition existant

Tout d'abord, vous devez ajouter les bases de données Trusted Extensions au serveur d'annuaire existant sur un système Oracle Solaris. En second lieu, pour activer les systèmes Trusted Extensions afin qu'ils accèdent au serveur d'annuaire, vous devez configurer un système Trusted Extensions afin qu'il soit le serveur proxy LDAP.

▼ Création d'un serveur proxy LDAP

Si un serveur LDAP existe déjà sur votre site, créez un serveur proxy sur un système Trusted Extensions.

Avant de commencer

Vous avez rempli le serveur LDAP à partir d'un client qui a été modifié afin de définir le paramètre `enableShadowUpdate` sur `TRUE`. Pour connaître les conditions requises, reportez-vous à la section "Création d'un client LDAP pour le serveur d'annuaire" à la page 90.

En outre, vous avez ajouté les bases de données contenant des informations relatives à Trusted Extensions sur le serveur LDAP à partir d'un client sur lequel le paramètre `enableShadowUpdate` a été défini sur `TRUE`. Pour plus d'informations, reportez-vous à la section "Remplissage du serveur Oracle Directory Server Enterprise Edition" à la page 93.

Vous devez être superutilisateur dans la zone globale.

1 Sur un système configuré avec Trusted Extensions, créez un serveur proxy.

Remarque – Vous devez exécuter deux commandes `ldapclient`. Une fois la commande `ldapclient init` exécutée, exécutez la commande `ldapclient modify` pour définir le paramètre `enableShadowUpdate` sur `TRUE`.

Vous trouverez ci-dessous des exemples de commandes. La commande `ldapclient init` définit des valeurs de proxy.

```
# ldapclient init \
-a proxyDN=cn=proxyagent,ou=profile,dc=west,dc=example,dc=com \
-a domainName=west.example.com \
-a profileName=pit1 \
-a proxyPassword=test1234 192.168.0.1
System successfully configured
```

La commande `ldapclient mod` permet la mise à jour en double.

```
# ldapclient mod -a enableShadowUpdate=TRUE \
-a adminDN=cn=admin,ou=profile,dc=west,dc=example,dc=com \
-a adminPassword=admin-password
System successfully configured
```

Pour plus d'informations, reportez-vous au Chapitre 12, “Setting Up LDAP Clients (Tasks)” du manuel *Oracle Solaris Administration: Naming and Directory Services*.

2 Vérifiez que le serveur proxy peut consulter les bases de données Trusted Extensions.

```
# ldaplist -l database
```

Erreurs fréquentes Pour connaître les stratégies de résolution des problèmes de configuration LDAP, reportez-vous au Chapitre 13, “LDAP Troubleshooting (Reference)” du manuel *Oracle Solaris Administration: Naming and Directory Services*.

Création d'un client LDAP Trusted Extensions

La procédure ci-après permet de créer un client LDAP pour un serveur d'annuaire Trusted Extensions.

▼ Établissement de la zone globale en tant que client LDAP dans Trusted Extensions

Cette procédure permet d'établir la configuration du service de nommage LDAP pour la zone globale sur un client LDAP.

Utilisez le script `txzonemgr`.

Remarque – Si vous envisagez de configurer un serveur de noms dans chaque zone étiquetée, vous êtes responsable de l'établissement de la connexion de client LDAP pour chaque zone étiquetée.

Avant de commencer Le serveur Oracle Directory Server Enterprise Edition, c'est-à-dire le serveur d'annuaire LDAP, doit exister. Le serveur doit être rempli avec les bases de données Trusted Extensions, et ce système client doit être en mesure de contacter le serveur. Le serveur d'annuaire doit donc avoir affecté un modèle de sécurité à ce client. Une affectation spécifique n'est pas nécessaire ; une affectation à l'aide de caractères génériques est suffisante.

Vous devez être dans le rôle `root` dans la zone globale.

1 Si vous utilisez DNS, ajoutez `dns` à la configuration `name-service/switch` .

Le fichier de commutation du service de nommage standard pour LDAP est trop restrictif pour Trusted Extensions.

a. Affichez la configuration actuelle.

```
# svccfg -s name-service/switch listprop config
config                      application
config/value_authorization  astring       solaris.smf.value.name-service.switch
config/default              astring       files ldap
config/netgroup             astring       ldap
config/printer              astring       "user files ldap"
```

b. Ajoutez `dns` à la propriété `host` et actualisez le service.

```
# svccfg -s name-service/switch setprop config/host = astring: "files dns ldap"
# svccfg -s name-service/switch:default refresh
```

c. Vérifiez la nouvelle configuration.

```
# svccfg -s name-service/switch listprop config
config                      application
config/value_authorization  astring       solaris.smf.value.name-service.switch
config/default              astring       files ldap
config/host                 astring       files dns ldap
config/netgroup             astring       ldap
config/printer              astring       "user files ldap"
```

Les bases de données Trusted Extensions utilisent la configuration par défaut `files ldap` et ne sont donc pas répertoriées.

2 Pour créer un client LDAP, exécutez la commande `txzonemgr` sans option.

```
# txzonemgr &
```

a. Double-cliquez sur la zone globale.

b. Sélectionnez Create LDAP Client (Créer client LDAP).

c. Répondez aux invites suivantes et cliquez sur OK après chaque réponse :

```
Enter Domain Name:                          Type the domain name
Enter Hostname of LDAP Server:              Type the name of the server
Enter IP Address of LDAP Server servername:     Type the IP address
Enter LDAP Proxy Password:              Type the password to the server
Confirm LDAP Proxy Password:            Retype the password to the server
Enter LDAP Profile Name:                Type the profile name
```

d. Validez ou annulez les valeurs affichées.

```
Proceed to create LDAP Client?
```

Lorsque vous confirmez l'opération, le script `txzonemgr` exécute la commande `ldapclient init`.

3 **Terminez la configuration du client en activant les mises à jour en double.**

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

4 **Vérifiez que les informations sur le serveur sont correctes.**

a. **Ouvrez une fenêtre de terminal et envoyez une requête au serveur LDAP.**

```
# ldapclient list
```

La sortie est similaire à la suivante :

```
NS_LDAP_FILE_VERSION= 2.0
NS_LDAP_BINDDN= cn=proxyagent,ou=profile,dc=domain-name
...
NS_LDAP_BIND_TIME= number
```

b. **Corrigez les erreurs, le cas échéant.**

Si vous obtenez une erreur, répétez les étapes de l'Étape 2 à l'Étape 4. Par exemple, l'erreur suivante peut indiquer que le système ne possède pas d'entrée sur le serveur LDAP :

```
LDAP ERROR (91): Can't connect to the LDAP server.
Failed to find defaultSearchBase for domain domain-name
```

Pour corriger cette erreur, vous devez vérifier le serveur LDAP.

PARTIE II

Administration de Trusted Extensions

Les chapitres de cette partie décrivent comment administrer Trusted Extensions.

Le Chapitre 6, “Concepts d'administration de Trusted Extensions” introduit la fonction Trusted Extensions.

Le Chapitre 7, “Outils d'administration de Trusted Extensions” décrit les programmes d'administration qui sont spécifiques à Trusted Extensions.

Le Chapitre 8, “Exigences de sécurité sur un système Trusted Extensions (présentation)” décrit les exigences en matière de sécurité qui sont requises et configurables dans Trusted Extensions.

Le Chapitre 9, “Exécution de tâches courantes dans Trusted Extensions (tâches)” présente l'administration Trusted Extensions.

Le Chapitre 10, “Utilisateurs, droits et rôles dans Trusted Extensions (présentation)” introduit le contrôle d'accès basé sur les rôles (RBAC) dans Trusted Extensions.

Le Chapitre 11, “Gestion des utilisateurs, des droits et des rôles dans Trusted Extensions (tâches) ” fournit des instructions sur la gestion des utilisateurs standard de Trusted Extensions.

Le Chapitre 12, “Administration à distance dans Trusted Extensions (tâches)” fournit des instructions sur l'administration à distance de Trusted Extensions.

Le Chapitre 13, “Gestion des zones dans Trusted Extensions (tâches)” fournit des instructions sur la gestion des zones étiquetées.

Le Chapitre 14, “Gestion et montage de fichiers dans Trusted Extensions (tâches)” fournit des instructions sur la gestion du montage et de la sauvegarde du système et décrit des tâches relatives aux fichiers dans Trusted Extensions.

Le Chapitre 15, “Gestion de réseaux de confiance (présentation)” fournit un aperçu des bases de données réseau et du routage dans Trusted Extensions.

Le Chapitre 16, “Gestion des réseaux dans Trusted Extensions (tâches) ” fournit des instructions sur la gestion des bases de données réseau et le routage dans Trusted Extensions.

Le Chapitre 18, “Messagerie multiniveau dans Trusted Extensions (présentation) ” décrit les problèmes spécifiquement liés à la messagerie dans Trusted Extensions.

Le Chapitre 19, “Gestion de l'impression étiquetée (tâches)” fournit des instructions sur la gestion de l'impression Trusted Extensions.

Le Chapitre 20, “Périphériques dans Trusted Extensions (présentation)” décrit les extensions fournies par Trusted Extensions pour la protection des périphériques dans Oracle Solaris.

Le Chapitre 21, “Gestion des périphériques pour Trusted Extensions (tâches) ” fournit des instructions sur la gestion de périphériques à l'aide du gestionnaire de périphériques (Device Manager).

Le Chapitre 22, “Audit de Trusted Extensions (présentation) ” fournit des informations relatives à l'audit spécifiques à Trusted Extensions.

Le Chapitre 23, “Gestion des logiciels dans Trusted Extensions (Référence)” décrit comment administrer les applications sur un système Trusted Extensions.

◆ ◆ ◆ CHAPITRE 6

Concepts d'administration de Trusted Extensions

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

Trusted Extensions et le SE Oracle Solaris

Le logiciel Trusted Extensions ajoute des étiquettes à un système qui exécute le SE Oracle Solaris. Les étiquettes appliquent un *contrôle d'accès obligatoire* (MAC). Le MAC et le contrôle d'accès discrétionnaire (DAC) 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 d'Oracle Solaris. Vous pouvez utiliser le shell sécurisé, BART, la structure cryptographique, IPsec et IP Filter avec Trusted Extensions. Toutes les fonctions du système de fichiers ZFS sont disponibles dans Trusted Extensions, y compris les instantanés et le chiffrement.

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. Reportez-vous également à l'Annexe C, “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 activées sur un système Trusted Extensions. Par exemple, de nombreux sites qui configurent Trusted Extensions requièrent une séparation des tâches lors de la création des utilisateurs et de l'affectation des attributs de sécurité.
- Trusted Extensions peut modifier le comportement par défaut d'Oracle Solaris. Par exemple, un système configuré avec Trusted Extensions exige l'allocation des périphériques.
- Trusted Extensions peut restreindre les options disponibles dans Oracle Solaris. Par exemple, toutes les zones sont étiquetées dans Trusted Extensions. Contrairement à ce qui se passe dans 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 une version multiniveau du bureau Oracle Solaris, Solaris Trusted Extensions (GNOME). Le nom peut être abrégé en Trusted GNOME.

- 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 l'interface utilisateur graphique Device Manager (Gestionnaire de périphériques) pour administrer les périphériques. En outre, la commande `updatehome` permet de placer les fichiers de démarrage dans les répertoires personnels des utilisateurs sous chaque étiquette.
- Trusted Extensions requiert l'utilisation d'interfaces utilisateur graphiques spécifiques pour l'administration. Par exemple, sur un système configuré avec Trusted Extensions, l'administration des zones étiquetées est assurée à l'aide du gestionnaire de zones étiquetées (Labeled Zone Manager), en plus de la commande `zonecfg`.
- 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. Par défaut, les utilisateurs standard ne peuvent pas arrêter le système.

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 écrans d'un système multiécran, Trusted GNOME affiche une bande de confiance sur chaque moniteur.

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 de périphériques (Device 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 le *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

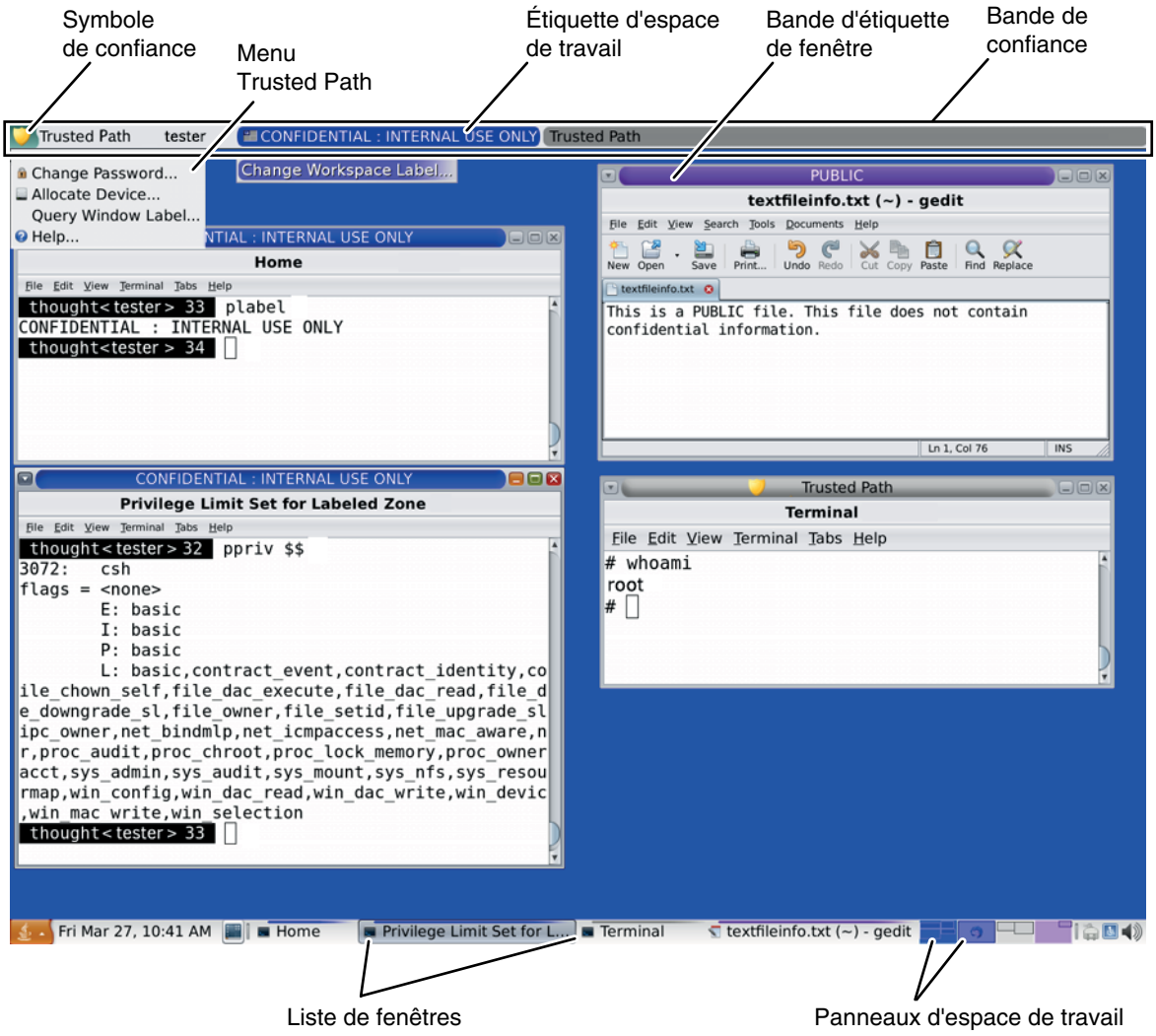
Protections Trusted Extensions

Le logiciel Trusted Extensions renforce la protection du SE Oracle Solaris. 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 nécessitent des mots de passe supplémentaires pour effectuer les tâches d'administration et 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. DansTrusted GNOME, 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 6–1.

FIGURE 6–1 Bureau multiniveau Trusted Extensions



Le logiciel au cœur même de la sécurité, la base informatique sécurisée (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 peuvent interagir 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 fournies par 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.

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`, `SECRET` ou `PUBLIC`. 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 allouables, les réseaux, les mémoires graphiques et les autres systèmes.

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 considérées 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 6–1 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`
`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 des composants** : 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 *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 graphiques et les commandes. 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`.
- **IPsec et IKE** : les associations de sécurité IPsec et les règles IKE ont des étiquettes.
- **Interfaces réseau** : des modèles de sécurité décrivant leur plage d'étiquettes sont assignés aux adresses IP (hôtes). Une étiquette par défaut est également attribuée aux hôtes sans étiquette par le système Trusted Extensions avec lequel ils communiquent.
- **Imprimantes et impression** : les imprimantes possèdent des plages d'étiquettes. Pour configurer les imprimantes dans Trusted Extensions, reportez-vous au Chapitre 19, “Gestion de l'impression étiquetée (tâches)”.
- **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 panneau de l'espace de travail et au-dessus de la barre de titre des fenêtres, comme illustré à la Figure 6–1.

  Lorsqu'une fenêtre est déplacée vers un espace de travail étiqueté différemment, la fenêtre conserve son étiquette d'origine. Les processus lancés dans cette fenêtre s'exécutent sous l'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)`.

Rôles et Trusted Extensions

Sur un système exécutant 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.

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.

Comme dans Oracle Solaris, les profils de droits sont à l'origine des capacités d'un rôle. Pour plus d'informations sur les profils de droits et les rôles, reportez-vous au Chapitre 8, “Utilisation des rôles et des privilèges (présentation)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

◆ ◆ ◆ CHAPITRE 7

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, applications et scripts de confiance. Le tableau ci-dessous contient un récapitulatif de ces outils d'administration.

TABLEAU 7–1 Outils d'administration de Trusted Extensions

Outil	Description	Pour plus d'informations
`/usr/sbin/txzonemgr`	Crée l'interface utilisateur graphique du gestionnaire de zones étiquetées (Labeled Zone Manager) permettant de créer et de configurer des zones étiquetées, mise en réseau comprise. Des options de ligne de commande permettent la création automatique de zones nommées par l'utilisateur.	Reportez-vous à la section "Création de zones étiquetées" à la page 58 et à la page de manuel `txzonemgr`(1M). `txzonemgr` est un script `zenity` (1).
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 de périphériques" à la page 115 et "Manipulation des périphériques dans Trusted Extensions (liste des tâches)" à la page 279.
Générateur d'étiquettes (Label Builder)	Constitue également un outil utilisateur. Il s'affiche lorsqu'un programme vous demande de choisir une étiquette.	Pour consulter un exemple, reportez-vous à la section "Procédure de modification d'une plage d'étiquettes d'utilisateur" à la page 155.
Gestionnaire de sélection (Selection Manager)	Autre outil destiné aux utilisateurs autorisés à modifier le niveau de sécurité des données. S'affiche lorsqu'un programme requiert la modification du niveau de sécurité de données.	Pour plus d'informations sur l'autorisation des utilisateurs, 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 160. Pour consulter un exemple, reportez-vous à la section "Procédure de déplacement de données entre les étiquettes" du manuel *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.
Commandes de Trusted Extensions	Permettent d'effectuer des tâches d'administration	Pour obtenir la liste des commandes d'administration et des fichiers de configuration, reportez-vous à l'Annexe D, "Liste des pages de manuel Trusted Extensions".

Script txzonemgr

La commande `/usr/sbin/txzonemgr` offre deux modes.

- Sous forme d'interface de ligne de commande, la commande crée des zones étiquetées à partir de fichiers existants. Exécutée avec l'option de commande `-c`, l'interface de ligne de commande crée et initialise deux zones étiquetées. L'option `-d` supprime toutes les zones étiquetées.
- Sous forme d'interface utilisateur graphique, le script affiche une boîte de dialogue portant le titre Labeled Zone Manager (Gestionnaire de zones étiquetées). Cette interface graphique vous guide lors de la création et de l'initialisation de zones étiquetées. Le script inclut le clonage d'une zone pour créer un instantané. En outre, l'interface utilisateur propose des menus pour la gestion réseau, le service de nommage et la configuration LDAP.

La commande `txzonemgr` exécute un script `zenity`(1). La boîte de dialogue du gestionnaire de zones étiquetées affiche uniquement les choix valides pour l'état de configuration actuel d'une zone étiquetée. Par exemple, si une zone est déjà étiquetée, l'option de menu Label (Étiquette) ne s'affiche pas.

Gestionnaire 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 de périphériques (Device Manager). Le gestionnaire 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 de périphériques, lequel exécute un autre script de nettoyage, démonte et libère le périphérique.

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

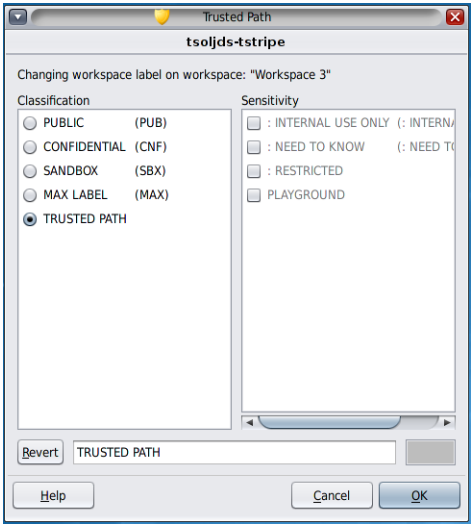
Pour plus d'informations sur la protection des périphériques dans Trusted Extensions, reportez-vous au Chapitre 21, “Gestion des périphériques pour Trusted Extensions (tâches) ”.

Gestionnaire de sélection dans Trusted Extensions

L'interface utilisateur graphique du gestionnaire de sélection (Selection Manager) s'affiche lorsque vous tentez de modifier l'étiquette d'un objet ou d'une sélection. Pour plus d'informations, reportez-vous à la section “Règles lors de la modification du niveau de sécurité des données” à la page 125.

Générateur d'étiquettes dans Trusted Extensions

L'interface utilisateur graphique du générateur d'étiquettes (Label Builder) 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 manuel *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. 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 composants figurant dans la colonne Sensitivity (Sensibilité) correspondent à la section `WORDS` (MOTS) du fichier `label_encodings`.

Les développeurs peuvent se servir de la commande `tgnome-selectlabel` pour construire des générateurs d'étiquettes pour leurs applications. Entrez `tgnome-selectlabel -h` pour afficher l'aide en ligne. Reportez-vous également au Chapitre 6, “Label Builder GUI” du manuel *Trusted Extensions Developer's Guide*.

Outils de ligne de commande dans Trusted Extensions

Les commandes propres à Trusted Extensions et les commandes modifiés par Trusted Extensions sont répertoriées dans le manuel de référence d'Oracle Solaris (*Oracle Solaris Reference Manual*). La commande `man` permet d'afficher toutes les commandes. Pour obtenir une description des commandes, des liens vers des exemples dans la collection de guides relatifs à Trusted Extensions et un lien vers les pages de manuel, reportez-vous à l'Annexe D, “Liste des pages de manuel Trusted Extensions”.

Fichiers de configuration dans Trusted Extensions

Trusted Extensions augmente le fichier `/etc/inet/ike/config` et y inclut les informations relatives aux étiquettes. La page de manuel `ike.config(4)` décrit le paramètre global `label_aware` ainsi que trois paramètres transform de la phase 1, `single_label`, `multi_label` et `wire_label`.

Remarque – Le fichier de configuration IKE contient un mot-clé, `label`, qui est utilisé pour rendre unique une règle IKE de phase 1. Le mot-clé IKE `label` est différent des étiquettes Trusted Extensions.

◆ ◆ ◆ CHAPITRE 8

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

Trusted Extensions utilise les mêmes fonctions de sécurité que celles fournies par 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.

Trusted Extensions diffère d'Oracle Solaris en ce que les systèmes sont généralement administrés en assumant un rôle. Comme dans le SE Oracle Solaris, les fichiers de configuration sont modifiés par le rôle `root`.

Rôles dans Trusted Extensions

Dans Trusted Extensions, le système est traditionnellement administré par le biais des rôles. Superutilisateur est le rôle `root` et est requis pour certaines tâches, comme le paramétrage des indicateurs d'audit, la modification d'un mot de passe de compte et la modification de fichiers système. Les rôles sont créés de la même manière que dans Oracle Solaris.

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

- **Rôle** `root`: créé lors de l'installation d'Oracle Solaris
- **Rôle d'administrateur de sécurité** : créé pendant ou après la configuration initiale par l'équipe de configuration initiale
- **Rôle d'administrateur système** : créé pendant ou après la configuration initiale par l'équipe chargée de la configuration initiale

Création de rôles dans Trusted Extensions

Pour administrer Trusted Extensions, vous créez des rôles qui répartissent les fonctions système et les fonctions de sécurité.

Le processus de création d'un rôle dans Trusted Extensions est le même que dans SE Oracle Solaris. Par défaut, les rôles sont affectés à la plage d'étiquettes d'administration de `ADMIN_HIGH` à `ADMIN_LOW`.

- Pour une présentation de la création de rôles, reportez-vous à la section "Utilisation de RBAC (tâches)" du manuel *Administration d'Oracle Solaris : services de sécurité*.
- Pour créer des rôles, reportez-vous à la section "Procédure de création d'un rôle" du manuel *Administration d'Oracle Solaris : services de sécurité*.

Choix d'un rôle dans Trusted Extensions

Sur le bureau de confiance, vous pouvez assumer un rôle affecté en cliquant sur votre nom d'utilisateur dans la bande de confiance, puis en sélectionnant le(s) rôle(s) de votre choix. Après avoir confirmé le mot de passe du rôle, l'espace de travail en cours bascule sur un espace de travail de rôle. Un espace de travail de rôle se situe dans la zone globale et possède l'attribut du chemin de confiance. Les espaces de travail des rôles sont des espaces de travail d'administration.

Interfaces de Trusted Extensions pour la configuration des fonctions de sécurité

Dans Trusted Extensions, vous pouvez étendre les fonctions de sécurité existantes. En outre, Trusted Extensions offre des fonctions de sécurité uniques.

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

Les mécanismes de sécurité d'Oracle Solaris suivants sont extensibles dans Trusted Extensions de la même manière que dans Oracle Solaris :

- **Classes d'audit** : l'ajout de classes d'audit est décrit au Chapitre 28, "Gestion de l'audit (tâches)" du manuel *Administration d'Oracle Solaris : services de sécurité*.

  Remarque – Les fournisseurs qui souhaitent ajouter des *événements d'audit* doivent contacter un représentant Oracle Solaris pour réserver des numéros d'événement et obtenir l'accès aux interfaces d'audit.

- **Rôles et profils de droits** : l'ajout de rôles et de profils de droits est décrit au Chapitre 9, "Utilisation du contrôle d'accès basé sur les rôles (tâches)" du manuel *Administration d'Oracle Solaris : services de sécurité*.
- **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 288.

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

Fonctions de sécurité Trusted Extensions uniques

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. Les espaces de travail et leurs objets sont étiquetés.
- **Gestionnaire de périphériques (Device Manager) :** par défaut, les périphériques sont protégés par des conditions d'allocation. L'interface graphique du gestionnaire de périphériques est l'interface destinée aux administrateurs et aux utilisateurs standard.
- **Menu Change Password (Modifier le mot de passe) :** ce menu vous permet de modifier votre mot de passe utilisateur ou de rôle.
- **Option de menu Change Workspace Label (Modifier l'étiquette de l'espace de travail)** : les utilisateurs des sessions multiniveau peuvent modifier l'étiquette de l'espace de travail. Un mot de passe peut être demandé aux utilisateurs lorsqu'ils entrent dans l'espace de travail d'une autre étiquette.

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 fournir des suggestions supplémentaires.

Utilisation d'e-mails

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

Informez les utilisateurs du fait qu'ils ne doivent 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, vous devez vous assurer que le nom d'utilisateur 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 (contrôle d'accès discrétionnaire) et de la protection MAC (contrôle d'accès obligatoire) pour les fichiers critiques. Sont notamment critiques les fichiers suivants :

- **Fichier** `shadow` : contient des mots de passe chiffrés. Reportez-vous à la page de manuel `shadow(4)`.
- **Fichier** `auth_attr` : contient des autorisations personnalisées. Reportez-vous à la page de manuel `auth_attr(4)`.
- **Fichier** `prof_attr` : contient des profils de droits personnalisés. Reportez-vous à la page de manuel `prof_attr(4)`.
- **Fichier** `exec_attr` : contient des commandes avec attributs de sécurité ajoutés aux profils de droits par le site. Reportez-vous à la page de manuel `exec_attr(4)`.

- **Piste d'audit** : contient les enregistrements d'audit collectés par le service. Reportez-vous à la page de manuel `audit.log(4)`.

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 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 (Selection Manager) sert d'intermédiaire pour le transfert. Le fichier `/usr/share/gnome/sel_config` contrôle les actions de modification de l'étiquette de fichiers et les opérations de couper-copier d'informations vers une autre étiquette. L'application `/usr/bin/tsoljdsselmgr` contrôle les opérations de glisser-déplacer 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 8–1 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 navigateurs de fichiers	Même étiquette	ID utilisateur identique	Aucun
	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`

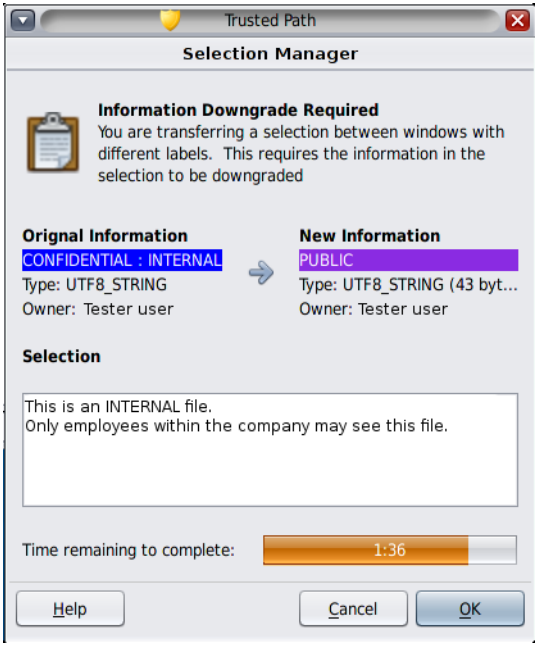
Des règles différentes s'appliquent aux sélections dans une fenêtre ou un fichier. L'opération de glisser-déposer de *sélections* nécessite toujours des étiquettes et des propriétaires identiques. L'opération de glisser-déposer entre les fenêtres est effectuée par le biais de l'application gestionnaire 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 8–2 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	Aucun
	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, deux lignes, 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 `/usr/share/gnome/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.

◆ ◆ ◆ CHAPITRE 9

Exécution de tâches courantes dans Trusted Extensions (tâches)

Ce chapitre vous initie à l'administration des systèmes Trusted Extensions et contient les tâches fréquemment effectuées sur ces systèmes.

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
Connexion à un système Trusted Extensions	Vous permet de vous connecter en toute sécurité.	"Connexion à Trusted Extensions" du manuel *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'utilisation des pages de manuel Trusted Extensions.	"Travail sur un système étiqueté" du manuel *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 manuel *Guide de l'utilisateur Oracle Solaris Trusted Extensions*

Tâche	Description	Voir
Choix d'un rôle à assumer	Vous permet de vous situer dans 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 130
Choix d'un espace de travail d'utilisateur	Vous permet de quitter la zone globale.	"Sortie de la zone globale dans Trusted Extensions " à la page 130

▼ 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.

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 153.

Avant de commencer Un rôle d'administration vous est affecté. Pour les pointeurs, reportez-vous à la section "Création de rôles dans Trusted Extensions " à la page 120.

1 **Cliquez sur *account-name* dans la bande de confiance.**

Sélectionnez un rôle dans la liste.

Pour connaître l'emplacement des fonctions du bureau Trusted Extensions reportez-vous à la Figure 6–1. Pour obtenir une explication de ces fonctions, reportez-vous au Chapitre 4, "Eléments de Trusted Extensions (Référence)" du manuel *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

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

Une fois l'authentification terminée, l'espace de travail en cours est modifié pour l'espace de travail du rôle.

▼ Sortie de la zone globale dans Trusted Extensions

Avant de commencer Vous vous trouvez dans la zone globale.

1 **Sélectionnez un espace de travail d'utilisateur à partir du panneau du bureau situé au bas de l'écran.**

2 **Ou cliquez sur votre nom de rôle dans la bande de confiance, puis sélectionnez votre nom d'utilisateur.**

L'espace de travail en cours est modifié pour un espace de travail d'utilisateur. Toutes les fenêtres créées ultérieurement dans cet espace de travail seront créées sous votre étiquette utilisateur.

Les fenêtres que vous avez créées dans l'espace de travail du rôle continuent de prendre en charge les processus sous l'étiquette de ce rôle. Les processus lancés dans ces fenêtres s'exécutent dans la zone globale avec des privilèges d'administration.

Pour plus d'informations, reportez-vous à la section "Travail sur un système étiqueté" du manuel *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

Tâches courantes dans Trusted Extensions (liste des tâches)

La liste des tâches ci-dessous décrit les procédures d'administration dans Trusted Extensions.

Tâche	Description	Voir
Modification du mot de passe pour `root`	Spécifie un nouveau mot de passe pour le rôle `root`.	"Procédure de modification du mot de passe pour `root`" à la page 132
Répercussion de la modification d'un mot de passe dans une zone étiquetée	Réinitialise la zone pour la mettre à jour après la modification d'un mot de passe.	"Procédure d'application d'un nouveau mot de passe utilisateur local dans une zone étiquetée" à la page 132
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 133
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 134
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 135
Allocation d'un périphérique	Permet aux utilisateurs d'allouer des périphériques. Permet d'utiliser un périphérique pour ajouter ou supprimer des informations du système.	"Procédure d'autorisation des utilisateurs à allouer un périphérique" du manuel *Administration d'Oracle Solaris : services de sécurité* "Procédure d'allocation d'un périphérique dans Trusted Extensions" du manuel *Guide de l'utilisateur Oracle Solaris Trusted Extensions*
Administration à distance d'un système	Administre les systèmes Trusted Extensions à partir d'un système distant.	Chapitre 12, "Administration à distance dans Trusted Extensions (tâches)"

▼ Procédure de modification du mot de passe pour root

Trusted Extensions fournit une interface graphique permettant de modifier votre mot de passe.

1. **Assumez le rôle `root`.**

   Pour connaître la procédure à suivre, reportez-vous à la section "Accès à la zone globale dans Trusted Extensions " à la page 130.

2. **Ouvrez le menu Trusted Path (Chemin de confiance) en cliquant sur le symbole de confiance dans la bande de confiance.**

3. **Choisissez Change Login Password (Changer de mot de passe de connexion).**

   Si des mots de passe distincts sont créés par zone, le menu peut lire l'option Change Workspace Password (Changer de mot de passe d'espace de travail).

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

▼ Procédure d'application d'un nouveau mot de passe utilisateur local dans une zone étiquetée

Les zones étiquetées doivent être réinitialisées lorsque les conditions suivantes sont remplies :

- Un ou plusieurs utilisateurs locaux ont changé leurs mots de passe.
- Toutes les zones utilisent une instance unique du démon de cache de service de nommage (`nscd`).
- Le système est géré avec des fichiers et non avec LDAP.

Avant de commencer Le profil de droits Zone Security doit vous être affecté.

- **Pour appliquer la modification du mot de passe, réinitialisez les zones étiquetées auxquelles les utilisateurs peuvent accéder.**

  Utilisez l'une des méthodes suivantes :

  - **Utilisez l'interface graphique utilisateur `txzonemgr`.**

    ```
    # txzonemgr &
    ```

    Dans le gestionnaire de zones étiquetées (Labeled Zone Manager), accédez à la zone étiquetée et, dans la liste des commandes, sélectionnez Halt (Arrêter), puis Boot (Init).

  - **Dans une fenêtre de terminal de la zone globale, utilisez les commandes d'administration de la zone.**

    Vous pouvez choisir d'éteindre ou d'arrêter le système.

- La commande `zlogin` permet d'arrêter correctement la zone.

```
# zlogin labeled-zone shutdown -i 0
# zoneadm -z labeled-zone boot
```

- La sous-commande `halt` permet d'ignorer les scripts de fermeture.

```
# zoneadm -z labeled-zone halt
# zoneadm -z labeled-zone boot
```

Erreurs fréquentes

Pour mettre à jour automatiquement les mots de passe des utilisateurs des zones étiquetées, vous devez soit configurer LDAP, soit configurer un service de nommage par zone. Vous pouvez également configurer les deux.

- Pour configurer LDAP, reportez-vous au Chapitre 5, “Configuration de LDAP pour Trusted Extensions (tâches)”.
- La configuration d'un service de nommage par zone requiert des compétences avancées en matière de gestion de réseaux. Pour plus d'informations sur cette procédure, reportez-vous à la section “Procédure de configuration d'un service de noms distinct pour chaque zone étiquetée” à la page 68.

▼ 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 9–1 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 9–2 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 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 130.

- **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 : INTERNAL USE ONLY"
    0x0004-08-48
    ```

    La chaîne n'est pas sensible à la casse mais les espaces doivent être respectés. Par exemple, les chaînes entre guillemets suivantes renvoient une étiquette hexadécimale :

    - `"CONFIDENTIAL : INTERNAL USE ONLY"`
    - `"cnf : Internal"`
    - `"confidential : internal"`

    Les chaînes entre guillemets suivantes renvoient une erreur d'analyse syntaxique :

    - `"confidential:internal"`

- `"confidential:internal"`

- **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 `label_encodings`, le texte équivalent à une étiquette d'autorisation n'inclut pas les deux-points (:).

Exemple 9–3 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 dans le rôle d'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

Comme dans Oracle Solaris, dans Trusted Extensions, le compte `root` permet de modifier les valeurs de sécurité par défaut sur un système.

Les répertoires `/etc/security` et `/etc/default` contiennent les valeurs de sécurité. Pour plus d'informations, reportez-vous au Chapitre 3, "Contrôle de l'accès aux systèmes (tâches)" du manuel *Administration d'Oracle Solaris : services de sécurité*.

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 dans le rôle `root` dans la zone globale.

- **Modifiez le fichier système.**

  Le tableau ci-dessous répertorie les fichiers de sécurité et les valeurs de sécurité pouvant être modifiées 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 de la section "Procédure de contrôle de toutes les tentatives de connexion ayant échoué" du manuel *Administration d'Oracle Solaris : services de sécurité*. Page de manuel `passwd(1)`

Fichier	Tâche	Pour plus d'informations
`etc/default/kbd`	Désactiver l'arrêt du clavier	"Procédure de désactivation de la séquence d'abandon d'un système" du manuel *Administration d'Oracle Solaris : services de sécurité* **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`. 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 10

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" à la page 69.

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.
- Les commandes dans un profil de droits Trusted Extensions comportent un attribut d'étiquette. La commande doit être effectuée dans une plage d'étiquettes ou sous une étiquette donnée.
- Le logiciel Trusted Extensions permet d'ajouter des privilèges et des autorisations à l'ensemble de privilèges et d'autorisations défini par 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.

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

- "Configuration et administration des comptes utilisateur (liste des tâches) " du manuel *Administration d'Oracle Solaris : Tâches courantes*
- Partie III, "Rôles, profils de droits et privilèges" du manuel *Administration d'Oracle Solaris : services de sécurité*

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 ;
- l'affectation du mot de passe initial ;
- 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 rôle `root` peut créer le profil.

Avant de créer un profil de droits, l'administrateur de sécurité doit analyser si des commandes 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.

Décisions à prendre avant de créer des utilisateurs dans Trusted Extensions

Les décisions suivantes ont une incidence sur les actions que les utilisateurs peuvent effectuer dans Trusted Extensions et sur l'effort nécessaire. 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 à l'origine 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 142.
- 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 150.
- Décidez si les utilisateurs peuvent accéder aux périphériques, tels que le microphone, l'unité de CD-ROM et les périphériques USB.

  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 292. Pour créer 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 288.

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 143.

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" à la page 29 et sur des exemples de la section *Trusted Extensions Label Administration*.

Les valeurs d'étiquettes explicitement définies par l'administrateur de sécurité pour des utilisateurs individuels remplacent les valeurs figurant dans le fichier `label_encodings`.

Valeurs par défaut du fichier policy.conf dans Trusted Extensions

Le fichier `/etc/security/policy.conf` contient les paramètres de sécurité par défaut du système. Trusted Extensions permet d'ajouter deux mots-clés à ce fichier. Pour changer les valeurs à l'échelle du système, ajoutez les paires *mot-clé =valeur* suivantes au fichier. Le tableau suivant répertorie les valeurs par défaut et les valeurs possibles de ces mots-clés.

TABLEAU 10–1 Paramètres de sécurité Trusted Extensions par défaut dans le fichier policy.conf

Mot-clé	Valeur par défaut	Valeurs possibles	Remarques
`IDLECMD`	`LOCK`	`LOCK` | `LOGOUT`	S'applique à l'utilisateur de connexion.
`IDLETIME`	`30`	`0` à `120` minutes	S'applique à l'utilisateur de connexion.

Les autorisations et les profils de droits 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" à la page 34 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

Pour les utilisateurs qui peuvent se connecter à plus d'une étiquette, vous pouvez également souhaiter paramétrer les fichiers auxiliaires `.copy_` et `.link_files` dans le répertoire personnel de l'étiquette minimale de chaque utilisateur. Pour plus d'informations, reportez-vous à la section "Fichiers `.copy_files` et `.link_files`" à la page 145.

Attributs de sécurité devant être affectés aux utilisateurs

L'administrateur de sécurité peut modifier les attributs de sécurité des nouveaux utilisateurs. Pour plus d'informations sur les fichiers contenant les valeurs par défaut, reportez-vous à la section "Attributs de sécurité utilisateur par défaut dans Trusted Extensions" à la page 142. Le tableau suivant présente les attributs de sécurité pouvant être affectés aux utilisateurs et l'effet de chaque affectation.

TABLEAU 10–2 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'affectation
Mot de passe	Aucun	Requis	L'utilisateur dispose d'un mot de passe
Rôles	Aucun	Facultatif	L'utilisateur peut assumer un rôle
Autorisations	Fichier `policy.conf`	Facultatif	L'utilisateur dispose d'autorisations supplémentaires
Profils de droits	Fichier `policy.conf`	Facultatif	L'utilisateur dispose de profils de droits supplémentaires
Étiquettes	Fichier `label_encodings`	Facultatif	L'utilisateur dispose d'une étiquette ou d'une plage d'accréditations par défaut différente.
Privilèges	Fichier `policy.conf`	Facultatif	L'utilisateur dispose d'un ensemble de privilèges différent
Utilisation du compte	Fichier `policy.conf`	Facultatif	L'utilisateur dispose d'un paramétrage différent pour l'ordinateur lorsque ce dernier est inactif
Audit	Noyau	Facultatif	L'audit auquel est soumis l'utilisateur n'est pas le même que celui prévu par les paramètres d'audit par défaut du système.

Affectation d'attributs de sécurité aux utilisateurs dans Trusted Extensions

Une fois que les comptes utilisateur ont été créés, l'administrateur de sécurité affecte des attributs de sécurité aux utilisateurs. 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.

Lorsque vous affectez des attributs de sécurité aux utilisateurs, prenez en compte les informations suivantes :

Affectation de mots de passe
L'administrateur système peut affecter des mots de passe aux comptes utilisateur lors de la création des comptes. Après cette affectation initiale, l'administrateur de sécurité ou l'utilisateur peut modifier le mot de passe.

Comme dans 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'affectation d'un rôle aux utilisateurs n'est pas obligatoire. Plusieurs rôles peuvent être affectés à un 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 à un utilisateur ajoute ces autorisations aux autorisations existantes. La meilleure pratique consiste à ajouter les autorisations à un profil de droits, puis à affecter le profil à l'utilisateur.

Affectation de profils de droits
Comme dans le SE Oracle Solaris, l'ordre des profils de droits est important. A l'exception des autorisations, le mécanisme des profils utilise la valeur de la première instance d'un attribut de sécurité assigné. Pour plus d'informations, reportez-vous à la section "Ordre de recherche pour les attributs de sécurité affectés" du manuel *Administration d'Oracle Solaris : services de sécurité*.

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'assignez pas de profil de droits incluant 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 le jeu de privilèges pour des utilisateurs individuels, reportez-vous à la section "Procédure de limitation du jeu de privilèges d'un utilisateur" à la page 159.

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, affecter des classes d'audit à un utilisateur modifie le masque de présélection de l'utilisateur. Pour plus d'informations sur l'audit, reportez-vous à la section Partie VII, "Audit dans Oracle Solaris" du manuel *Administration d'Oracle Solaris : services de sécurité* et au chapitre Chapitre 22, "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 150.

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                 .cshrc                  .mime_types
.aliases                .emacs                  .newsrc
.bashrc                 .login                  .signature
.bashrc.user            .mailrc                 .soffice
```

◆ ◆ ◆ CHAPITRE 11

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. La plupart de ces tâches sont effectuées avant que les utilisateurs standard puissent se connecter.

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 148
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 149
	Active l'économiseur d'écran ou déconnecte l'utilisateur après une durée définie d'inactivité du système.	Exemple 11–1
	Supprime les privilèges inutiles de tous les utilisateurs standard d'un système.	Exemple 11–2

Tâche	Description	Voir
Configuration de fichiers d'initialisation pour les utilisateurs	Configure les fichiers de démarrage tels que `.bashrc`, `.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 150
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 152
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 153

▼ 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 système Trusted Extensions.

Attention – Vous devez terminer cette tâche afin que les utilisateurs standard puissent accéder au 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 130.

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 au Tableau 1–2 in "Planification de la sécurité de l'utilisateur dans Trusted Extensions" à la page 34.

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

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

Attention – Le fichier `label_encodings` doit être identique sur tous les systèmes. Pour une méthode de distribution, reportez-vous aux sections "Copie de fichiers sur un média amovible dans Trusted Extensions" à la page 81 et "Copie de fichiers dans Trusted Extensions à partir d'un média amovible" à la page 82.

▼ 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 Oracle Solaris. Utilisez cette procédure pour modifier les paramètres par défaut pour tous les utilisateurs d'un système.

Avant de commencer Vous devez être dans le rôle `root` dans la zone globale. Pour plus d'informations, reportez-vous à la section "Accès à la zone globale dans Trusted Extensions " à la page 130.

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

   Pour les mots-clés de Trusted Extensions, reportez-vous au Tableau 10–1.

2. **Modifiez les paramètres.**

Exemple 11–1 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. Par conséquent, le rôle `root` ajoute la paire `IDLECMD` *keyword= value* au fichier `/etc/security/policy.conf` de la façon suivante :

```
IDLECMD=LOGOUT
```

L'administrateur veut également réduire la durée d'inactivité des systèmes avant la déconnexion. Par conséquent, le rôle `root` ajoute la paire `IDLETIME` *keyword=value* au fichier `policy.conf` de la façon suivante :

```
IDLETIME=10
```

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

Notez que si l'utilisateur de connexion assume un rôle, les valeurs `IDLECMD` et `IDLETIME` de l'utilisateur s'appliquent pour ce rôle.

Exemple 11–2 Modification du jeu de privilèges de base de chaque utilisateur

Dans cet exemple, l'administrateur de sécurité d'une installation de grande taille ne souhaite pas que les utilisateurs standard puissent voir les processus d'autres utilisateurs. Par conséquent, le rôle `root` supprime `proc_info` de l'ensemble de privilèges de base sur chaque système configuré avec Trusted Extensions. Le paramètre `PRIV_DEFAULT` du fichier `/etc/policy.conf` est modifié et ses commentaires sont annulés comme suit :

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

▼ 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 130.

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. Dans un éditeur, saisissez le nom complet du fichier `.copy_files`.

```
# vi /etc/skel/.copy_files
```

b. 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 145 si vous avez besoin de suggestions. Pour des exemples de fichiers, reportez-vous à l'Exemple 11–3.

3 Personnalisez le fichier `.link_files`.

a. Dans un éditeur, saisissez le nom complet du fichier `.link_files`.

```
# vi /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 fichiers à inclure dans les fichiers de démarrage, reportez-vous à la section "Personnalisation de l'environnement de travail d'un utilisateur " du manuel *Administration d'Oracle Solaris : Tâches courantes* .
- Pour plus d'informations, reportez-vous à la section "Procédure de personnalisation des fichiers d'initialisation utilisateur" du manuel *Administration d'Oracle Solaris : Tâches courantes* .

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 11–3 Personnalisation des fichiers de démarrage pour les utilisateurs

Dans cet exemple, l'administrateur système 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 système crée un fichier `.copy_files` et un fichier `.link_files` avec les contenus suivants :

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

## .link_files for regular users with C shells
## Link these files to my home directory in every zone
.bashrc
.bashrc.user
.cshrc
.login
:wq
```

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

Les fichiers personnalisés sont copiés dans le répertoire squelette approprié.

```
$ cp .copy_files .link_files .bashrc .bashrc.user .cshrc \
.login .profile .mailrc /etc/skelC
$ cp .copy_files .link_files .ksh .profile .mailrc \
/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 (Selection Manager) 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 130.

1 **Pour l'application Oracle OpenOffice, procédez comme suit :**

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

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

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

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

      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 GNOME 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 Oracle Solaris, `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 150.

▼ 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. **Saisissez votre nom d'utilisateur dans l'écran de connexion.**
2. **Dans le menu du bureau, sélectionnez Solaris Trusted Extensions, Failsafe Session (Session de secours) en bas de l'écran.**
3. **À l'invite, saisissez votre mot de passe.**
4. **Lorsque vous êtes invité à indiquer un autre mot de passe, saisissez le mot de passe root.**

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

Gestion des utilisateurs et des droits (Liste des tâches)

Dans Trusted Extensions, vous assumez le rôle d'administrateur de sécurité pour administrer les utilisateurs, les autorisations, les droits et les rôles. 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 d'une plage d'étiquettes d'utilisateur" à la page 155
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 155
Création d'un bureau limitant un utilisateur à quelques applications uniquement	Affecte des profils de droits qui permettent aux utilisateurs d'ouvrir uniquement les applications qui s'affichent sur le bureau. La ligne de commande est indisponible ou accepte peu de commandes.	"Limitation d'un utilisateur à des applications de bureau" à la page 157
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 159
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 159
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 160

Tâche	Description	Voir
Suppression d'un utilisateur du système.	Suppression complète d'un utilisateur et de ses processus	"Procédure de suppression d'un compte utilisateur d'un système Trusted Extensions" à la page 161

Procédure de modification d'une plage d'étiquettes d'utilisateur

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 autorisé à se connecter à la zone globale peut ensuite visualiser la liste des systèmes qui s'exécutent sur une étiquette particulière. L'utilisateur peut 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.

- **Effectuez l'une des opérations suivantes :**

  - **Pour étendre la plage d'étiquettes de l'utilisateur, assignez une autorisation de niveau supérieur.**

    ```
    # usermod -K min_label=INTERNAL -K clearance=ADMIN_HIGH jdoe
    ```

    Vous pouvez également étendre la plage d'étiquettes de l'utilisateur en diminuant l'étiquette minimale.

    ```
    # usermod -K min_label=PUBLIC -K clearance=INTERNAL jdoe
    ```

    Pour plus d'informations, reportez-vous aux pages de manuel `usermod(1M)` et `user_attr(4)`.

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

    ```
    # usermod -K min_label=INTERNAL -K clearance=INTERNAL jdoe
    ```

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 149.

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

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

Pour la procédure étape par étape, reportez-vous à la section "Procédure de création ou de modification d'un profil de droits" du manuel *Administration d'Oracle Solaris : services de sécurité*.

Les autorisations suivantes peuvent être utiles pour les utilisateurs :

- `solaris.device.allocate` : autorise un utilisateur à allouer un périphérique, tel qu'un microphone ou un CD-ROM.

  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.
- `solaris.label.file.downgrade` : autorise un utilisateur à diminuer le niveau de sécurité d'un fichier.
- `solaris.label.file.upgrade` : autorise un utilisateur à augmenter le niveau de sécurité d'un fichier.
- `solaris.label.win.downgrade` : autorise un utilisateur à sélectionner des informations dans un fichier de niveau supérieur et à les placer dans un fichier de niveau inférieur.
- `solaris.label.win.noview` : autorise un utilisateur à déplacer des informations sans visualiser les informations déplacées.
- `solaris.label.win.upgrade` : autorise un utilisateur à sélectionner les informations d'un fichier de niveau inférieur et à les placer dans un fichier de niveau supérieur.
- `solaris.login.remote` : autorise un utilisateur à se connecter à distance.
- `solaris.system.shutdown` : autorise un utilisateur à arrêter le système et à arrêter une zone.

2 Attribuez le profil de droits à un utilisateur ou à un rôle.

Pour la procédure étape par étape, reportez-vous à la section "Procédure de modification des propriétés RBAC d'un utilisateur" du manuel *Administration d'Oracle Solaris : services de sécurité*.

▼ Limitation d'un utilisateur à des applications de bureau

La sécurité de site peut exiger que les utilisateurs aient uniquement accès aux applications qu'ils peuvent ouvrir à partir d'une icône du bureau. Cette procédure affecte des profils de droits qui limitent l'accès des utilisateurs aux applications requises uniquement.

Remarque – Sur le bureau Trusted Extensions, l'exécution de commandes dépend toujours des profils de droits d'accès.

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 149.

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

1 **Créez un profil de droits appelé Desktop applets (Applets de bureau) permettant aux utilisateurs d'Oracle Solaris d'exécuter les applets de base sur leur bureau.**

Pour plus d'informations sur cette procédure, reportez-vous à la section "Procédure de limitation d'un utilisateur aux applications de bureau" du manuel *Administration d'Oracle Solaris : services de sécurité*.

2 **Créez un autre profil de droits d'accès permettant aux utilisateurs Trusted Extensions d'exécuter les applets de confiance requis sur leur bureau.**

Les lignes sont renvoyées à des fins d'affichage.

```
# profiles -p "Trusted Desktop Applets"
profiles:Trusted Desktop Applets>
set desc="Can use trusted desktop applications except terminal"
profiles:Trusted Desktop Applets> add cmd=/usr/dt/config/tsoljds-migration;end
profiles:Trusted Desktop Applets> add cmd=/usr/bin/tsoljds-xagent;end
profiles:Trusted Desktop Applets> commit
```

3 **Ajoutez le profil Desktop Applets en tant que profil de droits supplémentaire au profil Trusted Desktop Applets (Applets de bureau de confiance).**

Vous avez créé ce profil de droits à l'Étape 2.

```
profiles:Trusted Desktop Applets> add profiles="Desktop Applets"
profiles:Trusted Desktop Applets> commit
profiles:Trusted Desktop Applets> exit
```

4 **Assurez-vous que les entrées du profil de droits Trusted Desktop Applets sont correctes.**

Contrôlez les entrées à la recherche d'erreurs, de fautes de frappe, d'omissions ou de répétitions.

```
# profiles -p "Trusted Desktop Applets" info
Found profile in files repository.
name=Trusted Desktop Applets
```

```
desc=Can use trusted desktop applications except terminal
profiles=Desktop Applets
cmd=/usr/dt/config/tsoljds-migration
cmd=/usr/bin/tsoljds-xagent
```

Astuce – Vous pouvez créer un profil de droits pour une application ou une classe d'applications contenant des icônes de bureau. Ajoutez ensuite le profil de droits Trusted Desktop Applets en tant que profil de droits supplémentaire pour l'accès au bureau.

5 Affectez à l'utilisateur les profils de droit `Trusted Desktop applets` et `Stop`.

`# usermod -P "Trusted Desktop Applets,Stop"` *username*

Cet utilisateur peut utiliser le bureau de confiance, mais il ne peut ni lancer de fenêtre de terminal, ni agir en tant que Console User (Utilisateur de la console), ni bénéficier des droits inclus dans le profil de droits Basic Solaris User (Utilisateur Solaris de base).

Exemple 11–4 Autorisation d'un utilisateur de bureau à ouvrir une fenêtre de terminal

Dans cet exemple, l'administrateur permet à un utilisateur de bureau d'ouvrir une fenêtre de terminal. L'administrateur a déjà créé le profil de droits Desktop Applets pour les utilisateurs du bureau Oracle Solaris et le profil de droits Trusted Desktop Applets pour les utilisateurs de bureau Trusted Extensions dans le référentiel LDAP.

Tout d'abord, l'administrateur crée le profil de droits Terminal Window (Fenêtre de terminal) et vérifie son contenu.

```
# profiles -p "Terminal Window" -S ldap
profiles:Terminal Window> set desc="Can open a terminal window"
profiles:Terminal Window> add cmd=/usr/bin/gnome-terminal;end
profiles:Terminal Window> commit
profiles:Terminal Window> exit
# profiles -p "Terminal Window" info
Found profile in ldap repository.
name=Terminal Window
desc=Can open a terminal window
cmd=/usr/bin/gnome-terminal
```

Ensuite, il attribue ce profil de droits ainsi que le profil de droits All (Tout) à tous les utilisateurs du bureau nécessitant des fenêtres de terminal pour effectuer leurs tâches. Sans le profil de droits All, les utilisateurs ne pourraient pas exécuter les commandes UNIX qui ne requièrent pas de privilège, telles que `ls` et `cat`.

```
# usermod -P "Trusted Desktop Applets,Terminal Window,All,Stop" -S ldap jdoe
```

Grâce à cet ensemble de profils de droits, l'utilisateur `jdoe` peut utiliser le bureau et les fenêtres de terminal, mais ne peut pas agir en tant que Console User ni bénéficier des droits contenus dans le profil de droits Basic Solaris User.

▼ 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.

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

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

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

```
# usermod -K defaultpriv=basic,!proc_info,!proc_session,!file_link_any
```

En supprimant le privilège `proc_info`, vous empêchez l'utilisateur d'examiner les processus qui n'émanent pas de l'utilisateur. En supprimant le privilège `proc_session`, vous empêchez l'utilisateur d'examiner les processus à l'extérieur de sa session en cours. En supprimant le privilège `file_link_any`, vous empêchez l'utilisateur de créer des liens physiques vers des fichiers n'appartenant pas à l'utilisateur.

Voir aussi Pour obtenir un exemple de collecte des restrictions de privilège dans un profil de droits, reportez-vous aux exemples suivants : "Procédure de création ou de modification d'un profil de droits" du manuel *Administration d'Oracle Solaris : services de sécurité*.

Pour restreindre les privilèges de tous les utilisateurs sur un système, reportez-vous à l'Exemple 11–2.

▼ Procédure de désactivation du verrouillage du compte pour certains utilisateurs

Effectuez cette procédure pour tous les utilisateurs pouvant assumer un rôle.

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

- **Désactivez le verrouillage de comptes pour un utilisateur local.**

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

Pour désactiver le verrouillage de comptes pour un utilisateur LDAP, spécifiez le référentiel LDAP.

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

▼ 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, de répertoires ou de textes sélectionnés. 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 connaître la procédure, reportez-vous à la section "Procédure d'octroi de l'autorisation à modifier l'étiquette de fichiers à un utilisateur" à la page 185.

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 155 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. **Affectez le profil à des utilisateurs et des rôles appropriés.**

   Pour une procédure pas à pas, reportez-vous à la section "Procédure de modification des propriétés RBAC d'un utilisateur" du manuel *Administration d'Oracle Solaris : services de sécurité*.

▼ 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 dans la zone globale.

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

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

3. **Supprimez le compte utilisateur.**

   ```
   # userdel -r jdoe
   ```

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

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

Pour plus d'informations, reportez-vous à la section "Pratiques de suppression d'un utilisateur" à la page 124.

◆ ◆ ◆ CHAPITRE 12

Administration à distance dans Trusted Extensions (tâches)

Ce chapitre décrit comment configurer un système Trusted Extensions en vue d'une administration à distance et fournit des informations sur la connexion au système et sur son administration.

Remarque – Les méthodes de configuration requises par l'écouteur et d'autres systèmes distants ne répondent pas aux critères d'une configuration évaluée. Pour en savoir plus, reportez-vous à la section "Prise de connaissance de votre stratégie de sécurité du site" à la page 28.

Administration à distance dans Trusted Extensions

L'administration à distance présente un risque important pour la sécurité, en particulier pour les utilisateurs de systèmes non sécurisés. Par défaut, Trusted Extensions n'autorise pas l'administration à distance à partir de n'importe quel système.

Tant que le réseau n'est pas configuré, le modèle de sécurité `admin_low` est attribué à tous les hôtes à distance, c'est-à-dire que ces derniers sont reconnus en tant qu'hôtes sans étiquette. Tant que les zones étiquetées sont configurées, la seule zone disponible est la zone globale. Dans Trusted Extensions, la zone globale est la zone d'administration. Seul un rôle peut y accéder. Plus précisément, un compte doit contenir une plage d'étiquettes de `ADMIN_LOW` à `ADMIN_HIGH` pour atteindre la zone globale.

Dans cet état initial, les systèmes Trusted Extensions sont protégés contre les attaques à distance par plusieurs mécanismes. Ces mécanismes incluent les valeurs `netservices`, la stratégie `ssh` par défaut, la stratégie de connexion par défaut et la stratégie PAM par défaut.

- Durant l'installation, aucun service distant, à l'exception du shell sécurisé, n'est activé pour écouter sur le réseau.

  Toutefois, le service `ssh` ne peut pas être utilisé pour une connexion à distance par `root` ou par rôle en raison des stratégies PAM et de connexion `ssh`.
- Le compte `root` ne peut pas être utilisé pour établir des connexions distantes car `root` est un rôle. Les rôles ne peuvent pas se connecter, conformément à PAM.

  Même si `root` est modifié pour un compte utilisateur, la connexion par défaut et les stratégies `ssh` empêchent les connexions à distance de l'utilisateur `root`.
- Deux valeurs PAM par défaut empêchent les connexions à distance.

  Le module `pam_roles` rejette les connexions locales et à distance provenant des comptes de type `role`.

  Un module PAM de Trusted Extensions, `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.

Par conséquent, tout comme sur le système Oracle Solaris, l'administration à distance doit être configurée. Trusted Extensions ajoute deux exigences en matière de configuration, la plage d'étiquettes requise pour atteindre la zone globale et le module `pam_tsol_account`.

Méthodes d'administration de systèmes distants dans Trusted Extensions

Dans Trusted Extensions, vous devez utiliser le protocole `ssh` avec l'authentification basée sur les hôtes pour atteindre et administrer le système distant. L'authentification basée sur les hôtes permet à un compte utilisateur du même nom d'assumer un rôle sur le système Trusted Extensions distant.

Lorsque l'authentification basée sur les hôtes est utilisée, le client `ssh` envoie à la fois le nom d'utilisateur original et le nom de rôle vers le système distant, le serveur. Grâce à ces informations, le serveur peut transmettre un contenu suffisant au module `pam_roles` pour permettre l'endossement d'un rôle sans que le compte utilisateur n'ait à se connecter au serveur.

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

- **Administration à partir d'un système Trusted Extensions** : pour une administration à distance la plus sécurisée possible, les deux systèmes affectent leur paire à un modèle de sécurité CIPSO. Reportez-vous à l'Exemple 12–1.
- **Administration à partir d'un système sans étiquette** : si l'administration par un système Trusted Extensions n'est pas pratique, la stratégie du protocole réseau peut être assouplie en spécifiant l'option `allow_unlabeled` pour le module `pam_tsol_account` dans le fichier `pam.conf`.

  Si cette stratégie est assouplie, le modèle de réseau par défaut doit être modifié afin qu'aucun système arbitraire ne puisse accéder à la zone globale. Le modèle `admin_low` doit être utilisé avec parcimonie et l'adresse générique `0.0.0.0` ne doit pas être l'adresse par défaut de l'étiquette `ADMIN_LOW`. Pour plus d'informations, reportez-vous à la section "Procédure de limitation des hôtes pouvant être contactés sur le réseau de confiance" à la page 236.

Dans l'un ou l'autre des scénarios d'administration, pour utiliser le rôle `root` en vue d'une connexion à distance, vous devez assouplir la stratégie PAM en spécifiant l'option `allow_remote` pour le module `pam_roles`.

En règle générale, les administrateurs utilisent la commande `ssh` pour administrer des systèmes distants à partir de la ligne de commande. Avec l'option `-X`, les interfaces graphiques d'administration de Trusted Extensions peuvent être utilisées.

En outre, vous pouvez configurer le système Trusted Extensions distant avec le serveur Xvnc. La technologie VNC (Virtual Network Computing) peut également être utilisée pour afficher le bureau multiniveau à distance et pour administrer le système. Voir "Procédure de configuration d'un système Trusted Extensions à l'aide de Xvnc pour un accès à distance" à la page 168.

Configuration et administration à distance de systèmes dans Trusted Extensions (liste des tâches)

Après l'activation de l'administration à distance et avant la réinitialisation du système distant sur Trusted Extensions, vous pouvez configurer le système à l'aide de la technologie VNC ou du protocole `ssh`.

Tâche	Description	Voir
Activation de l'administration à distance d'un système Trusted Extensions	Active l'administration des systèmes Trusted Extensions à partir de clients `ssh` spécifiés.	"Activation de l'administration à distance sur un système Trusted Extensions distant" à la page 166

Tâche	Description	Voir
Activation de VNC	À partir de n'importe quel client, utilise le serveur Xvnc du système Trusted Extensions distant pour afficher la session multiniveau du serveur sur le client.	"Procédure de configuration d'un système Trusted Extensions à l'aide de Xvnc pour un accès à distance" à la page 168
Connexion à distance à un système Trusted Extensions	Assume un rôle sur le système distant pour l'administrer.	"Procédure de connexion et d'administration d'un système Trusted Extensions distant" à la page 170

Remarque – Consultez votre stratégie de sécurité pour déterminer les méthodes d'administration à distance possibles sur votre site.

▼ Activation de l'administration à distance sur un système Trusted Extensions distant

Dans cette procédure, vous autorisez l'authentification basée sur des hôtes sur un système distant Oracle Solaris avant d'y ajouter la fonction Trusted Extensions. Le système distant est le serveur `ssh`.

Avant de commencer Le système distant est installé avec Oracle Solaris, et vous pouvez accéder à ce système.

1 Sur les deux systèmes, activez l'authentification basée sur des hôtes.

Pour connaître la procédure, reportez-vous à la section "Procédure de configuration de l'authentification basée sur l'hôte pour Secure Shell" du manuel *Administration d'Oracle Solaris : services de sécurité*.

Remarque – N'utilisez pas la commande `cat`. Copiez et collez la clé publique via une connexion `ssh`. Si votre client ssh n'est pas un système Oracle Solaris, suivez les instructions de votre plate-forme permettant de configurer un client `ssh` avec l'authentification basée sur des hôtes.

Une fois cette étape terminée, vous disposez d'un compte d'utilisateur sur les deux systèmes qui est habilité à assumer le rôle `root`. Les comptes reçoivent un UID, un GID et une assignation de rôle identiques. Vous avez également généré des paires de clé publique ou privée et partagé des clés publiques.

2 Sur le serveur `ssh`, assouplissez la stratégie `ssh` afin d'autoriser la connexion à distance pour `root`.

```
# vi /etc/ssh/sshd_config
## Permit remote login by root
PermitRootLogin yes
```

Une étape ultérieure limite la connexion de `root` à un système et un utilisateur particulier.

Remarque – Étant donné que·l'administrateur assumera le rôle `root`, vous n'avez pas besoin d'assouplir la stratégie de connexion qui empêche la connexion à distance de `root`.

---

3 Sur le serveur `ssh`, redémarrez le service `ssh`.

```
# svcadm restart ssh
```

4 Sur le serveur `ssh`, dans le répertoire personnel de `root`, indiquez l'hôte et l'utilisateur de l'authentification basée sur des hôtes.

```
# cd
# vi .shosts
client-host username
```

Le fichier `.shosts` autorise *username* du système *client-host* à assumer le rôle `root` sur le serveur, lorsque une clé publique ou privée est partagée.

5 Sur le serveur `ssh`, assouplissez les deux stratégies PAM.

a. Autorisez la connexion à distance par rôles.

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

Cette stratégie autorise *username* du système *client-host* à assumer un rôle sur le serveur.

b. Autorisez les hôtes sans étiquette à contacter le système distant Trusted Extensions.

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

c. Copiez votre fichier `pam.conf` modifié dans `pam.conf.site`.

```
# cp /etc/pam.conf /etc/pam.conf.site
```

6 **Testez la configuration.**

a. **Ouvrez un nouveau terminal dans le système distant.**

b. **Dans une fenêtre appartenant à** *username* **de** *client-host*, **assumez le rôle `root` sur le système distant.**

```
% ssh -l root remote-system
```

7 **Une fois le bon fonctionnement de la configuration avéré, activez Trusted Extensions sur le système distant, puis réinitialisez-le.**

```
# svcadm enable -s labeld
# /usr/sbin/reboot
```

Exemple 12–1 Affectation d'un type d'hôte CIPSO pour l'administration à distance

Dans cet exemple, l'administrateur utilise un système Trusted Extensions pour configurer un hôte Trusted Extensions distant. Pour ce faire, l'administrateur utilise la commande `tncfg` sur chaque système distant pour définir le type d'hôte du système homologue.

remote-system `# tncfg -t cipso add host=192.168.1.12` *Client-host*

client-host `# tncfg -t cipso add host=192.168.1.22` *Remote system*

Étant donné qu'un système sans étiquette peut également configurer l'hôte Trusted Extensions distant, l'administrateur conserve l'option `allow_unlabeled` dans le fichier `pam.conf` de l'hôte distant.

Erreurs fréquentes Lorsque l'administrateur effectue une mise à niveau vers une nouvelle version du SE Oracle Solaris, aucun nouveau fichier `pam.conf` n'est installé. Pour une description de l'action du fichier `preserve=true` sur la mise à niveau, reportez-vous à la page de manuel `pkg`(5).

▼ Procédure de configuration d'un système Trusted Extensions à l'aide de Xvnc pour un accès à distance

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. Dans Trusted Extensions, les clients de n'importe quelle plate-forme peuvent se connecter à un serveur Xvnc exécutant Trusted Extensions accéder au serveur Xvnc, puis visualiser et travailler dans un bureau multiniveau.

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

Avant de commencer

Vous avez installé et configuré Trusted Extensions sur ce système qui sera utilisé en tant que serveur Xvnc. La zone globale de ce système possède une adresse IP fixe, c'est-à-dire qu'elle n'utilise pas le profil de configuration du réseau automatique, comme décrit dans la page de manuel `netcfg(1M)`.

Ce système reconnaît les clients VNC par nom d'hôte ou par adresse IP. Plus précisément, le modèle de sécurité `admin_low` identifie explicitement ou à l'aide d'un caractère générique les systèmes susceptibles d'être des clients VNC de ce serveur. Pour plus d'informations sur la configuration de la connexion sécurisée, reportez-vous à la section "Procédure de limitation des hôtes pouvant être contactés sur le réseau de confiance" à la page 236.

Si une session GNOME est en cours d'exécution sur la console du futur serveur Xvnc de Trusted Extensions, l'option Desktop Sharing (Partage du bureau) n'est pas activée.

Vous endossez le rôle `root` dans la zone globale du futur serveur Xvnc de Trusted Extensions.

1. **Chargez ou mettez à jour le logiciel Xvnc.**

   ```
   # packagemanager &
   ```

   Dans l'interface graphique du gestionnaire de packages, (Package Manager) recherchez les" vnc" et choisissez parmi les serveurs disponibles. Une première option est le logiciel du serveur TigerVNC X11/VNC.

2. **Activez le protocole X Display Manager Control Protocol.**

   Modifiez le fichier de configuration personnalisée GNOME Display Manager (gdm). Dans le fichier `/etc/gdm/custom.conf` , saisissez `Enable=true` sous le titre `[xdmcp]`,

   ```
   [xdmcp]
   Enable=true
   ```

3. **Dans le fichier `/etc/gdm/Xsession`, insérez la ligne suivante autour de la ligne 27.**

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

4. **Assouplissez la stratégie Trusted Extensions dans le fichier `TrustedExtensionsPolicy`.**

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

5. **Activez le service du serveur Xvnc.**

   ```
   # svcadm enable xvnc-inetd
   ```

6. **Fermez toutes les sessions GNOME actives sur ce serveur.**

   ```
   # svcadm restart gdm
   ```

   Attendez environ une minute que le gestionnaire de bureau redémarre. Il est ensuite possible pour un client VNC de se connecter.

7 **Vérifiez que le logiciel Xvnc est activé.**

```
# svcs | grep vnc
```

8 **Sur chaque client VNC de ce serveur Xvnc, installez le logiciel client VNC.**

Pour le système client, vous disposez d'un choix de logiciels. Vous pouvez utiliser le logiciel VNC à partir du référentiel Oracle Solaris.

9 **Pour afficher l'espace de travail du serveur Xvnc sur un client VNC, effectuez les opérations suivantes :**

a. **Dans une fenêtre de terminal du client, connectez-vous au serveur.**

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

Pour les options de commande, reportez-vous à la page de manuel `vncviewer`(1).

b. **Dans la fenêtre qui s'affiche, saisissez votre nom d'utilisateur 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 manuel *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

▼ Procédure de connexion et d'administration d'un système Trusted Extensions distant

Cette procédure vous permet d'utiliser la ligne de commande et l'interface graphique `txzonemgr` permettant d'administrer un système Trusted Extensions distant.

Avant de commencer L'utilisateur, le rôle et l'assignation de rôles sont définis de façon identique dans les systèmes locaux et distants, comme décrit dans la section "Activation de l'administration à distance sur un système Trusted Extensions distant" à la page 166.

1 **Sur le système du bureau, activez les processus à partir du système distant à afficher.**

```
desktop $ xhost + remote-sys
```

2 **Assurez-vous que vous êtes l'utilisateur nommé à l'identique sur les deux systèmes.**

3 **À partir d'une fenêtre de terminal, connectez-vous au système distant.**

Utilisez la commande `ssh` pour vous connecter.

```
desktop $ ssh -X -l identical-username remote-sys
Password:       Type the user's password
remote-sys $
```

L'option `-X` permet d'afficher les interfaces graphiques.

4 **Dans la même fenêtre de terminal, assumez le rôle qui est défini à l'identique sur les deux systèmes.**

Par exemple, assumez le rôle `root`.

```
remote-sys $ su - root
Password:      Type the root password
```

Vous êtes à présent dans la zone globale. Vous pouvez maintenant utiliser cette fenêtre de terminal pour administrer le système distant à partir de la ligne de commande. Les interfaces graphiques s'affichent sur votre écran. Voir l'Exemple 12–2.

Exemple 12–2 Configuration des zones étiquetées sur un système distant

Dans cet exemple, l'administrateur utilise l'interface graphique `txzonemgr` pour configurer des zones étiquetées sur un système distant étiqueté à partir d'un système de bureau étiqueté. Comme dans Oracle Solaris, l'administrateur autorise le serveur X à accéder au système du bureau à l'aide de l'option `-X` de la commande `ssh`. L'utilisateur `jandoe` est défini à l'identique sur les deux systèmes et peut assumer le rôle `remoterole`.

```
TXdesk1 $ xhost + TXnohead4

TXdesk1 $ ssh -X -l jandoe TXnohead4
Password: Ins1PwD1
TXnohead4 $
```

Pour atteindre la zone globale, l'administrateur utilise le compte `jandoe` afin d'assumer le rôle `remoterole`. Ce rôle est défini à l'identique sur les deux systèmes.

```
TXnohead4 # su - remoterole
Password: abcd1EFG
```

Dans le même terminal, l'administrateur dans le rôle `remoterole` démarre l'interface graphique `txzonemgr`.

```
TXnohead4 $ /usr/sbin/txzonemgr &
```

Le gestionnaire de zones étiquetées (Labeled Zone Manager) s'exécute sur le système distant et s'affiche sur le système local.

Exemple 12–3 Connexion à une zone étiquetée distante

L'administrateur souhaite modifier un fichier de configuration sur un système distant sous l'étiquette `PUBLIC`.

L'administrateur dispose de deux options.

- Soit il se connecte à distance à la zone globale, affiche la zone globale distante, modifie l'étiquette `PUBLIC`, puis ouvre une fenêtre de terminal et modifie le fichier.
- Soit il se connecte à la zone `PUBLIC` à l'aide de la commande `ssh` à partir d'une fenêtre de terminal `PUBLIC`, puis modifie le fichier.

Notez que si le système distant exécute un démon de service de nommage (`nscd`) pour toutes les zones, *et* si le système distant utilise le service de nommage de fichiers; le mot de passe de la zone distante est le mot de passe qui était en vigueur lors de la dernière réinitialisation de la zone. Si le mot de passe pour la zone `PUBLIC` distante a été modifié et si la zone n'a pas été réinitialisée après la modification, le mot de passe d'origine permet l'accès.

Erreurs fréquentes Si l'option `-X` ne fonctionne pas, l'installation d'un package peut être nécessaire. Le transfert X11 est désactivé lorsque le binaire `xauth` n'est pas installé. La commande suivante permet de charger le fichier binaire : **`pkg install pkg:/x11/session/xauth`**.

◆ ◆ ◆ CHAPITRE 13

Gestion des zones dans Trusted Extensions (tâches)

Ce chapitre décrit le fonctionnement des zones non globales ou *étiquetées* sur un système Trusted Extensions. Les procédures spécifiques aux zones sans étiquette 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`. Vous pouvez 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, la zone globale est uniquement une zone administrative. 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.

Sur un système Trusted Extensions, les systèmes de fichiers d'une zone sont généralement montés dans la zone globale en tant que système de fichiers 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.

Chaque zone est un système de fichiers ZFS discrets. Chaque zone peut être 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 aux sections Chapitre 14, “Gestion et montage de fichiers dans Trusted Extensions (tâches)” et “Montage des jeux de données ZFS étiquetés” à la page 193.

Les zones de Trusted Extensions sont basées sur le produit de zones d'Oracle Solaris Pour obtenir des informations de référence, reportez-vous à la section Partie II, “Oracle Solaris Zones” du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*.

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. Elle a considéré trois types de configurations comme indiqué dans la section “Accès aux zones étiquetées” à la page 32 qu'il est possible de résumer comme suit :

- 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.

- 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 un système en réseau auquel les utilisateurs standard vont se connecter. 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.

Un quatrième type de configuration pour une zone non globale est disponible dans les instances IP exclusives d'Oracle Solaris. Dans cette configuration, une zone non globale se voit attribuer sa propre instance d'IP et gère ses propres interfaces physiques. Chaque zone fonctionne comme si elle constituait un système distinct. Pour obtenir une description, reportez-vous à la section "Interfaces réseau de zones" du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*.

Si vous configurez des instances IP exclusives dans Trusted Extensions, chaque zone étiquetée fonctionne comme si elle est constituait un système *à niveau unique* distinct. Les fonctions de mise en réseau multiniveau de Trusted Extensions s'appuient sur les fonctions d'une pile IP partagée. Ce guide suppose que la mise en réseau est 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 de sécurité est affecté à l'adresse IP en communiquant des systèmes Trusted Extensions. La plage d'étiquettes ou l'ensemble d'étiquettes du modèle de sécurité 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 la plage d'étiquettes du modèle d'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.
- Dans une configuration par défaut, où la zone globale et les zones étiquetées partagent une adresse IP, un MLP pourrait être ajouté à une zone pour le service `ssh`. 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 un exemple, reportez-vous à la section “Procédure de création d'un port multiniveau pour une zone” à la page 241.

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*. Pour partager un système de fichiers étiqueté, reportez-vous à la section "Procédure de partage de systèmes de fichiers à partir d'une zone étiquetée" à la page 195.

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, le moyen le plus simple d'administrer des zones est d'utiliser le script shell, `/usr/sbin/txzonemgr` , fourni par Trusted Extensions. Ce script fournit un assistant basé sur les menus pour la création, l'installation, le démarrage et l'initialisation des zones. `txzonemgr` utilise la commande `zenity`. Pour plus d'informations, reportez-vous aux pages de manuel `txzonemgr(1M)` et `zenity`(1).

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 dans Trusted Extensions de la même manière 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 179
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 180
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 181
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 182

Tâche	Description	Voir
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 à modifier l'étiquette de fichiers à un utilisateur" à la page 185
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 183.
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 "Procédure interactive de création de zones étiquetées" à la page 59.
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 création d'un port multiniveau pour une zone" à la page 241 Exemple 16–19
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 198
Suppression d'une zone étiquetée	Supprime complètement une zone étiquetée du système.	"Suppression d'une zone non globale" du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*

▼ Procédure d'affichage des zones prêtes ou en cours d'exécution

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

1 Exécution de la commande `txzonemgr &`.

Les noms de zones, leur état et leurs étiquettes s'affichent dans une interface graphique.

2 Vous pouvez également utiliser la commande `zoneadm list -v`.

```
# zoneadm list -v
ID NAME       STATUS     PATH              BRAND       IP
 0 global     running    /                 ipkg        shared
 5 internal   running    /zone/internal    labeled     shared
 6 public     running    /zone/public      labeled     shared
```

La sortie ne comporte pas les étiquettes des zones.

▼ 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 Dans un éditeur, créez le script `getmounts`.

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_HIGH
/dev:   ADMIN_HIGH
/system/contract:        ADMIN_HIGH
/proc:                   ADMIN_HIGH
/system/volatile:        ADMIN_HIGH
/system/object:          ADMIN_HIGH
/lib/libc.so.1:          ADMIN_HIGH
/dev/fd:        ADMIN_HIGH
/tmp:           ADMIN_HIGH
/etc/mnttab:    ADMIN_HIGH
/export:        ADMIN_HIGH
/export/home:   ADMIN_HIGH
/export/home/jdoe:   ADMIN_HIGH
/zone/public:        ADMIN_HIGH
/rpool:              ADMIN_HIGH
/zone:               ADMIN_HIGH
/home/jdoe:          ADMIN_HIGH
/zone/public:        ADMIN_HIGH
/zone/snapshot:      ADMIN_HIGH
/zone/internal:      ADMIN_HIGH
...
```

Exemple 13–1 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, la sortie de test 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/jdoe:   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
```

3 Démarrez la zone.

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

Exemple 13–2 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 13–3 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. Vous devez être dans le rôle root dans la zone globale.

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 Activez l'ensemble de données à partager.

```
# zfs set sharenfs=on datasetdir/subdir
```

5 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 au niveau du fichier `/data` dans la zone. Cette étape permet de s'assurer que l'ensemble de données n'est pas monté avant que la zone ne soit initialisée.

6 Initialisez la zone étiquetée.

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

Lorsque la zone est initialisée, 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 13–4 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
```

Ensuite, l'administrateur partage l'ensemble de données.

```
# zfs set sharenfs=on 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
```

Ensuite, l'administrateur initialise la zone `needtoknow`.

```
# zoneadm -z needtoknow boot
```

L'ensemble de données est désormais accessible.

Les utilisateurs de la zone `restricted` dominant la zone `needtoknow` peuvent afficher l'ensemble de données monté en modifiant 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 à 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 La zone que vous envisagez de configurer doit être arrêtée. Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

1 Ouvrez le gestionnaire de zones étiquetées.

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

2 Configurez la zone afin de permettre la modification de l'étiquette.

a. Double-cliquez sur la zone.

b. Dans la liste, sélectionnez l'option Permit Relabeling (Autoriser le nouvel étiquetage).

3 Sélectionnez Boot (Init) pour redémarrer la zone.

4 Cliquez sur Cancel (Annuler) pour retourner à la liste de zones.

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 160.

Exemple 13–5 Désactivation de la rétrogradation à partir de la zone internal

Dans cet exemple, l'administrateur de sécurité veut empêcher la rétrogradation des fichiers `CNF: INTERNAL USE ONLY` sur un système précédemment utilisé pour effectuer une rétrogradation de fichiers.

L'administrateur utilise le gestionnaire de zones étiquetées pour arrêter la zone `internal` puis, dans le menu de la zone `internal`, sélectionne Deny Relabeling (Refuser le nouvel étiquetage).

◆ ◆ ◆ CHAPITRE 14

Gestion et montage de fichiers dans Trusted Extensions (tâches)

Ce chapitre décrit le fonctionnement des montages LOFS, NFS et ZFS 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 qu'Oracle Solaris. Étant donné que Trusted Extensions joint une étiquette unique pour chaque zone non globale, tous les fichiers et systèmes de fichiers 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 identiques peuvent être montés avec des autorisations de lecture/écriture.

Montages NFS dans Trusted Extensions

Les montages NFS dans Trusted Extensions sont similaires aux montages d'Oracle Solaris. Les différences surviennent dans l'application de la stratégie MAC. En outre, le script `txzonemgr` suppose que les répertoires personnels sont montés en tant que `/export/Home` .

Les partages NFS dans Trusted Extensions sont similaires aux partages d'Oracle Solaris dans une zone globale. En revanche, le partage d'une zone étiquetée dans un système multiniveau est unique à Trusted Extensions :

- **Partages et montages dans la zone globale :** le partage et le montage de fichiers dans la zone globale d'un système Trusted Extensions sont presque identiques à ceux effectués dans Oracle Solaris. Pour le montage des fichiers, vous pouvez utiliser l'agent de montage automatique et la commande `mount`. Pour le partage de fichiers, la propriété `sharenfs` des jeux de données de données ZFS est utilisée.
- **Montages dans des zones étiquetées :** le montage des fichiers dans des zones étiquetées de Trusted Extensions est presque identique au montage de fichiers dans des zones non globales d'Oracle Solaris. Pour le montage des fichiers, vous pouvez utiliser l'agent de montage automatique et la commande `mount`. Dans Trusted Extensions, un fichier de configuration `auto_home_`*zone-name* unique 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 des propriétés de partage NFS. Pour plus d'informations, reportez-vous à la section "Processus de zone globale et zones étiquetées" à la page 176.

Les étiquettes déterminent quels fichiers peuvent être montés. Les fichiers sont partagés et montés sous une étiquette particulière.

- Pour qu'un système Trusted Extensions puisse monter un système de fichiers sur un autre système Trusted Extensions le serveur et le client doivent posséder des modèles d'hôte distant compatibles de type `cipso`.

  Pour qu'un client Trusted Extensions écrive dans un système de fichiers monté via NFS, le système de fichiers doit être monté avec des autorisations de lecture/écriture *et* doit se trouver sous la même étiquette que le client.
- Pour qu'un système Trusted Extensions monte un système de fichiers à partir d'un système sans étiquette, la seule étiquette affectée au système sans étiquette par le système Trusted Extensions doit correspondre à l'étiquette du système Trusted Extensions.

  De même, pour qu'une zone étiquetée puisse monter un système de fichiers à partir d'un système sans étiquette, la seule étiquette affectée au système sans étiquette par le système Trusted Extensions doit correspondre à l'étiquette de la zone étiquetée.
- Les systèmes de fichiers dont les étiquettes sont différentes de la zone de montage et qui sont montés avec LOFS peuvent être visualisés, mais pas modifiés. Pour plus d'informations sur les montages NFS, reportez-vous à la section "Accès aux systèmes de fichiers montés NFS dans Trusted Extensions" à la page 189.

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 190.

Si la sécurité du site interdit l'affichage des objets de niveau inférieur, vous pouvez rendre les systèmes de fichiers 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 182.

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 Oracle Solaris, une zone non globale peut partager des systèmes de fichiers. De même, dans Trusted Extensions, une zone étiquetée peut partager des systèmes de fichiers. Pour partager des systèmes de fichiers à partir d'une zone étiquetée, activez les propriétés du partage ZFS du système de fichiers.

Lorsque l'état de la zone étiquetée est `ready` ou `running`, le système de fichiers est partagé sous l'étiquette de la zone. Pour plus d'informations sur cette procédure, reportez-vous à la section "Procédure de partage de systèmes de fichiers à partir d'une zone étiquetée" à la page 195.

Accès aux systèmes de fichiers montés NFS dans Trusted Extensions

Pour rendre les répertoires de niveau inférieur montés via FNS visibles pour les utilisateurs d'une zone de niveau supérieur, la préparation suivante est requise :

- **Configuration du serveur :** sur le serveur NFS, exportez le système de fichiers NFS en définissant ses propriétés de partage. Pour plus d'informations sur cette procédure, reportez-vous à la section "Procédure de partage de systèmes de fichiers à partir d'une zone étiquetée" à la page 195.

- **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 197.

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 191.

Les répertoires personnels sont créés au moment de la création des utilisateurs. Toutefois, ils sont créés dans la zone globale du serveur d'annuaires 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, seul le répertoire personnel de l'utilisateur est supprimé de la zone globale. 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 161.

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 "Procédure permettant aux utilisateurs d'accéder à leurs répertoires personnels distants sous chaque étiquette en se connectant à chaque serveur NFS" à la page 77.

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 initialisée, 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` en tant que répertoire source pour un remontage de `lofs` vers `/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* générée à partir d'une zone de niveau supérieur :

```
+auto_home_public
*    public-zone-IP-address:/export/home/&
```

Le script `txzonemgr` configure cette entrée `PUBLIC` dans le fichier `auto_master` de la zone globale :

```
+auto_master
/net        -hosts        -nosuid,nobrowse
/home        auto_home    -nobrowse
/zone/public/home      auto_home_public      -nobrowse
```

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

Le logiciel Trusted Extensions reconnaît les étiquettes dans les versions 3 et 4 de NFS (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 dans 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 plus d'informations sur cette procédure, reportez-vous à l'Exemple 16–19.

Le système Trusted Extensions peut également partager ses systèmes de fichiers avec des hôtes sans étiquette. Un système de fichiers qui est exporté vers un hôte sans étiquette est *inscriptible* si son étiquette est identique à l'étiquette affectée à l'hôte distant par la zone d'exportation. Un système de fichiers exporté vers un hôte sans étiquette est uniquement *lisible* si son étiquette est dominée par l'étiquette affectée au système distant.

Les communications avec des systèmes qui exécutent une version du logiciel Trusted Solaris ne sont possibles que sous une étiquette unique. Le système Trusted Extensions et le système Trusted Solaris doivent affecter à leur pair 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 à la commande `mount` pour les systèmes de fichiers distants est toujours NFS.

Montage des jeux de données ZFS étiquetés

ZFS fournit un attribut d'étiquette de sécurité, `mlslabel`, contenant l'étiquette des données dans le jeu de données. La propriété `mlslabel` peut être héritée. Lorsqu'un jeu de données ZFS dispose d'une étiquette explicite, le jeu de données ne peut pas être monté sur un système Oracle Solaris qui n'est pas configuré avec Trusted Extensions.

Si la propriété `mlslabel` n'est pas définie, elle est définie par défaut sur la chaîne `none`, ce qui indique qu'il n'y a aucune étiquette.

Lorsque vous montez un jeu de données ZFS dans une zone étiquetée, les opérations suivantes se produisent :

- Si le jeu de données n'est pas étiqueté, c'est-à-dire si la propriété `mlslabel` n'est pas définie, la valeur de la propriété `mlslabel` est modifiée sur l'étiquette de la zone de montage.

  Pour la zone globale, la propriété `mlslabel` n'est pas définie automatiquement. Si vous avez explicitement étiqueté le jeu de données `admin_low`, le jeu de données doit être monté en lecture seule.
- Si le jeu de données est étiqueté, le noyau vérifie que l'étiquette du jeu de données correspond à celle de la zone montage. Si les étiquettes ne correspondent pas, le montage échoue, sauf si la zone autorise les montages "read-down". Lorsque la zone autorise les montages "read-down", les systèmes de fichiers de niveau inférieur sont montés en lecture seule.

Pour définir la propriété `mlslabel` à partir de la ligne de commande, saisissez quelque chose de semblable à ce qui suit :

```
# zfs set mlslabel=public export/publicinfo
```

Le privilège `file_upgrade_sl` est requis pour définir une étiquette initiale ou pour modifier une étiquette non définie par défaut sur une étiquette de niveau supérieur. Le privilège `file_downgrade_sl` est nécessaire pour supprimer une étiquette, c'est-à-dire, pour définir l'étiquette sur `none`. Ce privilège est également requis pour modifier une étiquette non définie par défaut sur une étiquette de niveau inférieur.

Sauvegarde, partage et montage de fichiers étiquetés (liste des tâches)

La liste des tâches ci-dessous décrit les tâches courantes permettant d'effectuer la sauvegarde et la restauration de données de systèmes de fichiers étiquetés et de partager et monter des systèmes de fichiers étiquetés.

Tâche	Description	Voir
Sauvegarde de fichiers	Archive vos données.	"Procédure de sauvegarde de fichiers dans Trusted Extensions" à la page 194
Restauration de données	Permet de restaurer des données à partir d'une sauvegarde.	"Procédure de restauration de fichiers dans Trusted Extensions" à la page 195
Partage d'un système de fichiers étiqueté	Rend le système de fichiers étiqueté accessible aux utilisateurs d'autres systèmes.	"Procédure de partage de systèmes de fichiers à partir d'une zone étiquetée" à la page 195
Montage d'un système de fichiers partagé par une zone étiquetée	Permet au contenu d'un système de fichiers d'être monté en lecture-écriture dans une zone étiquetée sous la même étiquette. 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 197
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 sous chacune des étiquettes d'un système situé en dehors du serveur d'annuaires personnel NFS.	"Procédure permettant aux utilisateurs d'accéder à leurs répertoires personnels distants sous chaque étiquette en se connectant à chaque serveur NFS" à la page 77
Dissimulation des informations de niveau inférieur pour un utilisateur travaillant dans une étiquette de niveau supérieur	Empêche les informations de niveau inférieur d'être visionnées depuis un niveau supérieur.	"Procédure de désactivation du montage pour les fichiers de niveau inférieur " à la page 182
Dépannage des problèmes de montage de systèmes de fichiers	Résout les problèmes de montage d'un système de fichiers.	"Dépannage des échecs de montage dans Trusted Extensions" à la page 198

▼ Procédure de sauvegarde de fichiers dans Trusted Extensions

Avant de commencer Le profil de droits Media Backup doit vous être attribué. Vous vous trouvez dans la zone globale.

- **Pour plus d'informations sur les méthodes disponibles, reportez-vous à la section "Envoi et réception de données ZFS" du manuel** *Administration d'Oracle Solaris : Systèmes de fichiers ZFS*.

Attention – Seules les commandes suivantes préservent les étiquettes.

- `/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

  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

Avant de commencer Vous êtes dans le rôle `root` dans la zone globale.

- **Pour plus d'informations sur les méthodes disponibles, reportez-vous à la section "Envoi et réception de données ZFS" du manuel** *Administration d'Oracle Solaris : Systèmes de fichiers ZFS*.

Attention – Seules les commandes suivantes préservent les étiquettes.

- `/usr/lib/fs/ufs/ufsrestore` pour les restaurations importantes
- `/usr/sbin/tar xT` pour les petites restaurations

Pour plus d'informations sur l'option `T` de la commande `tar`, reportez-vous à la page de manuel `tar(1)`.

▼ Procédure de partage de systèmes de fichiers à partir d'une zone étiquetée

Pour monter ou partager des répertoires qui trouvent leur origine dans les zones étiquetées, définissez les propriétés du partage ZFS appropriées dans le système de fichiers, puis redémarrez la zone afin de 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 disposer du profil de droits ZFS File System Management.

1. **Créez un espace de travail sous l'étiquette du système de fichiers qui va être partagé.**

   Pour plus d'informations, reportez-vous à la section "Procédure d'ajout d'un espace de travail sous votre étiquette minimale" du manuel *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

2. **Dans la zone, créez le système de fichiers.**

   ```
   # zfs create rpool/wdocs1
   ```

3 **Partagez le système de fichiers en définissant des propriétés de partage NFS.**

Par exemple, le jeu de commandes ci-après partage un système de fichiers de documentation pour les auteurs. Le système de fichiers est partagé en lecture-écriture de sorte que les auteurs puissent modifier leurs documents sur ce serveur. Les programmes `setuid` sont interdits.

```
# zfs set share=name=wdocs1,path=/wdocs1,prot=nfs,setuid=off,
exec=off,devices=off rpool/wdocs1
# zfs set sharenfs=on rpool/wdocs1
```

La ligne de commande est renvoyée à des fins d'affichage.

4 **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 systèmes de fichiers de l'une des façons suivantes : 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, initialisez la zone.**

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

- **Si la zone est déjà en cours d'exécution, réinitialisez la zone.**

  `# zoneadm -z` *zone-name* `reboot`

5 **Affichez les systèmes de fichiers partagés à partir de votre système.**

Dans le rôle `root` de la zone globale, exécutez la commande suivante :

```
# zfs get all rpool
```

Pour plus d'informations, reportez-vous à la section "Envoi de requêtes sur les informations des systèmes de fichiers ZFS" du manuel *Administration d'Oracle Solaris : Systèmes de fichiers ZFS*

6 **Pour permettre au client de monter le système de fichiers partagé, reportez-vous à la section "Procédure de montage NFS de fichiers dans une zone étiquetée" à la page 197.**

Exemple 14–1 Partage du système de fichiers /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 système de fichiers `/export/reference` de la zone `public`..

Tout d'abord, l'administrateur modifie l'étiquette de l'espace de travail sur espace de travail `public`, puis ouvre une fenêtre de terminal. Dans la fenêtre, l'administrateur définit les propriétés `share` sélectionnées sur le système de fichiers `/reference`. La commande suivante est renvoyée à des fins d'affichage.

```
# zfs set share=name=reference,path=/reference,prot=nfs,
setuid=off,exec=off,devices=off,rdonly=on rpool/wdocs1
```

L'administrateur partage ensuite le système de fichiers.

```
# zfs set sharenfs=on rpool/reference
```

L'administrateur quitte l'espace de travail `public` et retourne dans l'espace de travail Trusted Path (Chemin de confiance). Étant donné que les utilisateurs ne sont pas autorisés à se connecter à ce serveur de fichiers, l'administrateur partage le système de fichiers en modifiant l'état de la zone sur prêt :

```
# zoneadm -z public ready
```

Les utilisateurs peuvent accéder au système de fichiers partagé une fois que celui-ci est monté 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 systèmes de fichiers provenant d'hôtes étiquetés et sans étiquette peuvent être montés sur un système étiqueté Trusted Extensions. Le système doit posséder une route vers le serveur de fichiers sous l'étiquette de la zone montage.

- Pour monter les fichiers en lecture-écriture à partir d'un hôte à étiquette unique, l'étiquette affectée à l'hôte distant doit correspondre à l'étiquette de la zone de montage. Deux configurations d'hôte distants sont possibles.
  - L'hôte distant se voit affecter la même étiquette que la zone de montage.
  - L'hôte distant est un serveur multiniveau qui inclut l'étiquette de la zone montage.
- Les systèmes de 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 qu'Oracle Solaris :

- Par défaut, les systèmes de fichiers sont montés lors de l'initialisation.
- Pour monter des systèmes de fichiers de façon dynamique, 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.

Avant de commencer Vous devez être sur le système client, dans la zone possédant l'étiquette des fichiers que vous souhaitez monter. Vérifiez que le système de fichiers que vous souhaitez monter est partagé. Si vous n'utilisez pas l'agent de montage automatique, vous devez disposer du profil de droits File System Management. Pour effectuer des montages à partir de serveurs de niveau inférieur, la zone de ce client doit être configurée avec le droit `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 sous votre étiquette minimale" du manuel *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

  - **Montage dynamique de fichiers.**

    Dans la zone étiquetée, utilisez la commande `mount`.

  - **Montage de fichiers lors de l'initialisation de la zone.**

  - **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.**

▼ Dépannage des échecs de montage dans Trusted Extensions

Avant de commencer Vous devez être dans la zone possédant l'étiquette du système de fichiers que vous souhaitez monter. Vous devez posséder le rôle `root`.

1 **Vérifiez que les systèmes de fichiers du serveur NFS sont partagés.**

2 Vérifiez les attributs de sécurité du serveur NFS.

a. Utilisez la commande `tninfo` ou `tncfg` pour rechercher l'adresse IP du serveur ou une plage d'adresses IP incluant le serveur NFS.

L'adresse peut être assignée directement, ou indirectement par le biais d'un mécanisme de caractère générique. L'adresse peut se trouver 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.

3 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.

4 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 15

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) 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.

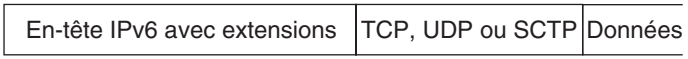
Le logiciel de gestion de réseaux de confiance veille à ce que la stratégie de sécurité de Trusted Extensions soit appliquée même lorsque les sujets (processus) et les objets (données) se trouvent sur des hôtes différents. La gestion de réseaux Trusted Extensions assure le respect du MAC dans des applications 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. L'interface graphique `txzonemgr` et la commande `tncfg` sont utilisées pour configurer le réseau.

Les systèmes qui exécutent le logiciel Trusted Extensions prennent en charge les communications réseau entre les systèmes Trusted Extensions et n'importe lequel des types de systèmes suivants :

- d'autres hôtes qui exécutent Trusted Extensions ;
- des hôtes 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 ;
- des hôtes 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 des commandes et fournit une interface utilisateur graphique pour 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 204.

  Les interfaces gèrent trois bases de données de configuration réseau Trusted Extensions, `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 205.
- Trusted Extensions ajoute les bases de données `tnrhtp` et `tnrhdb` aux propriétés du service SMF de commutation du service de nommage, `svc:/system/name-service/switch`.
- La section Partie I décrit comment définir les zones et les hôtes lorsque vous configurez le réseau. Pour des procédures supplémentaires, reportez-vous au Chapitre 16, "Gestion des réseaux dans Trusted Extensions (tâches) ".
- Trusted Extensions étend le fichier de configuration IKE, `/etc/inet/ike/config`. Pour plus d'informations, reportez-vous à la section "Administration d'IPsec avec étiquettes" à la page 217 et à la page de manuel `ike.config`(4)

Commandes réseau dans Trusted Extensions

Trusted Extensions ajoute les commandes suivantes pour administrer la gestion de réseaux de confiance :

- `tncfg` : cette commande crée, modifie et affiche la configuration de votre réseau Trusted Extensions. La commande `tncfg -t` permet de visualiser, de créer ou de modifier un modèle de sécurité donné. La commande `tncfg -z` permet de visualiser ou de modifier les propriétés réseau d'une zone donnée. Pour plus d'informations, reportez-vous à la page de manuel `tncfg(1M)`.
- `tnchkdb` : cette commande permet de vérifier que les bases de données du réseau de confiance sont correctes. La commande `tnchkdb` est appelée chaque fois que vous modifiez un modèle de sécurité (`tnrhtp`), une affectation de modèle de sécurité (`tnrhdb`) ou la configuration d'une zone (`tnzonecfg`) à l'aide de la commande `txzonemgr` ou de la commande `tncfg`. 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. 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. L'ordre de la recherche est dicté par le service SLF `name-service/switch`. Le démon `tnd` est démarré par le service `svc:/network/tnd` pendant l'initialisation. Ce service dépend de `svc:/network/ldap/client`.

  Dans un réseau LDAP, 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 :

- `ipadm` : la propriété d'adresse `all-zones` rend l'interface indiquée disponible pour chaque zone 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 `ipadm(1M)`.
- `netstat` : l'option `-R` étend l'utilisation de `netstat` d'Oracle Solaris 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 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.
- `ipseckey` : dans Trusted Extensions, les extensions suivantes sont disponibles pour étiqueter les paquets protégés par IPsec : `label` *label*, `outer-label` *label* et `implicit-label` *label*. Pour plus d'informations, reportez-vous à la page de manuel `ipseckey`(1M).

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 d'hôte à hôte.

- `tnzonecfg` : cette base de données locale enregistre les attributs liés à la sécurité des zones. La commande `tncfg` est l'interface permettant d'accéder à et de modifier cette base de données.

  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 à la page de manuel `label_encodings`(4). Pour une description des ports multiniveau, reportez-vous à la section “Zones et ports multiniveau” à la page 175.
- `tnrhtp` : cette base de données stocke des modèles qui décrivent les attributs de sécurité d'hôtes et de passerelles. La commande `tncfg` est l'interface permettant d'accéder à et de modifier cette base de données.

  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 206.
- `tnrhdb` : cette base de données contient les adresses IP et les plages d'adresses IP correspondant à tous les hôtes autorisés à communiquer avec ce système. La commande `tncfg` est l'interface permettant d'accéder à et de modifier cette base de données.

  Chaque hôte ou plage d'adresses IP 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.

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 et des attributs de sécurité identiques.

Les attributs de sécurité sont assignés aux systèmes distants (hôtes et routeurs) par le biais de modèles. L'administrateur de sécurité administre des modèles et les assigne à des systèmes distants. Si aucun modèle n'est assigné à un système distant, aucune communication n'est autorisée avec ce système.

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 207.
- Un ensemble d'attributs de sécurité appliqués à chaque type d'hôte.

Pour plus d'informations, reportez-vous à la section "Attributs de sécurité réseau dans Trusted Extensions" à la page 206.

Attributs de sécurité réseau dans Trusted Extensions

Un système Trusted Extensions est installé avec un ensemble de modèles de sécurité par défaut qui sont utilisés pour définir les propriétés d'étiquettes des hôtes distants. 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 de sécurité. Les hôtes auxquels aucun modèle n'est assigné ne peuvent pas communiquer avec les hôtes configurés à l'aide de Trusted Extensions. Les modèles sont stockés localement.

Les hôtes peuvent être ajoutés à un modèle de sécurité par le biais de leur adresse IP ou dans le cadre d'une plage d'adresses IP. Pour plus d'informations, reportez-vous à la section "Mécanisme de secours du réseau de confiance" à la page 209.

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 le système 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 section "Étiquette par défaut dans les modèles de sécurité" à la page 208.
- **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 auxiliaires** : 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 auxiliaires peuvent envoyer et recevoir des paquets correspondant à n'importe quelle étiquette de cet ensemble d'étiquettes. Le nombre maximal d'étiquettes auxiliaires 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 être trop peu contraignants 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 les systèmes 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*. La raison technique pour laquelle ces hôtes sont appelés "à étiquette unique" est que ces hôtes n'ont pas d'étiquette `admin_high` et `admin_low`.

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 de DOI différente de la valeur par défaut, vous devez utiliser cette valeur dans chaque modèle de sécurité, comme décrit à la section "Procédure de configuration du domaine d'interpretation" à la page 57.

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 dans le modèle de sécurité de l'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.

Étiquettes auxiliaires dans les modèles de sécurité

L'ensemble d'étiquettes auxiliaires, 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 auxiliaire n'est défini.

Mécanisme de secours du réseau de confiance

Une adresse IP hôte peut être ajoutée à un modèle de sécurité de manière directe ou indirecte. L'affectation directe ajoute l'adresse IP d'un hôte. L'affectation indirecte ajoute une plage d'adresses IP incluant celle de l'hôte. Pour trouver un hôte donné, le logiciel du réseau de confiance recherche d'abord l'adresse IP correspondante. 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. Pour consulter des exemples, reportez-vous au Tableau 15–1.

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 15–1 Entrées du mécanisme de secours et de l'adresse hôte Trusted Extensions

Version IP	Entrée hôte pour `host_type=cipso`	Adresses IP couvertes
IPv4	`192.168.118.57`	`192.168.118.57`
	`192.168.118.57/32`	`/32` définit une longueur de préfixe fixe de 32 bits.
	`192.168.118.128/26`	De `192.168.118.0` à `192.168.118.63`
	`192.168.118.0`	Toutes les adresses du sous-réseau `192.168.118.`.
	`192.168.118.0/24`	
	`192.168.0.0/24`	Toutes les adresses du sous-réseau `192.168.0.`.
	`192.168.0.0`	Toutes les adresses du sous-réseau `192.168.`.
	`192.168.0.0/16`	
	`192.0.0.0`	Toutes les adresses du sous-réseau `192.`.
	`192.0.0.0/8`	
	`192.168.118.0/32`	Adresse hôte `192.168.118.0`. N'est pas une plage d'adresses.
	`192.168.0.0/32`	Adresse hôte `192.168.0.0`. N'est pas une plage d'adresses.
	`192.0.0.0/32`	Adresse hôte `192.0.0.0`. N'est pas une plage d'adresses.
	`0.0.0.0/32`	Adresse hôte `0.0.0.0`. N'est pas une plage d'adresses.
	`0.0.0.0`	Toutes les adresses de tous les réseaux

TABLEAU 15–1 Entrées du mécanisme de secours et de l'adresse hôte Trusted Extensions *(Suite)*

Version IP	Entrée hôte pour `host_type=cipso`	Adresses IP couvertes
IPv6	`2001\:DB8\:22\:5000\:\:21f7`	`2001:DB8:22:5000::21f7`
	`2001\:DB8\:22\:5000\:\:0/52`	De `2001:DB8:22:5000::0` à `2001:DB8:22:5fff:ffff:ffff:ffff:ffff`
	`0\:\:0/0`	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`. En ajoutant l'entrée `0.0.0.0/32` au modèle de sécurité sans étiquette d'un système, vous permettez à des hôtes possédant l'adresse spécifique `0.0.0.0` de contacter le système. 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` pour une application servant des clients DHCP, reportez-vous à l'Exemple 16–16. Le réseau `0.0.0.0:admin_low` est l'entrée par défaut dans le modèle d'hôte non étiqueté `admin_low`. Les problèmes de sécurité susceptibles de requérir un changement de cette valeur par défaut sont répertoriés dans la section "Procédure de limitation des hôtes pouvant être contactés sur le réseau de confiance" à la page 236.

Pour plus d'informations sur les longueurs de préfixe dans les adresses IPv4 et IPv6, reportez-vous à la section "Choix du format d'adressage IP du réseau" du manuel *Administration d'Oracle Solaris : Services IP* et "IPv6 Addressing Overview" du manuel *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. Contrairement à Oracle Solaris, 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 effectués 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 auxiliaires.

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 d'hôtes prenant en charge l'étiquetage. Lorsque le paquet ne fournit pas d'étiquette, une étiquette par défaut est assignée au message à partir du modèle de sécurité. 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, 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.
- Pour toutes les destinations, l'étiquette du paquet sortant 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.
- 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 définie dans le modèle de sécurité. 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, 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.
  - Pour toutes les destinations, l'étiquette du paquet sortant 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.
  - 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 système 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 définie dans le modèle de sécurité. Dans le cas contraire, le paquet se voit affecter l'étiquette CIPSO spécifiée.
- 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. Vous pouvez configurer des routes permettant d'appliquer le 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 ajoutent l'interface réseau de la passerelle qui est connectée au réseau externe à un modèle à étiquette unique. Pour plus d'informations sur TCP/IP et sur le routage, reportez-vous aux sections suivantes :

- "Configuration d'un routeur IPv4" du manuel *Administration d'Oracle Solaris : Services IP*
- "Configuration des composants système sur le réseau" du manuel *Administration d'Oracle Solaris : Services IP*
- "Principales tâches d'administration TCP/IP (liste des tâches)" du manuel *Administration d'Oracle Solaris : Services IP*
- `netcfg`(1M)

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 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 212. 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 sous-réseau où

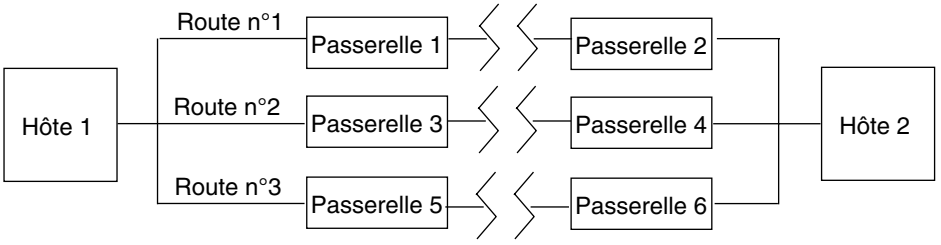
réside l'hôte n'est défini, l'hôte envoie le paquet vers une passerelle par défaut, lorsqu'une telle passerelle est définie. Plusieurs passerelles par défaut peuvent être définies et toutes sont traitées de façon égale.

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.

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 15–1 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 dérivés du modèle de sécurité de 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 l'option `delete` (supprimer) modifie les entrées de la table de routage.

Pour plus d'informations, reportez-vous aux pages de manuel `netstat(1M)` et `route(1M)`.

Trusted Extensions propose les interfaces suivantes pour modifier les entrées de table de routage :

- L'interface graphique `txzonemgr` permet d'affecter la route par défaut d'une interface.
- La commande `route -p` associée à l'option `add` (ajouter) ou l'option `delete` (supprimer) permet de modifier les entrées de la table de routage.

Pour consulter des exemples, reportez-vous à la section "Procédure d'ajout des routes par défaut" à la page 240.

Administration d'IPsec avec étiquettes

Les systèmes Trusted Extensions peuvent protéger des paquets réseau étiquetés au moyen d'IPsec. Les paquets IPsec peuvent être envoyés avec des étiquettes Trusted Extensions explicites ou implicites. Les étiquettes sont envoyées explicitement à l'aide d'options IP CIPSO et implicitement à l'aide d'associations de sécurité (SA) IPsec avec étiquettes. En outre, des paquets chiffrés par IPsec pourvus de différentes étiquettes implicites peuvent être mis en tunnel au sein d'un réseau sans étiquette.

Pour plus d'informations sur les concepts IPsec et les procédures de configuration générales, reportez-vous à la Partie III, "IPsec" du manuel *Administration d'Oracle Solaris : Services IP*. Pour plus d'informations sur les modifications apportées par Trusted Extensions aux procédures IPsec, reportez-vous à la section "Configuration d'IPsec avec étiquettes (liste des tâches)" à la page 243.

Étiquettes pour les échanges protégés par IPsec

Toutes les communications sur des systèmes Trusted Extensions, y compris les communications protégées par IPsec, doivent satisfaire aux contrôles d'accréditation des étiquettes de sécurité. Les contrôles sont décrits dans la section "Contrôles d'accréditation dans Trusted Extensions" à la page 212.

Les étiquettes appliquées à des paquets IPsec provenant d'une application d'une zone étiquetée qui doivent passer ces contrôles sont l'*étiquette intérieure*, l'*étiquette de transmission*, et l'*étiquette de gestion de clé* :

- **Étiquette de sécurité d'application :** étiquette de la zone dans laquelle réside l'application.
- **Étiquette intérieure :** étiquette des données de message non chiffrées avant l'application d'en-têtes AH ou ESP IPsec. Cette étiquette peut être différente de l'étiquette de sécurité de l'application lorsque l'option de socket `SO_MAC_EXEMPT` (MAC-exempt) ou des fonctions port multiniveau (MLP) sont utilisées. Lorsque vous sélectionnez des associations de sécurité (SA) et des règles IKE qui sont limitées par les étiquettes, IPsec et IKE utilisent cette étiquette intérieure.

  Par défaut, l'étiquette intérieure est identique à l'étiquette de sécurité de l'application. En règle générale, les applications aux deux extrémités ont la même étiquette. Toutefois, ce n'est pas nécessairement le cas pour la communication MAC-exempt ou MLP. Les paramètres de configuration IPsec peuvent définir la manière dont l'étiquette est transmise au sein du réseau, c'est-à-dire l'*étiquette de transmission*. Les paramètres de configuration IPsec ne peuvent pas définir la valeur de l'étiquette intérieure.
- **Étiquette de transmission :** étiquette des données de message chiffrées après l'application d'en-têtes AH ou ESP IPsec. Selon les fichiers de configuration IKE et IPsec, l'étiquette de transmission peut être différente de l'étiquette intérieure.
- **Étiquette de gestion de clé :** toutes les négociations IKE entre deux nœuds sont contrôlées au niveau d'une seule étiquette, indépendamment de l'étiquette du message d'application qui déclenche les négociations. L'étiquette des négociations IKE est définie dans le fichier `/etc/inet/ike/config` sur la base d'une règle par IKE.

Extensions d'étiquettes pour les associations de sécurité IPsec

Les *extensions d'étiquettes* IPsec sont utilisées sur les systèmes Trusted Extensions pour associer une étiquette au trafic qui transite au sein d'une association de sécurité (SA). Par défaut, IPsec n'utilise pas les extensions d'étiquettes et ignore donc les étiquettes. Quelle que soit l'étiquette Trusted Extensions, l'ensemble du trafic entre deux systèmes transite par une seule SA.

Les extensions d'étiquettes vous permettent d'effectuer les opérations suivantes :

- Configurer une SA IPsec différente à utiliser avec chaque étiquette Trusted Extensions. Cette configuration offre un mécanisme supplémentaire de transmission de l'étiquette du trafic transitant entre deux systèmes multiniveau.
- Spécifier une étiquette de transmission pour les textes de message chiffrés par IPsec qui diffèrent de la version non chiffrée des textes. Cette configuration prend en charge la transmission de données confidentielles chiffrées via un réseau moins sécurisé.

- Annuler l'utilisation des options IP CIPSO dans des paquets IP. Cette configuration permet au trafic étiqueté de transiter au travers de réseaux ne prenant pas en charge ou hostiles à CIPSO.

Vous pouvez indiquer si vous souhaitez utiliser les extensions d'étiquettes par le biais d'IKE comme décrit dans la section "Extensions d'étiquettes pour IKE" à la page 219, ou manuellement à l'aide de la commande `ipseckey`. Pour plus d'informations sur les fonctions d'extensions d'étiquettes, reportez-vous à la page de manuel `ipseckey(1M)`.

Lorsque vous utilisez des extensions d'étiquettes, la sélection de SA pour le trafic sortant prend en compte l'étiquette de sensibilité interne. L'étiquette de sécurité du trafic entrant est défini par l'étiquette de sécurité de la SA du paquet reçu.

Extensions d'étiquettes pour IKE

IKE sur les systèmes Trusted Extensions prend en charge la négociation d'étiquettes pour les SA avec les pairs prenant en charge les étiquettes. Vous pouvez contrôler ce mécanisme en utilisant les mots-clés suivants dans le fichier `/etc/inet/ike/config` :

- **label_aware :** permet au démon `in.iked` d'utiliser les interfaces d'étiquettes Trusted Extensions et de négocier les étiquettes avec les pairs.
- **single_label :** indique que le pair ne prend pas en charge la négociation d'étiquettes pour les SA.
- **multi_label :** indique que le pair prend en charge la négociation d'étiquettes pour les SA. IKE crée une nouvelle SA pour chaque étiquette supplémentaire rencontrée dans le trafic entre deux nœuds.
- **wire_label inner :** entraîne la création par le démon `in.iked` de SA étiquetées dans lesquelles l'étiquette de transmission est la même que l'étiquette intérieure. L'étiquette de gestion des clés est `ADMIN_LOW` lorsque le démon négocie avec des pairs `cipso`. L'étiquette de gestion des clés est l'étiquette par défaut du pair lorsque le démon négocie avec des pairs sans étiquette. Pour inclure les options IP CIPSO dans les paquets transmis, les règles Trusted Extensions normales doivent être suivies.
- **wire_label** *étiquette* **:** entraîne la création par le démon `in.iked` de SA étiquetées dans lesquelles l'étiquette de transmission est définie sur *étiquette*, quelle que soit la valeur de l'étiquette intérieure. Le démon `in.iked` effectue les négociations de gestion des clés à l'étiquette spécifiée. Les règles normales de Trusted Extensions sont suivies pour l'inclusion d'options IP CIPSO dans les paquets transmis.
- **wire_label none** *étiquette* **:** entraîne un comportement similaire à `wire_label` *étiquette*, à la différence près que les options IP sont supprimées sur les paquets IKE transmis et les paquets de données sous la SA.

Pour plus d'informations, reportez-vous à la page de manuel `ike.config(4)`.

Étiquettes et accréditation en IPsec mode tunnel

Lorsque des paquets de données d'application sont protégés par IPsec en mode tunnel, les paquets contiennent plusieurs en-têtes IP.

L'en-tête IP du protocole IKE contient la même paire adresse source et adresse de destination que l'en-tête IP externe du paquet de données d'application.

Trusted Extensions utilise les adresses d'en-têtes IP internes pour des contrôles d'accréditation des étiquettes internes. Trusted Extensions effectue des contrôles des étiquettes de transmission et de gestion des clés à l'aide des adresses d'en-têtes IP externes. Pour plus d'informations sur les contrôles d'accréditation, reportez-vous à la section “Contrôles d'accréditation dans Trusted Extensions” à la page 212.

Protections relatives à la confidentialité et à l'intégrité à l'aide des extensions d'étiquettes

Le tableau ci-dessous explique comment les protections IPsec de confidentialité et d'intégrité s'appliquent à l'étiquette de sécurité avec différentes configurations d'extensions d'étiquettes.

Association de sécurité	Confidentialité	Intégrité
Sans extensions d'étiquettes	L'étiquette est visible dans l'option IP CIPSO.	L'étiquette de message dans l'option IP CIPSO est couverte par AH, non par ESP. Reportez-vous à la note.
Avec extensions d'étiquettes	Une option IP CIPSO est visible, mais représente l'étiquette de transmission, qui peut être différente de l'étiquette intérieure du message.	L'intégrité d'une étiquette est implicitement assurée par l'existence d'une SA spécifique à l'étiquette. Une option IP CIPSO est assurée par AH. Reportez-vous à la note.
Avec extensions d'étiquettes et suppression de l'option IP CIPSO	L'étiquette du message n'est pas visible.	L'intégrité d'une étiquette est implicitement assurée par l'existence d'une SA spécifique à l'étiquette.

Remarque – Vous ne pouvez pas utiliser les protections relatives à l'intégrité AH d'IPsec pour protéger l'option IP CIPSO si des routeurs prenant en charge CIPSO risquent de supprimer ou d'ajouter l'option IP CIPSO pendant qu'un message parcourt le réseau. Toute modification apportée à la l'option IP CIPSO invalidera le message et entraînera la perte d'un paquet protégé par AH à sa destination.

◆ ◆ ◆ CHAPITRE 16

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 fournit des liens vers les listes de tâches répertoriant les procédures courantes de gestion de réseaux Trusted Extensions.

Tâche	Description	Voir
Affectation d'étiquettes à des hôtes et des réseaux	Crée des modèles d'hôte distants et assigne des hôtes aux modèles de sécurité.	"Étiquetage d'hôtes et de réseaux (liste des tâches)" à la page 224
Assignation de routes par défaut et configuration de ports multiniveau (MLP)	Configure des routes statiques permettant aux paquets étiquetés d'atteindre leur destination via des passerelles étiquetées et non étiquetées. Ajoute des MLP privés et partagés aux zones étiquetées et à la zone globale.	"Configuration des routes et ports multiniveau (MLP) (tâches) " à la page 240
Activation d'IPsec pour la protection des paquets étiquetés	Protège les paquets étiquetés à l'aide d'IPsec.	"Configuration d'IPsec avec étiquettes (liste des tâches)" à la page 243
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 248

Étiquetage d'hôtes et de réseaux (liste des tâches)

Le système Trusted Extensions peut contacter d'autres hôtes uniquement après avoir défini les attributs de sécurité de ces hôtes. Étant donné que les hôtes distants peuvent avoir des attributs de sécurité similaires, Trusted Extensions fournit des modèles de sécurité auxquels il est possible d'ajouter des hôtes.

La liste ci-dessous décrit les tâches que vous pouvez utiliser pour compléter les modèles de sécurité et les appliquer à des hôtes distants.

Tâche	Description	Voir
Affichage des modèles de sécurité	Affiche les modèles de sécurité disponibles.	“Procédure d'affichage des modèles de sécurité” à la page 225
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 226
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 230
Création de modèles de sécurité	Définit les attributs de sécurité de votre réseau de confiance.	“Procédure de création de modèles de sécurité” à la page 227
	Change la valeur du DOI en une valeur autre que 1.	“Procédure de configuration du domaine d'interpretation” à la page 57
	Pour les hôtes distants auxquels une étiquette spécifique est assignée.	Exemple 16–1
	Pour les hôtes distants agissant en tant que passerelles à étiquette unique.	Exemple 16–2
	Pour les hôtes distants qui restreignent le trafic à une plage d'étiquettes réduite.	Exemple 16–3
	Pour les hôtes distants contenant des étiquettes discrètes.	Exemple 16–4
	Pour les réseaux et hôtes distants sans étiquette.	Exemple 16–5
	Pour deux hôtes distants avec étiquettes disjointes du reste du réseau.	Exemple 16–6

Tâche	Description	Voir
Ajout d'un hôte à un modèle de sécurité	Ajoute une adresse IP à un modèle de sécurité.	"Procédure d'ajout d'un hôte au modèle de sécurité" à la page 231 Exemple 16–7 Exemple 16–8 Exemple 16–9 Exemple 16–10
Ajout d'adresses IP contiguës à un modèle de sécurité	Ajoute une plage d'adresses IP à un modèle de sécurité.	"Procédure d'ajout d'une plage d'hôtes au modèle de sécurité" à la page 234 Exemple 16–12 Exemple 16–13
Suppression d'un hôte d'un modèle de sécurité	Supprime la définition de sécurité d'un hôte.	Exemple 16–11
Spécification des hôtes autorisés à communiquer sous l'étiquette `admin_low`	Renforce la sécurité en spécifiant les hôtes qu'un système peut contacter au moment de l'initialisation.	"Procédure de limitation des hôtes pouvant être contactés sur le réseau de confiance" à la page 236
	Renforce la sécurité en spécifiant un réseau d'hôtes étiquetés que le système peut contacter au moment de l'initialisation.	Exemple 16–14
Création d'une entrée pour l'adresse hôte `0.0.0.0/32`.	Configure un serveur d'applications de manière à ce qu'il accepte le contact initial provenant d'un client distant.	Exemple 16–16

▼ Procédure d'affichage des modèles de sécurité

Vous pouvez visualiser la liste des modèles de sécurité et le contenu de chaque modèle. Les exemples de cette procédure sont les modèles de sécurité par défaut.

1 Répertoriez les modèles de sécurité disponibles.

```
# tncfg list
   cipso
   admin_low
```

2 Affichez le contenu des modèles répertoriés.

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

L'entrée `127.0.0.1/32` du modèle de sécurité `cipso` précédent identifie ce système comme étiqueté. Lorsqu'un pair attribue ce système au modèle d'hôte distant du pair à l'aide du `host_type` de `admin_low`, les deux systèmes peuvent échanger des paquets étiquetés.

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

L'entrée `0.0.0.0/0` du modèle de sécurité `admin_low` précédent permet à l'ensemble des hôtes qui ne sont pas explicitement assignés à un modèle de sécurité de contacter ce système. Ces hôtes sont reconnus en tant qu'hôtes sans étiquette.

- L'avantage de cette entrée est que tous les hôtes requis par le système au moment de l'initialisation, tels que les serveurs et les passerelles, peuvent être trouvés.
- L'inconvénient de cette entrée est que n'importe quel hôte se trouvant sur le réseau du système peut contacter ce système. Pour restreindre le nombre d'hôtes autorisés à contacter ce système, reportez-vous à la section "Procédure de limitation des hôtes pouvant être contactés sur le réseau de confiance" à la page 236.

▼ 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 sécurité Trusted Extensions.**

   Suivez les instructions de la section "Procédure d'affichage des modèles de sécurité" à la page 225 pour afficher les modèles de sécurité disponibles.

2. **Créez de nouveaux modèles de sécurité si vous souhaitez effectuer l'une des opérations suivantes pour les hôtes avec lesquels vous communiquez :**

   - Limiter la plage d'étiquettes d'un hôte ou d'un groupe d'hôtes.
   - Créer un hôte à étiquette unique sous une autre étiquette que `ADMIN_LOW`.
   - Utiliser une étiquette par défaut autre que `ADMIN_LOW` pour les hôtes non étiquetés.
   - Créer un hôte capable de reconnaître certaines étiquettes discrètes.
   - Utilisez un DOI autre que 1.

Étapes suivantes Pour ajouter des hôtes aux modèles de sécurité par défaut, reportez-vous à la section "Procédure d'ajout d'un hôte au modèle de sécurité" à la page 231.

Sinon, poursuivez à la section "Procédure de création de modèles de sécurité" à la page 227.

▼ Procédure de création de modèles de sécurité

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 des profils de droits Information Security ou Network Security ont été affectés peuvent modifier les valeurs de sécurité. Le rôle d'administrateur de sécurité inclut ces profils de droits.

1 **(Facultatif) Déterminez la version hexadécimale de chaque étiquette autre que `ADMIN_HIGH` et `ADMIN_LOW`.**

Pour les étiquettes comme `PUBLIC` , vous pouvez utiliser la chaîne d'étiquettes ou la valeur hexadécimale, `0x0002-08-08` comme valeurs d'étiquette. La commande `tncfg` accepte les deux formats.

```
# atohexlabel "confidential : internal use only"
0x0004-08-48
```

Pour plus d'informations, reportez-vous à la section "Obtention de l'équivalent hexadécimal d'une étiquette" à la page 134.

2 **Ne modifiez pas les modèles de sécurité par défaut.**

Pour permettre une assistance en cas de besoin, vous ne devez pas supprimer les modèles de sécurité par défaut. Vous pouvez copier et modifier ces modèles. Vous pouvez également ajouter et supprimer des hôtes assignés à ces modèles. 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 236.

3 **Créez un modèle de sécurité.**

La commande `tncfg -t` fournit trois façons de créer de nouveaux modèles.

- **Créer un modèle de sécurité à partir de zéro.**

  Utilisez la commande `tncfg` en mode interactif. La sous-commande `info` affiche les valeurs fournies par défaut. Utilisez la touche de tabulation pour compléter les propriétés et les valeurs partielles.

```
# tncfg -t newunlabeled
tncfg:newtemplate> info
   name=newunlabeled
   host_type=unlabeled
   doi=1
   def_label=ADMIN_LOW
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
tncfg:newunlabeled> set m<Tab>
set max_label=" set min_label="
tncfg:newunlabeled> set ma<Tab>
```

```
tncfg:newunlabeled> set max_label=ADMIN_LOW
...
```

Vous pouvez également fournir la liste complète des attributs d'un modèle de sécurité sur la ligne de commande. Les sous-commandes `set` sont séparées par des points-virgules. Lorsqu'une propriété est omise, la valeur par défaut lui est attribuée.

```
# tncfg -t newunlabeled set host_type=unlabeled;set doi=1; \
set min_label=ADMIN_LOW;set max_label=ADMIN_LOW
```

- **Copier et modifier un modèle de sécurité existant.**

```
# tncfg -t cipso
tncfg:cipso> set name=newcipso
tncfg:newcipso> info
name=newcipso
host_type=cipso
doi=1
min_label=ADMIN_LOW
max_label=ADMIN_HIGH
```

Les hôtes qui sont affectés au modèle de sécurité existant ne sont pas copiés dans le nouveau modèle.

- **Utiliser un fichier modèle créé par la sous-commande `export`.**

```
# tncfg -f unlab_1  -f template-file
tncfg: unlab1> set host_type=unlabeled
...
# tncfg -f template-file
```

Pour obtenir un exemple de modèle source pour l'importation, reportez-vous à la page de manuel `tncfg(1M)`.

Exemple 16–1 Création d'un modèle de sécurité pour une passerelle gérant des paquets sous une étiquette unique

Dans cet exemple, l'administrateur de sécurité définit une passerelle qui permet uniquement la transmission de paquets au niveau de l'étiquette `PUBLIC`.

```
# tncfg -t cipso_public
tncfg:cipso_public> set host_type=cipso
tncfg:cipso_public> set doi=1
tncfg:cipso_public> set min_label="public"
tncfg:cipso_public> set max_label="public"
tncfg:cipso_public> commit
tncfg:cipso_public> exit
```

L'administrateur de sécurité ajoute ensuite l'hôte de passerelle au modèle de sécurité. Pour des instructions sur l'ajout, reportez-vous à l'Exemple 16–7.

Exemple 16–2 Création d'un modèle de sécurité pour un routeur sans étiquette acheminant les paquets étiquetés

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. Ce routeur non étiqueté nécessite 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`.

L'administrateur de sécurité crée le modèle à partir de zéro.

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

L'administrateur de sécurité ajoute ensuite le routeur au modèle de sécurité. Pour des instructions sur l'ajout, reportez-vous à l'Exemple 16–8.

Exemple 16–3 Création d'un modèle de sécurité pour une passerelle avec une plage d'étiquettes limitée

Dans cet exemple, l'administrateur de sécurité crée une passerelle limitant les paquets à une plage d'étiquettes restreinte. L'administrateur crée un modèle de sécurité auquel il affecte ultérieurement l'hôte de passerelle.

```
# tncfg -t cipso_iuo_rstrct
tncfg:cipso_iuo_rstrct> set host_type=cipso
tncfg:cipso_iuo_rstrct> set doi=1
tncfg:cipso_iuo_rstrct> set min_label=0x0004-08-48
tncfg:cipso_iuo_rstrct> set max_label=0x0004-08-78
tncfg:cipso_iuo_rstrct> add host=192.168.131.78
tncfg:cipso_iuo_rstrct> exit
```

L'administrateur de sécurité ajoute ensuite l'hôte de passerelle au modèle de sécurité. Pour des instructions sur l'ajout, reportez-vous à l'Exemple 16–9.

Exemple 16–4 Création d'un modèle de sécurité avec étiquettes discrètes

Dans cet exemple, l'administrateur de sécurité crée un modèle de sécurité qui reconnaît uniquement deux étiquettes, `confidential : internal use only` et `confidential : restricted` . Tout autre trafic est rejeté.

L'administrateur doit tout d'abord veiller à saisir les étiquettes de façon précise. Le logiciel reconnaît les étiquettes en majuscules et en minuscules, en abrégé, mais ne peut pas reconnaître les étiquettes lorsque l'espacement n'est pas exact. Par exemple, l'étiquette `confidential :restricted` n'est pas valide.

```
# tncfg -t cipso_int_and_rst
tncfg:cipso_int_and_rst> set host_type=cipso
tncfg:cipso_int_and_rst> set doi=1
tncfg:cipso_int_and_rst> set min_label="cnf : internal use only"
tncfg:cipso_int_and_rst> set max_label="cnf : internal use only"
tncfg:cipso_int_and_rst> set aux_label="cnf : restricted"
tncfg:cipso_int_and_rst> exit
```

Exemple 16–5 Création d'un modèle de sécurité non étiqueté sous l'étiquette PUBLIC

Dans cet exemple, l'administrateur de sécurité crée un modèle à étiquette unique pour les hôtes autorisés à recevoir et envoyer des paquets sous l'étiquette `PUBLIC` uniquement. Ce modèle peut être affecté aux hôtes dont les systèmes de fichiers doivent être montés sur l'étiquette `PUBLIC` par les systèmes Trusted Extensions.

```
# tncfg -t public
tncfg:public> set host_type=unlabeled
tncfg:public> set doi=1
tncfg:public> set def_label="public"
tncfg:public> set min_sl="public"
tncfg:public> set max_sl="public"
tncfg:public> exit
```

L'administrateur de sécurité ajoute ensuite des hôtes au modèle de sécurité. Pour des instructions sur l'ajout, reportez-vous à l'Exemple 16–13.

Exemple 16–6 Création d'un modèle de sécurité étiqueté pour les développeurs

Dans cet exemple, l'administrateur de sécurité crée un modèle `cipso_sandbox` . Ce modèle de sécurité est assigné aux systèmes utilisés par les développeurs de logiciels de confiance. Cependant, leurs tests n'affectent pas les autres hôtes étiquetés, car l'étiquette `SANDBOX` est disjointe des autres étiquettes du réseau.

```
# tncfg -t cipso_sandbox
tncfg:cipso_sandbox> set host_type=cipso
tncfg:cipso_sandbox> set doi=1
tncfg:cipso_sandbox> set min_sl="SBX"
tncfg:cipso_sandbox> set max_sl="SBX"
tncfg:cipso_sandbox> exit
```

▼ Procédure d'ajout d'hôtes au réseau connu du système

Une fois que vous avez ajouté des hôtes et des groupes d'hôtes dans le fichier `/etc/hosts` du système, les hôtes sont connus du système. Seuls les hôtes connus peuvent être ajoutés à un modèle de sécurité.

Avant de commencer Vous êtes dans le rôle `root` dans la zone globale.

1 Ajoutez des hôtes individuels dans le fichier `/etc/hosts`.

```
# vi /etc/hosts

...
192.168.111.121   ahost
```

2 Ajoutez un groupe d'hôtes dans le fichier `/etc/hosts`.

```
# vi /etc/hosts

...
192.168.111.0   111-network
```

Étapes suivantes Poursuivez à la section "Procédure d'ajout d'un hôte au modèle de sécurité" à la page 231.

▼ Procédure d'ajout d'un hôte au modèle de sécurité

Avant de commencer Les éléments suivants doivent être en place :

- Le modèle de sécurité doit exister. Pour plus d'informations sur cette procédure, reportez-vous à la section "Procédure de création de modèles de sécurité" à la page 227.
- Les adresses IP doivent exister dans le fichier `/etc/hosts` ou pouvoir être résolues par DNS.

  Pour plus d'informations sur le fichier `hosts`, reportez-vous à la section "Procédure d'ajout d'hôtes au réseau connu du système " à la page 230.

  Pour DNS, reportez-vous à Chapitre 3, "Managing DNS (Tasks)" du manuel *Oracle Solaris Administration: Naming and Directory Services*.
- Les extrémités de l'étiquette doivent correspondre. Pour connaître les règles, reportez-vous à la section "Présentation du routage dans Trusted Extensions" à la page 211.
- Vous devez être dans le rôle d'administrateur de sécurité dans la zone globale.

1 Ajoutez un nom d'hôte ou une adresse IP à un modèle de sécurité.

Par exemple, ajoutez l'adresse IP `192.168.1.2` .

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.1.2
```

Si vous ajoutez un hôte précédemment ajouté à un autre modèle, vous êtes averti du fait que vous êtes en train de remplacer le modèle de sécurité qui lui est affecté. Par exemple :

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.1.22
192.168.1.2 previously matched the admin_low template
tncfg:cipso> info
...
host=192.168.1.2/32
tncfg:cipso> exit
```

2 Consultez le modèle de sécurité modifié.

Par exemple, la ligne ci-après montre l'adresse `192.168.1.2` ajoutée au modèle `cipso` :

```
tncfg:cipso> info
...
   host=192.168.1.2/32
```

La longueur du préfixe de `/32` indique que l'adresse est exacte.

3 Validez la modification et quittez le modèle de sécurité.

```
tncfg:cipso> commit
tncfg:cipso> exit
```

Pour supprimer une entrée d'hôte, reportez-vous à l'Exemple 16–11.

Exemple 16–7 Création d'une passerelle gérant des paquets sur une étiquette unique

Dans l'Exemple 16–1, l'administrateur crée un modèle de sécurité qui définit une passerelle permettant uniquement de transmettre des paquets à l'étiquette `PUBLIC`. Dans cet exemple, l'administrateur de sécurité s'assure que l'adresse IP de l'hôte de passerelle peut être résolue.

```
# arp 192.168.131.75
gateway-1.example.com (192.168.131.75) at 0:0:0:1:ab:cd
```

La commande `arp` vérifie que l'hôte est défini dans le fichier `/etc/hosts` du système ou qu'il peut être résolu par DNS.

L'administrateur ajoute ensuite l'hôte `gateway-1` au modèle de sécurité :

```
# tncfg -t cipso_public
tncfg:cipso_public> add host=192.168.131.75
tncfg:cipso_public> exit
```

Le système peut immédiatement envoyer et recevoir des paquets `public` via `gateway-1`.

Exemple 16–8 Création d'un routeur sans étiquette pour acheminer des paquets étiquetés

Dans l'Exemple 16–2, l'administrateur crée le modèle de sécurité du routeur. Dans cet exemple, l'administrateur s'assure que l'adresse IP du routeur peut être résolue.

```
# arp 192.168.131.82
router-1.example.com (192.168.131.82) at 0:0:0:2:ab:cd
```

La commande `arp` indique que l'hôte est défini dans le fichier `/etc/hosts` du système ou qu'il peut être résolu par DNS.

L'administrateur ajoute ensuite le routeur au modèle de sécurité.

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

Le système peut immédiatement envoyer et recevoir des paquets sur toutes les étiquettes via `routeur-1`.

Exemple 16–9 Création d'une passerelle avec une plage d'étiquettes limitée

Dans l'Exemple 16–3, l'administrateur créé un modèle de sécurité contenant une plage d'étiquettes limitée. Dans cet exemple, l'administrateur de sécurité s'assure que l'adresse IP de l'hôte de passerelle peut être résolue.

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

La commande `arp` indique que l'hôte est défini dans le fichier `/etc/hosts` du système ou qu'il peut être résolu par DNS.

L'administrateur ajoute ensuite la passerelle au modèle de sécurité.

```
# tncfg -t cipso_iuo_rstrct
tncfg:cipso_iuo_rstrct> add host=192.168.131.78
tncfg:cipso_iuo_rstrct> exit
```

Le système peut immédiatement envoyer et recevoir des paquets associés aux étiquettes `internal` et `restricted` via `gateway-ir`.

Exemple 16–10 Création d'un hôte étiqueté pour les développeurs

Dans l'Exemple 16–6, l'administrateur crée le modèle de sécurité `cipso_sandbox`. Dans cet exemple, l'administrateur de sécurité ajoute deux hôtes au modèle.

```
# tncfg -t cipso_sandbox
tncfg:cipso_sandbox> add host=196.168.129.102
tncfg:cipso_sandbox> add host=196.168.129.129
tncfg:cipso_sandbox> exit
```

Les développeurs utilisant les systèmes `196.168.129.102` et `196.168.129.129` peuvent communiquer les uns avec les autres à l'aide de l'étiquette `SANDBOX`.

Exemple 16–11 Suppression de plusieurs hôtes à partir d'un modèle de sécurité

Dans cet exemple, l'administrateur de sécurité supprime plusieurs hôtes à partir du modèle de sécurité `cipso`. L'administrateur utilise la sous-commande `info` pour afficher les hôtes, il saisit ensuite `remove`, puis copie-colle quatre entrées `host=`.

```
# tncfg -t cipso info
   name=cipso
   host_type=cipso
   doi=1
   min_label=ADMIN_LOW
```

```
   max_label=ADMIN_HIGH
   host=127.0.0.1/32
   host=192.168.1.2/32
   host=192.168.113.0/24
   host=192.168.113.100/25
   host=2001:a08:3903:200::0/56

# tncfg -t cipso
tncfg:cipso> remove host=192.168.1.2/32
tncfg:cipso> remove host=192.168.113.0/24
tncfg:cipso> remove host=192.168.113.100/25
tncfg:cipso> remove host=2001:a08:3903:200::0/56
tncfg:cipso> info
...
   max_label=ADMIN_HIGH
   host=127.0.0.1/32
   host=192.168.75.0/24
```

Après la suppression des hôtes, l'administrateur valide les modifications et quitte le modèle de sécurité.

```
tncfg:cipso> commit
tncfg:cipso> exit
#
```

▼ Procédure d'ajout d'une plage d'hôtes au modèle de sécurité

Avant de commencer Pour la configuration requise, reportez-vous à la section "Procédure d'ajout d'un hôte au modèle de sécurité" à la page 231

1 Pour affecter un modèle de sécurité à un sous-réseau, ajoutez l'adresse de sous-réseau au modèle.

Par exemple, ajoutez deux sous-réseaux au modèle `admin_low`, puis affichez le modèle de sécurité.

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.75.0
tncfg:cipso> add host=192.168.113.0
tncfg:cipso> info
...
host=192.168.75.0/24
host=192.168.113.0/24
tncfg:cipso> exit
```

La longueur du préfixe de `/24` indique que l'adresse, qui se termine par `.0`, représente un sous-réseau.

Remarque – Si vous ajoutez une plage d'hôtes précédemment ajoutés à un autre modèle, vous êtes averti du fait que vous êtes en train de remplacer le modèle de sécurité qui lui est affecté.

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.113.100/25
192.168.113.100/25 previously matched the admin_low template
```

2 **Pour affecter un modèle de sécurité à un groupe d'adresses IP contiguës, spécifiez l'adresse IP et la longueur du préfixe.**

Dans l'exemple suivant, la longueur du préfixe couvre la plage d'adresses de `192.168.113.0` à `192.168.113.127`. L'adresse inclut `192.168.113.100`.

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.113.100/25
tncfg:cipso> exit
```

Dans l'exemple suivant, la longueur du préfixe couvre les adresses IPv6 contiguës de `2001:a08:3903:200::0` à `2001:a08:3903:2ff:ffff:ffff:ffff:ffff` . L'adresse inclut `2001:a08:3903:201:20e:cff:fe08:58c`.

```
# tncfg -t cipso
tncfg:cipso> add host=2001:a08:3903:200::0/56
tncfg:cipso> info
...
host=2001:a08:3903:200::0/56
tncfg:cipso> exit
```

Si vous ne saisissez pas correctement une entrée, vous recevez un message semblable à ce qui suit :

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

Si vous ajoutez un hôte précédemment ajouté à un autre modèle, vous êtes averti du fait que vous êtes en train de remplacer le modèle de sécurité qui lui est affecté. Par exemple :

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.113.100/32
192.168.113.100/32 previously matched the admin_low template
tncfg:cipso> info
...
host=192.168.113.100/32
tncfg:cipso> exit
```

Le mécanisme de secours de Trusted Extensions garantit que cette affectation explicite remplace l'affectation précédente, comme indiqué à la section "Mécanisme de secours du réseau de confiance" à la page 209.

Exemple 16–12 Création d'hôtes sous des étiquettes discrètes

Dans l'Exemple 16–4, l'administrateur crée le modèle de sécurité qui reconnaît deux étiquettes. Dans cet exemple, l'administrateur de sécurité s'assure que chaque adresse IP de l'hôte peut être résolue.

```
# arp 192.168.132.21
host-auxset1.example.com (192.168.132.21) at 0:0:0:4:ab:cd
# arp 192.168.132.22
host-auxset2.example.com (192.168.132.22) at 0:0:0:5:ab:cd
# arp 192.168.132.23
host-auxset3.example.com (192.168.132.23) at 0:0:0:6:ab:cd
# arp 192.168.132.24
host-auxset4.example.com (192.168.132.24) at 0:0:0:7:ab:cd
```

La commande `arp` indique que les hôtes sont définis dans le fichier `/etc/hosts` du système ou qu'ils peuvent être résolus par DNS.

L'administrateur attribue ensuite la plage d'adresses IP au modèle de sécurité à l'aide d'une longueur de préfixe.

```
# tncfg -t cipso_int_rstrct
tncfg:cipso_int_rstrct> set host=192.168.132.0/24
```

Exemple 16–13 Création d'un sous-réseau non étiqueté sous l'étiquette PUBLIC

Dans l'Exemple 16–5, l'administrateur crée un modèle de sécurité qui définit un hôte `PUBLIC` à étiquette unique. Dans cet exemple, l'administrateur de sécurité affecte un sous-réseau à l'étiquette `PUBLIC`. Les utilisateurs du système sécurisé peuvent monter des systèmes de fichiers à partir de ce sous-réseau sous l'étiquette `PUBLIC`.

```
# tncfg -t public
tncfg:public> add host=10.10.0.0/16
tncfg:public> exit
```

Le sous-réseau peut être atteint immédiatement sous l'étiquette `PUBLIC`.

▼ 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, le modèle de sécurité `admin_low` par défaut définit tous les hôtes du réseau. Utilisez cette procédure pour énumérer des hôtes non étiquetés spécifiques.

Les valeurs du réseau de confiance local de chaque système permettent d'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 hôtes distants non définis par ailleurs (`0.0.0.0/0`) 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 `0.0.0.0/0` une fois le système installé. L'entrée doit être remplacée par des entrées correspondant à chacun des hôtes que le système contacte lors de l'initialisation.

Par exemple, les serveurs DNS, les serveurs d'annuaire personnel, les serveurs d'audit, les adresses de diffusion et de multidiffusion et les routeurs doivent être ajoutés de façon explicite à un modèle après la suppression de l'entrée générique `0.0.0.0/0`.

Si une application reconnaît initialement les clients sur l'adresse d'hôte `0.0.0.0/32`, vous devez ajouter l'entrée d'hôte `0.0.0.0/32` au modèle `admin_low`. 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 le fichier `/etc/hosts`.

1. **Assignez le modèle `admin_low` à chaque hôte sans étiquette qui doit être contacté au moment de l'initialisation.**
   - Ajoutez tous les hôtes sans étiquette qui doivent être contactés lors de l'initialisation.
   - Incluez tous les routeurs infra-réseau n'exécutant pas Trusted Extensions via lesquels ce système doit communiquer.
   - Retirez l'assignation `0.0.0.0/0`.
2. **Ajoutez des hôtes au modèle `admin_low`.**

   Ajoutez chaque hôte étiqueté qui doit être contacté lors de l'initialisation.
   - Incluez tous les routeurs infra-réseau exécutant Trusted Extensions via lesquels ce système doit communiquer.
   - Assurez-vous que toutes les interfaces réseau sont assignées au modèle.
   - Incluez les adresses de diffusion.
   - Ajoutez les plages d'hôtes étiquetés à contacter lors de l'initialisation.

   Pour un exemple de base de données, consultez l'Exemple 16–15.
3. **Assurez-vous que les assignations d'hôtes n'empêchent pas le système de s'initialiser.**

Exemple 16–14 Modification de l'étiquette de l'adresse IP 0.0.0.0/0

Dans cet exemple, l'administrateur crée un système de passerelle publique. L'administrateur supprime l'entrée d'hôte `0.0.0.0/0` à partir du modèle `admin_low` et ajoute l'entrée d'hôte `0.0.0.0/0` au modèle `public` sans étiquette. Le système reconnaît ensuite tout hôte non spécifiquement assigné à un autre modèle de sécurité comme un système sans étiquette possédant les attributs de sécurité du modèle de sécurité `public`.

```
# tncfg -t admin_low info
tncfg:admin_low> remove host=0.0.0.0      Wildcard address
tncfg:admin_low> exit

# tncfg -t public
tncfg:public> set host_type=unlabeled
tncfg:public> set doi=1
tncfg:public> set def_label="public"
tncfg:public> set min_sl="public"
tncfg:public> set max_sl="public"
tncfg:public> add host=0.0.0.0      Wildcard address
tncfg:public> exit
```

Exemple 16–15 Énumération des ordinateurs à contacter au moment de l'initialisation

Dans l'exemple suivant, l'administrateur configure le réseau de confiance du système Trusted Extensions avec deux interfaces réseau. Le système communique avec un autre réseau et des routeurs. Les hôtes distants sont assignés à l'un des trois modèles, `cipso`, `admin_low` ou `public`. Les commandes suivantes sont annotées.

```
# tncfg -t cipso
tncfg:admin_low> add host=127.0.0.1      Loopback address
tncfg:admin_low> add host=192.168.112.111      Interface 1 of this host
tncfg:admin_low> add host=192.168.113.111      Interface 2 of this host
tncfg:admin_low> add host=192.168.113.6      File server
tncfg:admin_low> add host=192.168.112.255      Subnet broadcast address
tncfg:admin_low> add host=192.168.113.255      Subnet broadcast address
tncfg:admin_low> add host=192.168.113.1      Router
tncfg:admin_low> add host=192.168.117.0/24      Another Trusted Extensions network
tncfg:admin_low> exit

# tncfg -t public
tncfg:public> add host=192.168.112.12      Specific network router
tncfg:public> add host=192.168.113.12      Specific network router
tncfg:public> add host=224.0.0.2      Multicast address
tncfg:admin_low> exit

# tncfg -t admin_low
tncfg:admin_low> add host=255.255.255.255      Broadcast address
tncfg:admin_low> exit
```

Après avoir spécifié les hôtes à contacter au moment de l'initialisation, l'administrateur supprime l'entrée `0.0.0.0/0` à partir du modèle `admin_low`.

```
# tncfg -t admin_low
tncfg:admin_low> remove host=0.0.0.0
tncfg:admin_low> exit
```

Exemple 16–16 Faire de l'adresse hôte 0.0.0.0/32 une adresse initiale valide

Dans cet exemple, l'administrateur de sécurité configure un serveur d'application de manière à ce qu'il accepte les requêtes de connexion initiales provenant de clients potentiels.

L'administrateur configure le réseau de confiance du serveur. Les entrées du serveur et du client sont annotées.

```
# tncfg -t cipso info
   name=cipso
   host_type=cipso
   doi=1
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
   host=127.0.0.1/32
   host=192.168.128.1/32      Application server address
   host=192.168.128.0/24      Application's client network
     Other addresses to be contacted at boot time
```

```
# tncfg -t admin_low info
   name=cipso
   host_type=cipso
   doi=1
   def_label=ADMIN_LOW
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
   host=192.168.128.0/24      Application's client network
   host=0.0.0.0/0       Wildcard address
     Other addresses to be contacted at boot time
```

Une fois cette phase de test réussie, l'administrateur verrouille la configuration en supprimant l'adresse générique par défaut, `0.0.0.0/0`, en validant la modification, puis en ajoutant l'adresse spécifique.

```
# tncfg -t admin_low info
tncfg:admin_low> remove host=0.0.0.0
tncfg:admin_low> commit
tncfg:admin_low> add host=0.0.0.0/32      For initial client contact
tncfg:admin_low> exit
```

La configuration `admin_low` finale s'affiche comme suit :

```
# tncfg -t admin_low
   name=cipso
   host_type=cipso
```

```
doi=1
def_label=ADMIN_LOW
min_label=ADMIN_LOW
max_label=ADMIN_HIGH
192.168.128.0/24      Application's client network
host=0.0.0.0/32       For initial client contact
  Other addresses to be contacted at boot time
```

L'entrée `0.0.0.0/32` autorise uniquement les clients de l'application à atteindre le serveur d'application.

Configuration des routes et ports multiniveau (MLP) (tâches)

Les routes statiques permettant aux paquets étiquetés d'atteindre leur destination via des passerelles étiquetées et sans étiquette. Les MLP permettent à une application d'utiliser un point d'entrée pour atteindre toutes les zones.

▼ Procédure d'ajout des routes par défaut

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

Assignez chaque hôte, réseau et passerelle de destination à un modèle de sécurité. Pour plus d'informations, reportez-vous à la section "Procédure d'ajout d'un hôte au modèle de sécurité" à la page 231 and "Procédure d'ajout d'une plage d'hôtes au modèle de sécurité" à la page 234.

1. **Utilisez l'interface graphique `txzonemgr` pour créer des routes par défaut.**

   ```
   # txzonemgr &
   ```

2. **Double-cliquez sur la zone pour laquelle vous souhaitez définir la route par défaut, puis double-cliquez sur son entrée d'adresse IP.**

   Si la zone possède plusieurs adresses IP, choisissez l'entrée de l'interface souhaitée.

3. **À l'invite, entrez l'adresse IP du routeur et cliquez sur OK.**

Remarque – Pour supprimer ou modifier le routeur par défaut, supprimez l'entrée, créez à nouveau l'entrée IP, puis ajoutez le routeur. Si la zone ne possède qu'une seule adresse IP, vous devez supprimer l'instance IP pour supprimer l'entrée.

Exemple 16–17 Utilisation de la commande route afin de définir la route par défaut pour la zone globale

Dans cet exemple, l'administrateur utilise la commande `route` pour créer une route par défaut pour la zone globale.

```
# route add default 192.168.113.1 -static
```

Procédure de création d'un port multiniveau pour une zone

Vous pouvez ajouter des MLP privés et partagés à des zones étiquetées et à la zone globale.

Cette procédure est utilisée lorsqu'une application qui s'exécute à l'intérieur d'une zone étiquetée requiert un port multiniveau (MLP) pour communiquer avec la zone. Dans cette procédure, un proxy Web communique avec la zone.

Avant de commencer Vous devez être dans le rôle `root` dans la zone globale. Le système doit avoir au moins deux adresses IP et la zone étiquetée est arrêtée.

1. **Ajoutez l'hôte proxy et l'hôte de services Web au fichier `/etc/hosts` .**

   ```
   ## /etc/hosts file
   ...
   proxy-host-name  IP-address
   web-service-host-name IP-address
   ```

2. **Configurez la zone.**

   Par exemple, vous pouvez configurer la zone `public` de manière à ce qu'elle reconnaisse les paquets explicitement étiquetés `PUBLIC`. Pour cette configuration, le modèle de sécurité est nommé `webprox`.

   ```
   # tncfg -t webprox
   tncfg:public> set name=webprox
   tncfg:public> set host_type=cipso
   tncfg:public> set min_label=public
   tncfg:public> set max_label=public
   tncfg:public> add host=mywebproxy.oracle.com      host name associated with public zone
   tncfg:public> add host=10.1.2.3/16      IP address of public zone
   tncfg:public> exit
   ```

3. **Configurez le MLP.**

   Par exemple, le service de proxy Web peut communiquer avec la zone `PUBLIC` via l'interface `8080/tcp` .

   ```
   # tncfg -z public add mlp_shared=8080/tcp
   # tncfg -z public add mlp_private=8080/tcp
   ```

4. **Pour ajouter les MLP au noyau, initialisez la zone.**

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

5. **Dans la zone globale, ajoutez des routes pour les nouvelles adresses.**

   Pour ajouter des routes, effectuez les étapes décrites dans la section “Procédure d'ajout des routes par défaut” à la page 240.

Exemple 16–18 Configuration d'un MLP à l'aide de l'interface graphique txzonemgr

L'administrateur configure le service de proxy Web en ouvrant le gestionnaire de zones étiquetées (Labeled Zone Manager).

```
# txzonemgr &
```

L'administrateur clique deux fois sur la zone `PUBLIC`, puis sur les ports `Configure Multilevel Ports`. Il sélectionne ensuite la ligne `Private interfaces` et clique deux fois dessus. La sélection prend ensuite l'apparence d'une zone de saisie semblable à ce qui suit :

```
Private interfaces:111/tcp;111/udp
```

L'administrateur saisit ensuite le proxy Web en le séparant de ce qui précède par un point-virgule

```
Private interfaces:111/tcp;111/udp;8080/tcp
```

Une fois la saisie privée terminée, l'administrateur saisit le proxy Web dans le champ `Shared interfaces`.

```
Shared interfaces:111/tcp;111/udp;8080/tcp
```

Une fenêtre contextuelle indique que les ports multiniveau de la zone `public` devront être activés à la prochaine initialisation de la zone.

Exemple 16–19 Configuration d'un port multiniveau privé pour NFSv3 sur udp

Dans cet exemple, l'administrateur active les montages "read-down" NFSv3 sur `udp`. L'administrateur a la possibilité d'utiliser la commande `tncfg`.

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

L'interface graphique `txzonemgr` fournit une autre manière de définir le MLP.

Dans le gestionnaire de zones étiquetées (Labeled Zone Manager), l'administrateur clique deux fois sur la zone `global`, puis sur `Configure Multilevel Ports`. Dans le menu MLP, l'administrateur sélectionne la ligne `Private interfaces` et clique deux fois dessus avant d'ajouter le port/protocole.

```
Private interfaces:111/tcp;111/udp;8080/tcp
```

Une fenêtre contextuelle indique que les ports multiniveau de la zone`global` devront être activés à la prochaine initialisation de la zone.

Exemple 16–20 Affichage de ports multiniveau sur un système

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
```

Configuration d'IPsec avec étiquettes (liste des tâches)

La liste ci-dessous décrit les tâches permettant d'ajouter des étiquettes aux protections IPsec.

Tâche	Description	Voir
Utilisation d'IPsec avec Trusted Extensions	Ajoute des étiquettes aux protections IPsec.	"Procédure d'application des protections IPsec dans un réseau Trusted Extensions multiniveau" à la page 244
Utilisation d'IPsec avec Trusted Extensions dans un réseau non sécurisé	Met en tunnel les paquets IPsec dans un réseau sans étiquette.	"Procédure de configuration d'un tunnel au sein d'un réseau non autorisé" à la page 246

▼ Procédure d'application des protections IPsec dans un réseau Trusted Extensions multiniveau

Dans cette procédure, vous devez configurer IPsec sur deux systèmes Trusted Extensions pour gérer les conditions suivantes :

- Les deux systèmes, `enigma` et `partym` sont des systèmes Trusted Extensions multiniveau exécutés dans un réseau multiniveau.
- Les données d'application sont cryptées et protégées contre toute modification non autorisée au sein du réseau.
- L'étiquette de sécurité des données est visible dans le formulaire sous forme d'une option IP CIPSO à disposition des routeurs multiniveau et des périphériques de sécurité sur le chemin situé entre les systèmes `enigma` et `partym`.
- Les étiquettes de sécurité échangées par `enigma` et `partym` sont protégées contre toute modification non autorisée.

Avant de commencer Vous êtes dans le rôle `root` dans la zone globale.

1 Ajoutez les hôtes `enigma` et `partym` à un modèle de sécurité CIPSO.

Suivez les procédures décrites dans la section "Étiquetage d'hôtes et de réseaux (liste des tâches)" à la page 224. Utilisez un modèle avec un type d'hôte CIPSO.

2 Configurez IPsec pour les systèmes `enigma` et `partym`.

Pour connaître cette procédure , reportez-vous à la section "Sécurisation du trafic entre deux systèmes à l'aide d'IPsec" du manuel *Administration d'Oracle Solaris : Services IP*. Utilisez IKE pour la gestion des clés, comme décrit dans l'étape suivante.

3 Ajoutez des étiquettes à des négociations IKE.

Suivez la procédure décrite dans la section "Configuration du protocole IKE avec des clés prépartagées" du manuel *Administration d'Oracle Solaris : Services IP*, puis modifiez le fichier `ike/config`comme suit :

a. Ajoutez les mots-clés `label_aware`, `multi_label` et `wire_label` `inner` dans le fichier `/etc/inet/ike/config` du système `enigma`.

Le fichier qui en résulte se présente comme indiqué ci-dessous. Les éléments ajoutés à l'étiquette sont mis en surbrillance.

```
    ### ike/config file on enigma, 192.168.116.16
    ## Global parameters
    #
## Use IKE to exchange security labels.
    label_aware
  #
        ## Defaults that individual rules can override.
```

```
    p1_xform
          { auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
    p2_pfs 2
    #
  ## The rule to communicate with partym
      # Label must be unique
    { label "enigma-partym"
          local_addr 192.168.116.16
          remote_addr 192.168.13.213
          multi_label
          wire_label inner
          p1_xform
           { auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
          p2_pfs 5
    }
```

b. Ajoutez les mêmes mots-clés dans le fichier `ike/config` du système `partym`.

```
    ### ike/config file on partym, 192.168.13.213
    ## Global Parameters
    #
## Use IKE to exchange security labels.
    label_aware
    #
        p1_xform
          { auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
    p2_pfs 2
    ## The rule to communicate with enigma
    # Label must be unique
    { label "partym-enigma"
          local_addr 192.168.13.213
          remote_addr 192.168.116.16
          multi_label
          wire_label inner
    p1_xform
           { auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
        p2_pfs 5
    }
```

4 Si la protection AH des options IP CIPSO ne peut pas être utilisée sur le réseau, utilisez l'authentification ESP.

Pour gérer l'authentification, utilisez `encr_auth_algs` plutôt qu'`auth_algs` dans le fichier `/etc/inet/ipsecinit.conf`. L'authentification ESP ne couvre pas l'en-tête IP ni les options IP, mais elle authentifie toutes les informations qui suivent l'en-tête ESP.

```
{laddr enigma raddr partym} ipsec {encr_algs any encr_auth_algs any sa shared}
```

Remarque – Vous pouvez également ajouter des étiquettes aux systèmes protégés par des certificats. Les certificats de clé publique sont gérés dans la zone globale sur les systèmes Trusted Extensions. Modifiez les fichiers `ike/config` de façon similaire lorsque vous effectuez les étapes de la procédure décrite dans la section "Configuration du protocole IKE avec des certificats de clés publiques" du manuel *Administration d'Oracle Solaris : Services IP*.

▼ Procédure de configuration d'un tunnel au sein d'un réseau non autorisé

Cette procédure permet de configurer un tunnel IPsec au sein d'un réseau public entre deux systèmes de passerelle VPN Trusted Extensions. L'exemple utilisé dans cette procédure est basé sur la configuration illustrée dans la section "Description de la topologie réseau requise par les tâches IPsec afin de protéger un VPN" du manuel *Administration d'Oracle Solaris : Services IP*.

L'illustration présuppose les modifications suivantes :

- Les sous-réseaux `10` sont des réseaux de confiance multiniveau. Les étiquettes de sécurité de l'option IP CIPSO sont visibles sur ces LAN.
- Les sous-réseaux `192.168` sont des réseaux non sécurisés à étiquette unique fonctionnant sous l'étiquette `PUBLIC`. Ces réseaux ne prennent pas en charge les options IP CIPSO.
- Le trafic étiqueté entre `euro-vpn` et `calif-vpn` est protégé contre les modifications non autorisées.

Avant de commencer Vous êtes dans le rôle `root` dans la zone globale.

1 Suivez les procédures décrites dans la section "Étiquetage d'hôtes et de réseaux (liste des tâches)" à la page 224 pour définir ce qui suit :

a. Ajoutez les adresses IP `10.0.0.0/8` à un modèle de sécurité étiqueté.

Utilisez un modèle avec un type d'hôte CIPSO. Conservez la plage d'étiquettes par défaut, `ADMIN_LOW` à `ADMIN_HIGH`.

b. Ajoutez les adresses IP `192.168.0.0/16` à un modèle de sécurité sans étiquette sous l'étiquette `PUBLIC`.

Utilisez un modèle à l'aide d'un type d'hôte sans étiquette. Définissez l'étiquette par défaut sur `PUBLIC`. Conservez la plage d'étiquettes par défaut, `ADMIN_LOW` à `ADMIN_HIGH`.

c. Ajoutez les adresses Internet `Calif-vpn` et `Euro-vpn`, puis `192.168.13.213` et `192.168.116.16` à un modèle CIPSO.

Conservez la plage d'étiquettes par défaut.

2 Créez un tunnel IPsec.

Suivez les procédures décrites dans la section "Procédure de protection d'un VPN avec IPsec en mode Tunnel" du manuel *Administration d'Oracle Solaris : Services IP*. Utilisez IKE pour la gestion des clés, comme décrit dans l'étape suivante.

3 Ajoutez des étiquettes à des négociations IKE.

Suivez la procédure décrite dans la section "Configuration du protocole IKE avec des clés prépartagées" du manuel *Administration d'Oracle Solaris : Services IP*, puis modifiez le fichier `ike/config`comme suit :

a. Ajoutez les mots-clés `label_aware`, `multi_label` et `wire_label none PUBLIC` dans le fichier `etc/inet/ike/config` du système `euro-vpn`.

Le fichier qui en résulte se présente comme indiqué ci-dessous. Les éléments ajoutés à l'étiquette sont mis en surbrillance.

```
        ### ike/config file on euro-vpn, 192.168.116.16
    ## Global parameters
    #
## Use IKE to exchange security labels.
    label_aware
    #
        ## Defaults that individual rules can override.
    p1_xform
          { auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
    p2_pfs 2
    #
   ## The rule to communicate with calif-vpn
       # Label must be unique
    { label "eurovpn-califvpn"
          local_addr 192.168.116.16
          remote_addr 192.168.13.213
          multi_label
          wire_label none PUBLIC
          p1_xform
           { auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
          p2_pfs 5
        }
```

b. Ajoutez les mêmes mots-clés au fichier `ike/config` sur le système `calif-vpn`.

```
    ### ike/config file on calif-vpn, 192.168.13.213
    ## Global Parameters
    #
## Use IKE to exchange security labels.
    label_aware
    #
        p1_xform
          { auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
    p2_pfs 2
    ## The rule to communicate with euro-vpn
    # Label must be unique
    { label "califvpn-eurovpn"
          local_addr 192.168.13.213
          remote_addr 192.168.116.16
          multi_label
          wire_label none PUBLIC
    p1_xform
           { auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
        p2_pfs 5
    }
```

Remarque – Vous pouvez également ajouter des étiquettes aux systèmes protégés par des certificats. Modifiez les fichiers `ike/config` de façon similaire lorsque vous effectuez les étapes de la procédure décrite dans la section "Configuration du protocole IKE avec des certificats de clés publiques" du manuel *Administration d'Oracle Solaris : Services IP*.

Dépannage du réseau de confiance (liste des tâches)

La liste ci-dessous décrit les tâches à effectuer pour déboguer votre réseau Trusted Extensions.

Tâche	Description	Voir
Identification de la raison pour laquelle un système et un hôte distant ne peuvent pas communiquer	Vérifie que les interfaces de chaque système sont actives.	"Procédure de vérification de l'affichage des interfaces du système" à la page 248
	Utilise les outils de débogage lorsqu'un système et un hôte distant ne parviennent pas communiquer les uns avec les autres.	"Débogage du réseau Trusted Extensions" à la page 249
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 252

▼ Procédure de vérification de l'affichage des interfaces du système

Utilisez cette procédure si votre système ne communique pas avec les hôtes comme prévu.

Avant de commencer Vous devez accéder à la zone globale dans un rôle habilité à vérifier les valeurs d'attribut du réseau. Les rôles d'administrateur de sécurité et d'administrateur système sont habilités à vérifier ces valeurs.

1 Assurez-vous que l'interface réseau est active.

Vous pouvez utiliser l'interface utilisateur du gestionnaire de zones étiquetées (Labeled Zone Manager) ou la commande `ipadm` pour afficher les interfaces du système.

- **Ouvrez le gestionnaire de zones étiquetées (Labeled Zone Manager), puis double-cliquez sur la zone qui vous intéresse.**

  ```
  # txzonemgr &
  ```

  Sélectionnez Configure Network Interfaces (Configurer les interfaces réseau) et vérifiez que la valeur de la colonne `Status` de la zone est `Up`.

- **Vous pouvez également utiliser la commande `ipadm show-addr`.**

```
# ipadm show-addr
...
ADDROBJ           TYPE      STATE        ADDR
lo0/v4            static    ok           127.0.0.1/8
net0/_a           dhcp      down         10.131.132.133/23
net0:0/_a         dhcp      down         10.131.132.175/23
```

  La valeur des interfaces `net0` doit être `ok`. Pour plus d'informations sur la commande `ipadm`, reportez-vous à la page de manuel `ipadm(1M)`.

2. **Si l'interface n'est pas visible, affichez-la.**

   a. **Dans l'interface graphique du gestionnaire de zones étiquetées, cliquez deux fois sur la zone dont vous souhaitez afficher l'interface.**

   b. **Sélectionnez Configurer les interfaces réseau.**

   c. **Double-cliquez sur l'interface dont l'état est `Down`.**

   d. **Sélectionnez Bring Up (Afficher), puis cliquez sur OK.**

   e. **Cliquez sur Cancel (Annuler) ou sur OK.**

▼ Débogage du réseau Trusted Extensions

Pour déboguer deux hôtes censés communiquer mais qui ne le font pas, vous pouvez utiliser les outils de débogage Trusted Extensions et Oracle 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 les commandes spécifiques à Trusted Extensions, reportez-vous à l'Annexe D, “Liste des pages de manuel Trusted Extensions”.

- 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 178.
- Pour le débogage des montages NFS, reportez-vous à la section “Dépannage des échecs de montage dans Trusted Extensions” à la page 198.

Avant de commencer

Vous devez accéder à la zone globale dans un rôle habilité à vérifier les valeurs d'attribut du réseau. Les rôles d'administrateur de sécurité et d'administrateur système sont habilités à vérifier ces valeurs. Seul le rôle `root` est habilité à modifier ces fichiers.

1. **Vérifiez que les hôtes qui ne parviennent pas à communiquer utilisent le même service de nommage.**

   a. **Sur chaque système, vérifiez les valeurs des bases de données Trusted Extensions dans le service `name-service/switch`.**

   ```
   # svccfg -s name-service/switch listprop config
   config/value_authorization  astring  solaris.smf.value.name-service.switch
   config/default              astring  ldap
   ...
   config/tnrhtp               astring  "files ldap"
   config/tnrhdb               astring  "files ldap"
   ```

   b. **Si les valeurs sont différentes en fonction des hôtes, corrigez les valeurs sur les hôtes concernés.**

   ```
   # svccfg -s name-service/switch setprop config/tnrhtp="files ldap"
   # svccfg -s name-service/switch setprop config/tnrhdb="files ldap"
   ```

   c. **Ensuite, redémarrez le démon du service de nommage sur ces hôtes.**

   ```
   # svcadm restart name-service/switch
   ```

2. **Assurez-vous que chaque hôte est défini correctement en affichant les attributs de sécurité pour la source, la destination et les hôtes de passerelle dans la transmission.**

   Utilisez la ligne de commande pour vérifier que les informations de réseau sont correctes. Vérifiez que l'affectation sur chaque hôte correspond à l'affectation sur les autres hôtes du réseau. Selon la vue que vous souhaitez, utilisez la commande `tncfg`, la commande `tninfo` ou l'interface graphique `txzonemgr`.

   - **Affichage d'une définition de modèle.**

     La commande `tninfo -t` affiche les étiquettes dans la chaîne et le format hexadécimal.

     ```
     $ 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
     ```

   - **Affichage d'un modèle et des hôtes qui lui sont affectés.**

     La commande `tncfg -t` affiche les étiquettes au format d'une chaîne de caractères et répertorie les hôtes affectés.

     ```
     $ tncfg -t template info
        name=<template-name>
        host_type=<one of cipso or unlabeled>
        doi=1
        min_label=<minimum-label>
        max_label=<maximum-label>
        host=127.0.0.1/32           /** Localhost **/
     ```

```
host=192.168.1.2/32          /** LDAP server **/
host=192.168.1.22/32         /** Gateway to LDAP server **/
host=192.168.113.0/24        /** Additional network **/
host=192.168.113.100/25            /** Additional network **/
host=2001:a08:3903:200::0/56     /** Additional network **/
```

- **Affichage de l'adresse IP et du modèle de sécurité affecté pour un hôte spécifique.**

  La commande `tninfo -h` affiche l'adresse IP de l'hôte spécifié et le nom du modèle de sécurité qui lui est assigné.

  ```
  $ tninfo -h hostname
  IP Address: IP-address
  Template: template-name
  ```

  La commande `tncfg get host=` affiche le nom du modèle de sécurité qui définit l'hôte spécifié.

  ```
  $ tncfg get host=hostname|IP-address[/prefix]
  template-name
  ```

- **Affichage des ports multiniveau (MLP) pour une zone.**

  La commande `tncfg -z` répertorie un MLP par ligne.

  ```
  $ tncfg -z zone-name info [mlp_private | mlp_shared]
  mlp_private=<port/protocol-that-is-specific-to-this-zone-only>
  mlp_shared=<port/protocol-that-the-zone-shares-with-other-zones>
  ```

  La commande `tninfo -m` répertorie les MLP privés sur une ligne et les MLP partagés sur une seconde ligne. Les MLP sont séparés par des points-virgules.

  ```
  $ tninfo -m zone-name
  private: ports-that-are-specific-to-this-zone-only
  shared: ports-that-the-zone-shares-with-other-zones
  ```

  Pour afficher l'interface graphique des MLP, utilisez la commande `txzonemgr`. Double-cliquez sur la zone, puis sélectionnez Configure Multilevel Ports (Configurer des ports multiniveau).

3 Corrigez les informations erronées.

a. Pour modifier ou vérifier les informations de sécurité réseau, utilisez les commandes d'administration du réseau de confiance, `tncfg` et `txzonemgr`. Pour vérifier la syntaxe des bases de données, utilisez la commande `tnchkdb`.

Par exemple, la sortie suivante indique qu'un nom de modèle, `internal_cipso` , n'est pas défini :

```
# tnchkdb
     checking /etc/security/tsol/tnrhtp ...
     checking /etc/security/tsol/tnrhdb ...
tnchkdb: unknown template name: internal_cipso at line 49
tnchkdb: unknown template name: internal_cipso at line 50
tnchkdb: unknown template name: internal_cipso at line 51
```

```
checking /etc/security/tsol/tnzonecfg ...
```

L'erreur indique que les commandes `tncfg` et `txzonemgr` n'ont pas été utilisées pour créer et affecter le modèle de sécurité `internal_cipso`.

Pour réparer et remplacer le fichier `tnrhdb` avec le fichier d'origine, utilisez la commande `tncfg` pour créer et affecter des modèles de sécurité.

b. Pour vider la mémoire cache du noyau, réinitialisez le système.

Pendant l'initialisation, des informations de base de données sont inscrites dans le cache. Le service SMF, `name-service/switch` détermine si les bases de données locales ou LDAP sont utilisées pour remplir le noyau.

4 Collectez des informations de transmission pour assister le débogage.

a. Contrôlez votre configuration de routage.

```
$ route get [ip] -secattr sl=label,doi=integer
```

Pour plus d'informations, reportez-vous à la page de manuel `route(1M)`.

b. Visualisez les informations d'étiquette dans les paquets.

```
$ 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)`.

c. Visualisez les entrées de la table de routage et les attributs de sécurité sur des sockets.

```
$ netstat -aR
```

L'option `-aR` affiche les attributs de sécurité étendus des sockets.

```
$ netstat -rR
```

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.

a. Utilisez la commande `tncfg` ou `tninfo` pour consulter les informations.

```
# tncfg get host=LDAP-server
# tncfg get host=gateway-to-LDAP-server

# tninfo -h LDAP-server
# tninfo -h gateway-to-LDAP-server
```

b. Déterminez la route vers le serveur.

```
# route get LDAP-server
```

Si une assignation de modèle est incorrecte, assignez l'hôte au modèle approprié.

2 Consultez et, si nécessaire, 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` du fichier `/etc/hosts`.

3 Si vous utilisez un DNS, vérifiez la configuration du service `svc:/network/dns/client`.

```
# svccfg -s dns/client listprop config
config                          application
config/value_authorization      astring       solaris.smf.value.name-service.dns.switch
config/nameserver               astring       192.168.8.25 192.168.122.7
```

4 Pour modifier les valeurs, utilisez la commande `svccfg`.

```
# svccfg -s dns/client setprop config/search = astring: example1.domain.com
# svccfg -s dns/client setprop config/nameserver = net_address: 192.168.8.35
# svccfg -s dns/client:default refresh
# svccfg -s dns/client:default validate
# svcadm enable dns/client
# svcadm refresh name-service/switch
# nslookup some-system
Server:         192.168.135.35
Address:        192.168.135.35#53

Name:   some-system.example1.domain.com
Address: 10.138.8.22
Name:   some-system.example1.domain.com
Address: 10.138.8.23
```

5 **Vérifiez que les entrées `tnrhdb` et `tnrhtp` du service `name-service/switch` sont exactes.**

Dans la sortie suivante, les entrées `tnrhdb` et `tnrhtp` ne sont pas répertoriées. Par conséquent, ces bases de données utilisent les services de nommage `files ldap` par défaut, dans cet ordre.

```
# svccfg -s name-service/switch listprop config
config                      application
config/value_authorization  astring       solaris.smf.value.name-service.switch
config/default              astring       "files ldap"
config/host                 astring       "files dns"
config/netgroup             astring       ldap
```

6 **Vérifiez que le client est correctement configuré sur le serveur.**

```
# ldaplist -l tnrhdb client-IP-address
```

7 **Vérifiez que les interfaces de vos zones étiquetées sont correctement configurées sur le serveur LDAP.**

```
# ldaplist -l tnrhdb client-zone-IP-address
```

8 **Vérifiez que vous êtes en mesure de contacter 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
...
```

9 **Configurez le serveur LDAP, puis réinitialisez.**

a. **Pour plus d'informations sur cette procédure, reportez-vous à la section "Établissement de la zone globale en tant que client LDAP dans Trusted Extensions" à la page 96.**

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 et réinitialisez le système.**

```
# zoneadm list
zone1
zone2
,
,
,
```

```
# zoneadm -z zone1 halt
# zoneadm -z zone2 halt
.
.
.
# reboot
```

Vous pouvez également utiliser l'interface graphique `txzonemgr` pour arrêter les zones étiquetées.

◆ ◆ ◆ CHAPITRE 17

Trusted Extensions et LDAP (présentation)

Ce chapitre décrit l'utilisation du serveur 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. Le service `svc:/system/name-service/switch` détermine le service de nommage à utiliser. 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 durant la configuration du système.

Trusted Extensions ajoute deux bases de données d'un réseau de confiance vers le serveur d'annuaire : `tnrhdb` et `tnrhtp`.

- Pour plus d'informations sur l'utilisation du service de nommage LDAP dans Oracle Solaris, reportez-vous à la section *Oracle Solaris Administration: Naming and Directory Services* .
- La configuration du serveur d'annuaire pour Trusted Extensions est décrite au Chapitre 5, "Configuration de LDAP pour Trusted Extensions (tâches)". Les systèmes Trusted Extensions peuvent être clients d'un serveur d'annuaire Oracle Solaris à l'aide d'un proxy de serveur d'annuaire configuré avec Trusted Extensions.
- La configuration des clients du serveur d'annuaire Trusted Extensions est décrite dans la section "Création d'un client LDAP Trusted Extensions " à la page 96.

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

Systèmes Trusted Extensions gérés localement

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

Sur un système Trusted Extensions géré localement, les informations de configuration sont conservées dans les fichiers des répertoires `/etc`, `/etc/security` et `/etc/security/tsol.`

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 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 manuel *Oracle Solaris Administration: Naming and Directory Services*.
- Pour résoudre 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 252.
- Pour résoudre d'autres problèmes de connexion LDAP du client au serveur, reportez-vous au Chapitre 13, “LDAP Troubleshooting (Reference)” du manuel *Oracle Solaris Administration: Naming and Directory Services*.
- 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 les versions 6 ou 7 du serveur LDAP du logiciel Oracle Directory Server Enterprise Edition saisissez ce qui suit :

```
# 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 les versions 6 ou 7 du logiciel Oracle Directory Server Enterprise Edition saisissez ce qui suit :

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

◆ ◆ ◆ CHAPITRE 18

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. 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 150.

Fonctions de messagerie Trusted Extensions

Dans Trusted Extensions, le rôle d'administrateur système configure et administre les serveurs de courrier en fonction des instructions décrites au Chapitre 13, "Services de messagerie (tâches)" du manuel *Administration d'Oracle Solaris : Services réseau*. En outre, l'administrateur de sécurité détermine la configuration requise des fonctions de messagerie Trusted Extensions.

Les aspects de gestion de la messagerie 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 obtenir une description de ces fichiers, reportez-vous à la page de manuel `updatehome(1)`. Pour consulter des suggestions de configuration, reportez-vous à la section "Fichiers `.copy_files` et `.link_files`" à la page 145.

- 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 Thunderbird comme messagerie multiniveau, vous devez configurer le client de messagerie Thunderbird sous chaque étiquette pour le spécifier en tant que serveur de courrier. Le serveur de courrier ne doit pas nécessairement être identique pour toutes les étiquettes mais le serveur doit être spécifié.

- Trusted Extensions contrôle les étiquettes de l'hôte et de l'utilisateur avant d'envoyer ou de transférer du courrier.
  - Le logiciel vérifie que le courrier s'inscrit dans la plage d'accréditations de l'hôte. Les vérifications sont décrites dans cette liste ainsi que dans la section "Contrôles d'accréditation dans Trusted Extensions" à la page 212.
  - Le logiciel vérifie que le courrier 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 le courrier correspondant à leur étiquette en cours.

    Pour contacter un utilisateur standard par e-mail, un rôle d'administration doit envoyer un courrier 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 19

Gestion de l'impression étiquetée (tâches)

Ce chapitre décrit comment sortir des étiquettes sur des impressions Trusted Extensions.

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.

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 assignent des étiquettes aux serveurs d'impression et aux imprimantes.

Trusted Extensions prend en charge l'impression à niveau unique et l'impression multiniveau. Par défaut, l'impression à niveau unique est configurée. L'impression multiniveau est uniquement implémentée dans la zone globale. Pour utiliser le serveur d'impression de la zone globale, une zone étiquetée doit être configurée en tant qu'instance d'IP ou sous la forme d'une carte d'interface réseau virtuel (VNIC). L'adresse doit être 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 affectée au serveur d'impression Oracle Solaris. 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 affectée au serveur d'impression.

Sorties d'imprimante étiquetées

Trusted Extensions imprime les étiquettes sur les pages de corps de texte, les pages de garde et les pages de fin. Les informations proviennent du fichier `label_encodings`.

L'administrateur de sécurité peut également configurer des comptes utilisateurs pour qu'ils utilisent des imprimantes n'imprimant pas d'étiquettes sur la sortie.

Impression PostScript d'informations de sécurité

L'impression étiquetée dans Trusted Extensions repose sur les fonctions d'impression d'Oracle Solaris Dans le SE Oracle Solaris, l'option `job-sheets` gère la création de la page de garde. Pour implémenter l'étiquetage, le travail d'impression est converti 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.

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. Pour plus d'informations, reportez-vous au Chapitre 15, "Configuration et administration d'imprimantes à l'aide de CUPS (tâches)" du manuel *Administration d'Oracle Solaris : Tâches courantes* .

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 267
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 en tant que serveur d'impression à niveau unique" à la page 265
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 268
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 270

▼ Procédure de configuration d'une zone en tant que serveur d'impression à niveau 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 sous votre étiquette minimale" du manuel *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 manuel *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

3 **Définissez les caractéristiques de chaque imprimante connectée.**

   a. **Sous l'étiquette de la zone, modifiez le fichier de configuration du serveur d'impression CUPS : `/etc/cups/cupsd.conf`.**

4 **Affectez la feuille de travail appropriée à chaque imprimante connectée au serveur d'impression.**

   Par exemple, les spécifications suivantes permettent de créer une feuille étiquetée appropriée :

```
#CUPS-BANNER for INTERNAL print jobs
Show job-id job-name job-originating-user-name job-originating-host-name job-billing
Header CONFIDENTIAL : INTERNAL USE ONLY
Footer CONFIDENTIAL : INTERNAL USE ONLY
Image images/cups.png
```

   Utilisez la commande suivante :

```
$ lpadmin -p printer -o job-sheets-default=labeled,labeled
```

   Les imprimantes connectées peuvent uniquement imprimer des travaux ayant l'étiquette de la zone.

5 **Testez l'imprimante.**

Remarque – Pour des raisons de sécurité, les fichiers possédant une étiquette d'administration, `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 (Oracle OpenOffice par exemple), de votre navigateur et de votre éditeur.**

   c. **Vérifiez que les étiquettes s'impriment correctement.**

Voir aussi

- **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 268

▼ 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 Activez l'impression multiniveau en configurant la zone globale à l'aide du port du serveur d'impression, `515/tcp`.

```
# tncfg -z global add mlp_shared=515/tcp
# tncfg -z global add mlp_private=515/tcp
```

2 Définissez les caractéristiques de chaque imprimante connectée.

```
# 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
```

3 Configurez chaque imprimante connectée au serveur d'impression avec une feuille de travail étiquetée.

```
$ lpadmin -p printer -o job-sheets-default=labeled,labeled
```

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.

4 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. Créez un fichier `/etc/cups/client.conf` dans chaque zone étiquetée.

Ce fichier se connecte au démon `cupsd` dans la zone globale pour le service d'impression. Modifiez ce fichier afin d'inclure le nom du serveur d'impression et son adresse IP. Pour plus d'informations sur le fichier de configuration, reportez-vous à la page de manuel `client.conf`(5).

c. (Facultatif) Définissez l'imprimante comme imprimante par défaut.

```
# lpadmin -d printer-name
```

5 **Testez l'imprimante dans chaque zone étiquetée.**

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 (Oracle OpenOffice par exemple), de votre navigateur et de votre éditeur.**

c. **Vérifiez que les étiquettes 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 270
- **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 268

▼ 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'une zone en tant que serveur d'impression à niveau unique” à la page 265
- “Procédure de configuration d'un serveur d'impression multiniveau et des imprimantes correspondantes” à la page 267

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

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 manuel *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.**

  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 manuel *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.

Remarque – Pour des raisons de sécurité, les fichiers possédant une étiquette d'administration, `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 (Oracle OpenOffice par exemple), de votre navigateur et de votre éditeur.

c. Vérifiez que les étiquettes 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 de sécurité dans la zone globale.

1 Démarrez le gestionnaire de périphériques (Device Manager).

Sélectionnez l'option Allocate Device (Allouer un périphérique) dans le menu Trusted Path (Chemin de confiance).

2. **Cliquez sur le bouton Administration pour afficher la boîte de dialogue Device Administration (Administration des périphériques).**

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 Configuration (Configuration de périphérique).**

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 (Label Builder). Pour plus d'informations sur le générateur d'étiquettes, reportez-vous à la section "Générateur d'étiquettes dans Trusted Extensions" à la page 116.

   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 de périphériques.**

◆ ◆ ◆ CHAPITRE 20

Périphériques dans Trusted Extensions (présentation)

Ce chapitre décrit les extensions fournies par Trusted Extensions pour la protection de périphériques.

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 la fonction 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 de périphériques (Device Manager).

Pour plus d'informations sur la protection des périphériques dans Oracle Solaris, reportez-vous au Chapitre 5, "Contrôle de l'accès aux périphériques (tâches)" du manuel *Administration d'Oracle Solaris : services de sécurité*.

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 média 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 qu'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 "Configuration de la stratégie de périphériques (liste des tâches)" du manuel *Administration d'Oracle Solaris : services de sécurité*. 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. Oracle Solaris propose des scripts pour les lecteurs de bande ainsi que pour 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 "Scripts de nettoyage de périphériques" du manuel *Administration d'Oracle Solaris : services de sécurité*.

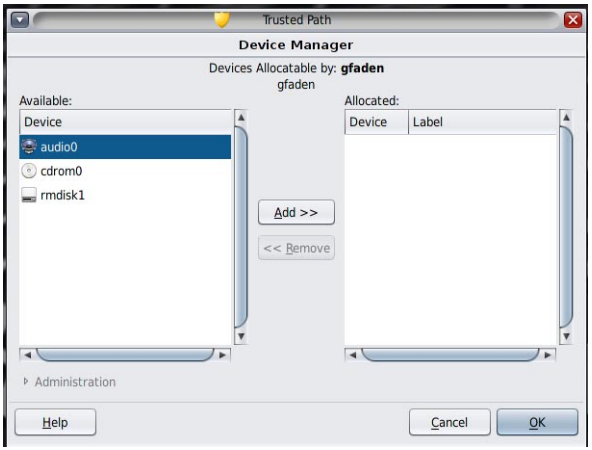
Pour le logiciel Trusted Extensions, les scripts de nettoyage de périphériques doivent satisfaire à certaines exigences. Les conditions requises sont décrites dans la page de manuel `device_clean(5)`.

Interface graphique du gestionnaire de périphériques

Le gestionnaire de périphériques (Device Manager) est utilisé par les administrateurs pour administrer les périphériques allouables et non allouables. Le gestionnaire 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).

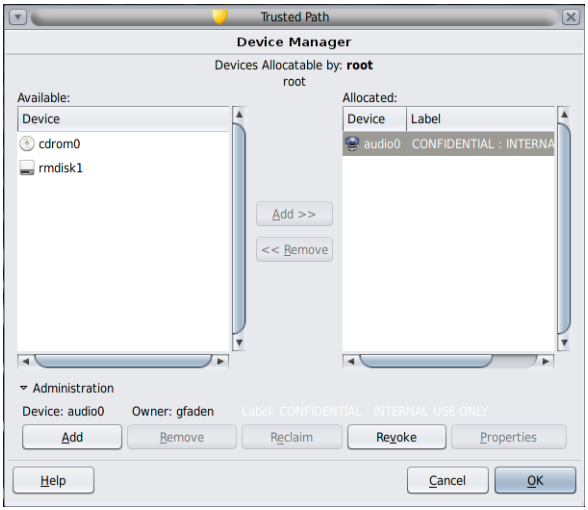
L'interface graphique utilisateur est appelée Device Manager (Gestionnaire de périphériques). Cette interface graphique est démarrée à partir du menu Trusted Path (Chemin de confiance) en sélectionnant Allocate Device (Allouer un périphérique). La figure ci-dessous illustre un gestionnaire de périphériques ouvert par un utilisateur autorisé à allouer le périphérique `audio`.

FIGURE 20–1 Gestionnaire 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).



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 média 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.
- S'assurer que les étiquettes des informations importées (lues) depuis les médias 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 d'Oracle Solaris reportez-vous à la section "Protection de périphériques (référence)" du manuel *Administration d'Oracle Solaris : services de sécurité*.

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 "Allocation forcée d'un périphérique" du manuel *Administration d'Oracle Solaris : services de sécurité* et "Libération forcée d'un périphérique" du manuel *Administration d'Oracle Solaris : services de sécurité*.

Pour consulter les interfaces de ligne de commande Trusted Extensions, reportez-vous aux pages de manuel `add_allocatable`(1M) et `remove_allocatable`(1M).

◆ ◆ ◆ CHAPITRE 21

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 suivante renvoie à des listes de tâches s'adressant aux administrateurs et utilisateurs pour 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 280
Gestion des périphériques	Configure des périphériques pour les utilisateurs standard.	"Gestion des périphériques dans Trusted Extensions (liste des tâches)" à la page 280
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 288

Utilisation de périphériques dans Trusted Extensions (liste des tâches)

Dans Trusted Extensions, tous les rôles sont autorisés à allouer un périphérique. De même que les utilisateurs, les rôles doivent utiliser le gestionnaire de périphériques (Device Manager). La commande `allocate` d'Oracle Solaris ne fonctionne pas dans Trusted Extensions. La liste des tâches ci-dessous renvoie aux procédures d'utilisation de périphériques dans Trusted Extensions.

Tâche	Voir
Allocation et libération d'un périphérique	"Procédure d'allocation d'un périphérique dans Trusted Extensions" du manuel *Guide de l'utilisateur Oracle Solaris Trusted Extensions*
Utilisation d'un média portable pour le transfert de fichiers	"Copie de fichiers dans Trusted Extensions à partir d'un média amovible" à la page 82 "Copie de fichiers sur un média amovible dans Trusted Extensions" à la page 81

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.	"Configuration de la stratégie de périphériques (liste des tâches)" du manuel *Administration d'Oracle Solaris : services de sécurité*
Octroi de l'autorisation d'allouer un périphérique à des utilisateurs	Le rôle d'administrateur de sécurité affecte à l'utilisateur un profil de doits comportant l'autorisation Allocate Device (Allouer un périphérique).	"Procédure d'autorisation des utilisateurs à allouer un périphérique" du manuel *Administration d'Oracle Solaris : services de sécurité*
	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 288
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 281

Tâche	Description	Voir
Révocation ou récupération d'un périphérique	Utilise le gestionnaire de périphériques (Device Manager) pour rendre disponible un périphérique.	"Procédure de révocation ou de récupération d'un périphérique dans Trusted Extensions" à la page 285
	Utilise les commandes d'Oracle Solaris pour rendre disponible ou indisponible un périphérique.	"Allocation forcée d'un périphérique" du manuel *Administration d'Oracle Solaris : services de sécurité* "Libération forcée d'un périphérique" du manuel *Administration d'Oracle Solaris : services de sécurité*
Interdiction de l'accès à un périphérique allouable	Offre un contrôle d'accès détaillé à un périphérique.	Exemple 21–2
	Permet d'interdire l'accès à un périphérique allouable à tous les utilisateurs.	Exemple 21–1
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 286
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 287

▼ 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.

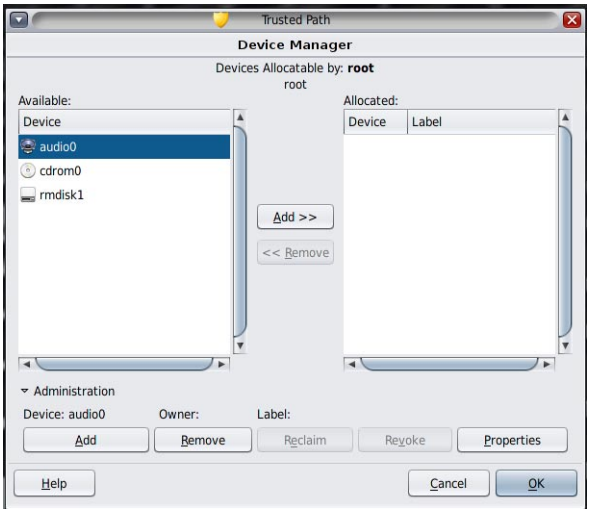
Les périphériques suivants peuvent être alloués pour permettre leur utilisation :

- `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 média USB enfichable à chaud.

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

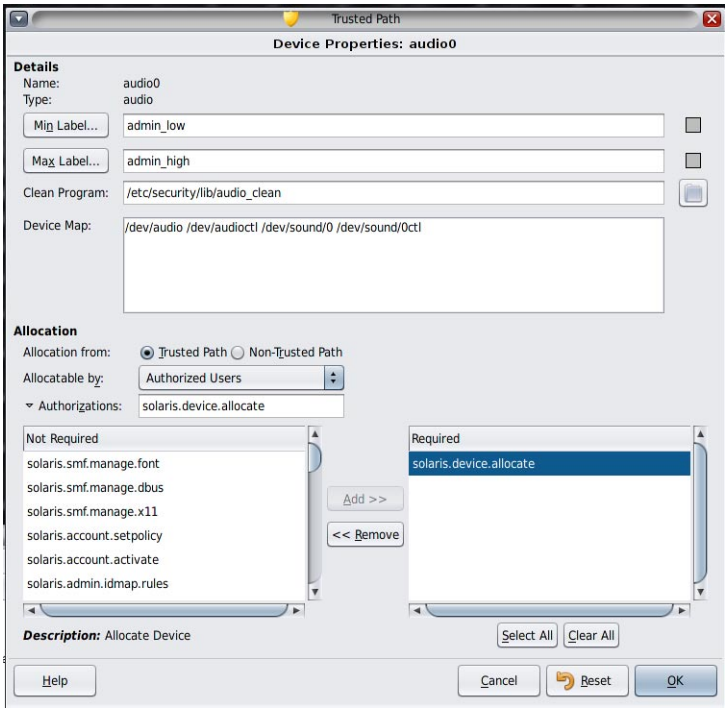
1 **Dans le menu Trusted Path (Chemin de confiance), sélectionnez Allocate Device (Allouer un périphérique).**

Le gestionnaire de périphériques (Device Manager) apparaît.



2 Affichez les paramètres de sécurité par défaut.

Cliquez sur Administration, puis mettez le périphérique en surbrillance. La figure suivante montre un périphérique audio en cours de visualisation par le rôle `root`.



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 (Label Builder). Pour plus d'informations sur le générateur d'étiquettes, reportez-vous à la section "Générateur d'étiquettes dans Trusted Extensions" à la page 116.

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 Device Configuration (Configuration de périphériques), sous For Allocations From Trusted Path (Pour des allocations à partir d'un 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.

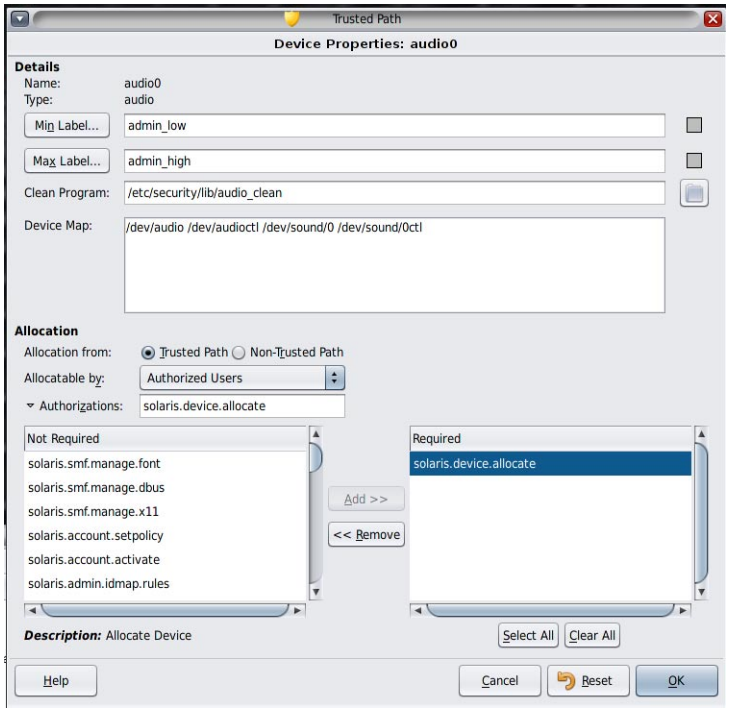
- **Pour exiger que les utilisateurs soient autorisés, sélectionnez l'option Allocatable by Authorized Users (Allouable par Utilisateurs autorisés).**

- **Pour rendre le périphérique non allouable par des utilisateurs distants, sélectionnez No Users.**

- **Pour rendre le périphérique allouable par n'importe quel utilisateur, sélectionnez All Users.**

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 288.

7 **Cliquez sur OK pour enregistrer vos modifications.**

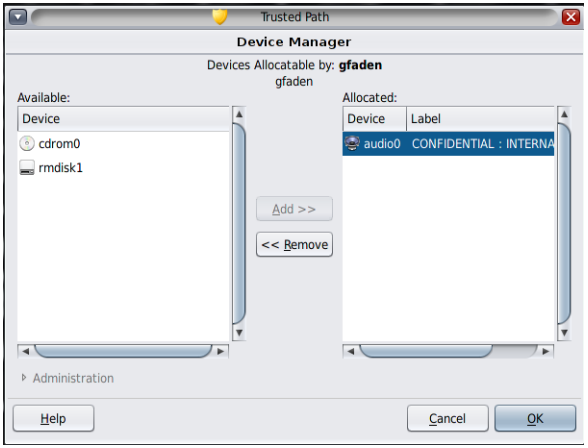
▼ Procédure de révocation ou de récupération d'un périphérique dans Trusted Extensions

Si un périphérique n'est pas répertorié dans le gestionnaire de périphériques (Device Manager), il est peut-être déjà alloué ou présente une 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 Administration.**

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 de périphériques.**

▼ Procédure de protection des périphériques non allouables dans Trusted Extensions

L'option No Users (Aucun utilisateur) dans la section Allocatable By (Allouable 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 de périphériques, cliquez sur le bouton Administration.**
3. **Sélectionnez la nouvelle imprimante ou la nouvelle mémoire graphique.**
   a. **Pour rendre le périphérique non allouable, cliquez sur No Users (Aucun utilisateur).**
   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 (Label Builder). Pour plus d'informations sur le générateur d'étiquettes, reportez-vous à la section "Générateur d'étiquettes dans Trusted Extensions" à la page 116.
      ii. **Définissez l'étiquette maximale.**
         Cliquez sur le bouton Max Label... (Étiquette max). Choisissez une étiquette maximale dans le générateur d'étiquettes.

Exemple 21–1 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 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 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 médias amovibles, le script tente d'éjecter le média si l'utilisateur ne le fait pas. Le script place le périphérique dans l'état d'erreur d'allocation si le média 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 `root` dans la zone globale.

1. **Copiez le script dans le répertoire `/etc/security/lib`.**
2. **Dans la boîte de dialogue Device Properties (Propriétés de périphériques), spécifiez le chemin d'accès complet au script.**
   a. **Ouvrez le gestionnaire de périphériques.**
   b. **Cliquez sur le bouton Administration.**
   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 289
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 292
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 292

▼ 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 utilisation d'autorisations, reportez-vous à l'Exemple 21–1.

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

1. **Modifiez le fichier `auth_attr`.**

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=`*Company*`Grant.html`
   domain-suffix`.`*domain-prefix*`.grant.device:::Grant` *Company* `Device Authorizations::help=`*Company*`GrantDevice.html`
   domain-suffix`.`*domain-prefix*`.device.allocate.tape:::Allocate Tape Device::help=`*Company*`TapeAllocate.html`
   domain-suffix`.`*domain-prefix*`.device.allocate.floppy:::Allocate Floppy Device::help=`*Company*`FloppyAllocate.html`

4. **Enregistrez le fichier et fermez l'éditeur.**

5. **Si vous utilisez LDAP comme service de nommage, mettez à jour les entrées `auth_attr` sur le serveur Oracle Directory Server Enterprise Edition (serveur d'annuaire).**

   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.**

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 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 292.

Exemple 21–2 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 21–3 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 de périphériques est présentée ci-dessous :

  Le chemin de confiance permet aux utilisateurs autorisés d'utiliser le gestionnaire de périphériques lors de l'allocation de 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 289.

1. **Suivez la procédure "Procédure de configuration d'un périphérique dans Trusted Extensions" à la page 281.**

   a. **Sélectionnez le périphérique que vous souhaitez protéger au moyen des nouvelles autorisations.**

   b. **Cliquez sur le bouton Administration.**

   c. **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 155.

- **Assignez à l'utilisateur un profil de droits qui contient l'autorisation Allocate Device.**
  Pour la procédure étape par étape, reportez-vous à la section "Procédure de modification des propriétés RBAC d'un utilisateur" du manuel *Administration d'Oracle Solaris : services de sécurité*.

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 médias) ;
- Media Restore (Restauration des médias) ;
- 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 21–4 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 289.
2. Dans le gestionnaire de périphériques (Device Manager), il ajoute les nouvelles autorisations de périphérique aux unités de bande et 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 22

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, l'audit est configuré et administré de façon similaire à celui d'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.
- L'audit par zone n'est pas recommandé, car il nécessite un compte `root` dans une zone étiquetée.
- 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. L'administrateur système prévoit l'espace disque requis pour les fichiers d'audit, crée un serveur d'administration d'audit, et passe en revue les journaux d'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 27, "Planification de l'audit" du manuel *Administration d'Oracle Solaris : services de sécurité*.

Responsabilités des rôles pour l'administration de l'audit

Dans Trusted Extensions, l'audit relève de la responsabilité d'autres rôles.

- Le rôle `root` assigne les indicateurs d'audit à des utilisateurs et des profils de droits, et modifie les fichiers système, tels que le script `audit_warn`.
- Le rôle d'administrateur système définit les disques et le réseau de stockage de l'audit. Ce rôle permet également de consulter les enregistrements d'audit.
- Le rôle d'administrateur de sécurité détermine ce qui doit être audité et configure l'audit. L'équipe chargée de la configuration initiale a créé ce rôle en effectuant les étapes décrites dans la section "Procédure de création du rôle d'administrateur sécurité dans Trusted Extensions" à la page 70.

Remarque – Un système enregistre seulement les événements dans les classes d'audit que l'administrateur de sécurité a présélectionnées. 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

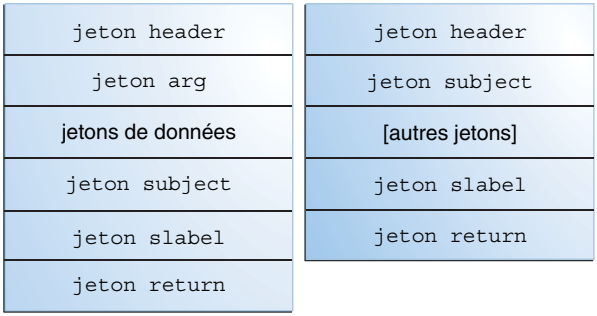
Les procédures de configuration et de gestion de l'audit dans Trusted Extensions diffèrent légèrement des procédures dans Oracle Solaris. Dans Trusted Extensions, la configuration d'audit est effectuée dans la zone globale. Étant donné que l'audit par zone n'est pas configuré, les actions de l'utilisateur sont auditées de manière identique dans la zone globale et les zones étiquetées. L'étiquette de chaque événement audité est incluse dans l'enregistrement d'audit.

- L'administrateur de sécurité peut sélectionner les stratégies d'audit qui sont spécifiques à Trusted Extensions, `windata_down` et `windata_up` .
- Durant la vérification des enregistrements d'audit, l'administrateur système peut sélectionner les enregistrements d'audit par étiquette. Pour plus d'informations, reportez-vous à la page de manuel `auditreduce(1M)`.

Référence de l'audit Trusted Extensions

Le logiciel Trusted Extensions ajoute des options de classes d'audit, d'événements d'audit, de jetons d'audit et de stratégie d'audit dans Oracle Solaris. Plusieurs commandes d'audit sont étendues pour permettre la prise en charge des étiquettes. La figure ci-dessous est un exemple type d'enregistrement d'audit du noyau Trusted Extensions et d'enregistrement d'audit au niveau de l'utilisateur.

FIGURE 22–1 Structures d'enregistrement d'audit type sur un système étiqueté



Classes d'audit de Trusted Extensions

Trusted Extensions ajoute les classes d'audit X Windows à Oracle Solaris. 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)`.

Les événements d'audit du serveur X sont mappés à ces classes selon les critères suivants :

- **xa :** cette classe surveille l'accès au serveur X, c'est-à-dire la connexion et la déconnexion du client X.
- **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 l'audit uniquement en cas de réussite. Lorsque des événements xs sont sélectionnés pour l'audit 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 à Oracle Solaris sont répertoriés par ordre alphabétique dans le tableau ci-dessous. Les définitions des jetons sont répertoriées dans la page de manuel `audit.log(4)`.

TABLEAU 22–1 Jetons d'audit de Trusted Extensions

Nom de variable	Description
"Jeton `label`" à la page 299	Étiquette de sensibilité
"Jeton `xatom`" à la page 299	Identification de l'atome de la fenêtre X
"Jeton `xcolormap`" à la page 299	Informations sur la couleur de la fenêtre X
"Jeton `xcursor`" à la page 299	Informations sur le curseur de la fenêtre X
"Jeton `xfont`" à la page 299	Informations sur les polices de la fenêtre X
"Jeton `xgc`" à la page 299	Informations sur le contexte graphique de la fenêtre X
"Jeton `xpixmap`" à la page 300	Informations sur les mappages de pixels de la fenêtre X
"Jeton `xproperty`" à la page 300	Informations sur la propriété de la fenêtre X
"Jeton `xselect`" à la page 300	Informations sur les données de la fenêtre X
"Jeton `xwindow`" à la page 300	Informations sur la fenêtre de la fenêtre X

Jeton label

Le jeton `label` contient une étiquette de sensibilité.

La commande `praudit -x` affiche un jeton `label` comme suit :

```
<sensitivity_label>ADMIN_LOW</sensitivity_label>
```

Jeton xatom

Le jeton `xatom` identifie un atome X.

La commande `praudit` affiche un jeton `xatom` comme suit :

```
X atom,_DT_SAVE_MODE
```

Jeton xcolormap

Le jeton `xcolormap` contient des informations sur l'utilisation des palettes de couleurs, y compris l'identificateur du serveur X et l'ID utilisateur du créateur.

La commande `praudit` affiche un jeton `xcolormap` comme suit :

```
<X_colormap xid="0x08c00005" xcreator-uid="srv"/>
```

Jeton xcursor

Le jeton `xcursor` contient des informations sur l'utilisation du curseur, y compris l'identificateur du serveur Y et l'ID utilisateur du créateur.

La commande `praudit` affiche un jeton `xcursor` comme suit :

```
X cursor,0x0f400006,srv
```

Jeton xfont

Le jeton `xfont` contient des informations sur l'utilisation de police, y compris l'identificateur du serveur X et l'ID utilisateur du créateur.

La commande `praudit` affiche un jeton `xfont` comme suit :

```
<X_font xid="0x08c00001" xcreator-uid="srv"/>
```

Jeton xgc

Le jeton `xgc` contient des informations sur le contexte graphique d'une fenêtre X.

La commande `praudit` affiche un jeton `xgc` comme suit :

```
Xgraphic context,0x002f2ca0,srv
```

```
<X_graphic_context xid="0x30002804" xcreator-uid="srv"/>
```

Jeton xpixmap

Le jeton `xpixmap` contient des informations sur l'utilisation des mappages de pixels, y compris l'identificateur du serveur X et l'ID utilisateur du créateur.

La commande `praudit -x` affiche un jeton `xpixmap` comme suit :

```
<X_pixmap xid="0x2f002004" xcreator-uid="srv"/>
```

Jeton xproperty

Le jeton `xproperty` contient des informations sur les différentes propriétés d'une fenêtre, telles que l'identificateur du serveur X, l'ID utilisateur du créateur et l'identificateur de l'atome.

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.

La commande `praudit` affiche un jeton `xselect` comme suit :

```
X selection,entryfield,halogen
```

Jeton xwindow

Le jeton `xwindow` identifie le serveur X et l'ID utilisateur du créateur.

La commande `praudit` affiche un jeton `xwindow` comme suit :

```
<X_window xid="0x07400001" xcreator-uid="srv"/>
```

Options de stratégie d'audit de Trusted Extensions

Trusted Extensions ajoute deux options de stratégie d'audit de fenêtre aux options de stratégie d'audit existantes.

```
$ 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 `auditrecord` sont étendues pour gérer les informations 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 `auditrecord` inclut les événements d'audit de Trusted Extensions.

◆ ◆ ◆ CHAPITRE 23

Gestion des logiciels dans Trusted Extensions (Référence)

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.

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 et les zones, reportez-vous au Chapitre 24, “A propos de l’installation automatique et des packages dans un système Oracle Solaris 11 comportant des zones installées” du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*.

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 média amovible nécessite une autorisation. Un compte avec l'autorisation Allouer un périphérique peut importer ou exporter des données à partir d'un média 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 pour le logiciel Oracle Solaris

Trusted Extensions utilise les mêmes mécanismes de sécurité qu'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 "Eléments et concepts de base RBAC" du manuel *Administration d'Oracle Solaris : services de sécurité*. Reportez-vous également à la page de manuel `auth_attr(4)` man page.
- **Privilèges :** des privilèges peuvent être assignés à des programmes et des processus. Pour plus d'informations sur les privilèges, reportez-vous au Chapitre 8, "Utilisation des rôles et des privilèges (présentation)" du manuel *Administration d'Oracle Solaris : services de sécurité*. 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 "Utilisation de l'utilitaire ppriv" du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*.
- **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 "Profils de droits RBAC" du manuel *Administration d'Oracle Solaris : services de sécurité*.
- **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 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 11 Security* . Pour voir des exemples de code pour Trusted Extensions, reportez-vous au *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 consulter 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.

◆ ◆ ◆ ANNEXE A

Stratégie de sécurité du site

Cette annexe traite des problèmes de stratégie de sécurité du site et suggère des ouvrages de référence et sites Web contenant davantage d'informations :

Création et gestion d'une stratégie de sécurité

Chaque site Trusted Extensions est unique et doit déterminer sa propre stratégie de sécurité. Effectuez les tâches suivantes lors de la création et de la gestion d'une stratégie de sécurité.

- Mettez en place une équipe de sécurité. L'équipe de sécurité doit disposer de représentants dans l'équipe de direction, l'équipe de ressources humaines, l'équipe de gestion et les administrateurs des systèmes informatiques et l'équipe de gestion des installations. Cette équipe doit réviser les stratégies et procédures des administrateurs Trusted Extensions et recommander des stratégies de sécurité générales qui s'appliquent à tous les utilisateurs du système.
- Formez le personnel d'administration et de gestion à la stratégie de sécurité du site. Tout le personnel impliqué dans la gestion et l'administration du site doit connaître la stratégie de sécurité. Les stratégies de sécurité ne doivent pas être mises à disposition des utilisateurs standard car ces informations ont une incidence directe sur la sécurité des systèmes informatiques.
- Formez les utilisateurs sur le logiciel Trusted Extensions et la stratégie de sécurité. Tous les utilisateurs doivent se familiariser avec le *Guide de l'utilisateur Oracle Solaris Trusted Extensions*. Étant donné que les utilisateurs sont généralement les premiers à savoir qu'un système ne fonctionne pas correctement, ils doivent connaître le système et signaler tout

problème qui survient à l'administrateur système. Pour garantir un environnement sécurisé, les utilisateurs doivent immédiatement avertir les administrateurs système s'ils constatent l'un des problèmes suivants :

- une erreur dans la dernière heure de connexion signalée au début de chaque session ;
- une modification inhabituelle des données d'un fichier ;
- la perte ou le vol d'impressions interprétables par l'utilisateur ;
- l'impossibilité d'utiliser une fonction utilisateur.

- Appliquez la stratégie de sécurité. Si la stratégie de sécurité n'est pas suivie et mise en œuvre, les données contenues dans le système configuré avec Trusted Extensions ne sont pas sécurisées. Des procédures doivent être établies afin d'enregistrer les problèmes et les mesures appliquées pour résoudre les incidents.
- Révisez régulièrement la stratégie de sécurité. L'équipe de sécurité doit effectuer une révision périodique de la stratégie de sécurité et de tous les incidents qui se sont produits depuis la dernière révision. Des ajustements de la stratégie peuvent contribuer à une sécurité accrue.

Stratégie de sécurité du site et Trusted Extensions

L'administrateur sécurité doit concevoir le réseau Trusted Extensions en fonction de la stratégie de sécurité du site. La stratégie de sécurité dicte les décisions en matière de configuration, par exemple :

- Degré de contrôle effectué pour tous les utilisateurs et pour certaines classes d'événements.
- Degré de contrôle effectué pour les utilisateurs dans les rôles et pour certaines classes d'événements.
- Quantité de données d'audit gérées, archivées et révisées.
- Étiquettes utilisées dans le système et visibilité des étiquettes `ADMIN_LOW` et `ADMIN_HIGH` pour les utilisateurs standard.
- Autorisations utilisateur affectées à des personnes.
- Périphériques (le cas échéant) pouvant être alloués par certains utilisateurs standard.
- Plages d'étiquettes définies pour les systèmes, les imprimantes et autres périphériques.
- Utilisation de Trusted Extensions dans une configuration évaluée ou non.

Recommandations relatives à la sécurité informatique

Tenez compte de la liste de conseils suivante lorsque vous élaborez une stratégie de sécurité pour votre site.

- Définissez la valeur d'étiquette maximale d'un système configuré avec Trusted Extensions afin qu'elle ne soit pas supérieure à la valeur maximale du niveau de sécurité du travail effectué sur le site.
- Enregistrez manuellement les réinitialisations du système, les pannes d'alimentation et les arrêts dans un journal du site.
- Documentez les dommages du système de fichiers et analysez tous les fichiers affectés à la recherche d'éventuelles violations des règles de sécurité.
- Ne fournissez les guides d'utilisation et la documentation destinée aux administrateurs qu'aux personnes nécessitant réellement d'accéder à ces informations.
- Rapportez et documentez tout comportement inhabituel ou inattendu des logiciels Trusted Extensions et déterminez la cause de l'erreur.
- Si possible, affectez au moins deux personnes à l'administration des systèmes configurés avec Trusted Extensions. Affectez une personne à l'autorisation d'administrateur sécurité pour les décisions relatives à la sécurité. Affectez une autre personne à l'autorisation d'administrateur système pour les tâches de gestion du système.
- Mettez en place une routine de sauvegarde régulière.
- Affectez les autorisations uniquement aux utilisateurs qui en ont besoin et qui les utiliseront correctement.
- Affectez des privilèges à des programmes uniquement s'ils requièrent ces privilèges pour fonctionner, et s'ils ont été examinés et que leur fiabilité dans l'utilisation des privilèges a été attestée. Passez en revue les privilèges sur les programmes Trusted Extensions existants et orientez-vous sur ceux-ci pour définir les privilèges de nouveaux programmes.
- Consultez et analysez régulièrement les informations d'audit. Examinez les événements irréguliers pour déterminer leur cause.
- Réduisez le nombre d'ID administrateur.
- Réduisez le nombre de programmes setuid et setgid. Utilisez les autorisations, les privilèges et les rôles pour exécuter le programme et empêcher son utilisation inappropriée.
- Assurez-vous qu'un administrateur vérifie régulièrement que les utilisateurs standard ont un shell de connexion valide.
- Assurez-vous qu'un administrateur vérifie régulièrement que les utilisateurs standard disposent de valeurs d'ID utilisateur valides et non de valeurs d'ID administrateur système.

Recommandations relatives à la sécurité physique

Tenez compte de la liste de conseils suivante lorsque vous élaborez une stratégie de sécurité pour votre site.

- Limitez l'accès aux systèmes configurés avec Trusted Extensions. Les emplacements les plus sécurisés sont généralement les pièces intérieures, ailleurs qu'au rez-de-chaussée.
- Surveillez et documentez l'accès aux systèmes configurés avec Trusted Extensions.
- Fixez l'équipement informatique à des objets de grande taille tels que des tables et des bureaux pour empêcher le vol. Lorsque l'équipement est fixé à un objet en bois, augmentez la résistance de l'objet en y ajoutant des plaques métalliques.
- Envisagez l'utilisation de médias de stockage amovibles pour les informations sensibles. Verrouillez tous les médias amovibles lorsqu'ils ne sont pas en cours d'utilisation.
- Stockez les sauvegardes système et les archives dans un endroit sûr distinct de l'emplacement des systèmes.
- Limitez l'accès physique aux médias de sauvegarde et d'archivage de la même manière que vous limitez l'accès aux systèmes.
- Installez un détecteur de température dans la pièce où se trouvent les systèmes informatiques pour détecter toute déviation de la plage de températures spécifiée par le fabricant. La plage de valeurs recommandée s'étend de 10 °C à 32 °C.
- Installez un détecteur d'eau dans la pièce où se trouvent les systèmes informatiques afin de détecter la présence d'eau sur le sol, dans les cavités en dessous du sol et dans le plafond.
- Installez un détecteur de fumée afin de détecter les incendies et installez un système anti-incendie.
- Installez un détecteur d'humidité afin de détecter un taux d'humidité trop ou pas assez élevé.
- Envisagez d'installer un système de protection TEMPEST si les machines n'en sont pas équipées. Ce système peut s'avérer approprié sur les murs, les sols et les plafonds des installations.
- N'autorisez que des techniciens certifiés à ouvrir et fermer le système TEMPEST afin de garantir sa capacité à intercepter les radiations électromagnétiques.
- Vérifiez la présence de brèches physiques qui permettraient l'accès à l'installation ou aux salles où se trouve l'équipement informatique. Recherchez les ouvertures sous des sols surélevés, dans des plafonds suspendus, les équipements de ventilation sur les toits et dans les murs entre le mur d'origine et le doublage.
- Interdisez de manger, boire et fumer dans les espaces réservés aux installations informatiques ou à proximité du matériel informatique. Définissez des zones où le personnel peut se livrer à ces activités sans danger pour l'équipement informatique.
- Protégez les plans architecturaux de l'installation informatique.
- Limitez l'utilisation de schémas fonctionnels, plans des installations et photographies de l'installation informatique.

Recommandations relatives à la sécurité du personnel

Tenez compte de la liste de conseils suivante lorsque vous élaborez une stratégie de sécurité pour votre site.

- Vérifiez les packages, documents et médias de stockage lorsqu'ils arrivent et avant qu'ils ne quittent un site sécurisé.
- Exigez que le personnel et les visiteurs portent des badges d'identification en permanence.
- Utilisez des badges d'identification difficiles à copier ou contrefaire.
- Définissez des zones interdites aux visiteurs et marquez-les clairement.
- Escortez les visiteurs à tout moment.

Violations de sécurité courantes

Aucun ordinateur n'est entièrement sécurisé : la sécurité d'une installation informatique dépend de la sécurité de chacune des personnes qui l'utilisent. Des utilisateurs soigneux ou des équipements supplémentaires permettent de prévenir la plupart des actions qui ne respectent pas la sécurité. Cependant, la liste suivante donne des exemples de problèmes susceptibles de se produire :

- Des utilisateurs donnent leur mot de passe à d'autres individus qui ne devraient pas avoir accès au système.
- Des utilisateurs écrivent leur mot de passe et perdent ou oublient le billet sur lequel ils ont écrit leur mot de passe dans un endroit non sécurisé.
- Des utilisateurs choisissent en tant que mot de passe un mot ou un nom facile à deviner.
- Des utilisateurs apprennent le mot de passe d'un autre utilisateur en le regardant saisir son mot de passe.
- Des utilisateurs non autorisés suppriment, remplacent ou altèrent physiquement le matériel.
- Des utilisateurs laissent leurs systèmes sans surveillance sans verrouiller l'écran.
- Des utilisateurs modifient les autorisations d'un fichier pour permettre à d'autres utilisateurs de le lire.
- Des utilisateurs modifient les étiquettes d'un fichier pour permettre à d'autres utilisateurs de le lire.
- Des utilisateurs jettent des copies papier de documents sensibles sans les broyer ou laissent ces mêmes documents dans des endroits non sécurisés.
- Des utilisateurs laissent les portes d'accès ouvertes.
- Des utilisateurs perdent leurs clés.
- Des utilisateurs ne verrouillent pas les médias de stockage amovibles.

- Les écrans d'ordinateur sont visibles à travers les fenêtres extérieures.
- Les câbles réseau sont abîmés.
- Un système d'écoute électronique capte les signaux émis par l'équipement informatique.
- Les pannes de courant, les surtensions et les pics détruisent les données.
- Les tremblements de terre, inondations, tornades, ouragans et la foudre peuvent détruire des données.
- Les interférences électromagnétiques externes telles que l'activité solaire peuvent brouiller les fichiers.

Références de sécurité supplémentaires

Les publications du gouvernement décrivent de manière détaillée les normes, les stratégies, les méthodes et la terminologie associée à la sécurité informatique. Des guides destinés aux administrateurs de systèmes UNIX et utiles pour mieux comprendre les problèmes de sécurité UNIX et leurs solutions sont également répertoriés ici.

Des ressources sont aussi disponibles sur le Web. Le site Web CERT (`http://www.cert.org`) en particulier alerte les entreprises et utilisateurs aux failles de sécurité des logiciels. Le site SANS Institute (`http://www.sans.org/`) propose des formations, un long glossaire de termes, ainsi qu'une liste à jour des principales menaces issues d'Internet.

U.S. Government Publications

The U.S. government offers many of its publications on the web. The Computer Security Resource Center (CSRC) of the National Institute of Standards and Technology (NIST) publishes articles on computer security. The following are a sample of the publications that can be downloaded from the NIST site (`http://csrc.nist.gov/index.html`).

- *An Introduction to Computer Security: The NIST Handbook*. SP 800-12, October 1995.
- *Standard Security Label for Information Transfer*. FIPS-188, September 1994.
- Swanson, Marianne and Barbara Guttman. *Generally Accepted Principles and Practices for Securing Information Technology Systems*. SP 800-14, September 1996.
- Tracy, Miles, Wayne Jensen, and Scott Bisker. *Guidelines on Electronic Mail Security*. SP 800-45, September 2002. Section E.7 concerns securely configuring LDAP for mail.
- Wilson, Mark and Joan Hash. *Building an Information Technology Security Awareness and Training Program*. SP 800-61, January 2004. Includes a useful glossary.
- Grace, Tim, Karen Kent, and Brian Kim. *Computer Security Incident Handling Guidelines*. SP 800-50, September 2002. Section E.7 concerns securely configuring LDAP for mail.
- Scarfone, Karen,Wayne Jansen, and Miles Tracy. *Guide to General Server Security* SP 800-123, July 2008.

- Souppaya, Murugiah, John Wack, and Karen Kent. *Security Configuration Checklists Program for IT Products*. SP 800-70, May 2005.

Publications relatives à la sécurité UNIX

Ingénieurs de sécurité Sun Microsystems. *Solaris 10 Security Essentials*. Prentice Hall, 2009.

Chirillo, John and Edgar Danielyan. *Sun Certified Security Administration for Solaris 9 & 10 Study Guide*. McGraw-Hill/Osborne, 2005.

Garfinkel, Simson, Gene Spafford, and Alan Schwartz. *Practical UNIX and Internet Security, 3rd Edition*. O'Reilly & Associates, Inc, Sebastopol, CA, 2006.

Publications relatives à la sécurité générale du système informatique

Brunette, Glenn M. and Christoph L. *Toward Systemically Secure IT Architectures*. Sun Microsystems, Inc, juin 2005.

Kaufman, Charlie, Radia Perlman, and Mike Speciner. *Network Security: Private Communication in a Public World, 2nd Edition*. Prentice-Hall, 2002.

Pfleeger, Charles P. and Shari Lawrence Pfleeger. *Security in Computing*. Prentice Hall PTR, 2006.

Privacy for Pragmatists: A Privacy Practitioner's Guide to Sustainable Compliance. Sun Microsystems, Inc, août 2005.

Rhodes-Ousley, Mark, Roberta Bragg, and Keith Strassberg. *Network Security: The Complete Reference*. McGraw-Hill/Osborne, 2004.

Stoll, Cliff. *The Cuckoo's Egg*. Doubleday, 1989.

Publications UNIX générales

Bach, Maurice J. *Conception du système UNIX*. Prentice Hall, Englewood Cliffs, NJ, 1986.

Nemeth, Evi, Garth Snyder et Scott Seebas. *UNIX, Guide de l'administrateur*. Prentice Hall, Englewood Cliffs, NJ, 1989.

◆ ◆ ◆ ANNEXE B

Liste de contrôle de configuration pour Trusted Extensions

Cette liste de contrôle fournit une vue d'ensemble des principales tâches de configuration pour Trusted Extensions. Les tâches moins importantes sont décrites dans les tâches principales. La liste de contrôle ne remplace en rien les procédures décrites dans ce guide.

Liste de contrôle de configuration de Trusted Extensions

La liste suivante récapitule les éléments nécessaires pour activer et configurer Trusted Extensions sur votre site. Les tâches qui sont décrites ailleurs sont liées par référence croisées.

1. Lecture.
   - Lisez les cinq premiers chapitres de la Partie II.
   - Intégrez les exigences en matière de sécurité du site.
   - Lisez l'annexe "Stratégie de sécurité du site et Trusted Extensions" à la page 308.
2. Préparation.
   - Définissez le mot de passe `root`.
   - Définissez le niveau de sécurité PROM ou BIOS.
   - Définissez le mot de passe PROM ou BIOS.
   - Décidez si des périphériques peuvent être connectés.
   - Décider si l'accès aux imprimantes à distance est autorisé.
   - Décidez si l'accès aux réseaux sans étiquette est autorisé.
3. Activation de Trusted Extensions. Reportez-vous à la section "Activation du service Trusted Extensions et connexion" à la page 48.
   a. Installez le SE Oracle Solaris.
   b. Chargez les packages Trusted Extensions.
   c. Activez `svc:/system/labeld`, le service Trusted Extensions.
   d. Réinitialisez le système.
4. (Facultatif) Personnalisez la zone globale. Reportez-vous à la section "Configuration de la zone globale dans Trusted Extensions" à la page 53.

a. Si vous utilisez IPv6, activez IPv6 pour Trusted Extensions.
b. Si vous utilisez un DOI différent de `1`, définissez-le dans le fichier `/etc/system` et dans chaque modèle de sécurité.
c. Vérifiez et installez le fichier `label_encodings` de votre site.
d. Réinitialisez le système.

5. Ajoutez des zones étiquetées. Reportez-vous à la section "Création de zones étiquetées" à la page 58.
   a. Configurez automatiquement deux zones étiquetées.
   b. Configurez manuellement vos zones étiquetées.
   c. Créez un espace de travail étiqueté.
6. Configurez le service de nommage LDAP. Reportez-vous au Chapitre 5, "Configuration de LDAP pour Trusted Extensions (tâches)".

   Créez un serveur proxy Trusted Extensions ou un serveur LDAP Trusted Extensions. Le service de nommage de fichiers ne requiert aucune configuration.
7. Configurez les interfaces et le routage pour la zone globale et les zones étiquetées. Reportez-vous à la section "Configuration des interfaces réseau dans Trusted Extensions" à la page 63.
8. Configurez le réseau. Reportez-vous à la section "Étiquetage d'hôtes et de réseaux (liste des tâches)" à la page 224.
   - Identifiez les hôtes à étiquette unique et les hôtes à plage limitée.
   - Déterminez les étiquettes à appliquer aux données entrant à partir d'hôtes sans étiquette.
   - Personnalisez les modèles de sécurité.
   - Affectez des hôtes spécifiques à des modèles de sécurité.
   - Affectez des sous-réseaux à des modèles de sécurité.
9. Exécutez d'autres configurations.
   a. Configurez les connexions réseau pour LDAP.
      - Affectez le serveur LDAP ou un serveur proxy au type d'hôte `cipso` dans tous les modèles de sécurité.
      - Affectez les clients LDAP au type d'hôte `cipso` dans tous les modèles de sécurité.
      - Faites du système local un client du serveur LDAP.
   b. Configurez les utilisateurs locaux et les rôles d'administration locaux. Reportez-vous à la section "Création de rôles et d'utilisateurs dans Trusted Extensions" à la page 69.
      - Créez le rôle d'administrateur de sécurité.
      - Créez un utilisateur local pouvant assumer le rôle d'administrateur de sécurité.
      - Créez d'autres rôles et éventuellement d'autres utilisateurs locaux pouvant assumer ces rôles.

c. Créez des répertoires personnels sur chacune des étiquettes auxquelles l'utilisateur peut accéder. Reportez-vous à la section "Création de répertoires personnels centralisés dans Trusted Extensions" à la page 76.

- Créez des répertoires personnels sur un serveur NFS.
- Créez des répertoires personnels ZFS locaux pouvant être chiffrés.
- (Facultatif) Empêchez les utilisateurs de lire leurs répertoires personnels de niveau inférieur.

d. Configurez l'impression. Reportez-vous à la section "Configuration de l'impression étiquetée (liste des tâches)" à la page 265.

e. Configurez les périphériques. Reportez-vous à la section "Manipulation des périphériques dans Trusted Extensions (liste des tâches)" à la page 279.

i. Affectez le profil de gestion des périphériques ou le profil d'administrateur système à un rôle.

ii. Pour que les périphériques puissent être utilisés, procédez de l'une des manières suivantes :

- Par système, rendez les périphériques allouables.
- Affectez l'autorisation Allocate Device (Allouer un périphérique) aux rôles et utilisateurs sélectionnés.

f. Configurez les fonctions d'Oracle Solaris.

- Configurez l'audit.
- Configurez les valeurs de sécurité du système.
- Autorisez des clients LDAP spécifiques à administrer LDAP.
- Configurez les utilisateurs dans LDAP.
- Configurez les rôles réseau dans LDAP.

g. Montez et partagez les systèmes de fichiers. Reportez-vous au Chapitre 14, "Gestion et montage de fichiers dans Trusted Extensions (tâches)".

◆ ◆ ◆ ANNEXE C

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 bibliothèques et des appels système, reportez-vous à l'Annexe D, “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 :

Script `txzonemgr`
: 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 nommage, et permettant de rendre la zone globale cliente d'un serveur LDAP existant. Dans la version Oracle Solaris 11 la commande `txzonemgr -c` permet de contourner les menus pour créer les deux premières zones étiquetées.

Gestionnaire de périphériques (Device 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.

L'utilitaire `tgnome-selectlabel` vous permet de personnaliser un générateur d'étiquettes. Reportez-vous à la section "tgnome-selectlabel Utility" du manuel *Trusted Extensions Developer's Guide*,

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 (Login/Workspace) Password (Modifier le mot de passe (connexion/espace de travail)). Dans Trusted JDS, vous accédez au menu Trusted Path (Chemin de confiance) 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 117.

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 de toutes les interfaces Trusted Extensions, reportez-vous à la section Annexe D, "Liste des pages de manuel Trusted Extensions".
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 systèmes de fichiers montés NFS dans Trusted Extensions" à la page 189.
	Trusted Extensions ajoute des autorisations à la base de données `auth_attr`.
	Trusted Extensions ajoute des fichiers exécutables 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 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 142.
	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 297.
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 :

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 médias 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.
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.

Options limitées dans Trusted Extensions

Trusted Extensions restreint l'éventail des options de configuration d'Oracle Solaris :

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. Les zones non globales sont des zones étiquetées. Les utilisateurs travaillent dans des zones étiquetées.

◆ ◆ ◆ ANNEXE D

Liste des pages de manuel Trusted Extensions

Trusted Extensions est une configuration du SE Oracle Solaris. Cette annexe fournit une description des pages de manuel qui contiennent des informations relatives à Trusted Extensions.

Pages de manuel Trusted Extensions par ordre alphabétique

Les pages de manuel suivantes s'appliquent uniquement aux systèmes configurés avec Trusted Extensions. La description contient des liens vers des exemples ou des explications concernant ces fonctions dans la collections de guides relatifs à Trusted Extensions.

Page de manuel Trusted Extensions	Objectif et liens vers des informations complémentaires
`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. Reportez-vous à la section "Procédure de configuration d'un périphérique dans Trusted Extensions" à la page 281.
`atohexlabel`(1M)	Convertit une étiquette lisible par l'utilisateur en son équivalent textuel interne. Pour consulter un exemple, reportez-vous à la section "Obtention de l'équivalent hexadécimal d'une étiquette" à la page 134.
`blcompare`(3TSOL)	Compare des étiquettes binaires.

`blminmax`(3TSOL)	Détermine le lien entre deux étiquettes.
`chk_encodings`(1M)	Vérifie la syntaxe du fichier label_encodings. Pour consulter des exemples, reportez-vous à la section "How to Debug a label_encodings File" du manuel *Trusted Extensions Label Administration* et à l'Exemple 4–1.
`fgetlabel`(2)	Identifie l'étiquette du fichier
`getlabel`(1)	Affiche l'étiquette des fichiers ou des répertoires sélectionnés. Pour consulter un exemple, reportez-vous à la section "Procédure d'affichage des étiquettes de fichiers montés" à la page 180.
`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. "Acquiring a Sensitivity Label" du manuel *Trusted Extensions Developer's Guide*
`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

	Pour consulter un exemple, reportez-vous à la section “Obtention d'une étiquette lisible à partir de sa forme hexadécimale ” à la page 135.
`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
	Pour un exemple d'utilisation, reportez-vous à la section “Procédure de connexion et d'administration d'un système Trusted Extensions distant” à la page 170.
`plabel`(1)	Identifie l'étiquette d'un processus
`remove_allocatable`(1M)	Empêche l'allocation d'un périphérique en supprimant l'entrée correspondante dans les bases de données d'allocation de périphériques
	Pour consulter un exemple, reportez-vous à la section “Procédure de configuration d'un périphérique dans Trusted Extensions” à la page 281.
`sel_config`(4)	Correspond aux règles de sélection pour les opérations copier, couper, coller et glisser-déposer
	Reportez-vous à la section “Règles lors de la modification du niveau de sécurité des données” à la page 125.
`setflabel`(3TSOL)	Déplace un fichier vers une zone possédant l'étiquette de sensibilité correspondante

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.
str_to_label(3TSOL)	Redistribue des chaînes lisibles par l'utilisateur à une étiquette
tncfg(1M)	Gère les bases de données du réseau de confiance. Constitue une alternative à l'interface utilisateur graphique `txzonmgr` pour la gestion des réseaux de confiance. La sous-commande `list` affiche les caractéristiques de sécurité d'interfaces réseau. `tncfg` fournit des informations plus exhaustives que la commande `tninfo`. Pour consulter plusieurs exemples, reportez-vous au Chapitre 16, “Gestion des réseaux dans Trusted Extensions (tâches) ”.
tnctl(1M)	Configure les paramètres réseau de Trusted Extensions Vous pouvez également utiliser la commande `tncfg`. Reportez-vous à l'Exemple 12–1.
tnd(1M)	Exécute le démon du réseau de confiance lorsque le service de nommage LDAP est activé.
tninfo(1M)	Affiche les informations réseau et les statistiques Trusted Extensions au niveau du noyau. “Débogage du réseau Trusted Extensions” à la page 249. Vous pouvez également utiliser la commande `tncfg` et l'interface utilisateur graphique `txzonemgr`. Pour consulter une comparaison avec la commande `tncfg`, reportez-vous à la section “Dépannage des échecs de montage dans Trusted Extensions” à la page 198.
trusted_extensions(5)	Présente Trusted Extensions
txzonemgr(1M)	Gère les zones étiquetées et les interfaces réseau. Les options de la ligne de commande permettent

	la création automatique de deux zones. Cette commande accepte comme entrée un fichier de configuration et permet la suppression de zones. `txzonemgr` est un script `zenity` (1). Reportez-vous aux sections "Création de zones étiquetées" à la page 58 et "Dépannage du réseau de confiance (liste des tâches)" à la page 248.
`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
Utilitaire `tgnome-selectlabel`	Permet de créer une interface utilisateur graphique de générateur d'étiquettes (Label Builder) Pour plus d'informations, reportez-vous à la section "tgnome-selectlabel Utility" du manuel *Trusted Extensions Developer's Guide*.
`updatehome(1)`	Met à jour les fichiers de copie et de liaison du répertoire personnel pour l'étiquette en cours Reportez-vous à la section "Procédure de configuration des fichiers de démarrage pour les utilisateurs dans Trusted Extensions " à la page 150.
`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 Trusted Extensions et liens vers des informations complémentaires
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. Dans Trusted Extensions, les utilisateurs standard n'utilisent pas cette commande. Pour connaître la procédure utilisateur, reportez-vous à la section "Procédure d'allocation d'un périphérique dans Trusted Extensions" du manuel *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

auditconfig(1M)	Ajoute la stratégie de fenêtres, les classes d'audit, les événements d'audit et les jetons d'audit pour les informations étiquetées.
auditreduce(1M)	Ajoute l'option `-l` pour sélectionner les enregistrements d'audit par étiquette. Pour consulter des exemples, reportez-vous à la section "Procédure de sélection des événements d'audit de la piste d'audit" du manuel *Administration d'Oracle Solaris : services de sécurité*.
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. 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. Pour plus d'informations, reportez-vous à la section "Modifications apportées à l'automonteur dans Trusted Extensions" à la page 191.
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. Dans Trusted Extensions, les utilisateurs standard n'utilisent pas cette commande. Pour connaître la procédure utilisateur, reportez-vous à la section "Procédure d'allocation d'un périphérique dans Trusted Extensions" du manuel *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.
device_clean(5)	Est appelé par défaut dans Trusted Extensions
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
ikeadm(1M)	Ajoute un indicateur de débogage, `0x0400`, pour les processus IKE étiquetés.

ike.config(4)	Ajoute le paramètre global `label_aware` et trois mots de passe transform de la phase 1, `single_label`, `multi_label` et `wire_label`
in.iked(1M)	Prend en charge la négociation d'associations de sécurité étiquetées via les ports UDP multiniveau 500 et 4500 dans la zone globale. Reportez-vous également à la page de manuel ike.config(4).
ipadm(1M)	Ajoute l'interface `all-zones` en tant que valeur de propriété permanente. Pour consulter un exemple, reportez-vous à la section "Procédure de vérification de l'affichage des interfaces du système" à la page 248.
ipseckey(1M)	Ajoute les extensions `label`, `outer-label` et `implicit-label`. Ces extensions associent des étiquettes Trusted Extensions au trafic transitant au sein d'une association de sécurité.
is_system_labeled(3C)	Détermine si le système est configuré avec Trusted Extensions
ldaplist(1)	Ajoute les bases de données réseau Trusted Extensions dans LDAP
list_devices(1)	Ajoute des attributs, tels que des étiquettes, associés à un périphérique. 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.
netstat(1M)	Ajoute l'option `-R` pour afficher les attributs de sécurité étendus pour les sockets et les entrées de table de routage.. Pour consulter un exemple, reportez-vous à la section "Dépannage des échecs de montage dans Trusted Extensions" à la page 198.
pf_key(7P)	Ajoute des étiquettes aux associations de sécurité (SA) IPsec
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. Ajoute l'option -secattr pour afficher les attributs de sécurité de la route : cipso, doi, max_sl et min_sl. Pour consulter un exemple, reportez-vous à la section "Dépannage des échecs de montage dans Trusted Extensions" à la page 198.
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
socket.h(3HEAD)	Prend en charge l'option SO_MAC_EXEMPT pour les homologues sans étiquette
tar(1)	Ajoute l'option -T pour archiver et extraire les fichiers et répertoires étiquetés. Reportez-vous aux sections "Procédure de sauvegarde de fichiers dans Trusted Extensions" à la page 194 et "Procédure de restauration de fichiers dans Trusted Extensions" à la page 195.
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 les attributs de sécurité utilisateur idletime, idlecmd, clearance et min_label spécifiques à Trusted Extensions Reportez-vous à la section "Planification de la sécurité de l'utilisateur dans Trusted Extensions" à la page 34.

Glossaire

administrateur de sécurité Dans une organisation où des informations sensibles doivent être protégées, la ou les personnes qui définissent et appliquent la stratégie de sécurité du site. Ces personnes sont autorisées à accéder à toutes les informations en cours de traitement sur le site. Dans le logiciel, le rôle d'administration d'administrateur de sécurité est affecté à une ou plusieurs personnes qui disposent de l'autorisation appropriée. Ces administrateurs configurent les attributs de sécurité de tous les utilisateurs et hôtes, afin que le logiciel applique la stratégie de sécurité du site. Voir également administrateur système.

administrateur système Dans Trusted Extensions, rôle de confiance affecté à l'utilisateur ou aux utilisateurs chargé(s) de réaliser des tâches standard d'administration du système, telles que la configuration des éléments non liés à la sécurité des comptes utilisateur. Voir également administrateur de sécurité.

adresse IP Adresse de protocole Internet. Numéro unique qui permet d'identifier un système en réseau afin qu'il puisse communiquer par le biais de protocoles Internet. Dans IPv4, l'adresse se compose de quatre nombres séparés par des points. La plupart du temps, chaque partie de l'adresse IP est un nombre compris entre 0 et 225. Cependant, le premier nombre doit être inférieur à 224 et le dernier numéro ne peut pas être égal à 0.

Les adresses IP sont logiquement scindées en deux parties : le réseau et le système sur le réseau. Le numéro du réseau est similaire à un indicatif de zone téléphonique. En relation avec le réseau, le numéro de système est semblable à un indicatif régional.

allocation Mécanisme par lequel l'accès à un périphérique est contrôlé. Voir allocation de périphériques.

allocation de périphériques Mécanisme de protection des informations sur un périphérique allouable afin d'en empêcher l'accès par toute personne autre que l'utilisateur qui alloue le périphérique. Jusqu'à ce qu'un périphérique soit libéré, personne d'autre que l'utilisateur qui l'a alloué ne peut accéder à toutes les informations qui lui sont associées. Pour pouvoir allouer un périphérique, l'utilisateur doit disposer de l'autorisation d'allocation de périphériques (Device Allocation) attribuée par l'administrateur de sécurité.

attributs de sécurité Attribut utilisé pour l'application de la stratégie de sécurité Trusted Extensions. Divers ensembles d'attributs de sécurité sont affectés aux processus, utilisateurs, zones, hôtes, périphériques allouables et autres objets.

autorisation Droit accordé à un utilisateur ou à un rôle d'effectuer une action qui n'est normalement pas autorisée par la stratégie de sécurité. Les autorisations sont accordées dans des profils de droits. Certaines commandes nécessitent que l'utilisateur dispose de certaines autorisations. Par exemple, pour imprimer un fichier PostScript, l'utilisateur doit posséder l'autorisation d'impression Postscript.

autorisation utilisateur autorisation affectée par l'administrateur de sécurité qui définit la limite supérieure de l'ensemble d'étiquettes avec lesquelles un utilisateur peut travailler à tout moment. L'utilisateur peut décider d'accepter la valeur par défaut ou limiter davantage l'autorisation au cours d'une session de connexion particulière.

autorisation Limite supérieure de l'ensemble d'étiquettes avec lequel un utilisateur peut travailler. La limite inférieure est l'étiquette minimale affectée par l'administrateur de sécurité. Une autorisation peut être de deux types : autorisation de session ou autorisation utilisateur.

bande de confiance Zone qui ne peut pas être falsifiée. Dans Trusted GNOME la bande est en haut. La bande fournit une indication visuelle sur l'état du système de multifenêtrage : un indicateur de chemin de confiance et l'étiquette de sensibilité de la fenêtre. Quand les étiquettes de sensibilité sont configurées de manière à ne pas être visibles pour un utilisateur, la bande de confiance est réduite à une icône qui affiche uniquement l'indicateur de chemin de confiance.

base de données tnrhdb Base de données d'hôte distant du réseau de confiance. Cette base de données affecte un ensemble de caractéristiques d'étiquettes à un hôte distant. La base de données est accessible sous forme d'un fichier dans `/etc/security/tsol/tnrhdb,`.

base de données tnrhtp Modèle d'hôte distant du réseau de confiance. Cette base de données définit l'ensemble d'étiquettes caractéristiques pouvant être affectées à un hôte distant. La base de données est également accessible sous forme de fichier dans `/etc/security/tsol/tnrhtp`.

bases de données de réseau de confiance `tnrhtp`, le modèle d'hôte distant du réseau de confiance et `tnrhdb`, la base de données d'hôte distant du réseau de confiance, définissent ensemble les hôtes distants avec lesquels un système Trusted Extensions peut communiquer.

bits d'autorisation Type de contrôle d'accès discrétionnaire dans lequel le propriétaire spécifie un ensemble de bits pour indiquer qui peut lire, écrire ou exécuter un fichier ou un répertoire. Trois ensembles d'autorisations différents sont affectés à chaque fichier ou répertoire : un pour le propriétaire, un pour le groupe du propriétaire et un pour le reste.

bureau multiniveau Sur un système Oracle Solaris configuré avec Trusted Extensions, les utilisateurs peuvent exécuter un bureau sous une étiquette particulière. Si l'utilisateur est autorisé à travailler sous plus d'une étiquette, l'utilisateur peut créer un espace de travail distinct pour travailler sous chaque étiquette. Sur ce bureau multiniveau, les utilisateurs autorisés peuvent effectuer des couper-coller entre plusieurs fenêtres sous différentes étiquettes, recevoir du courrier correspondant à différentes étiquettes et visualiser et utiliser des fenêtres étiquetées dans les espaces de travail d'une autre étiquette.

chemin de confiance Sur un système Oracle Solaris configuré avec Trusted Extensions, le chemin de confiance est un moyen fiable et inaltérable de communiquer avec le système. Le chemin de confiance est utilisé pour s'assurer que les fonctions d'administration ne peuvent pas être compromises. Les fonctions utilisateur nécessitant protection, telles que la modification de mot de passe, utilisent également le chemin de confiance. Lorsque le chemin de confiance est actif, le bureau affiche un indicateur d'inviolabilité.

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

client Système connecté à un réseau.

compartiment Composant non hiérarchique d'une étiquette utilisé avec le composant classification pour former une autorisation ou une étiquette. Un compartiment représente un ensemble d'informations qui pourraient être utilisées par un service d'ingénierie ou une équipe de projet multidisciplinaire.

configuration de l'étiquette Choix effectué lors de l'installation de Trusted Extensions entre une étiquette unique ou plusieurs étiquettes de sensibilité. Dans la plupart des cas, la configuration de l'étiquette est identique sur tous les systèmes de votre site.

configuration évaluée Un ou plusieurs hôtes Trusted Extensions en cours d'exécution dans une configuration certifiée comme répondant aux critères spécifiques définis par un organisme de certification. Aux États-Unis, il s'agit du TCSEC. L'organisme d'évaluation et de certification est la NSA.

- Le logiciel Trusted Extensions configuré sur la version Solaris 10 11/06 est certifié conforme aux Critères Communs v2.3 [août 2005] (une norme ISO) au niveau d'assurance (EAL) 4, ainsi que par rapport à plusieurs profils de protection.
- Par le biais d'une assurance continuité, la NSA a certifié le logiciel Trusted Extensions configuré sur la version Solaris 10 5/09.

Le niveau B+1 des Critères Communs v2 (CCv2) et les profils de protection ont rendu la norme TCSEC américaine caduque. Un accord de reconnaissance mutuelle pour CCv2 a été signé par les États-Unis, le Royaume-Uni, le Canada, le Danemark, les Pays-Bas, l'Allemagne et la France.

La cible de configuration Trusted Extensions fournit des fonctionnalités similaires aux niveaux TCSEC C2 et B1, avec des fonctionnalités supplémentaires.

contrôle d'accès discrétionnaire Type d'accès accordé ou refusé par le propriétaire d'un fichier ou d'un répertoire, à sa discrétion. Trusted Extensions fournit deux types de contrôle d'accès discrétionnaire (DAC) : les bits d'autorisation UNIX et les listes de contrôle d'accès (ACL).

contrôle d'accès obligatoire Contrôle d'accès basé sur la comparaison de l'étiquette de sensibilité d'un fichier, d'un répertoire ou d'un périphérique avec l'étiquette de sensibilité du processus qui tente d'y accéder. La règle MAC, read equal–read down, s'applique lorsqu'un processus à étiquette unique tente de lire un fichier sur une étiquette inférieure. La règle MAC, write equal-read down, s'applique lorsqu'un processus à étiquette unique tente d'écrire dans un répertoire sur une autre étiquette.

DAC Voir contrôle d'accès discrétionnaire.

domaine Une partie de la hiérarchie d'attribution de noms relative à Internet. Il représente un groupe de systèmes sur un réseau local qui partagent les fichiers d'administration.

domaine d'interprétation (DOI, Domain of Interpretation) Sur un système Oracle Solaris configuré avec Trusted Extensions, le domaine d'interprétation est utilisé pour différencier les fichiers `label_encodings` qui peuvent avoir des étiquettes similaires définies. Le DOI est un ensemble de règles qui traduit les attributs de sécurité de paquets réseau en leur représentation par le fichier `label_encodings` local. Lorsque des systèmes ont le même DOI, ils partagent ce jeu de règles et peuvent traduire les paquets réseau étiquetés.

ensemble d'étiquettes Voir ensemble d'étiquettes de sécurité.

ensemble d'étiquettes de sécurité Spécifie un ensemble distinct d'étiquettes de sécurité pour une entrée base de données tnrhtp. Les hôtes affectés à un modèle avec un ensemble d'étiquettes de sécurité peuvent envoyer et recevoir des paquets correspondant à toutes les étiquettes de l'ensemble.

équipe chargée de la configuration initiale Équipe d'au moins deux personnes qui supervise l'activation et la configuration du logiciel Trusted Extensions. Un membre de l'équipe est responsable des décisions de sécurité, l'autre des décisions d'administration système.

étiquette Identificateur de sécurité affecté à un objet. L'étiquette est basée sur le niveau auquel les informations contenues dans cet objet doivent être protégées. Selon la manière dont l'administrateur de sécurité a configuré l'utilisateur, celui-ci peut voir l'étiquette de sensibilité ou aucune étiquette. Les étiquettes sont définies dans le fichier label_encodings.

étiquette CIPSO Option de sécurité IP commune. CIPSO correspond à l'étiquette standard implémentée par Trusted Extensions.

étiquette de sensibilité étiquette de sécurité affectée à un objet ou un processus. L'étiquette est utilisée pour limiter l'accès en fonction du niveau de sécurité des données qui sont contenues dans l'objet ou le processus.

étiquette initiale étiquette minimale affectée à un utilisateur ou à un rôle, et étiquette de l'espace de travail initial de l'utilisateur. L'étiquette initiale est l'étiquette la plus basse avec laquelle l'utilisateur ou le rôle peut travailler.

étiquette minimale Limite inférieure des étiquettes de sensibilité d'un utilisateur et limite inférieure des étiquettes de sensibilité du système. L'étiquette minimale définie par l'administrateur de sécurité lors de la spécification des attributs de sécurité d'un utilisateur est l'étiquette de sensibilité du premier espace de travail de l'utilisateur lors de sa première connexion. L'étiquette de confidentialité spécifiée dans le champ d'étiquette minimale par l'administrateur de sécurité dans le fichier `label_encodings` définit la limite inférieure pour le système.

fichier .copy_files Fichier de configuration facultatif sur un système multiétiquettes. Ce fichier contient une liste de fichiers de démarrage, tels que `.cshrc` ou `.mozilla`, que l'environnement utilisateur ou les applications utilisateur requièrent pour le bon fonctionnement du système ou de l'application. Les fichiers répertoriés dans `.copy_files` sont ensuite *copiés* dans le répertoire personnel de l'utilisateur à des étiquettes supérieures, lorsque ces répertoires sont créés. Voir également fichier .link_files.

fichier .link_files Fichier de configuration facultatif sur un système multiétiquettes. Ce fichier contient une liste de fichiers de démarrage, tels que `.cshrc` ou `.mozilla`, que l'environnement utilisateur ou les applications utilisateur requièrent pour le bon fonctionnement du système ou de l'application. Les fichiers répertoriés dans `.link_files` sont ensuite *liés* au répertoire personnel de l'utilisateur à des étiquettes supérieures, lorsque ces répertoires sont créés. Voir également fichier .copy_files.

fichier label_encodings Fichier dans lequel l'étiquette de sensibilité complète est définie, tout comme les plages d'accréditation, l'affichage des étiquettes, la visibilité par défaut des étiquettes, l'autorisation utilisateur par défaut, ainsi que d'autres aspects des étiquettes.

GFI Government Furnished Information (informations fournies par le gouvernement). Dans ce manuel, cela se réfère à un fichier label_encodings fourni par le gouvernement américain. Afin d'utiliser un fichier GFI avec le logiciel Trusted Extensions, vous devez ajouter la section `LOCAL DEFINITIONS` spécifique à Oracle à la fin du fichier GFI. Pour plus d'informations, reportez-vous au Chapitre 5, "Customizing the LOCAL DEFINITIONS Section (Tasks)" du manuel *Trusted Extensions Label Administration*.

hors de la configuration évaluée Lorsqu'un logiciel identifié comme pouvant satisfaire aux critères d'une configuration évaluée est configuré avec des paramètres qui ne répondent pas aux critères de sécurité, il est décrit comme se trouvant *hors de la configuration évaluée*.

hôte distant Système différent du système local. Un hôte distant peut être un hôte sans étiquette ou un hôte étiqueté.

hôte étiqueté système étiqueté faisant partie d'un réseau de confiance de systèmes étiquetés.

hôte sans étiquette Système en réseau envoyant des paquets réseau sans étiquette, tel qu'un système exécutant le SE Oracle Solaris.

MAC Voir contrôle d'accès obligatoire.

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

nom d'hôte Nom qui identifie un système auprès d'autres systèmes d'un réseau. Ce nom doit être unique parmi tous les systèmes au sein d'un domaine donné. Généralement, un domaine identifie une organisation unique. Un nom d'hôte peut se composer de n'importe quelle combinaison de lettres, chiffres, signes moins (–), mais il ne peut pas commencer ni se terminer par un signe moins.

nom de domaine L'identification d'un groupe de systèmes. Un nom de domaine se compose d'une séquence de noms de composants, séparés par un point (par exemple : `example1.town.state.country.org`). Un nom de domaine se lit de gauche à droite en commençant par des noms de composants qui identifient des zones d'autorité administrative générales, et généralement distantes.

périphérique Les périphériques englobent les imprimantes, ordinateurs, lecteurs de bandes, lecteurs de disquettes, lecteurs de CD-ROM, lecteurs de DVD, les périphériques audio et les périphériques pseudo-terminal internes. Les périphériques sont soumis à la stratégie read equal-write equal MAC. L'accès aux périphériques amovibles, tels que lecteurs de DVD, est contrôlé par l'allocation de périphériques.

plage d'accréditations Ensemble d'étiquettes de sensibilité approuvées pour une classe d'utilisateurs ou de ressources. Ensemble d'étiquettes valides. Voir également plage d'accréditations du système et plage d'accréditations de l'utilisateur.

plage d'accréditations de l'utilisateur Ensemble de toutes les étiquettes sur lesquelles un utilisateur standard peut travailler sur le système. L'administrateur de sécurité du site spécifie la plage dans le fichier label_encodings. Les règles pour les étiquettes bien formées qui définissent la plage d'accréditations du système sont également limitées par les valeurs de la section `ACCREDITATION RANGE` du fichier : limite supérieure, limite inférieure, contraintes de combinaisons et autres restrictions.

plage d'accréditations du système Ensemble de toutes les étiquettes valides créées en fonction des règles définies par l'administrateur de sécurité dans le fichier label_encodings, plus les deux étiquettes d'administration utilisées sur tous les systèmes configurés avec Trusted Extensions. Les étiquettes d'administration sont `ADMIN_LOW` et `ADMIN_HIGH` .

plage d'étiquettes Ensemble d'étiquettes de sensibilité affectées à des commandes, des zones et des périphériques allouables. La plage est définie en spécifiant une étiquette maximale et une étiquette minimale. Pour les commandes, les étiquettes minimale et maximale limitent les étiquettes sur lesquelles la commande peut être exécutée. Une seule étiquette de sensibilité est affectée aux hôtes distants qui ne reconnaissent pas les étiquettes, tout comme tous les autres hôtes que l'administrateur de sécurité souhaite limiter à une étiquette unique. Une plage d'étiquettes limite les étiquettes sur lesquelles les périphériques peuvent être alloués, ainsi que les étiquettes sur lesquelles les informations peuvent être stockées ou traitées lors de l'utilisation du périphérique.

port multiniveau (MLP) Sur un système Oracle Solaris configuré avec Trusted Extensions, un MLP est utilisé pour fournir un service multiniveau dans une zone. Par défaut, le serveur X est un service multiniveau défini dans la zone globale. Un MLP est spécifié par le numéro de port et le protocole. Par exemple, le MLP du serveur X pour le bureau multiniveau est spécifié par 6000-6003 et le protocole TCP.

privilège Pouvoirs accordés à un processus en train d'exécuter une commande. L'ensemble complet de privilèges décrit l'intégralité des capacités de votre système, des fonctions de base aux capacités d'administration. Les privilèges qui contournent la stratégie de sécurité, tels que le réglage de l'horloge sur un système, peuvent être accordés par l'administrateur de sécurité du site.

processus Action qui exécute une commande pour le compte de l'utilisateur qui invoque la commande. Un processus reçoit un certain nombre d'attributs de sécurité à partir de l'utilisateur, y compris l'ID utilisateur (UID), l'ID de groupe (GID), la liste de groupe supplémentaire et l'ID d'audit (AUID) de l'utilisateur. Les attributs de sécurité reçus par un processus incluent tous les privilèges disponibles pour la commande en cours d'exécution et l'étiquette de sensibilité de l'espace de travail actif.

profil de droits Mécanisme permettant de grouper les commandes et les attributs de sécurité affectés à ces fichiers exécutables. Les profils de droits permettant aux administrateurs Oracle Solaris de contrôler qui peut exécuter les commandes et de contrôler les attributs de ces commandes lors de leur exécution. Lorsqu'un utilisateur se connecte, tous les droits qui lui sont affectés sont applicables et l'utilisateur peut accéder à toutes les commandes et autorisations qui lui sont affectées dans l'ensemble de ses profils de droits.

relations d'étiquettes Sur un système Oracle Solaris configuré avec Trusted Extensions, une étiquette peut dominer une autre étiquette, être égale à une autre étiquette ou être disjointe d'une autre étiquette. Par exemple, l'étiquette `Top Secret` domine l'étiquette `Secret`. Pour deux systèmes avec le même domaine d'interprétation (DOI, Domain of Interpretation), l'étiquette `Top Secret` sur un système est égale à l'étiquette `Top Secret` sur l'autre système.

réseau fermé Réseau de systèmes configurés avec Trusted Extensions. Le réseau est séparé de tout hôte autre que Trusted Extensions. La séparation peut être physique, si aucun câble ne s'étend au-delà du réseau Trusted Extensions. La séparation peut aussi être marquée dans le logiciel, où les hôtes Trusted Extensions ne reconnaissent que les hôtes Trusted Extensions. La saisie de données à partir de l'extérieur du réseau est limitée aux périphériques connectés aux hôtes Trusted Extensions. Contraire de réseau ouvert.

réseau ouvert Réseau d'hôtes Trusted Extensions connectés physiquement à d'autres réseaux et qui utilisent le logiciel Trusted Extensions pour communiquer avec des hôtes autres que Trusted Extensions. Contraire de réseau fermé.

rôle Un rôle est semblable à un utilisateur, à la différence qu'un rôle ne peut pas se connecter. En règle générale, un rôle est utilisé pour affecter des capacités d'administration. Les rôles sont limités à un ensemble donné de commandes et d'autorisations. Voir rôle d'administration.

rôle d'administration Un rôle attribuant les autorisations requises, les commandes privilégiées et le chemin de confiance attributs de sécurité permettant d'autoriser le rôle à effectuer des tâches administratives. Les rôles effectuent un sous-ensemble de fonctions du superutilisateur Oracle Solaris telles que la sauvegarde ou l'audit.

rôle de confiance Voir rôle d'administration.

script txzonemgr Le script `/usr/sbin/txzonemgr` fournit une interface graphique simple pour la gestion des zones étiquetées. Le script fournit également des éléments de menu pour les options de gestion de réseaux. `txzonemgr` est exécuté par l'utilisateur root dans la zone globale.

séparation des tâches Stratégie de sécurité nécessitant deux administrateurs ou rôles pour créer et authentifier un utilisateur. Un administrateur ou un rôle est responsable de la création de l'utilisateur, du répertoire personnel de l'utilisateur et d'autres tâches d'administration de base. L'autre administrateur ou rôle est responsable des attributs de sécurité de l'utilisateur, tels que le mot de passe et la plage d'étiquettes.

service de nommage Base de données distribuée d'un réseau dans laquelle figurent les informations clés relatives à tous les systèmes du réseau et qui permettent aux systèmes de communiquer entre eux. En l'absence de service de nommage, chaque système doit maintenir sa propre copie des informations système dans les fichiers `/etc` locaux.

shell de profil Shell spécial qui reconnaît les attributs de sécurité, tels que les privilèges, autorisations et UID et GID spéciaux. Un shell de profil limite généralement le nombre de commandes disponibles à l'utilisateur, mais peut permettre à ces commandes de s'exécuter avec davantage de droits. Le shell de profil est le shell par défaut d'un rôle de confiance.

stratégie de sécurité Sur un hôte Trusted Extensions, ensemble de DAC, MAC et règles d'étiquetage qui définissent l'accès aux informations. Sur le site d'un client, ensemble des règles qui définissent la sensibilité des informations en cours de traitement sur ce site et mesures utilisées pour protéger les informations de tout accès non autorisé.

système Nom générique pour un ordinateur. Après l'installation, un système sur un réseau est souvent appelé hôte.

système de fichiers Ensemble de fichiers et de répertoires qui, lorsqu'il est défini dans une hiérarchie logique, constitue un ensemble structuré et organisé d'informations. Les systèmes de fichiers peuvent être montés à partir de votre système local ou d'un système distant.

système étiqueté Système exécutant un système d'exploitation multiniveau, tel que Trusted Extensions ou SELinux avec MLS activé. Le système peut envoyer et recevoir des paquets réseau étiquetés d'une option CIPSO dans l'en-tête des paquets.

système sans étiquette Sur un système Oracle Solaris configuré avec Trusted Extensions, un système sans étiquette est un système qui n'exécute pas de système d'exploitation multiniveau, tel que Trusted Extensions ou SELinux avec MLS activé. Un système sans étiquette n'envoie pas de paquets étiquetés. Si le système Trusted Extensions communiquant a attribué une étiquette unique au système sans étiquette, la communication réseau entre le système Trusted Extensions et le système sans étiquette aura lieu sur cette étiquette. Un système sans étiquette est également appelé système à niveau unique.

systèmes en réseau Groupe de systèmes connectés via le matériel et les logiciels, parfois appelé réseau local (LAN). Une configuration de systèmes en réseau utilise un ou plusieurs serveurs.

systèmes non en réseau Ordinateurs qui ne sont pas reliés à un réseau ou qui ne dépendent d'aucun autre hôte.

zone étiquetée Sur un système Oracle Solaris configuré avec Trusted Extensions, une étiquette unique est affectée à chaque zone. Bien que la zone globale soit étiquetée, une *zone étiquetée* se rapporte généralement à une zone non globale à laquelle une étiquette est affectée. Les zones étiquetées possèdent deux caractéristiques qui les distinguent des zones non globales d'un système Oracle Solaris configuré sans étiquette. D'une part, les zones étiquetées doivent utiliser le même pool d'ID utilisateur et d'ID de groupe. D'autre part, les zones étiquetées peuvent partager les adresses IP.

zone marquée Dans Trusted Extensions, une zone non globale étiquetée. Plus généralement, une zone non globale contenant des environnements d'exploitation non natifs. Reportez-vous à la page de manuel `brands(5)`.

Index

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

X

Z